NAUKOWA I AKADEMICKA SIEĆ KOMPUTEROWA

oraz

BIURO ŁĄCZNOŚCI KOMENDY GŁÓWNEJ POLICJI

MATERIAŁY SEMINARIUM „MIEDZESZYN `97"

21-23 MAJA 1997 r.

NAUKOWA I AKADEMICKA SIEĆ KOMPUTEROWA

oraz

BIURO ŁĄCZNOŚCI KOMENDY GŁÓWNEJ POLICJI

MATERIAŁY SEMINARIUM „MIEDZESZYN '97"

21-23 maja 1997 r.

Warszawa 1997
ISBN 83-902314-6-8

Rada Programowa:

Przewodniczący:	Tomasz Hofmokl i Włodzimierz Zaleszczyk
Członkowie:	Roman Adamiec Maria Baranowska Wiesław Filar Maciej Kotarski Maciej Kozłowski Jerzy Krasowski Wiktor Krzanowski Mirosław Machalski Krzysztof Silicki Andrzej Zienkiewicz
Prowadzący Seminarium:	Andrzej Zienkiewicz

Wstęp

Naukowa i Akademicka Sieć Komputerowa NASK specjalizuje się w działaniu w „luce technologicznej", to znaczy tam, gdzie naszym zadaniem jest miejsce dla jednostki badawczo-rozwojowej. Omawiane na ostatnich seminariach problemy usług internetowych stały się domeną działania wielkich operatorów jak Telekomunikacja Polska SA oraz ponad stu, a licząc ilością wniosków o uzyskanie licencji - kilkuset usługodawców. Podstawowym problemem staje się zaplecze tych usług, przede wszystkim bezpieczeństwo, co widoczne jest w szybkim rozwoju sieci o ograniczonej dostępności, takich jak sieci korporacyjne. NASK i w tej dziedzinie angażuje swoje siły i środki. Naturalną jest również konieczność zmiany partnera strategicznego i z tego powodu siódme z kolei seminarium NASK w Miedzeszynie po raz pierwszy jest organizowane wspólnie z Biurem Łączności Komendy Głównej Policji.

W ciągu roku, który upłynął od ostatniego seminarium, w polskich sieciach komputerowych nastąpiło wiele zmian. Warto wymienić kilka z nich:

- *Nastąpiło zasadnicze udostępnienie dostępu do usług Internetu, w czym rolę wiodącą przejmuje stopniowo POLPAK T oraz kilkuset usługodawców różnej skali.*
- *Pojawia się konkurencja na rynku usług bazowych co spowodowało zróżnicowaną ofertę kanałów cyfrowych zarówno w zakresie łączności międzynarodowej jak i krajowej.*
- *Pojawiają się pierwsze przesłanki istotnego obniżenia cen za dzierżawę kanałów cyfrowych oferowanych na rynku polskim.*
- *Nadal zwiększa się ilość węzłów NASK, a łączna szybkość łączy zagranicznych wzrosła prawie dwukrotnie, do 10 Mbps w kierunku do Polski i 6.5 Mbps z Polski.*
- *BŁ KGP oraz NASK wprowadziły mieszane połączenia izochroniczne i pakietowe na jednym łączu, co istotnie przybliża realizację rzeczywistych usług multimedialnych w oparciu o sieć transmisji danych.*
- *BŁ KGP i NASK uruchomiły i oddały do użytku sieć warszawską w pełnym zakresie usług obejmującym ogólnie jednostki finansowane ze sfery budżetowej.*
- *BŁ KGP i NASK wprowadzają na liniach międzymiastowych usługi ATM (Asynchronous Transfer Mode), co wprowadza powszechnie usługi izochroniczne na linie międzymiastowe.*
- *NASK zawarł umowę z Unisource Bussines Network na świadczenie międzynarodowych usług Frame Relay oraz LAN Interconnect.*
- *Dziewięciu operatorów sieci metropolitalnych (MAN), oferujących usługi przede wszystkim dla środowiska naukowego i akademickiego, zawarło z NASK-iem umowę na zestawienie i utrzymanie sieci korporacyjnej, łączącej tych operatorów ze sobą oraz z Internetem w skali krajowej i międzynarodowej.*
- *BŁ KGP i NASK uruchamiają węzeł bezpiecznego dostępu do Internetu dla szeroko rozumianej administracji państwowej.*

SPIS TREŚCI

PRAWNE, INSTYTUCJONALNE I ORGANIZACYJNE ASPEKTY BEZPIECZEŃSTWA TELEINFORMACYJNEGO w RZECZYPOSPOLITEJ POLSKIEJ

Mirosław Machalski

Biuro Bezpieczeństwa Łączności i Informatyki
Urzędu Ochrony Państwa
02-517 Warszawa, ul. Rakowiecka 2b, tel. 6013268, fax. 6014270

1. Wstęp

Charakterystyczną cechą schyłku naszego wieku jest lawinowy wzrost popytu i podaży na informacje niezbędne w procesach administracyjnych, naukowych, gospodarczych, politycznych i społecznych. Zapotrzebowanie to - w dodatnim sprzężeniu zwrotnym z systemami informacyjnymi, a szczególnie teleinformacyjnymi - powoduje, że informacja dostarczona terminowo, niezawodnie i bezpiecznie staje się dobrem strategicznym. Zbliżamy się milowymi krokami do „globalnego społeczeństwa informacyjnego" (uzależnionego od informacji). Wszechobecność coraz bardziej wyrafinowanych systemów teleinformacyjnych (łączności i informatyki) jest już faktem.

Jak wielkie znaczenie dla współczesnego świata ma jego informacyjna integracja świadczy fakt utworzenia zgodnie z planem działania Komisji Europejskiej specjalnego organu o nazwie Biuro Projektów Społeczeństwa Informacyjnego (Information Society Project Office).

Informacje gromadzone, przetwarzane i przesyłane w systemach teleinformacyjnych, w stopniu różnym w różnych instytucjach - ale zawsze znaczącym - mają charakter niejawny

Jednocześnie pogłębia się luka pomiędzy koniecznością zabezpieczania informacji a faktycznie stosowanymi sposobami ochrony. Obok profesjonalnych, kompleksowych rozwiązań, coraz częściej pojawiają się metody i sposoby, które faktycznie wprowadzają dodatkowe zagrożenie dla „teleinformacji".

2. Stan formalno-prawny w Rzeczypospolitej

2. 1. Regulacje ustawowe

Podstawowym aktem prawnym, regulującym procedury bezpieczeństwa teleinformacyjnego w RP jest ustawa z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej (Dz. U. Nr 40, poz. 271). Definiuje ona pojęcia tajemnicy państwowej i służbowej:

- tajemnicę państwową stanowi wiadomość, której ujawnienie ... może narazić na szkodę obronność, bezpieczeństwo lub inny ważny interes państwa. Klasyfikuje się ją jako wiadomość „Tajne Specjalnego Znaczenia" (dla wiadomości mających szczególne znaczenie dla obronności lub bezpieczeństwa państwa) lub „Tajne".

- tajemnicę służbową stanowi wiadomość ..., z którą pracownik zapoznał się w związku z pełnieniem swoich obowiązków, której ujawnienie może narazić na szkodę interes społeczny, uzasadniony interes tej jednostki organizacyjnej lub obywatela. Tajemnicę służbową klasyfikuje się jako „Poufne".

- Zarządzenie Nr 60/83 Ministra Spraw Wewnętrznych z 29 czerwca 1983 r. w sprawie szczegółowych zasad i sposobów postępowania z wiadomościami stanowiącymi tajemnicę państwową i służbową. Określa ono między innymi:

  - obowiązki i uprawnienia kierowników i pracowników jednostek organizacyjnych w zakresie przepisów o ochronie tajemnicy;
  - zasady klasyfikowania wiadomości i sporządzania dokumentów;
  - zasady organizacji i funkcjonowania kancelarii tajnych oraz obiegu dokumentów stanowiących tajemnicę państwową i służbową;
  - warunki organizowania konferencji i narad, na których mają być omawiane zagadnienia stanowiące tajemnicę;
  - zasady ochrony dokumentów tajnych podczas prac w terenie;
  - zasady zabezpieczania pomieszczeń, w których znajdują się wiadomości stanowiące tajemnicę państwową i służbową;
  - zasady spedycji przesyłek stanowiących tajemnicę;
  - tryb niszczenia dokumentów;
  - zasady kontroli i nadzoru stany ochrony tajemnicy.

- Zarządzenie Nr 56/83 Ministra Spraw Wewnętrznych z 29 czerwca 1983 r. w sprawie zasad, trybu i sposobu przewożenia, wydawania i ochrony dokumentów oraz innych przedmiotów stanowiących tajemnicę państwową. Określa ono miedzy innymi:

  - Pocztę Specjalną MSW jako organizację upoważnioną do spedycji przesyłek stanowiących tajemnicę państwową;
  - strukturę organizacyjną Poczty Specjalnej MSW i zasady jej wykorzystywania;
  - wymagania na kształt, wielkość i sposób pakowania przesyłek specjalnych.

- Inne zarządzenia MSW - dostępne wyłącznie dla osób dopuszczonych do wiadomości stanowiących tajemnicę państwową - regulujące zasady przesyłania wiadomości stanowiących tajemnicę państwową technicznymi systemami łączności oraz ich ochrony (w tym kryptograficznej). Przepisy te zabraniają między innymi stosowania kryptografii[1] bez zgody Dyrektora Biura Szyfrów Urzędu Ochrony Państwa (aktualnie Biura Bezpieczeństwa Łączności i Informatyki UOP).

W odróżnieniu od regulacji ustawowych, zarządzenia powyższe skupiają się głównie nad ochroną wiadomości stanowiących tajemnicę państwową ale przetwarzanych, przechowywanych i przesyłanych z zastosowaniem „konwencjonalnych" technik biurowych - a więc dotyczą przede wszystkim papierowych nośników informacji. Znaczną część tych przepisów można (i trzeba) zastosować wprost do systemów teleinformacyjnych, jednakże nie wyczerpują one specyficznych wymagań bezpieczeństwa współczesnych systemów teleinformacyjnych.

2. 3. Przewidywane zmiany w prawie w zakresie bezpieczeństwa teleinformacyjnego.

Jednym z istotniejszych wyznaczników kierunków zmian prawa polskiego regulującego procedury ochrony tajemnicy państwowej i służbowej - w tym również (a może nawet przede wszystkim) w systemach teleinformacyjnych - są ratyfikowane przez

[1] kryptografii w ogóle - nie tylko w specjalnych systemach teleinformacyjnych

informacji UZE, zakłada się powołanie i funkcjonowanie Krajowych Władz ds. Bezpieczeństwa (KWB) odpowiedzialnych za:

- przechowywanie niejawnych informacji UZE w organizacjach rządowych lub agencjach publicznych i prywatnych, w kraju i za granicą;
- zapewnienie, że wszyscy zatrudnieni (również obcokrajowcy) w krajowych organizacjach związanych z UZE, zostali poddani procedurze sprawdzenia;
- opracowanie procedur w celu zapewnienia warunków bezpieczeństwa informacji.

KWB realizują krajową politykę ochrony informacji bezpośrednio lub za pośrednictwem tzw. Mianowanych Władz ds. Bezpieczeństwa[3]. Przeglądając znane i uznane na świecie rozwiązania w tym zakresie, stwierdzić należy, że najczęściej są to organizacje paramilitarne, podporządkowane bezpośrednio lub pośrednio Premierowi.

2. 4. Inne - związane z bezpieczeństwem teleinformacyjnym - przepisy prawa

Istnieje szereg innych - rangi ustawy - przepisów prawnych, regulujących niektóre zagadnienia związane z bezpieczeństwem teleinformacyjnym. Zaliczyć do nich należy przede wszystkim:

- ustawę z dnia 2 grudnia 1993 r. o zasadach szczególnej kontroli obrotu z zagranicą towarami i technologiami w związku z porozumieniami i zobowiązaniami międzynarodowymi wraz z wydanym na jej podstawie Zarządzeniem Ministra Współpracy Gospodarczej z Zagranicą z dnia 20 grudnia 1996 r. w sprawie ustalenia wykazu towarów i technologii objętych szczególną kontrolą obrotu z zagranicą (kategoria 5 - komputery, telekomunikacja i ochrona informacji);
- ustawę z dnia 3 kwietnia 1993 r. o badaniach i certyfikacji wraz z Rozporządzeniem Rady Ministrów w sprawie zakresu i trybu stosowania przepisów o badaniach i certyfikacji do wyrobów produkowanych w kraju i importowanych wyłącznie na potrzeby obronności i bezpieczeństwa państwa, a także właściwości tych organów (na tej podstawie **Minister Spraw Wewnętrznych** Decyzją nr 1842/96 z dnia 23 września 1996 r. w sprawie badań i certyfikacji wyrobów o przeznaczeniu specjalnym w laboratoriach badawczych i jednostce certyfikującej **powołał Jednostkę Certyfikującą Urządzeń i Systemów Kryptograficznych oraz Kompatybilności Elektromagnetycznej w Biurze Szyfrów UOP[4] a także Laboratoria Badawcze)[5]**

W niektórych innych (obowiązujących lub projektowanych) przepisach prawa można się również doszukać regulacji „zahaczających" o problematykę bezpieczeństwa teleinformacyjnego. Są to na przykład:

- ustawa z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników (Dz. U. 95.142.702 z dnia 12 grudnia 1995 r.)

  - Art. 15 1. Urzędy skarbowe obowiązane są do zachowania tajemnicy odnośnie do danych zawartych w dokumentacji, o której mowa w art. 13 ust. 1 (Dokumentacja związana z nadaniem NIP oraz aktualizowaniem danych zawartych w zgłoszeniach identyfikacyjnych ...);

---

[3] Na szczególną uwagę zasługują rozwiązania wprowadzone w Republice Niemieckiej ustawą o utworzeniu Urzędu Federalnego ds. Bezpieczeństwa w Technice Informacji z dnia 17 grudnia 1990 r. (Federalny Dziennik Ustaw, rocznik 1990, cz. I).

[4] Obecnie - od 20 grudnia 1996 r. - Biuro Bezpieczeństwa Łączności i Informatyki UOP

[5] Aktualnie trwają przygotowania do rozpoczęcia budowy procesu Certyfikacji Personelu Bezpieczeństwa Teleinformacyjnego

3. 1. Ustawa o ochronie tajemnicy państwowej i służbowej

Art. 18. 1. Nadzór nad ochroną tajemnicy państwowej i służbowej sprawują:

- naczelne i centralne organy państwowe - w stosunku do jednostek organizacyjnych im podległych oraz przez nie nadzorowanych,

- terenowe organy administracji państwowej stopnia wojewódzkiego - w stosunku do jednostek organizacyjnych podporządkowanych radom narodowym;

- kierownicy jednostek - w pozostałych państwowych, spółdzielczych i społecznych jednostkach organizacyjnych.

Art. 19. 1. Minister Spraw Wewnętrznych sprawuje ogólną koordynację w zakresie organizacji ochrony tajemnicy państwowej i służbowej oraz określa szczegółowe zasady i sposób postępowania z wiadomościami stanowiącymi tajemnice państwową i służbową.

Art. 20. 1. Minister Obrony Narodowej w porozumieniu z Ministrem Spraw Wewnętrznych określa szczegółowe zasady i sposób postępowania z wiadomościami stanowiącymi tajemnicę państwowa o szczególnie ważnym znaczeniu dla obronności Państwa i Sił Zbrojnych.

Reforma „Centrum Administracyjnego" nie wprowadziła zmian „wprost" do ustawy o ochronie tajemnicy państwowej i służbowej. Jednakże wcześniej wyłączony został z resortu spraw wewnętrznych i podporządkowany bezpośrednio Premierowi RP Urząd Ochrony Państwa. Kompetencje tego urzędu (w tym i w dziedzinie bezpieczeństwa teleinformacyjnego) określone zostały w odrębnej ustawie (patrz następny podpunkt).

Natomiast w ustawie z dnia 8 sierpnia 1996 r. „Przepisy wprowadzające ustawy reformujące funkcjonowanie gospodarki i administracji publicznej" (Dz. U. Nr 106, poz. 497) zapisano:

art. 7. Do zakresu działania Ministra Spraw Wewnętrznych i Administracji przechodzą zadania i kompetencje należące dotychczas do:
1) Ministra Spraw Wewnętrznych, określone w przepisach ustaw i innych aktach prawnych z mocą ustawy oraz wynikające z przepisów wydanych na podstawie upoważnień zawartych w ustawach lub w innych aktach prawnych z mocą ustawy, chyba że przepisy niniejszej ustawy lub przepisy odrębne stanowią inaczej.

3. 2. Ustawa o Urzędzie Ochrony Państwa

Art. 1. 2. Do zadań Szefa Urzędu Ochrony Państwa należy:

...

5) rozpoznawanie i przeciwdziałanie naruszeniom tajemnicy państwowej,

...

7) kryptograficzna ochrona wiadomości stanowiących tajemnicę państwową i służbową, przekazywanych przez techniczne środki łączności na potrzeby organów administracji państwowej i państwowych instytucji finansowych i gospodarczych.

Aktualnie - jeszcze w trakcie uzgodnień (przygotowany na podstawie art. 1 ust. 5 ustawy z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa) - jest projekt Rozporządzenia Prezesa Rady Ministrów w sprawie określenia organów administracji państwowej oraz zakresu i trybu wykonywania przez nie obowiązków niezbędnych do realizacji zadań związanych z kryptograficzną ochroną wiadomości stanowiących tajemnicę państwową i służbową przekazywanych przez techniczne środki łączności na potrzeby organów administracji państwowej i państwowych instytucji finansowych i gospodarczych. Rozporządzenie to precyzuje procedury organizowania i utrzymywania bezpieczeństwa informacji klasyfikowanych w specjalnych systemów teleinformacyjnych.

Podkreślić należy, że jednym z czynników *niezbędnym do realizacji zadań związanych z kryptograficzną ochroną wiadomości,* jest zapewnienie ochrony również dla kryptografii[6]. Truizmem - ale wartym przypomnienia - jest fakt, że metodyka i sposoby ochrony specjalnych systemów teleinformacyjnych i kryptografii stosowanej w tych systemach są zbieżne.

Zbliżony zapis istnieje również w Przepisach Bezpieczeństwa UZE - Część X, Rozdział III, § 31 *„Wszelkie informacje i urządzenia, które zapewniają kontrolę dostępu do systemu lub sieci EPD, są chronione zgodnie z zasadami odnoszącymi się do najwyższego stopnia i kategorii tajności informacji, do której mogą umożliwić dostęp".*

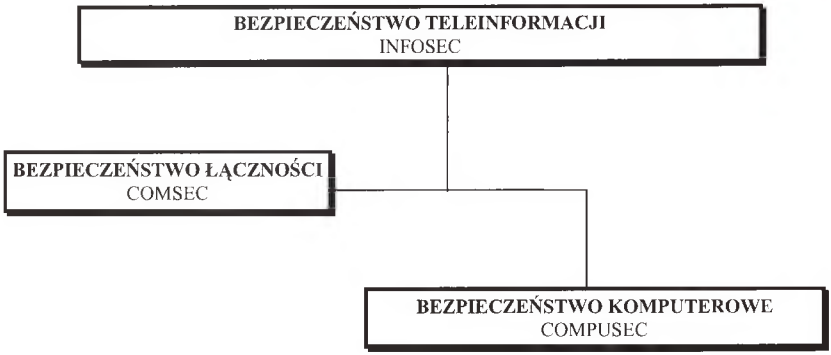
4. Kreowanie polityki bezpieczeństwa teleinformacyjnego

Każda organizacja dysponuje informacjami, które powinny lub muszą być chronione. Do informacji które muszą być chronione bezwzględnie zaliczają się informacje klasyfikowane (stanowiące tajemnicę państwową lub służbową). Polityka bezpieczeństwa teleinformacyjnego w takich przypadkach musi być kreowana - zgodnie z wymaganiami ustawy o ochronie tajemnicy państwowej i służbowej - w ścisłym uzgodnieniu z właściwymi organami (MSWiA, UOP, MON). Punktem wyjściowym jest tu zawsze uruchomienie procedur opisanych w Zarządzeniu Nr 60/83 Ministra Spraw Wewnętrznych z 29 czerwca 1983 r. w sprawie szczegółowych zasad i sposobów postępowania z wiadomościami stanowiącymi tajemnicę państwową i służbową (uzyskanie dopuszczenia do wiadomości klasyfikowanych, utworzenie organu lub stanowiska odpowiedzialnego za bezpieczeństwo, zorganizowanie kancelarii tajnej, systemu obiegu informacji niejawnych, itd.). Podkreślić należy, że procedury te należy uruchomić natychmiast (pierwszy warunek skuteczności), gdy tylko zaistnieje uzasadniona potrzeba dostępu do wiadomości klasyfikowanych (a nie dopiero w momencie ich uzyskania). Dalszy tryb postępowania - kreowania polityki bezpieczeństwa informacyjnego i teleinformacyjnego - uzależniony jest od specyficznych dla każdej organizacji uwarunkowań.

Nieco odmiennie powinna być kreowana polityka bezpieczeństwa teleinformacyjnego w organizacjach nie dysponujących informacjami klasyfikowanymi. Organizacje takie często chcą i powinny chronić informacje z innych - istotnych dla nich względów. Obserwacje stosowanych trybów postępowania w dziedzinie bezpieczeństwa teleinformacyjnego w takich organizacjach prowadzą do wniosku, że rzadko są to działania systemowe, kompleksowe i skuteczne. Niekiedy wręcz zastosowane po amatorsku i wybiórczo zabezpieczenia zdecydowanie obniżają poziom bezpieczeństwa informacji.

[6] Rodzima kryptografia jest jednym z najcenniejszych „skarbów" każdego państwa, i musi być szczególnie chroniona

ochrony przed - lub zapobieżeniu ujawnienia nieupoważnionym osobom, manipulacji, modyfikacji, skasowania informacji lub odmowie wykonania usługi.



Podkreślić należy, że pojęcie „bezpieczeństwo łączności" jest znacznie szersze niż „bezpieczeństwo transmisyjne" i obejmuje cały kompleks zagadnień związanych z bezpiecznym - tradycyjnym przesyłaniem różnorodnych informacji. W pojęciu tym mieści się więc przesyłanie Pocztą Specjalną przedmiotów zawierających tajemnicę państwową (np. dowodów rzeczowych) a także popularnej do dziś, tzw. „floppy net" - czyli przesyłanie pocztą (ewentualnie specjalnymi kurierami) elektronicznych nośników informacji.

Organizacyjno - strukturalny obraz elementów bezpieczeństwa systemów teleinformacyjnych przedstawia się następująco:

- **Bezpieczeństwo fizyczne** (physical security) - ochrona obiektów, osób i dokumentów związanych z przetwarzaniem informacji przed dostępem fizycznym i bezpośrednią obserwacją, procedury dopuszczeniowe i sprawdzające;

- **Bezpieczeństwo transmisji** (transmission security) - ochrona przed rozpoznaniem struktury sieci teleinformacyjnych, trafiku, identyfikacji uczestników ruchu, dostępu do urządzeń transmisyjnych itp.;
- **Bezpieczeństwo emisji** (emission security) - ochrona przed wykorzystaniem emisji ujawniającej informacje oraz przed atakiem elektromagnetycznym (celowym lub przypadkowym);

- **Bezpieczeństwo kryptograficzne** (cryptosecurity) - ochrona wiadomości poprzez szyfrowanie.

Dopiero kompleksowe, zsynchronizowane zastosowanie powyższych

- ewentualność konieczności etapowego wprowadzania polityki bezpieczeństwa ⇒ ustalenie priorytetów;
- konieczność zagwarantowania w budżecie środków finansowych na utrzymanie i rozwój systemu bezpieczeństwa;

e) organizację i zarządzanie
- zorganizowanie służby (lub stanowiska) bezpieczeństwa teleinformacyjnego oraz (lub zmodernizowanie istniejącego) systemu bezpieczeństwa fizycznego;
- zorganizowanie i wdrożenie systemu zarządzania informacjami (kto i w jakim trybie podejmuje decyzje o zakwalifikowaniu i przeznaczeniu jakich informacji);
- zorganizowanie i wdrożenie systemu zarządzania bezpieczeństwem[10];
- sformułowanie i wprowadzenie zadań dla personelu bezpieczeństwa teleinformacyjnego oraz bezpieczeństwa fizycznego;
- zorganizowanie i wdrożenie systemu kontroli (wewnętrznych i zewnętrznych);
- zorganizowanie i wdrożenie systemu szkoleń i egzaminów okresowych;
- zorganizowanie i wdrożenie systemu sprawdzeń i dopuszczeń osobowych;
- opracowanie i wdrożenie procedur awaryjnych i kryzysowych
- dobór i odpowiednie przystosowanie pomieszczeń przeznaczonych do przetwarzania, przechowywania i przesyłania informacji;

f) legislację i stosowane procedury
- weryfikację regulaminów i przepisów wewnętrznych;
- procedury bezpieczeństwa fizycznego;
- procedury bezpieczeństwa transmisyjnego;
- procedury bezpieczeństwa elektromagnetycznego;
- procedury bezpieczeństwa kryptograficznego;

g) eksploatację
- opracowanie i wdrożenie regulaminów i procedur eksploatacyjnych systemów, urządzeń, sieci - dla każdego stanowiska osobno;
- opracowanie i wdrożenie systemu reagowania na typowe i nietypowe (dziwne, często zdaniem użytkownika niegroźne lub niezrozumiałe) zjawiska pojawiające się w procesie eksploatacji;

h) technologię i technikę
- nie zawsze najnowsza technika i technologia jest „najbezpieczniejsza";
- technika i technologia bez „panującego" nad nią człowieka (i to nie jednego) jest źródłem bardzo poważnych zagrożeń;
- „obiegowe" informacje o bezpieczeństwie konkretnej techniki i technologii (w tym zabezpieczeń) są często błędne;
- technika i technologia musi być dobierana do istniejących i przewidywanych potrzeb, nie należy bezkrytycznie stosować się do „obowiązującej mody";
- należy dążyć (o ile to jest możliwe) do stosowania własnych, krajowych rozwiązań;
- należy eliminować (a co najmniej ograniczać) możliwość zdalnego, zewnętrznego (np. modemowego) serwisowania urządzeń i systemów;

Powyższy „katalog zaleceń" nie jest z pewnością kompletny. W dziedzinie

[10] w tym bezpieczeństwa systemu zabezpieczeń

BEZPIECZEŃSTWO SIECI TELEKOMUNIKACYJNYCH

Andrzej Zienkiewicz

1. Wprowadzenie

W krótkim referacie niesposób umieścić pełną wiedzę na temat bezpieczeństwa sieci teleinformatycznych. Postaram się zamieścić jedynie katalog problemów z jakimi spotkaliśmy się i spotykamy w czasie projektowania, budowy i eksploatacji sicci budowanych i operowanych przez NASK oraz ze współudziałem NASK. Uporządkowanie problemów jest nieco inne niż w referacie wprowadzającym. Wynika ono ze specyficznego spojrzenia na bezpieczeństwo sieci przez technologa i operatora. Odmienne uporządkowanie nie oznacza, że istnieją sprzeczności pomiędzy referatami co do meritum sprawy. Inne uporządkowanie wynika jedynie z innego podziału problemów dla potrzeb projektowania sieci i związanego z tym opisywania rodzajów zagrożeń i wymagań bezpieczeństwa.

Atak na sieć może dotyczyć przechwycenia informacji użytkownika lub uniemożliwić przesłanie tych informacji. Przechwytywanie informacji wymaga uzyskania dostępu di sieci w dowolnym jej punkcie oraz odczytania przesyłanej informacji i zapamiętania celem odpowiedniej obróbki. Czym dalej od urządzenia bezpośredniego użytkownika tym większy problem ze zgromadzeniem informacji oraz wydzieleniem części nas interesującej. Na przykład w szkielecie pracującym z szybkościami rzędu 155 Mbps przechwycenie informacji wymaga urządzeń o wielkiej pojemności, a wydzielenie informacji bardzo skomplikowanej obróbki zgromadzonych zbiorów. Wobec tego atak na informacje w sieci, chociażby z przyczyn czysto ekonomicznych, powinien następować możliwie blisko urządzenia użytkownika. Wtedy wyłuskanie interesującej informacji jest łatwe i nie wymaga wielkich urządzeń gromadzących dane. Odwrotnie atak na przesyłanie informacji będzie najskuteczniejszy im bardziej magistralnej części sieci dotyczy. Już tylko te dwa aspekty tłumaczą dlaczego ochrona informacji musi zaczynać się na urządzeniu użytkownika, powinna być wykonywana przez użytkownika w sposób możliwie indywidualny. Natomiast sama sieć wymaga ochrony przede wszystkim w zakresie podnoszącym niezawodność przesyłania. W referacie zajmiemy w pierwszej kolejności ochroną niezawodności działania sieci, wspominając tylko o ochronie informacji w sieci.

2. Ochrona sieci

Ochronę sieci można rozważać w trzech aspektach: ochrona niezawodności, ochronę informacji użytkownika oraz ochronę przed niepowołanym dostępem do sieci. Wszystkie aspekty ochrony sieci będziemy rozważać w ramach środków, którymi operuje posiadacz sieci. To znaczy, że inne środki, jak na przykład dzierżawione łącza fizyczne lub kanały cyfrowe, traktowane są jako parametry zewnętrzne, na które w czasie operowania siecią ma się wpływ ograniczony w dłuższym okresie czasu i żaden w okresach krótkich.

3. Ochrona niezawodności działania sieci

Przez niezawodność działania sieci rozumiemy tutaj stopień pewności (prawdopodobieństwo) uzyskania połączenia oraz przesłania informacji po uzyskanym połączeniu. W referacie rozważono środki przeciwdziałania czterem rodzajom przyczyn zakłócających działania sieci:

3.3 Błędna praca wyposażenia sieciowego w warunkach wyjątkowych

Tego rodzaju sytuacje muszą być przewidziane, jakkolwiek ich rodzaj nie może być z góry ustalony. Dla wyjścia z tego rodzaju zakłóceń można zaproponować kilka środków.
a) Scenariusze restartu systemu lub jego fragmentów z odzyskaniem informacji użytkownika.
b) Automatyczne restarty fragmentów systemu oparte na time-outowych przerwaniach w przypadku wyczerpania przewidzianych projektem prób odzysku pracy połączenia lub przesłania informacji.
c) Dobór rozwiązań renomowanych dostawców oraz zapewnienie stałej współpracy zespołów autorskich usuwających możliwości powstania sytuacji wyjątkowych.

Trzeba zauważyć, że błąd w pracy sieci, w tym i centrum zarządzania, nie powinien powodować zatrzymania jej pracy. Umożliwia to, na przykład, prawie natychmiastowe uruchomienie centrum zastępczego.

3.4 Zniszczenie węzła sieci

Przez zniszczenie węzła sieci rozumiemy jakąkolwiek przyczynę, nieusuwalną w krótkim czasie (do kilku godzin) uniemożliwiającą pracę węzła sieci. Wypadnięcie węzła przy założonej technologii i systemie zarządzania siecią nie narusza w istotny sposób pracy sieci. Jednak części sieci bezpośrednio dołączone do węzła tylko jednym łączem zostają pozbawione łączności. Zmniejsza się również rezerwa bezpieczeństwa większych części sieci wobec wyłączenia potencjalnych dróg obejściowych przechodzących przez węzeł. Dla przeciwdziałania takiej sytuacji powinno się przewidywać:
a) Przygotowanie ruchomych wozów telekomunikacyjnych wyposażonych w infrastrukturę potrzebną dla pracy węzła jak zasilanie, klimatyzacja, łączność awaryjna itp.
b) Stworzenie rezerwy wyposażenia typowego węzła pozwalającej na szybkie zestawienie wyposażenia w wozie transmisyjnym. Rezerwowe wyposażenie będzie stale dołączone do sieci i wykorzystywane do zadań pomocniczych w taki sposób, aby istniała pewność jego natychmiastowej sprawności.
c) W rejonie węzła powinny być zapewnione punkty włączenia się w linie transmisji poza obiektem mieszczącym węzeł na wypadek uszkodzenie lub zniszczenia obiektu. Połączenie między ruchomym węzłem a punktami rezerwowych podłączeń mogą wykorzystywać różne media od połączeń przewodowych, przez wiązki radiowe, podczerwieni itp.

3.5 Przeciążenie sieci

Przeciążenie sieci wobec istniejących obecnie i dających się przewidzieć w przyszłości ograniczeń finansowych jest wysoce prawdopodobne. Zwłaszcza, że obecny system finansowania sieci nie wpływa na samo-ograniczanie się użytkowników. W tej sytuacji powinno się przewidywać kilka środków przeciwdziałania.
a) Wyposażanie sieci w urządzenia i technologie pozwalające na zwiększanie szybkości przesyłania w miarę pojawiających się możliwości zapłaty za łącza transmisji.
b) Dobór technologii kompatybilnych dla różnych szybkości przesyłania w taki sposób, aby wprowadzanie nowych przystosowanych do większych szybkości przesyłania nie powodował utraty funkcjonalności urządzeń pracujących w sieci.
c) Możliwość tworzenia priorytetowych kanałów przesyłania dla szczególnie ważnych połączeń.
d) Wprowadzanie gwarantowanego pasma przesyłania, tak aby praca chociażby spowolniona była możliwa.
e) Wprowadzenie systemu umów i rozliczeń wpływającego na racjonalizację abonentów w sieci.

Wyżej wymienione informacje nie dotyczą specjalnych węzłów, gdzie na polecenie abonenta gromadzi się informacje do publicznego użytku, w celu ograniczenia wejść użytkowników do wnętrza sieci .

5. Ochrona sieci przed niepowołanym dostępem

W referacie zaznaczono kilka metod ochrony sieci przed niepowołanym dostępem.

a) Wszystkie urządzenia sieci muszą być w specjalnie wydzielonych pomieszczeniach wyposażonych w zamknięcia szyfrowe i centralny system monitorowania wejścia do pomieszczeń oraz rejestr osób wchodzących i wychodzących z pomieszczenia.

b) Szczególnie ważne wyposażenie systemu powinno być ulokowane w obiektach bronionych odpowiedniej klasy.

c) Sieć powinna być wyposażona w system wykrywający próby ingerencji oraz rejestrację tych ingerencji. Linie i urządzenia, tam gdzie zaistniało podejrzenie obcej ingerencji do czasu wyjaśnienia zostają czasowo wyłączone z ruchu. Dla transmisji szczególnie ważnych powinien być stosowany zmieniany w czasie system przesyłania.

d) Wyposażenie sieci powinno być centralnie sterowane i monitorowane. Nie oznacza to możliwości ingerencji w całej sieci w przypadku opanowania centrum sterowania. Sieć powinna być podzielona na strefy i obszary dostępu w ten sposób, że dla każdego operatora części sieci, do których nie ma uprawnień przedstawiają się jako "czarne skrzynki" widoczne jedynie przez skutki ich działania.

e) Powinien być wprowadzony zhierarchizowany system autoryzacji dostępu i jego aktualizacji. Działania operatorów powinny być możliwe dopiero po weryfikacji znanego centralnie hasła dostępu znanego operatorowi oraz hasła czasowego (zmieniającego się na przykład co 60') odczytywanego z osobistego wskaźnika posiadanego przez operatora.

f) Sieć powinna działać pod nadzorem specjalnej służby bezpieczeństwa sieci i jej abonentów.

6. Podsumowanie

Jak z powyższego katalogu wynika nie tylko ochrona informacji, na przykład poprzez szyfrowanie, maskowanie, fałszowanie, jest istotna w sieci telekomunikacyjnej. Metody ochrony informacji są skuteczne tylko w sieci, która jest przystosowana dla bezpiecznego działania.

Wyżej wymieniony katalog problemów nie pretenduje do kompletności, wynika on z wieloletnich doświadczeń z budowy i eksploatacji sieci teleinformatycznych. Autor sądzi, że wyżej zaznaczone problemy są istotne w każdej odpowiedzialnie udostępnianej sieci telekomunikacyjnej, nie tylko w sieci o podwyższonym bezpieczeństwie.

7. Zakończenie

Porównanie wymagań przedstawionych w poprzednim i obecnym referacie z "siermiężną" rzeczywistością może skłaniać do unikania stosowania sieci telekomunikacyjnych w ogóle. Z tego powodu chcemy zwrócić uwagę na kilka okoliczności.:

- Największym wrogiem bezpieczeństwa sieci telekomunikacyjnych jest, jak to napisał mój poprzednik, budżet, to znaczy niewystarczająca ilość środków na pełną realizację optymalnych rozwiązań. Jednak też i dla atakujących sieć problemem jest posiadanie środków na bardziej wyrafinowany atak. Na przykład przechwycenie informacji w sieci multimedialnej, o dużej przepustowości, wymaga posiadania silnych narzędzi, które pozwolą przechwycić przesyłaną

WPROWADZENIE DO TECHNOLOGII PODWYŻSZAJĄCYCH BEZPIECZEŃSTWO KORZYSTANIA Z SIECI TELEINFORMATYCZNYCH

Andrzej Białecki

Naukowa i Akademicka Sieć Komputerowa
Warszawa, ul. Bartycka 18, tel. 410041 w 229

1. Wstęp

Żywiołowy rozwój Internetu, a zwłaszcza wykorzystanie go do celów komercyjnych, spowodował wzrost zainteresowania zagadnieniami bezpieczeństwa przesyłania danych sieciami teleinformatycznymi. I nie bez powodu - coraz częściej bowiem obserwuje się przypadki nieuprawnionego dostępu do informacji przechowywanych lub przesyłanych w formie elektronicznej.

Większość obecnie eksploatowanych sieci teleinformatycznych (z Internetem włącznie) nie była, niestety, projektowana od samego początku z myślą o bezpieczeństwie. Środki ochrony przesyłanych nimi informacji były co najwyżej dodawane do już istniejących protokołów i rozwiązań konfiguracyjnych, co powodowało, że ich skuteczność była niewielka. Do dziś najbardziej rozpowszechnione usługi związane z wymianą danych nie posiadają dobrych zabezpieczeń przed przechwyceniem i/lub zmianą przesyłanych danych.

W miarę rozwoju Internetu technologie i protokoły, które zostały w nim pomyślnie przetestowane, były przenoszone również na inne sieci informatyczne. Były one do tej pory mniej podatne na niebezpieczeństwo ingerencji w powierzane im dane ze względu na swój ograniczony zasięg i specyficzne rozwiązania. Dały one początek tzw. intranetom, oraz sieciom korporacyjnym, w których warstwą transportową jest protokół TCP/IP. W konsekwencji tego obecnie wiele sieci prywatnych, nie podłączonych do Internetu, dzieli z nim jego słabości w dziedzinie zabezpieczeń.

Od kilku lat obserwujemy burzliwy rozwój zastosowań sieci do celów komercyjnych i rządowych. Związane jest to nieuchronnie z pytaniem o rozwój technologii podwyższających bezpieczeństwo korzystania z istniejących, niezbyt bezpiecznie zaprojektowanych sieci teleinformatycznych.

W dalszej części artykułu omówione zostaną problemy związane z tą dziedziną, oraz niektóre z proponowanych rozwiązań.

2. Podejście systemowe do bezpieczeństwa sieci.

Organizacja wdrażająca u siebie metody wymiany informacji drogą elektroniczną może łatwo popaść w jedną z kilku pułapek. Przytoczmy dwa przykłady:

- organizacja posiada (lub stwarza) bardzo dobry system uprawnień poszczególnych osób do sklasyfikowanych informacji, system dostępu do pomieszczeń i urządzeń, instaluje zabezpieczenia przed emisją elektromagnetyczną. Po czym podłącza swoją sieć lokalną bezpośrednio do Internetu, żeby każdy pracownik mógł korzystać z dobrodziejstw łączności sieciowej. Po kilku miesiącach okazuje się, że wszystkie poufne informacje z maszyny dyrektora trafiły do rąk konkurencji.

- ewentualnie możliwość stosowania niepodrabialnych podpisów cyfrowych.

Wiele z tych elementów jest realizowanych wspólnie przez konkretne rozwiązania. Nie wszystkie też są w danej sytuacji niezbędne.

Sprzęt sieciowy:

- firewall: bezpieczne podłączenie sieci lokalnej/korporacyjnej do Internetu,
- VPN (Virtual Private Network): bezpieczna transmisja danych po niezabezpieczonych łączach.

W następnych punktach zostaną omówione powyższe zagadnienia związane z bezpieczeństwem przesyłania danych, oraz stosowane w typowych sytuacjach rozwiązania. Należy podkreślić, że wymienione technologie z powodzeniem są wykorzystywane zarówno w typowych sieciach lokalnych, jak i w rozbudowanych sieciach korporacyjnych oraz w sieci Internet.

3.1 Usługi w sieciach korporacyjnych i lokalnych.

Uwierzytelnianie i autoryzacja użytkowników.

W przypadku sieci korporacyjnej, rozciągającej się zazwyczaj na dużym geograficznie obszarze i wykorzystywanej przez rzesze użytkowników, zapewnienie bezpiecznych usług w tej dziedzinie staje się prawdziwym wyzwaniem. Poszczególnym administratorom trudno jest panować nad mnogością kont użytkowników i ich uprawnieniami. Dodatkowo dochodzą problemy ze słabymi hasłami i niemożnością pilnowania użytkowników znajdujących się w odległych oddziałach. Kolejnym problemem jest słabość popularnych protokołów (ftp, telnet), które pozwalają na łatwe przechwycenie standardowych haseł.

Odpowiedzią na te problemy są między innymi mechanizmy silnej autentyzacji (uwierzytelniania) użytkowników. Wykorzystywane są w nich techniki synchronizacji czasowej i haseł jednokrotnych w połączeniu z algorytmami kryptograficznymi. Oto istniejące standardy, oraz niektóre z rozwiązań:

Standardy:

- FIPS (Federal Information Processing Standards)

  Jest to zbiór powszechnie dostępnych dokumentów przygotowywanych przez NIST (National Institute of Standards and Technology, USA). Zawierają one rekomendowane przez tę agencję technologie i algorytmy stosowane w celu zwiększania bezpieczeństwa przesyłania danych. Ujmują one w sposób syntetyczny sposoby stosowania oraz konkretne rozwiązania. Przykładowo, FIPS PUB 46-2 zawiera rekomendację algorytmu DES, a FIPS PUB 180 - opis stosowania algorytmu SHA (Secure Hash Algorithm), na którym został oparty standard podpisów cyfrowych (DSS). Natomiast publikacja FIPS 190 omawia szczegółowo różnorodne sposoby mocnego uwierzytelniania, m. in. przy pomocy tokenów (smart cards), technik biometrycznych (odciski palców, wzór siatkówki). Podaje również konkretne przykłady implementacji tych technik.

Niektóre rozwiązania:

- SecurID (Security Dynamics, Inc)

  Rozwiązanie wykorzystujące hasła jednokrotne generowane przez tzw. tokeny, czyli urządzenia wielkości karty kredytowej, zawierające wyświetlacz ze zmieniającym się co jakiś czas pseudolosowym kodem. Jest to uwierzytelnianie dwuskładnikowe: użytkownik

rozwiązywane jest to na wiele sposobów i w różnych warstwach transmisyjnych. Niektóre z wymienionych już rozwiązań (Kerberos) zapewniają również poufność.

Rozwiązania obejmujące szyfrowanie przez sprzęt sieciowy przedstawione zostaną dalej. Usługa niezaprzeczalności obecnie stosowana jest prawie wyłącznie dla celów poczty elektronicznej, i tam też zostanie omówiona. Natomiast poniżej opisane są technologie i standardy programowego zabezpieczania transmisji danych.

Standardy:

- IPSec (oraz przyszły standard IP v.6)

  Zabezpieczenie to polega na „poprawieniu" istniejącego protokołu transportowego sieci Internet tak, aby pomagał w określeniu autentyczności przesyłanych danych. Zasadnicze zmiany polegają na wprowadzeniu tzw. nagłówka autentyzacji (Authentication Header = AH). Zawarty w nim kryptograficzny skrót (MD5) zawartości pakietu gwarantuje jego niezmienność. Protokół ten może również stosować algorytm RSA, zapewniając niezaprzeczalność nadania informacji. Dodatkowo można zastosować tzw. ESP (Encapsulating Security Payload) pozwalający na zaszyfrowanie zawartości pakietu IP. Mimo istniejących już dość długo standardów, protokoły te na razie nie są zbyt rozpowszechnione. Szersze ich zastosowanie nastąpi dopiero podczas przechodzenia sieci Internet na protokół IP v.6.

Popularne techniki:

- F-Secure (DataFellows Inc.), oraz SSH (wersja public domain dla systemu Unix)

  Jest to programowy sposób zabezpieczenia typowych sposobów transmisji danych, jak FTP, telnet i X-Window, poprzez szyfrowanie całej sesji użytkownika na poziomie aplikacji. Dzięki łatwości użytkowania, różnorodności algorytmów szyfrowania, a przede wszystkim dostępności wersji dla różnych systemów operacyjnych (Unix, Windows) pakiet ten zyskał ostatnio ogromną popularność, stanowiąc solidną i tanią alternatywę dla innych rozwiązań. Podstawą jego działania są algorytmy kluczy publicznych w połączeniu z algorytmami symetrycznymi, co zapewnia szybkość działania i łatwość wymiany kluczy.

- SSL (Secure Socket Layer)

  Protokół ten umożliwia szyfrowanie transmisji związanej z usługą World Wide Web. Wykorzystuje on certyfikaty w standardzie X.509 w celu potwierdzenia tożsamości serwera. Dzięki temu protokołowi możliwe jest przesyłanie przez sieć publiczną np. numerów kart kredytowych. To zresztą było główną motywacją dla jego powstania.

  Przeglądarka WWW użytkownika jest wyposażona w zestaw znanych (zaufanych) certyfikatów. W momencie połączenia serwer wysyła swój certyfikat (klucz publiczny) do przeglądarki, która porównuje go ze swoją kopią. W przypadku zgodności, generowane są klucze sesyjne i rozpoczyna się szyfrowana wymiana informacji z użytkownikiem. Natomiast jeśli certyfikaty nie zgadzają się (lub nie ma odpowiedniego certyfikatu w bazie użytkownika), pojawia się ostrzeżenie i prośba o zatwierdzenie (lub odrzucenie) przysłanego, niepewnego certyfikatu serwera. Użytkownik może się w tym momencie zwrócić do znanego mu urzędu certyfikacyjnego z prośbą o potwierdzenie tożsamości serwera, i na tej podstawie zadecydować o dalszej wymianie informacji.

autentyczności przesyłanych informacji na podstawie posiadanych identyfikatorów (certyfikatów) użytkowników.

W większości rozwiązań odbywa się to w ten sposób, że każdy użytkownik chcący brać udział w bezpiecznej wymianie danych, musi się zwrócić do urzędu o wystawienie certyfikatu, potwierdzającego jego tożsamość. Zazwyczaj procedura ta obejmuje osobiste i pisemne potwierdzenie, poparte zwyczajnymi dokumentami. Następnie na tej podstawie urząd generuje klucze publiczny i prywatny, którymi użytkownik od tej pory będzie się posługiwał. W samym urzędzie pozostaje klucz publiczny dla celów późniejszego potwierdzania tożsamości użytkownika wobec innych uczestników wymiany danych.

W przypadku podejrzenia o np. wykradzenie klucza prywatnego, lub zmiany danych osobowych zawartych w kluczu, użytkownik zwraca się do urzędu o unieważnienie dotychczasowego certyfikatu, i wystawienie nowego.

Z dotychczas wymienionych rozwiązań jedynie PEM HEART udostępnia usługę urzędu certyfikacyjnego. Jednak wbrew pozorom, jest to usługa, którą można nawet w chwili obecnej szeroko wykorzystać do bezpiecznych transakcji przez WWW. Protokół SSL, zaimplementowany w przeglądarkach WWW czołowych producentów, opiera się właśnie na istnieniu urzędu certyfikacyjnego.

NASK, w ramach swoich zadań, pełni również rolę urzędu certyfikacyjnego w stosunku do tych, którzy chcą mieć możliwość potwierdzania tożsamości użytkowników lub serwerów wobec stron trzecich. Oferowane certyfikaty są zgodne z PEM, co pozwala m.in. na certyfikację serwerów WWW (np. firmy Netscape), oraz hierarchiczną certyfikację własnych urzędów dla potrzeb sieci korporacyjnych.

3.2 Zabezpieczanie styków międzysieciowych.

W tym punkcie przedstawione zostaną stosowane obecnie technologie zwiększające bezpieczeństwo korzystania z sieci publicznej (Internet), lub też pozwalające na logiczne wydzielenie połączeń o podwyższonych zabezpieczeniach.

Styk z siecią rozległą: firewall.

Obecnie stało się już dobrym standardem, że organizacje czułe na punkcie bezpieczeństwa wymiany danych podłączają do Internetu swoje sieci lokalne i korporacyjne poprzez tzw. firewall.

Jest to dedykowane urządzenie (lub grupa urządzeń), którego głównym zadaniem jest zabezpieczenie sieci wewnętrznej przed nieuprawnionym dostępem z zewnątrz. Drugim jego zadaniem jest zapewnienie kontrolowanego dostępu użytkowników wewnętrznych do sieci rozległej. Jako jedyny punkt styku obydwu sieci, firewall zapewnia przestrzeganie ustawionych na nim zasad korzystania z sieci. Na nim odbywa się uwierzytelnianie użytkowników chcących skorzystać z zasobów znajdujących się po drugiej stronie firewalla. Może on też tworzyć bezpieczne połączenia wirtualne (VPN -Virtual Private Networks) z innymi częściami sieci korporacyjnych, posługując się w tym celu publicznymi, niezabezpieczonymi łączami.

Niezwykle istotnym zagadnieniem jest zastosowanie mocnej autentyzacji użytkowników, zwłaszcza tych, którzy mają mieć dostęp z sieci zewnętrznej do danych zgromadzonych w sieci lokalnej. Standardowe systemy haseł wielokrotnego użycia są w tym wypadku mocno nieadekwatne - ich stosowanie naraża bezpieczeństwo całej sieci wewnętrznej. Dlatego obecnie wszystkie

systemu, zapewniając bardzo dobrą wydajność. Nie bez znaczenia jest rozbudowany interfejs graficzny, obrazujący stan poszczególnych połączeń i obiektów w chronionej sieci.

- Gauntlet (Trusted Information Systems, Inc.)

  Produkt ten oferuje podobne możliwości, jednak działa w oparciu o tzw. proxy (application level). Charakterystyczna dla tego typu firewalli jest (oprócz mniejszej szybkości działania) surowa polityka, związana z koniecznością autoryzacji każdego połączenia, oraz ograniczenia do kilku podstawowych usług sieciowych (telnet, ftp, http). Również oferuje możliwości translacji adresów i tworzenia sieci wirtualnych, oraz mocne uwierzytelnianie.

- FWTK (Trusted Information Systems, Inc.)

  Okrojona nieco (ale publicznie dostępna) wersja powyższego produktu. Ze względu na dostępność bardzo szeroko stosowana w przypadku mniejszych sieci. Konfiguracja jest dosyć siermiężna ze względu na brak aplikacji zarządzającej poszczególnymi modułami. Mimo tego, pakiet ten oferuje podstawowe możliwości technologii proxy w połączeniu z mocną autentyzacją.

Szyfrowanie transmisji przez sprzęt sieciowy.

W celu zabezpieczenia transmisji np. pomiędzy oddziałami firmy, podłączonymi poprzez publiczne, niepewne sieci (np. Internet), stosowane jest szyfrowanie pomiędzy wybranymi maszynami na poziomie różnych protokołów transmisyjnych. Jak to zostało wspomniane powyżej, niekiedy taką możliwość oferują firewalle - wówczas realizowana jest ona na drodze programowej. Istnieją także rozwiązania z użyciem sprzętu sieciowego takiego jak: szyfrujące modemy i karty sieciowe, routery i inne urządzenia specjalne.

- Cisco IOS (Cisco Systems)

  Szyfrowanie realizowane jest programowo w tańszych modelach routerów, lub sprzętowo w routerach klasy high-end. Pozwala na stworzenie bezpiecznego tunelu komunikacyjnego między parą routerów, wykorzystującego potencjalnie niebezpieczne połączenia sieciowe. W ten sposób powstaje tzw. VPN (Virtual Private Network). Rozwiązanie to pozwala na selektywne szyfrowanie poszczególnych pakietów w zależności od ich adresu źródła i przeznaczenia, dzięki czemu możliwe jest stworzenie kilku oddzielnie szyfrowanych kanałów.

- KryptoLan (Sectra Inc.)

  Są to urządzenia oferujące szyfrowanie sprzętowe. Proponowane są dwie wersje: jedno pozwala na stworzenie VPN w rozległej sieci organizacji, udostępniając szyfrowanie na poziomie protokołu IP. Drugie umożliwia wydzielenie specjalnych podsieci w sieci lokalnej, szyfrowanych na poziomie warstwy łącza danych, np. Ethernet. Dzięki temu niektóre typy transmisji danych są szczególnie chronione przed dostępem pozostałych użytkowników sieci lokalnej. Elastyczne konfigurowanie zbioru maszyn biorących udział w szyfrowanej transmisji pozwala na szybkie tworzenie np. zespołów pracujących nad szczególnie poufnymi projektami, bez konieczności budowania za każdym razem wydzielonej sieci.

Bezpieczeństwo szyfrowanych danych jest bezpośrednio zależne od długości użytego klucza. Powszechnie przyjmuje się, że klucz DES o długości 40 bitów jest niebezpiecznie krótki - przeciętnie wyposażony napastnik jest w stanie go odkryć w dosyć krótkim czasie (rzędu godzin). Natomiast długość klucza 56 bitów stawia wymagania obliczeniowe na poziomie obecnych możliwości jednostki rządowej. Oczywiście, zawsze należy brać pod uwagę jaki jest okres ważności przesyłanych danych - być może 40 bitów w zupełności wystarczy. Poniżej zamieszczone jest zestawienie przedstawione w 1996 roku przez grupę czołowych kryptografów.

Typ napastnika	Budżet	Narzędzia	Czas i koszt (40 bitów)	Czas i koszt (56 bitów)	Długość klucza bezpiecznego w 1995r
przeciętny hacker	nikły	wolny czas maszyny	1 tydzień	niemożliwe	45 bitów
j/w	$400	układ FPGA	5 godz ($0,08)	38 lat ($5000)	50 bitów
mała firma	$10000	układ FPGA	12 min. ($0,08)	18 mies. ($5000)	55 bitów
dział dużej firmy	$300K	układ FPGA	24 s ($0,08)	19 dni ($5000)	60 bitów
		lub ASIC	0,18 s ($0,001)	3 godz. ($38)	
duża firma	$10M	układ FPGA	0,7 s ($0,08)	13 godz. ($5000)	70 bitów
		lub ASIC	0,005 s ($0,001)	6 min ($38)	
agencja wywiadowcza	$300M	układ ASIC	0,0002 s ($0,001)	12 s ($38)	75 bitów

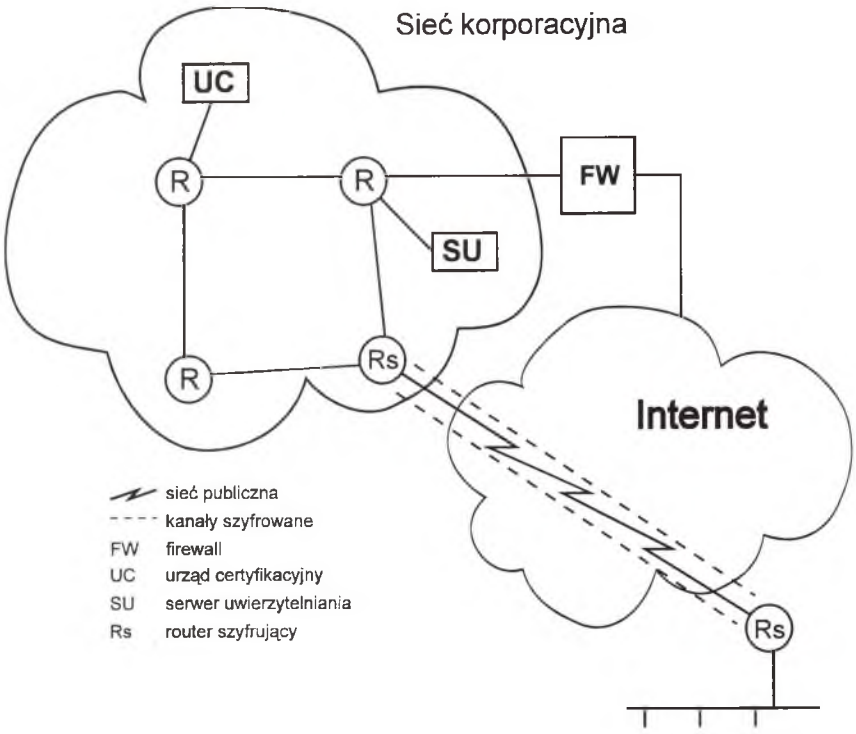
Jak widać z powyższego zestawienia, technologie posługujące się 40 bitowym kluczem DES należy traktować obecnie jako nie zapewniające wystarczającego zabezpieczenia nawet przed przypadkowym napastnikiem. Dla napastnika zdeterminowanego i dysponującego odpowiednim budżetem nie oferują praktycznie żadnego zabezpieczenia.

4.3 Algorytmy asymetryczne (z kluczem publicznym)

Istota działania tych algorytmów zasadza się na możliwości utworzenia takiej pary kluczy, że wiadomości zaszyfrowanej jednym z nich nie da się odszyfrować nim samym, natomiast da się odszyfrować drugim kluczem. Dodatkowo, niemożliwe jest utworzenie jednego klucza na podstawie znajomości drugiego.

W praktyce oznacza to, że jeden z kluczy (tzw. klucz publiczny) może być szeroko rozprowadzony wśród uczestników wymiany informacji. Posługując się nim, będą oni mogli zaszyfrować wiadomości dla posiadacza klucza prywatnego, a tylko on będzie je w stanie odszyfrować.

Scenariusz nawiązania szyfrowanej łączności może więc być następujący: uczestnik A wysyła do B swój klucz publiczny. W odpowiedzi B wysyła do A również swój klucz publiczny. A szyfruje



Ilustracja 1. Przykładowa konfiguracja bezpiecznej sieci przesyłania danych

Wykorzystanie przez intruzów oprogramowania dostępnego w sieci na przykładzie danych w zakresie lokalizowania komputerów do zaatakowania

Z danych CERT NASK wynika, iż w zakresie technik lokalizowania komputerów do zaatakowania intruzi wykorzystują rozmaite metody tzw. "skanowania" sieci i "próbkowania" komputerów w sieci. Metody te, wg. zanotowanych przypadków w Polsce, opierają się na wykorzystaniu istniejących w sieci programów i skryptów Są to skrypty wykonujące automatycznie setki a nawet tysiące prób "połączeń" z określoną grupa adresów w sieci w celu wykrycia i wykorzystania luk w systemach tych komputerów a także wykorzystywane są typowe pakiety skanujące, które są używane zarówno przez administratorów sieci w celu zbadania realnego poziomu bezpieczeństwa zarządzanego komputera czy sieci jak też używają ich intruzi.

Wykryte przypadki sniffingu (podsłuchiwanie cudzych pakietów w sieci) zdecydowanie dominowały w działalności hackerskiej w drugiej połowie 1996 roku.

W sieci Internet, a konkretnie na serwerach - głównie akademickich - znajduje się oprogramowanie, które może służyć do przygotowania lub przeprowadzenia zdalnego ataku na cudzy system komputerowy. Znaleźć można także opisy i instrukcje w jaki sposób można dokonać włamania czy też oszustwa przy pomocy Internetu i komputera (zanotowano np. przypadek upowszechnienia na serwerze akademickim instrukcji w języku polskim, jak dokonywać przy pomocy Internetu oszustw w dziedzinie kart płatniczych). Oprogramowanie ułatwiające przygotowywanie bądź atakowanie cudzych systemów można podzielić na kilka rodzajów:

a)pakiety służące do półautomatycznych testów stopnia zabezpieczenia komputerów (np. osławiony SATAN) lub monitorowania sieci i urządzeń

(zgodnie ze swym przeznaczeniem mają służyć administratorom sieci do testowania zarządzanych przez siebie komputerów - powszechnie jednak używają ich hackerzy aby „badać" zabezpieczenie cudzych sieci lub podsłuchiwać pakiety w celu ewentualnego późniejszego zaatakowania cudzych systemów)

Istnienie i dostępność tego typu programów nie musi być niczym nagannym. Potencjalne zagrożenie wynika z praktyki: paradoksalnie nie wszyscy administratorzy znają i wykorzystują to oprogramowanie w przeciwieństwie do sieciowych włamywaczy, którzy stosują je nagminnie.

b) programy i skrypty stworzone i opublikowane w sieci przez włamywaczy służące eksploatowaniu rozmaitych słabości systemów operacyjnych, sieciowych i oprogramowania użytkowego stosowanego w Internecie

(w tej grupie znajdują się wirusy, bomby logiczne, konie trojańskie, sniffery i inne programy oraz skrypty używane przez rozmaitych intruzów)
Programy takie często dostają się w ręce niedoświadczonych osób, któreza czynają je wykorzystywać do włamywania sie do cudzych systemów. Obecnie zauważa się coraz większa liczbę przypadków poważnych włamań powodowanych przez mało doświadczonych włamywaczy używających groźnych („profesjonalnych") narzędzi dostępnych w Internecie. Na niektórych serwerach w Polsce (głównie akademickich znajduja sie prawdziwe „skarbnice" oprogramowania, które może być wykorzystane do włamań na cudze systemy.

Co robią intruzi w czasie udanych włamań ?

Typowy scenariusz ataku na system komputerowy składa się z kilku etapów:

- zlokalizowanie systemu do zaatakowania
- zdobycie dostępu do konta legalnego użytkownika systemu poprzez łamanie łatwych haseł bądź podsłuchanie hasła
- wykorzystanie dziur w konfiguracji i w oprogramowaniu systemowym w celu wejścia na konto uprzywilejowane
- zatarcie śladów działalności (usunięcie zapisów z pamiętników - audit log)
- przeprowadzenie nieuprawnionych działań
- zainstalowanie „konia trojańskiego" dla aktualnego i przyszłego wykorzystania
- ataki na inne komputery w sieci lokalnej

Intruzi atakujący systemy komputerowe znajdujące się w sieci częstokroć posługują się kilkoma złamanymi wcześniej kontami na różnych maszynach logując się kolejno z jednego na drugie. Utrudnia to śledzenie miejsca, z którego tak naprawdę przeprowadzony był atak.

W punkcie „przeprowadzenie nieuprawnionych działań" intruzi dokonują takich czynności jakie są rzeczywistym celem ich ataków. Zgodnie ze statystyką CERT NASK w Polsce najczęściej spotykane działania to:

- wprowadzanie zmian w zaatakowanym systemie (modyfikacje ważnych plików np. /etc/passwd),
- podmienianie plików systemowych - (ang. deamons) - np. telnetd ,
- instalacja modułów "koni trojańskich", instalowanie snifferów),
- ingerowanie w prywatność (np. przeglądanie cudzej poczty elektronicznej)
- powodowanie szkód moralnych i zaburzeń w komunikacji (nieuprawniona ingerencja w treść stron WWW),
- przechowywanie i kolportowanie pornografii - w tym dziecięcej

Działania wymienione w pierwszych dwóch punktach mają na celu uzyskanie pełnej kontroli nad zaatakowanym systemem. W dodatku często jest to przeprowadzane w taki sposób aby legalny administrator systemu nie zauważył faktu przejęcia kontroli nad komputerem przez intruza. Intruz może wykorzystywać kontrolowany przez siebie komputer do ataków na inne systemy, składowania na nim niepożądanych plików (np. pirackiego oprogramowania), wykorzystywania jego mocy obliczeniowej do np. łamania plików z hasłami bądź też kradzieży informacji. Z kolei instalacja snifferów czy modułów zapewniających tzw. tylne drzwi do systemu ma na celu przygotowanie pola do ataku na inne komputery w danej sieci lokalnej oraz zapewnienie sobie łatwego dostępu do złamanego komputera w przyszłości.

Trzy ostatnie typy działań czyli **ingerowanie w prywatność, powodowanie szkód moralnych oraz zaburzeń w komunikacji a także rozpowszechnianie nielegalnych czy niepożądanych treści** są już typowymi czynnościami powodującymi określone szkody kwalifikującymi się wręcz do ścigania na drodze prawnej. Istnieją w Polsce precedensy, gdzie organa ścigania powzięły z pozytywnym skutkiem określone czynności przeciwko sprawcom ww. czynów.

Na uwagę zasługuje ogromna ilość a także rozkład domenowy próbkowanych hostów (czyli komputerów, które były obiektem prób do przeprowadzenia ataku). Dane zgromadzone przez CERT NASK świadczą, ze ponad 7% komputerów w polskim Internecie było próbkowanych Na szczęście tylko nikły procent (<1%) z próbkowanych komputerów uległ udanemu atakowi hackerów - jednak CERT NASK podkreśla, ze statystyka ta dotyczy zgłoszonych incydentów Nie wiadomo ile prób i udanych ataków nie jest w ogóle zgłaszanych i rejestrowanych.

DIAGRAMY

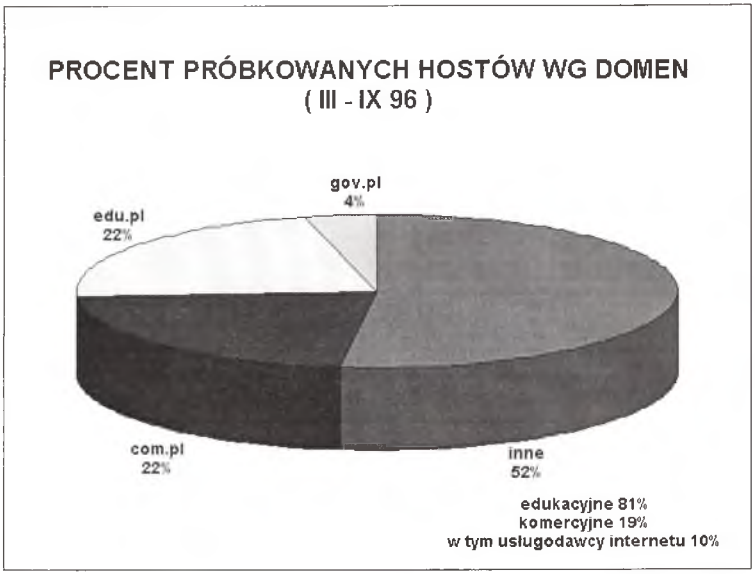


Diagram nr1

Diagram nr1 pokazuje podział procentowy na główne domeny ilości próbkowanych hostów w obsłużonych przez CERT NASK incydentach. W kategorii "inne" umieszczono domeny typu np: miasto.pl lub nazwa.pl . W ramach grupy "inne" znalazły się podmioty o profilu edukacyjnym (81%) bądź komercyjnym 19% (do tej ostatniej grupy zaliczono też dostawców internetu).

Na podstawie diagramu nr 1 opracowano diagram nr 2.

Kategoria "wszystkie" dotyczy wszystkich hostów zarejestrowanych w domenie .pl. Dane jakie przedstawiają te wykresy, choć prezentują stan za okres marzec - październik, można odnieść do całego okresu działalności CERT NASK w 1996, gdyż próbkowanie polskich hostów na dużą skalę miało miejsce głównie we wspomnianym wcześniejszym okresie.
Uważna analiza danych trzech zaprezentowanych diagramów pozwala wysnuć bardzo ciekawe wnioski. Niewątpliwie najwięcej próbkowanych komputerów należy do grupy : edukacja. Jest to poniekąd zrozumiałe ponieważ hostów należących do uczelni, instytutów badawczych i innych placówek akademickich jest w polskim Internecie zdecydowanie najwięcej. Na drugim miejscu są komputery z grupy komercyjnej a na trzecim z grupy rządowej. Jednak rzut oka na diagram trzeci wskazuje, że ilościach względnych (ilość atakowanych komputerów w stosunku do wszystkich zarejestrowanych w danej kategorii) „edukacja" wcale nie jest tą najchętniej atakowana kategorią komputerów (6,3%). Relatywnie większym zainteresowaniem cieszą się komputery z grupy „rządowe" , z których aż 8,7% było próbkowanych w tym samym okresie. Największym, w stosunku do ich ilości, zainteresowaniem włamywaczy cieszą się komputery z grupy: komercyjni (14,6% próbkowanych hostów).

głównie Komitet Techniczny TC110 Electromagnetic Compatybility, oraz Komitety Przedmiotowe. W Polsce instytucją opracowującą polskie normy (PN) jest Polski Komitet Normalizacyjny. Normy Polskie są obecnie tworzone w zgodności z zaleceniami europejskimi i międzynarodowymi.

W Europie Zachodniej podstawę w dziedzinie kompatybilności elektromagnetycznej stanowi wytyczna (ang. directive) 89/336/EEC (*Tabela* 1) opublikowana w Oficjalnym Dzienniku Unii Europejskiej (ang. Official Journal on the European Union). Na podstawie tej wytycznej wraz z uzupełnieniem 92/31/EEC oraz na bazie normy CISPR 22 (ang. Internacional Special Committee of Radio Interference) powstał harmonizowany standard EN 550022 (tzn. zwierający harmonizowane procedury testowe i wzorce odniesienia). Określa on wartości graniczne oraz opisuje metody pomiaru charakterystyk interferencji radiowych urządzeń techniki informatycznej.
Ponad to Europejska Komisja opracowała i ratyfikowała dwa źródłowe standardy (ang. generic standard) dotyczące kompatybilności elektromagnetycznej *(Tabela 2)*:

- **EN 50081-1; 1992** - Kompatybilność elektromagnetyczna - Źródłowy standard emisji
  Część. 1 Pomieszczenia i urządzenia powszechnego użytku, komercyjne i środowisko przemysłu lekkiego
  EN 50081-2; 1993 - Część. 2 Pomieszczenia i urządzenia środowisko przemysłu ciężkiego
- **EN 50082-1; 1995** - Kompatybilność elektromagnetyczna - Źródłowy standard odporności
  Część. 1 Pomieszczenia i urządzenia powszechnego użytku, komercyjne i środowisko przemysłu lekkiego
  EN 50082-2; 1994 - Część. 2 Pomieszczenia i urządzenia środowisko przemysłu ciężkiego

Obydwie normy mają głównie zastosowanie dla urządzeń elektronicznych i elektrycznych oraz do systemów i instalacji wytwarzających zakłócenia elektromagnetyczne lub narażonych na ich działanie. Sieci teleinformatyczne należy traktować jako składowe techniki informatycznej IT (ang. Information Technology) i telekomunikacyjnego wyposażenia końcowego TTE (ang. Telecommunication Terminal Equipment). Muszą one spełniać wymagania odpowiednich standardów stowarzyszonych z normami **EN 50081 i EN 50082.**

Jeśli chodzi o normy krajowe, to podstawowe zagadnienia dotyczące kompatybilności elektromagnetycznej przedstawione zostały w trzech normach opracowanych w latach osiemdziesiątych:

- **PN-80/T-01005** - Przemysłowe zakłócenia radioelektryczne. Nazwy i określenia podstawowe.
- **PN-86/E-06600** - Automatyka i pomiary przemysłowe. Kompatybilność elektromagnetyczna urządzeń. Ogólne wymagania i badania.
- **PN-89/E-06251** - Przemysłowe zakłócenia radioelektryczne. Techniczne urządzenia informatyki. Dopuszczalne poziomy zakłóceń. Wymagania i badania.

Tabela 1

Wytyczna	Oznaczenie wytycznej	Uwagi:
Dyrektywa EMC	89/336/EEC	Kompatybilność elektromagnetyczna
Uzupełnienie 1 Dyrektywy EMC	92/31/EEC	Powołano normę: EN 55022,
Uzupełnienie 2 Dyrektywy EMC	93/68/EEC	EN 50082-1

*Tabela 3. Zakres norm stowarzyszonych z normą **EN 50081-1; 1992***

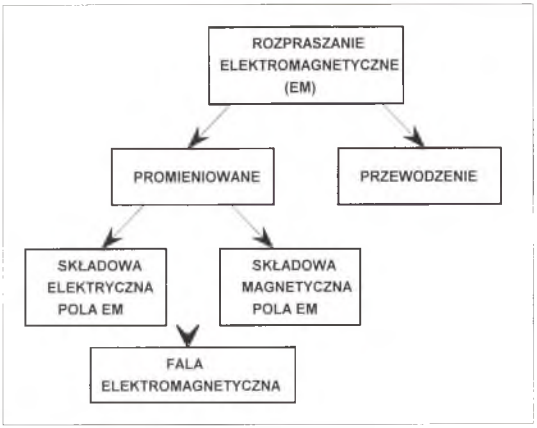
Standard IEC	Standard europejski EN	Zakres
IEC 50(161)	-	Międzynarodowy Słownik Elektrotechniczny Rozdział 161: Kompatybilność elektromagnetyczna
IEC 555-1	EN 60555-1	Rozkłady emisji w systemach zasilania powodowane przez urządzenia domowe oraz podobny sprzęt elektryczny Część 1: Definicje
IEC 555-2 (mod)	EN 60555-2	Część 2: Harmoniczne
IEC 555-3	EN 60555-3	Część 3: Fluktuacje napięcia
CISPR 14 (mod)	EN 55014	Wartości graniczne i metody pomiaru charakterystyk interferencji radiowych elektronicznych urządzeń domowych, urządzeń przenośnych oraz podobnych urządzeń elektrycznych
CISPR 22 (mod)	EN 55022	Wartości graniczne i metody pomiaru charakterystyk interferencji radiowych urządzeń techniki informatycznej

*Tabela 4. Zakres norm stowarzyszonych z normą **EN 50081-2; 1993***

Standard IEC	Standard europejski EN	Zakres
IEC 50(161)	-	Międzynarodowy Słownik Elektrotechniczny Rozdział 161: Kompatybilność elektromagnetyczna
CISPR 11 (mod)	EN 55011	Wartości graniczne i metody pomiaru charakterystyk zakłóceń radiowych urządzeń przemysłowych , badawczych, i medycznych (ISM) pracujących w zakresie częstotliwości radiowych
CISPR 14	EN 55014	Wartości graniczne i metody pomiaru charakterystyk zakłóceń radiowych od silników elektrycznych i urządzeń ciepłowniczych przeznaczonych dla domowych i podobnych potrzeb, maszyn elektrycznych, oraz podobnego sprzętu elektrycznego.
CISPR 22:1985 (mod)	EN 55022:1987	Wartości graniczne i metody pomiaru charakterystyk interferencji radiowych urządzeń techniki informatycznej

*Tabela 5. Zakres norm stowarzyszonych z normą **EN 50082-1; 1995***

Standard IEC	Standard europejski EN	Zakres
IEC 50(161)	-	Międzynarodowy Słownik Elektrotechniczny Rozdział 161: Kompatybilność elektromagnetyczna
IEC 1000-4-2	EN 61000-4-2;1995	Kompatybilność elektromagnetyczna (EMC) Część 4: Testowanie i techniki pomiarowe Sekcja 2: Wymagania dotyczące wyładowań elektrostatycznych
IEC 1000-4-4	EN 61000-4-4;1995	Sekcja 4: Wymagania dotyczące szybkich wyładowań elektrycznych
IEC 1000-4-5	EN 61000-4-5;1995	Sekcja 5: Testowanie odporności na przeciążenia
IEC 1000-4-8	EN 61000-4-8;1993	Sekcja 8: Testowanie odporności na pola magnetyczne o częstotliwości zasilania



Rys. 1. Drogi rozpraszania elektromagnetycznego

3.1. Rozpraszanie elektromagnetyczne w sieciach teleinformatycznych

Współczesne metody detekcji skrajnie słabych sygnałów obarczonych szumami i zakłóceniami o dużej intensywności umożliwiają wykrycie sygnałów o poziomach mniejszych o ponad 40 dB od poziomu szumów cieplnych w obwodach elektrycznych. W systemach teleinformatycznych detekcja transmitowanych sygnałów jest możliwa dzięki emisji wielu składowych widma transmitowanego sygnału.

3.1.1. Mechanizm rozpraszania elektromagnetycznego

Urządzenia cyfrowe wykorzystują sygnały binarne, tzn. zero-jedynkowe. Czas przejścia z jednego stanu do drugiego często jest krótszy od nanosekundy. Równocześnie zmienia się natężenie prądu płynącego w liniach sygnałowych i zasilających. W konsekwencji obwody te promieniują energię elektromagnetyczną w zakresie od częstotliwości akustycznych do kilkuset MHz, a dla niektórych urządzeń nawet ponad 1 GHz. Większość emitowanej energii skupia się jednak w paśmie poniżej 300 MHz.

Szczególnym rodzajem urządzeń cyfrowych jest sprzęt sieciowy i komputerowy. Mamy tu do czynienia praktycznie ze wszystkimi zjawiskami tworzenia i rozchodzenia się energii elektromagnetycznej, charakterystycznymi dla urządzeń cyfrowych (wynika to z istnienia w instalacjach komputerowych zasilaczy, modemów, monitorów ekranowych, i wielu innych urządzeń peryferyjnych oraz połączeń w ramach sieci).

Jak już zostało wspomniane istnieją cztery drogi przenoszenia rozproszenia elektromagnetycznego. Należy zwrócić uwagę na dwie z dróg emisji energii. Pierwsza przez przewody, a więc za pośrednictwem sieci i linii elektrycznych, a druga przez promieniowanie, czyli rozchodzenie się energii w otaczającej przestrzeni w postaci fal elektromagnetycznych. Należy zwrócić uwagę, że często występują razem obydwa zjawiska.

3.1.2. Źródła rozpraszania elektromagnetycznego w sieciach teleinformatycznych

Źródłami rozpraszania elektromagnetycznego w sieciach teleinformatycznych są urządzenia aktywne i bierne. W szczególności można wyróżnić:

- układy scalone wraz z doprowadzeniami sygnałów, np. zegarowych, sterujących;

Powszechne szyfrowanie informacji jest trudne, gdyż jest bardzo kosztowne, a dystrybucja i stosowanie kluczy wymaga dużo czasu i zasobów. Zastosowanie skutecznego szyfrowania danych w systemach informatycznych, mimo iż jest nieodzowne dla zapewnienia poufności przetwarzania i transmisji informacji, nie jest w stanie zwykle zapewnić wysokiej protekcji systemu przed niepowołanym dostępem do wiadomości chronionych ze względu na niepożądana emisję wiadomości pierwotnej *(Rys. 2).*

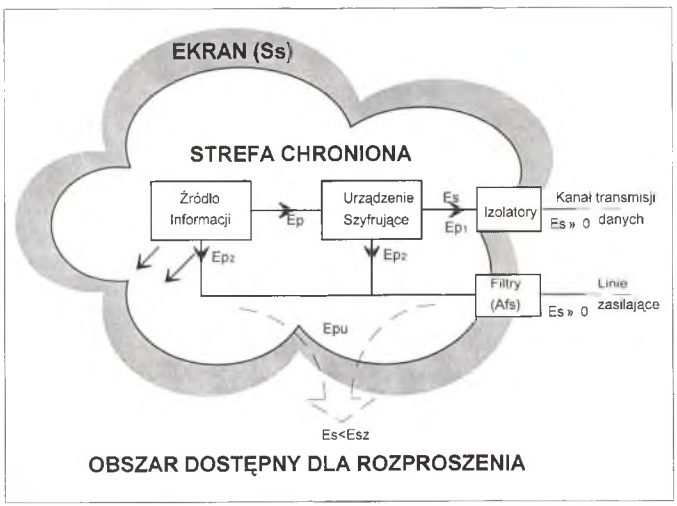
W sieciach teleinformatycznych, które powinny być chronione przed możliwością elektromagnetycznej detekcji wiadomości, należy ograniczyć emisyjność składowych widma wiadomości. W takich systemach powinny być spełnione wymagania w zakresie dopuszczalnego rozproszenia elektromagnetycznego. Te wymagania można spełnić przez osiągnięcie w rozpatrywanym systemie stopnia protekcji ***ps>1*** w całym zakresie częstotliwości, w którym występują składowe widma wiadomości. Stopień protekcji *ps* wyraża się zależnością:

$$ps = Ed/Es \qquad (1)$$

przy czym: ***Ed*** *- minimalny poziom emisji widma wiadomości przy którym istnieje potencjalna możliwość detekcji elektromagnetycznej wiadomości,*

Es *- emisja widma wiadomości przez system jako całość.*

Zależność ta powinna być spełniona dla każdej z możliwych dróg rozpraszania elektromagnetycznego wiadomości.



Es - emisja widma wiadomości pierwotnej przez system jako całość
Esz - emisja szumów,
Epu - dopuszczalny poziom emisji widma wiadomości pierwotnej,
Ss - skuteczność ekranowania ekranu,
Afs - skuteczność filtrów.

Rys. 3. Schemat instalacji systemu ze skutecznym szyfrowaniem i ochroną przed rozpraszaniem elektromagnetycznym informacji

Obszar chroniony stanowi strefę ekranowaną o odpowiednio dużej skuteczności ekranowania *Ss [dB],* wyposażoną w filtry elektryczne o odpowiedniej skuteczności *Afs.* Urządzenia systemu zainstalowanego w tej strefie powinny mieć odpowiednio ograniczona emisyjność *Epu,* tak aby

Dla urządzeń i systemów teleinformatycznych najbardziej niebezpiecznym i najczęściej występującym rodzajem narażeń elektromagnetycznych są zakłócenia .Podstawowe źródła emisji zakłóceń elektromagnetycznych impulsowe EMI (ang. Electromagnetic Interference) to:

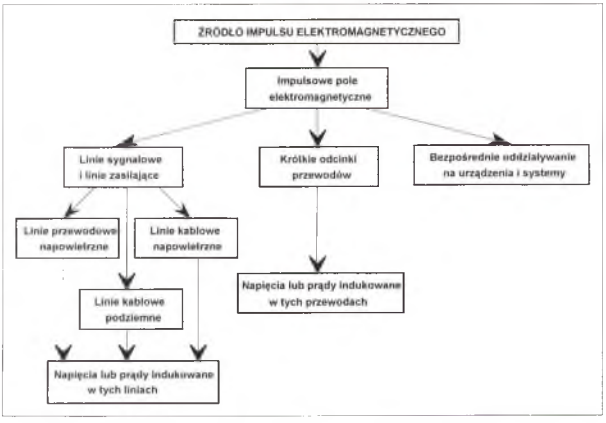
- wyładowania atmosferyczne,
- wyładowania elektrostatyczne,
- procesy łączeniowe i zwarcia w systemach dystrybucji mocy,
- efekty komutacji,
- efekty iskrzenia,
- chwilowe zaniki napięć,
- przepięcia w lokalnej sieci energetycznej,
- wybuchy nuklearne.

Narażenia elektromagnetyczne można również podzielić ze względu na sposób ich powstawania na:

- zakłócenia przypadkowe ,
- zakłócenia celowe.

4.1. Oddziaływanie zakłóceń impulsowych na urządzenia teleinformatyczne

Impuls elektroniczny indukuje prądy i napięcia we wszystkich obiektach przewodzących , które należy traktować jako anteny (niekoniecznie zamierzone). Indukowane impulsy prądu lub napięcia mogą dotrzeć do urządzeń elektronicznych dołączonych do tych obiektów i spowodować zakłócenie ich pracy, a nawet uszkodzenie. W urządzeniach elektronicznych szczególnie istotne są przepięcia i przetężenia, chwilowe i krótkotrwałe zaniki, oraz inne zakłócenia indukowane w liniach zasilających, torach sygnałowych i odcinkach przewodów łączących poszczególne urządzenia obiektu, a także bezpośrednie oddziaływanie pola elektromagnetycznego *(Rys. 5).*



Rys. 5. Sposoby oddziaływania impulsów elektromagnetycznych na urządzenia i systemy teleinformatyczne

Na Rys. 6 przedstawiono przykład oddziaływania impulsu elektromagnetycznego na pewien obiekt teleinformatyczny. Energia impulsu może dotrzeć do urządzeń telekomunikacyjnych przez napowietrzne i podziemne linie energetyczne i tory sygnałowe, przez anteny i falowody, przez otwory (drzwi i okna) w ścianach budynku, w którym znajdują się urządzenia, a także bezpośrednio. Tłumienie wnoszone przez ściany zależy od materiału, z którego je wykonano.

Przez odporność rozumie się zdolność pracującego urządzenia lub systemu do zachowania swoich właściwości poprawnego działania, podczas oddziaływania określonych zakłóceń elektromagnetycznych lub umownych sygnałów zakłócających.

Podatność jest reakcją pracującego urządzenia lub systemu na określone zakłócenia elektromagnetyczne lub umowne sygnały zakłócające, wyrażoną zmianami właściwości urządzenia lub systemu w funkcji parametrów zakłócenia.

Wytrzymałość jest zdolnością pracującego urządzenia lub systemu do zachowania swoich pierwotnych właściwości po ustąpieniu oddziaływania określonych zakłóceń elektromagnetycznych lub umownych sygnałów zakłócających.

W zależności od poziomu odporności urządzenia lub systemu na impulsowe urządzenia elektromagnetyczne zaliczane są one do jednej z pięciu klas:

- urządzenia i systemy bez ochrony (poziom odporności nie zdefiniowany),
- urządzenia i systemy o normalnym poziomie odporności,
- urządzenia i systemy o normalnej odporności,
- urządzenia i systemy o wysokiej odporności,
- urządzenia i systemy o specjalnej odporności.

Najwyższe wymagania stawia się urządzeniom i systemom pracującym w obecności silnych zakłóceń impulsowych lub narażonych na działanie takich zakłóceń, w miejscach gdzie ich niezawodna praca wiąże się z bezpieczeństwem ludzi, z prawidłowym działaniem ważnych systemów teleinformatycznych i żywotnych z punktu widzenia interesów państwa oraz obronności kraju. Aby określone urządzenie lub system można było zakwalifikować do jednej z pięciu wyżej przedstawionych klas, należy określić kryteria poprawności działania urządzeń lub systemów poddanych działaniu impulsowych narażeń elektromagnetycznych (symulowanych zwykle w warunkach laboratoryjnych sygnałami umownymi). Kryteria te powinny być uzgodnione z użytkownikiem. Na ogół stosuje się następującą skalę ocen:

- nie występują objawy i efekty zakłóceń właściwości urządzenia;
- występują chwilowe objawy i efekty zakłóceń właściwości urządzenia, likwidowane samoczynnie, które nie dotyczą podstawowych właściwości funkcjonalnych urządzenia i nie powodują zagrożenia dla procesu technologicznego i obsługi - są dopuszczone przez użytkownika;
- występują objawy i efekty zakłóceń właściwości urządzenia, do zlikwidowania których konieczna jest interwencja obsługi - są niedopuszczalne przez użytkownika;
- występuje trwała utrata właściwości urządzenia spowodowana uszkodzeniami.

Ścisłe określenie poziomów odporności, podatności i wytrzymałości wymaga badań polegających na obserwowaniu i rejestracji zachowania się obiektu w warunkach płynnie lub skokowo zwiększonego poziomu umownego sygnału zakłócającego. Minimalny poziom umownego sygnału zakłócającego, przy którym występują objawy i efekty zakłócenia, uważa się za zmierzony poziom podatności urządzenia lub systemu na dany umowny sygnał zakłócający. Maksymalny poziom sygnału umownego (określony zwykle w normie przedmiotowej), przy którym urządzenie działa poprawnie przez czas badania, jest zmierzonym poziomem umownego sygnału zakłócającego, przy którym następuje trwałe uszkodzenie podzespołów urządzenia lub systemu, jest zmierzonym poziomem wytrzymałości na dane umowne zakłócenie.

5. Minimalizacja rozpraszania elektromagnetycznego informacji użytecznej i ochrona przed narażeniami elektromagnetycznymi w sieciach teleinformatycznych

Chcąc minimalizować rozproszenie elektromagnetyczne informacji użytecznej z punktu widzenia ochrony przed niepożądaną detekcja należy:

- szyfrować przesyłane i przetwarzane informacje,

stosowane obudowy plastykowe. Do tych konstrukcji opracowano liczne technologie zapewniające ekranujące właściwości takich obudów. Między innymi:

- metalizowanie,
- natryskiwanie i malowanie obudów pokryciami przewodzącymi,
- stosowanie przewodzących mas plastycznych do tłoczenia obudów,
- stosowanie elastycznych tkanin przewodzących wykonanych z metalizowanych włókien, połączonych z masą plastyczną w procesie tłoczenia obudowy,
- wykorzystanie samoprzylepnych przewodzących folii nakładanych na obudowę.

5.1.2. Ekranowanie kabli

Stosuje się dwie metody minimalizacji rozpraszania elektromagnetycznego sieciowych instalacji kablowych. Pierwsza z nich polega na ekranowaniu torów kablowych. Druga wykorzystuje zjawisko kompensacji zakłóceń w torach symetrycznych. Stosowanie ekranowania kabli wymaga spełnienia wielu warunków (dobre uziemienie, brak „pętli prądowych", mała impedancja połączeń ekranów) a w praktyce jest trudne do wykonania. Odporność torów symetrycznych na zakłócenia impulsowe jest szczególnie istotna w przypadku braku dobrze zdefiniowanego uziemienia. Ekranowanie torów symetrycznych może zmniejszyć rozpraszanie elektromagnetyczne informacji użytecznej lecz źle wykonane może je zwiększyć.

W sieciach komputerowych stosuje się dwa podstawowe typy kabli miedzianych:

- kabel symetryczny typu „skrętka",
- kabel współosiowy.

Dla zapewnienia dobrego ekranowania przewodów należy:

- minimalizować długości nieekranowanych części przewodu,
- zapewnić dobre uziemienie ekranu.

Przewód ekranujący (ekran) powinien być dołączony do masy tylko z jednej strony, w przeciwnym bowiem razie z połączenia mas powstać może pętla prądowa. Przy większej liczbie źródeł rozproszenia należy każde połączenie oddzielnie ekranować.

W przypadku kabli symetrycznych (skręconej pary przewodów) jeżeli prądy w obu przewodach są równe to linie pola od jednej pary znoszą się nawzajem. Większe tłumienie rozproszenia w tym przypadku można uzyskać przez dodatkowe ekranowanie skręconych przewodów.

W przypadku kabli koncentrycznych przewód zewnętrzny stanowi przewodzącą powierzchnie, na której kończą się linie sił pola elektrycznego pochodzące od przewodu wewnętrznego. Jeżeli w ekranie spowoduje się przepływ prądu równego i przeciwnie skierowanego niż w przewodzie wewnętrznym, to wytworzy on równe, lecz przeciwnie skierowane pole magnetyczne. Pole to znosi się z polem magnetycznym wytwarzanym przez przewód wewnętrzny na zewnątrz ekranu.

6. Wnioski

Ważnym elementem budowy systemu bezpieczeństwa sieci teleinformatycznej z punktu widzenia kompatybilności elektromagnetycznej jest zrównoważenie kosztów ochrony informacji z możliwościami jej potencjalnej detekcji, zakłócenia lub zniszczenia. Zazwyczaj koszty związane z ochroną sieci teleinformatycznych znacznie przewyższają koszty potencjalnej detekcji informacji przesyłanych w tych sieciach.

Należy również pamiętać, że sieci teleinformatyczne budowane z urządzeń odpowiadających wymaganiom kompatybilnościowym z chwilą ich połączenia mogą generować duże zakłócenia elektromagnetyczne będące wynikiem źle wykonanej instalacji a nie materiałów i urządzeń.

BEZPIECZNY DOSTĘP DO SIECI INTERNET DLA URZĘDÓW ADMINISTRACJI I INSTYTUCJI PUBLICZNYCH

Krzysztof Silicki

Naukowa Akademicka Sieć Komputerowa NASK, ul. Bartycka 18, 00-716 Warszawa
e-mail: krzysiek@nask.pl

Charakter zagrożeń związanych z dołączeniem do Internetu implikuje środki organizacyjno-techniczne jakie muszą być podjęte w celu zapewnienia właściwego stopnia bezpieczeństwa dołączanych sieci i ich użytkowników odpowiadającego charakterowi dołączających się instytucji.

Zagrożenia sieci, które są dołączane do sieci Internet wynikają z szeregu czynników, wśród ktorych najistotnjiejsze to:

- sama istota Internetu jako konglomeratu sieci gdzie :
  - nie ma centralnej kontroli
  - nie ma centralnego autorytetu
  - brak standardowej, zaakceptowanej przez wszystkich polityki (np. bezpieczeństwa)
  - brak międzynarodowego prawodawstwa w dziedzinie przestępstw komputerowych
- słabości protokołu TCP/IP
- słabe punkty systemów operacyjnych komputerów dołączanych do Internetu (Unix, NT,...)
- ogromna dynamika rozwoju, która z jednej strony stanowi o sile Internetu - lecz z drugiej strony stanowi wyzwanie w dziedzinie zapewnienia bezpieczeństwa w szybko ewoluującym środowisku

Każda organizacja, firma , placówka musi wypracować skuteczną politykę ochrony zasobów w sieci w związku z planami dołączenie do sieci publicznej o globalnym charakterze jaką jest Internet. Istnieje w tym zakresie wiele wzorców jednak każdy abonent sieci ma własną specyfikę, ktorą należy uwzględnić. Prowadzi to do konieczności opracowania. wdrożenia i działania zgodnego z przyjętym programem bezpieczeństwa.

Istota i waga programu bezpieczeństwa (security policy)

Program bezpieczeństwa (security policy) jest to zbiór przyjętych zasad określających stanowisko firmy wobec problemu bezpieczeństwa. Program taki określa zakres akceptowanych zachowań, oraz konsekwencji w przypadku ich naruszenia. Wszystkie decyzje w zakresie bezpieczeństwa powinny wynikać z przyjętych wcześniej założeń a także wprowadzane w życie zasady w zakresie bezpieczeństwa muszą mieścić się w określonych przez program granicach. Program bezpieczeństwa wymaga także wykonania analizy poziomu ryzyka i określenia jego akceptowalnego progu. Musi też nastąpić dokładna klasyfikacja danych i dobranie odpowiednich środków ochrony -proporcjonalnych do wartości danych (tzw. próg opłacalności ochrony). Koszty rozwiązań, a ich efektywność to problem, który decyduje o powodzeniu (lub klęsce) przyjętych mechanizmów ochrony

Bezpieczny system rządzi się kilkoma zasadami:

- Ścisłym zdefiniowaniem uprawnień użytkowników do zasobów w sieci
- Związaną z powyższym zasadą niedostępności danych określonych kategorii dla nieuprawnionych użytkowników.

- kto ma dostęp do serwisu ?
- gdzie może się połączyć ?
- co i w jaki sposób może dostać się do naszej sieci ?
- a nawet: jaki rodzaj przeglądarki będzie stosowany ?

HTTPD reprezentuje z kolei protokół związany z serwerem WWW. W przypadku serwera informacyjnego, którego przykładem jest WWW pytania są jeszcze poważniejsze:

- kto ma prawo do udostępniania, jakich treści ?
- używanie mechanizmów podwyższających atrakcyjność serwisu lecz obbniżajacych bezpieczeństwo (aplety Java, skrypty CGI)
- gdzie powinien stać serwer ?
- czy da się go skutecznie ochronić ?

Styk miedzy sieciami - przegrody typu firewall

Czym jest firewall ? Jest to:
- system lub grupa systemów stanowiących fizyczną implementacje styku pomiędzy co najmniej dwoma sieciami
- mechanizm użyty dla ochrony styku pomiędzy siecią własną a siecią zewnętrzną oparty o założenia programu bezpieczeństwa

Wbrew pozorom z używaniem firewalla także wiążą się zagrożenia. Częstokroć sam fakt posiadania przegrody typu firewall „usypia czujność" administratorów. Jest kilka czynników , które decydują o skuteczności przegrody typu firewall:

- cały ruch z zewnątrz do sieci wenętrznej musi przechodzić przez firewall
- zasady filtrowania ruchu muszą być zgodne z założeniami przyjętej polityki
- sam firewall musi być odporny na ataki
  - pamiętajmy, że metody ataków ulegają ciągłej ewolucji
- firewall jest tak dobry jak:
  - polityka którą implementuje
  - jakość tej implementacji
  - poziom obsługi i zarządzania

Problemy organizacyjne

Warte wielokrotnego podkreślenia jest konieczność położenie właściwego nacisku na kwestie organizacyjne. Tu również wyłania się szereg pytań i problemów, które muszą znaleść rozwiązanie:

- Kto jest odpowiedzialny za wprowadzenie i przestrzeganie programu bezpieczeństwa ?
- Jaki jest zakres akceptowalnych zachowań ?
- Jakie są konsekwencje naruszania zasad polityki ?
- Czy wprowadzona polityka jest akceptowana (przez kierownictwo i samych użytkowników)?

Praktyczne wskazówki wynikające z obserwacji NASK są następujące:

Specyfika i wymagania sieci teleinformatycznych urzędów administracji i instytucji publicznych pod względem bezpieczeństwa

Należy założyć, iż użytkownicy sieci administracji publicznej powinni mieć możliwość wymiany danych w trzech kategoriach ochrony:

1. dane poufne, tajne w sieci chronionej urzędów administracji
2. ruch w sieci „korporacyjnej'' urzędów
3. dostęp do Internetu

Transmisja danych z kategorii 1 wymaga oczywiście całkowitego odseparowania od danych z pozostałych kategorii. Separacja ruchu kategorii 2 i 3 w możliwej do wyobrazenia i najczęściej wystepujacej sytuacji kiedy te same stacje robocze (te same sieci lokalne) w urzędach służą do przesyłania danych conajmniej zastrzeżonych i dostępu do Internetu wymaga zastosowania nowoczesnych metod transmisji i silnego uwierzytelnienia z zastosowaniem elementów kryptografii. Oczywiście w sytuacji braku barier ekonomicznych można by sobie było wyobrazić całkowity rozdział ruchu na poziomie sieci lokalnych urzędów w oparciu o dedykowane LANy dla kategorii „2" i „3". W realnym świecie sytuacja taka jest jednak trudna do zaakceptowania. Na tym przykładzie widać jasno zależność pomiędzy efektywnością rozwiązania w stosunku do kosztów, które można (i należy) ponieść.

Separacja sieci

Sieć administracji państwowej powinna być właściwie odseparowana od sieci o charakterze publicznym lub sieci mających połączenie z sieciami publicznymi.

Styk z Internetem

Sieci lokalne (lub ich fragmenty) , które mają mieć połączenie z Internetem powinny mieć owo połączenie zrealizowane tak, aby zapewniało odpowiedni poziom bezpieczeństwa i kontroli w ramach założonego programu (security policy).

W tym celu należy opracować specjalizowany program bezpieczeństwa dla sieci administracji, które przeznaczone są do łączności z sieciami publicznymi (w szczególności Internetem)

Program musi opisywać rodzaje usług jakie będą dostępne dla użytkowników wewnętrznych w sieci zewnętrznej (Internet) jak również usługi (zasoby) udostępniane dla użytkowników z zewnątrz.
Należy także określić tryby korzystania z wyżej wspomnianych usług tzn. np. listę (grupy) użytkowników i ich uprawnienia.

Użytkownikom , o których mowa wyżej należy stworzyć odpowiednie warunki i wymogi do bezpiecznego i wiarygodnego uwierzytelniania przy korzystaniu z założonych (zdefiniowanych dla nich) uprawnień (rekomendowane jest uwierzytelnienie za pomocą systemu haseł jednokrotnego użycia).

Styk z Internetem powinien być zaprojektowany tak aby realizował założoną w projekcie technicznym i w programie bezpieczeństwa funkcjonalność i bezpieczeństwo.

W ten sposób hasło użytkownika staje się bezpieczne niezależnie od tego czy jest użyte w sieci wewnętrznej czy „na terenie" przegrody (firewall). Bezpieczne uwierzytelnienie w obrębie przegrody jest newralgicznym punktem ochrony.

Zarządzanie

System przegrody musi być sprawnie zarządzany i musi dawać możliwość zapamiętywania zdarzeń (tzw. audit log)

Wszelkie serwery publicznie dostępne powinny być zlokalizowane na oddzielnym segmencie sieci. Powinny być także wyposażone w aktywne mechanizmy wykrywania niebezpiecznych sytuacji (spowodowanych udostępnieniem serwisów takich jak WWW dla rzeszy uzytkowników pozostajacych poza kontrolą bezpośrednią). Serwery publiczne powinny być też wyposażone w możliwości szybkiej rekonstrukcji w razie zaistnienia nieprzewidzianych sytuacji zagrażających lub naruszajacych bezpieczeństwo.

Należy podkreślić, że istnienie „centralnej" przegrody typu firewall nie wyklucza istnienia lokalnych firewalli sieci poszczególnych jednostek administracji i instytucji publicznych.

Jak wspomniano wcześniej separacja ruchu „Internetowego" i komunikacji pomiędzy poszczególnymi jednostkami administracji (nazwana siecią „korporacyjną'' dla podkreślenia jej niepublicznego charakteru) może być z powodzeniem zrealizowana przy wykorzystaniu rozwiązań szyfracji połączeń IP (tych połączeń, które tego wymagają). Przykładami technologii i rozwiązań realizujących selektywną szyfrację połączeń - gdzie urządzenia decydują (na podstawie zadanej konfiguracji), pakiety jakich relacji mają być szyfrowane a w jakich relacjach ruch może się odbywać w sposób jawny - są rozwiązania opisane w referatach *„Wprowadzenie do technologii podwyższających bezpieczeństwo korzystania z sieci teleinformatycznych"* oraz: *„Doświadczenia we wdrażaniu technologii podwyższających bezpieczeństwo"*

i utrzymanie odpowiedniej polityki bezpieczeństwa, jasno precyzującej zagrożenia, stosowane zabezpieczenia, szczegółowe kompetencje i odpowiedzialność pracowników.

Informacje winny być dostępne jedynie upoważnionym osobom i to wyłącznie w zakresie niezbędnym. Informacja powinna być zabezpieczona przed nieuprawnioną modyfikacją, utratą lub zniszczeniem i dostępna bez przerw dla tych, którzy mają prawo jej wymagać. Powinny bezwzględnie istnieć mechanizmy ewaluacji poprawności i efektywności zastosowanych mechanizmów bezpieczeństwa.

Istotny jest również rodzaj wykorzystywanego systemu informatycznego. Opracowano i standaryzowano następujące klasy bezpieczeństwa systemów:

D - ochrona minimalna (praktyczny jej brak);
C1- identyfikacja użytkowników i ich upoważnień;
C2- kontrola dostępu do wyróżnionych danych;
B1- etykietowanie ochronne zasobów (np. klauzule tajności);
B2- zaawansowany mechanizm jądra ochrony, stałe monitorowanie i dokumentowanie prac;
B3- szczegółowe domeny ochronne;
A1- najwyższa klasa - system zawiera wszystkie mechanizmy klas niższych i jest rygorystycznie weryfikowany już od fazy projektowej.

Niestety, większość dostępnych produktów informatycznych oferuje poziom nie wyższy niż C1. Niektóre systemy operacyjne posiadają cechy klasy C2 (np. Solaris, AIX, NetWare 4), a niekiedy nawet bywają rozszerzone do klasy B1. Są też systemy aplikacji umożliwiające wykorzystanie środowisk klasy B1 (np. system zarządzania relacyjną bazą danych Trusted Oracle7). Komercyjne systemy klasy B2 spotyka się rzadko, a klasy B3 i A1 nie spotyka się praktycznie w ogóle.

1.2 Bezpieczeństwo komunikacji

Komunikacja w sieci lokalnej na ogół wiąże się ze nieco innymi zagrożeniami dla jej bezpieczeństwa. Głównymi problemami są tu komunikaty rozgłoszeniowe i ewentualność podsłuchania ruchu. Najczęściej istnieją możliwości odseparowania ruchu poszczególnych podsieci (tzw. *zamknięte grupy użytkowników*), a nawet fizycznej ochrony dostępu do sieci. Szczególną rolę odgrywa tu dobrze zaprojektowana i bezwzględnie przestrzegana polityka bezpieczeństwa poszczególnych sieci. Jednak w przypadku połączenia sieci lokalnych siecią rozległą, wewnętrzna polityka sieci lokalnych najczęściej jest niewystarczająca. Sieci rozległe cechują się bowiem zupełnie inną klasą zagrożeń. Często nie posiadają żadnych wbudowanych mechanizmów ochrony przesyłanych danych, odpowiedzialność za bezpieczeństwo spada zatem na użytkowników. W ogólności więc, to same sieci lokalne muszą zabezpieczać wzajemną komunikację poprzez sieć rozległą. Wymaga to od wszystkich potencjalnie komunikujących się sieci lokalnych spójnej polityki bezpieczeństwa globalnego.

2. Problemy i mechanizmy bezpieczeństwa

2.1 Podstawowe problemy bezpieczeństwa

Do podstawowych problemów ochrony informacji należą następujące zagadnienia: poufność informacji (*confidentiality*), nienaruszalność danych (*integrity*) oraz uwierzytelnianie użytkowników danych (*authentication*).

2.3 Mechanizmy bezpieczeństwa

Poufność informacji

Podstawą ochrony poufności informacji jest uniemożliwienie dostępu do zasobów osobom nieuprawnionym oraz ograniczenie możliwości podsłuchu komunikacji. Osiąga się to stosując w odpowiednim stopniu mechanizmy kryptograficzne (szyfrowanie symetryczne - metodą klucza prywatnego, np. DES, 3DES, lub niesymetryczne - metodą klucza publicznego, np. RSA). W sieciach lokalnych można podsłuch utrudnić poprzez zastosowanie medium światłowodowego oraz mechanizmów sztucznego wypełniania ruchu w sieci (*traffic padding*), w celu utrudnienia intruzowi orientacji i zdobycia pożytecznych informacji. W przypadku wykorzystania publicznych łączy komunikacyjnych, realizuje się często koncepcję zamkniętych grup użytkowników. Ich wzajemna komunikacja podlegać może szyfrowaniu, a nad bezpieczeństwem i kontrolą dostępu do sieci lokalnych (serwerów) czuwać mogą mechanizmy filtracji ruchu sieciowego (np. tzw. ściany ogniowe, ang. *firewall*).

Nienaruszalność informacji

Nienaruszalność informacji osiągana jest w ogólności poprzez obowiązkową kontrolę dostępu do danych (*access control*) i rejestrację operacji na danych (*auditing*). Integralność komunikacji jest osiągana najczęściej za pomocą mechanizmu podpisu elektronicznego, np. MD5, DSS.

Uwierzytelnianie użytkowników

W celu dokonania bezpiecznego uwierzytelniania można stosować metody odporne na próby podszycia się pod użytkowników uprawnionych (np. przechwycenie haseł), takie jak szyfrowanie procesu rejestracji nowej sesji użytkownika połączone z podpisem elektronicznym lub wykorzystanie haseł jednokrotnych.

3. Bezpieczeństwo w systemach baz danych

Obecnie dostępne na rynku komercyjne systemy baz danych dostarczają wielu środków technicznych wspierających realizację polityki bezpieczeństwa dla systemów informatycznych. Wsparcie to obejmuje:

- identyfikację użytkowników,
- kontrolę dostępu,
- szyfrowanie informacji przesyłanej w sieci komputerowej,
- obserwowanie działań użytkowników (*auditing*).

3.1 Identyfikacja użytkowników

Najpopularniejszym sposobem weryfikacji tożsamości użytkowników jest identyfikacja przez hasło. Identyfikacja ta może być przeprowadzona przez system operacyjny lub przez system bazy danych. Weryfikacja tożsamości przez system operacyjny jest skuteczna jedynie w przypadku systemu zcentralizowanego lub systemu rozproszonego z homogenicznym systemem identyfikacji np. NIS. Rozproszone, heterogeniczne systemy informatyczne wymagają identyfikacji przez system bazy danych.

Hasła użytkowników są przechowywane w postaci zaszyfrowanej najczęściej za pomocą algorytmu DES i dostępne jedynie administratorowi bazy danych (*Database Administrator* - DBA). Odrębnym zagadnieniem jest weryfikacja tożsamości użytkownika i uprawnień użytkownika, który uruchamia system bazy danych. Jego identyfikacja musi być przeprowadzona przez system operacyjny, gdyż usługi systemu bazy danych w tym momencie nie są jeszcze dostępne.

Na potrzeby systemów przetwarzania informacji o zróżnicowanych wymaganiach bezpieczeństwa i kontroli dostępu został opracowany obowiązkowy model kontroli dostępu (*Mandatory Access Control*). Model MAC posiada wszystkie mechanizmy modelu DAC oraz dodatkowo wprowadza ochronę wielopoziomową (*Multilevel Secure* - MLS). Mechanizm MLS wymusza obowiązkową ochronę danych z ziarnistością pojedynczych rekordów. W modelu DAC taka ochrona nie jest obowiązkowa i wymaga implementacji za pomocą perspektyw. Mechanizm MLS opiera się na hierarchicznie powiązanymi etykietami trwale złączonymi z informacją. Autoryzacja dostępu następuje przez porównanie etykiety danych z etykietą użytkownika ustaloną przez system operacyjny lub przez system bazy danych. Operacja modyfikacji jest dozwolona jedynie jeżeli etykieta użytkownika jest identyczna etykietą danych. Operacja odczytu jest możliwa jeżeli etykieta użytkownika jest identyczna lub dominuje nad etykietą danych.

Mechanizmy modelu MAC wchodzą w skład poziomu ochrony danych B1. Aby cały system informatyczny spełniał wymagania poziomu B1 to zarówno system operacyjny jak i system bazy danych musi je spełniać. Na rynku znajduje się szereg systemów operacyjnym posiadających certyfikat dla poziomu ochrony B1, przykładowo: DEC SEVMS VAX, DEC MLS+, Sun Trusted Solaris, HP-UX BLS, Sequent Trusted/PTX, itp. Reprezentantem systemów baz danych spełniających wymagania poziomu B1 jest Trusted Oracle7.

3.3 Szyfrowanie informacji

Bardzo ważnym zagadnieniem jest ochrona danych przesyłanych w sieci publicznej. Jedynym skutecznym rozwiązaniem jest ich szyfrowanie. Procesem szyfrowania i deszyfrowania informacji mogą się zajmować dedykowane urządzenia sieciowe. Rozwiązanie to jest jednak bardzo kosztowne. Bardziej ekonomicznym rozwiązaniem jest szyfrowanie programowe. Wiele systemów baz danych wspiera technikę szyfrowania przesyłanych danych przez sieć publiczną. Szyfrowaniu podlegają: dane, zlecenia SQL, zdalne wywołania funkcji i ich wyniki zwrotne, identyfikatory użytkowników i ich hasła. Najczęściej wykorzystywane są algorytmy RSA oraz DES. W celu zabezpieczenia się przed złamaniem klucza, dla każdej sesji połączeniowej jest generowany nowy klucz wg algorytmu Diffie-Hellmana.

Równie istotnym zagadnieniem jest zagwarantowanie nienaruszalności danych. Integralność danych mogłaby być naruszona przez podmianę pakietów i ich zawartości. Najprostszym sposobem ochrony integralności jest przesyłanie podpisów elektronicznych w postaci szyfrowanych sum kontrolnych. Mechanizm ten umożliwia wykrycie modyfikacji, zamiany lub utraty pakietu. Wykrycie niespójności transmitowanych danych natychmiast przerywa sesje. Najczęściej wykorzystywanym algorytmem jest MD5.

Istotnym zagadnieniem jest ochrona danych bazy danych na skradzionym nośniku. Odczytanie danych prosto z nośnika nie jest trywialne ponieważ organizacja danych w komercyjnych bazach danych nie jest w pełni publikowana, ponadto po dłuższej eksploatacji w wyniku zjawiska łańcuchowania i migracji rekordów powiązania między danymi są bardzo skomplikowane. W celu utrudnienia odczytania informacji można je rozproszyć na różne nośniki. Innym sposobem jest zapis informacji w niestandardowym formacie, np. na urządzeniu surowym (*raw device*). Najlepszym sposobem zabezpieczenia jest szyfrowanie. To rozwiązanie spotyka się jednak z szeregiem ograniczeń. Nie wygodnym jest szyfrowanie danych na poziomie aplikacji, gdyż algorytmy szyfrujące nie zachowują porządku wartości i z tego powodu w pewnych przypadkach niepoprawnie będą działać struktury przyśpieszające dostęp do danych np. indeksy. Przykładowo: przed zaszyfrowaniem wartość 4 jest mniejsza od 5, a po zaszyfrowaniu trudno powiedzieć, w każdym razie im lepszy algorytm szyfrujący (tak samo jak funkcja hashowa) tym bardziej rozproszy

[Davis92] D. Davis, "Network Security Via Private-Key Certificates", USENIX Proceedings, UNIX Security Symposium III; September 1992.

[Galvin92] J.M. Galvin, D.M. Balenson, "Security Aspects of a UNIX PEM Implementation", USENIX Proceedings, UNIX Security Symposium III; September 1992.

[Garfinkel91] S. Garfinkel, G. Spafford, *Practical Unix Security*, O'Reilly and Associates, 1991.

[Pelc95] Z. Pelc, "Ochrona w statystycznych bazach danych", *Unix Forum*, nr 6(14) 1994, s.43-46 i nr 1(15) 1995, s.31-37.

[Silicki93] K. Silicki, "Bezpieczeństwo w systemach otwartych", *Net forum*, nr 2 1993, s.30-31, nr 3 1993, s.20-22., nr 5 1993, s.4-10.

[Szafrański94] B. Szafrański, "Ochrona danych", *Unix Forum*, nr 3(11) 1994, s.4548 i nr.4(12) 1994, s.46-50.

[Wiseth96] K. Wiseth, "Safety Net", Oracle Magazine, July/August 1996, str.43-58.

Uzasadnieniem wysiłku włożonego w badania i konstrukcję systemów tolerujących uszkodzenia jest szeroki zakres ich zastosowań, obejmujący aplikacje bankowe i giełdowe, systemy kontroli lotów, medyczne systemy monitorujące, automatykę przemysłową oraz wiele innych.

2. Tolerancja uszkodzeń

2.1 Klasyfikacja uszkodzeń

Klasyfikacja uszkodzeń (awarii) systemów informatycznych dokonywana jest na ogół według: składników systemu, czasu trwania awarii i ich skutków, zachowania się systemu po awarii. Wyróżnia się zatem uszkodzenia pamięci masowej, pamięci operacyjnej, procesora, medium komunikacyjnego, procesu systemowego, procesu aplikacyjnego.

Ze względu na czas trwania wyróżnia się: **przejściowe** (zanikające po pewnym nieznanym z góry czasie, np. losowe zakłócenie transmisji), **okresowe** (powtarzające się co pewien czas lub przy dojściu systemu do pewnego stanu, np. luźne przyłącze), **permanentne** (raz zaistniałe powodują zablokowanie pracy systemu, aż do czasu jawnego usunięcia przyczyny i naprawy systemu, np. uszkodzenie procesora lub dysku, czy awaria oprogramowania).

W wyniku wystąpienia uszkodzenia system znajduje się w niepoprawnym (z punktu widzenia przetwarzania) stanie. Restart systemu polega na przywróceniu pewnego stanu poprawnego. W zależności od tego jak ów powrót przebiega, mamy do czynienia z: **amnezją** (gdy system znajdzie się po restarcie w predefiniowanym stanie niezależnym od stanu, w którym nastąpiło uszkodzenie), **częściową amnezją** (gdy część nowego stanu jest uzależniona od stanu, w którym nastąpiło uszkodzenie (tak się dzieje w przypadku zastosowania punktów kontrolnych), **pauzą** (gdy system restartuje w stanie identycznym ze stanem, w którym nastąpiło uszkodzenie), **zatrzymaniem** (gdy system nie jest restartowany).

Jeśli uszkodzony proces przestaje uczestniczyć w przetwarzaniu aż do restartu, mamy do czynienia z modelem *fail-stop* lub *fail-silent*. Często jednak w praktyce uszkodzony proces kontynuuje przetwarzanie lecz w niewłaściwy sposób, potencjalnie zakłócający pracę pozostałych, poprawnych procesów. Taki model nazywa się Bizantyjskim (*Byzantine faults*). Jest on dość trudny z punktu widzenia konstrukcji systemu tolerującego uszkodzenia, gdyż komplikuje (a nawet uniemożliwia) jednoznaczną detekcję uszkodzenia procesu.

2.2 Odtwarzanie danych

Możliwość wystąpienia awarii jest związana z koniecznością zapewnienia mechanizmu odtworzenia danych po uszkodzeniu procesu. Możliwe są dwa podstawowe podejścia: odtwarzanie postępowe (*forward recovery*) i wsteczne (*backward recovery*). Odtwarzanie postępowe stosuje się jeśli natura uszkodzeń i ich skutków jest taka, iż mogą one zostać kompletnie i dokładnie skompensowane, na przykład w wyniku zastosowaniu kodów korekcyjnych. Jeśli jednakże kompensacja szkód w bieżącym stanie systemu nie jest możliwa, wówczas należy zastosować odtwarzanie wsteczne, polegające na zapisywaniu co pewien czas w pamięci nieulotnej tzw. punktów kontrolnych (*checkpoints*) reprezentujących pewien spójny stan przetwarzania i w przypadku wystąpienia awarii, wznowieniu przetwarzania od ostatniego pamiętanego stanu.

Warto zauważyć, że odtwarzanie wsteczne jest niezależne od rodzaju uszkodzenia i zakresu szkód. Dlatego jest ono częściej stosowane niż odtwarzanie postępowe, mimo że problem wyznaczania globalnego stanu spójnego (punktu kontrolnego), jest bardzo złożony a jego rozwiązanie kosztowne, ze względu na narzut czasowy wprowadzany przez zapis punktów kontrolnych oraz konieczność powtarzania części obliczeń.

backup wymaga detektora błędów i uwzględnienia dynamiki grup, lecz powoduje mniejsze obciążenie systemu.

2.5 Systemy niezawodnej komunikacji grupowej

Zadaniem tych systemów jest realizacja niezawodnej komunikacji grupowej z uporządkowaniem wiadomości (*reliable ordered multicast*). Najprostszym rodzajem uporządkowania jest uporządkowanie przyczynowe (*causal order*) [Lamport78]. Komunikaty grupowe są adresowane do grupy procesów, której skład może się dynamicznie zmieniać wskutek uszkodzeń lub reaktywacji poszczególnych procesów. Bieżący skład grupy nazywa się **konfiguracją** lub **obrazem** grupy.

Awaria jednego z procesów konfiguracji wprowadza niebezpieczeństwo utraty spójności uporządkowania komunikatów. Powstaje tym samym problem zachowania **wirtualnego synchronizmu** pracy procesów (*virtual synchrony*), który gwarantuje, iż każdy ze sprawnych procesów danej konfiguracji odbiera tę samą sekwencję komunikatów. Najwyższa spójność osiągana jest przy pełnym uporządkowaniu komunikacji (*total order*).

Systemy niezawodnej komunikacji grupowej wykorzystują infrastrukturę sieciową, na ogół do warstwy sieciowej lub transportowej modelu odniesienia OSI włącznie. Niekiedy infrastruktura ta udostępnia sprzętowe adresowanie rozgłoszeniowe (*broadcast*) lub grupowe (*multicast*). System może, jeśli potrafi, wykorzystać takie udogodnienie.

Najpopularniejsze aktualnie systemy rozproszone tolerujące uszkodzenia, wykorzystujące niezawodną komunikację grupową to: Psync [Peterson89], Isis [Birman90], Amoeba [Tanenbaum91], Delta-4 [Verissimo91] Totem [Agarval92], Transis [Amir92], Horus [vanRenesse93], RMP [Whetten94], Trans/Total [Moser94], Relacs [Babaoglu95], Phoenix [Malloth96]. Przegląd części z tych systemów można znaleźć w [Brzeziński97].

3. Tolerancja uszkodzeń w systemach baz danych

Elementem wyróżniającym system bazy danych od innych rodzajów systemów informatycznych jest transakcyjny charakter przetwarzania. Transakcja jest zbiorem sekwencji operacji charakteryzującym się określonymi własnościami w skrócie nazywanymi ACID. Do tych własności zalicza się:

- atomowość (*Atomicity*) - transakcja jest wykonywana w całości lub wcale;
- spójność (*Consistency*) - transakcja przeprowadza bazę danych z jednego stanu spójnego w drugi (przez stan spójny rozumie się taki stan bazy danych, który poprawnie reprezentuje modelowane obiekty rzeczywiste);
- izolacja (*Isolation*) - transakcja jest izolowana od zmian wprowadzonych w czasie jej trwania przez inne transakcje, zmiany wprowadzone przez transakcje są dostępne dopiero po ich zatwierdzeniu,
- trwałość (*Durability*) - zmiany wprowadzone przez zatwierdzone transakcje są permanentne.

W klasycznym modelu transakcyjnym, własność izolacji oznacza, że współbieżnie wykonywane transakcje nie mogą ze sobą kooperować. Powoduje to, że awaria jednej z transakcji nie ma żadnych konsekwencji dla pozostałych, współbieżnie wykonywanych transakcji. Ograniczenia narzucone przez model transakcyjny upraszczają problem odtwarzania stanu spójnego w porównaniu z ogólnym przetwarzaniem rozproszonym.

Podstawą dla budowy systemów tolerujących błędy jest redundancja. Komponenty systemu informatycznego podlegające redundancji to: dane, procesy i łącza komunikacyjne. Najbardziej newralgicznym elementem systemów baz danych są dane, aby zagwarantować ich trwałość należy

bezpieczeństwa i zabezpieczonego dziennika bazy danych można całkowicie odtworzyć dane bazy danych z czasu tuż przed awarią.

Odzyskiwanie danych na podstawie zabezpieczonego dziennika jest długotrwałe, ponieważ wymaga powtórzenia wszystkich operacji wykonanych na bazie danych od wykonania ostatniej kopii bezpieczeństwa. Dla systemów wymagających dostępności danych 24 godziny na dobę rozwiązanie to może nie być satysfakcjonujące. W tym przypadku systemy baz danych wymagają zastosowania technologii macierzy dyskowych, serwerów zapasowych lub gron serwerów.

Macierz dyskowa jest to urządzenie składające się ze zbioru współpracujących dysków i sprzętowego sterownika. Urządzenie to dostarcza interfejs dostępu do tych dysków i gwarantuje różny zakres redundancji danych wg specyfikacji RAID (*Redundant Arrays of Inexpensive Disks*) opracowanej na Uniwersytecie w Berkeley i następnie rozszerzanej przez przemysł. Ponadto, macierze dyskowe charakteryzują się zwielokrotnioną wielkością transferu danych zbioru kooperujących dysków w porównaniu z pojedynczym dyskiem. Zakres i implementacja redundancji została określona przez poszczególne poziomy RAID. Poziom 0 RAID nie dostarcza żadnej redundancji danych. Poziom pierwszy implementuje mechanizm sprzętowo utrzymywanych kopii lustrzanych. Poziom ten wymaga podwojenia liczby dysków w stosunku do wykorzystywanej przestrzeni dyskowej. Poziomy 2, 3 i 4 RAID wykorzystują kody korekcyjne przechowywane na dedykowanym dysku. Dodatkowo dane są rozpraszane na różne dyski (*striping*). Poziomy te różnią się ziarnem rozpraszanej informacji, poziom 2 i 3 rozprasza dane z ziarnistością bitu, poziom 4 z ziarnem bloku lub sektora. Poziomy te wymagają jedynie jednego dodatkowego dysku. Poziom 5 RAID dodatkowo wprowadza rozproszenie kodów korekcyjnych. Macierze dyskowe pracujące na poziomach 1-5 tolerują awarie jednego z dysków, awaria drugiego dysku doprowadza do utraty danych. Poziom 6 RAID wprowadza wyliczanie kodów korekcyjne dla wierszy i kolumn macierzy dyskowej i rozprasza je na różnych dyskach. W ten sposób macierz dyskowa toleruje awarie dwóch dysków, dopiero awaria trzeciego nośnika powoduje utratę danych. Poziom 7 umożliwia elastyczną definicję skali generowania i pielęgnacji redundantnych kodów korekcyjnych zwiększając tolerancję na awarię aż do czterech równoczesnych awarii dysków.

Dla zapewnienia ciągłości pracy 24 godziny dobę systemy baz danych wykorzystują również technologię serwerów zapasowych i gron serwerów. Technologie te umożliwiają, oprócz redundancji danych, również redundancję przetwarzania.

W technologii serwerów zapasowych wyróżnia się jeden serwer, który jest wyłączony z bieżącego przetwarzania, i którego zadaniem jest podjęcie pracy w przypadku upadku systemu podstawowego. Zaopatrzenie w dane, niezbędne do podjęcia przetwarzania przez serwer zapasowy, realizowane jest na dwa sposoby. Pierwszym sposobem jest wyodrębnienie, współdzielonych przez system podstawowy i zapasowy nośników danych (najczęściej macierzy dyskowych). Rozwiązanie to jest zbliżone do technologii gron serwerów. Drugim sposobem jest pielęgnacja kopii danych przez serwer zapasowy, rozwiązanie to wymaga bardzo szybkiego łącza komunikacyjnego. Powielaniu może podlegać cała baza danych, jednakże zastosowanie tego rozwiązania dla bardzo aktywnych systemów może spowodować znaczne obniżenie efektywności działania systemu, gdyż byłyby przesyłane bardzo często bardzo duże wolumeny danych. Innym rozwiązaniem problemu utrzymywania kopii bazy danych może być powielanie jedynie dziennika bazy danych, który zawiera dane przyrostowe. W tym przypadku system zapasowy w trybie ciągłym odczytuje zmiany w oryginalnej bazie danych zapisane w dzienniku bazy danych i aplikuje je do własnej kopii bazy danych.

Technologia gron serwerów umożliwia zbiorowi systemów baz danych równoczesne operowanie na tej samej bazie danych, która jest umieszczona na współdzielonym nośniku danych wysoce tolerującym awarie. W przypadku awarii jednej maszyny przetwarzanie może być

zwiększenia ryzyka zablokowania. Niekorzystne zjawisko zablokowania może zostać spowodowane awarią dowolnego koordynatora.

Niezależnie od sposobu sterowania protokół 2PC jest stosunkowo wrażliwy na awarię węzłów koordynujących. Problem ten został wyeliminowany w trójfazowym protokole zatwierdzania [Skeen81]. W protokole tym wprowadzono dodatkową fazę, dzięki której w przypadku awarii koordynatora pozostałe węzły mogą wybrać nowego koordynatora.

Ze względu na mniejszą złożoność, w komercyjnych systemach baz danych zazwyczaj stosuje się dwufazowy protokół zatwierdzania transakcji.

3.3 Synchroniczna replikacja danych

Ze względu na specyfikę przetwarzania danych w systemach baz danych wyróżniamy dwa rodzaje replikacji: synchroniczną i asynchroniczną.

W replikacji synchronicznej, modyfikacja danych źródłowych oraz wszystkich kopii odbywa się w ramach tej samej transakcji. Replikacja synchroniczna gwarantuje pełną spójność przetwarzanych danych. Modyfikacja replik danych, w replikacji asynchronicznej, odbywa się w niezależnych transakcjach. Replikacja asynchroniczna osłabia spójność danych, co w pewnych zastosowaniach jest akceptowalne.

Najpopularniejszym mechanizmem wykorzystywanym przez systemy baz danych do synchronicznej replikacji danych jest protokół ROWA (*Read One Write All*). W protokole tym operacja odczytu wymaga dostępu jedynie do jednej kopii, natomiast do wykonania operacji zapisu wymagany jest dostęp do wszystkich replik danych. Wadą tego rozwiązania jest możliwość zablokowania wszystkich operacji na replikowanych danych, jeżeli dojdzie do awarii chociaż jednego węzła lub środowiska komunikacyjnego.

W synchronicznym środowisku komunikacyjnym Protokoły ROWA-A (*Read One Write All Avaible*) oraz Primary Copy ROWA eliminują wadę blokowania operacji modyfikacji replik w przypadku awarii jednego z węzłów, lecz są nieodporne na awarię środowiska komunikacyjnego, w szczególności na zjawisko podziału sieci. Z tego powodu są one nieprzydatne dla synchronicznej replikacji danych, lecz mogą stanowić podstawę dla replikacji asynchronicznej.

Najefektywniejsze mechanizmy wspierające synchroniczną replikację danych dostarczają protokoły oparte na głosowaniu (*Quorum Consensus* - QC). W algorytmach typu QC operacje odczytu lub zapisu wykonywane na replikowanych danych mogą być wykonane tylko jeżeli większość węzłów wyrazi na tą operację zgodę. Algorytmy typu QC w odróżnieniu od ROWA nie preferują operacji odczytu. Protokoły oparte na QC są odporne zarówno na awarię węzłów jak i również na częściową awarię środowiska komunikacyjnego. Przetwarzanie ulega zablokowaniu jedynie w części sieci nie posiadającej większości. Dużą zaletą tych protokołów jest możliwość transparentnego odblokowania przetwarzania w odciętej od większości części sieci po naprawieniu awarii.

W chwili obecnej komercyjne systemy baz danych wykorzystują głównie protokół ROWA (nieodporny na awarie), protokoły z rodziny QC są natomiast częściej implementowane w systemach eksperymentalnych.

[Brzeziński97] J. Brzeziński, M. Szychowiak Systemy rozproszone tolerujące uszkodzenia. *Materiały konferencyjne POLMAN97,* 1997, pp. 292-304.

[Casavant94] T.L. Casavant, M. Singhal, "Readings in Distributed Computing Systems", IEEE Computer Society Press, 1994, chapter 5.

[Chandra91] T.D. Chandra, S. Toueg, "Unreliable Failure Detectors for Reliable Distributed Systems", In *Proc. 10th ACM Symp. Principles of Distributed Computing*, ACM Press, 1991, pp.325-340.

[Fisher85] M. Fisher, N. Lynch, M. Paterson, "Impossibility of Distributed Consensus with One Faulty Process", In *Journal of ACM, vol. 32*, 1985, pp.374-382.

[Lamport78] L. Lamport, "Time, Clocks, and the Ordering of Events in a Distributed System", *Communication of the ACM #21*, 1978, pp.558-565.

[Malloth96] C.P. Malloth, "Conception and Implementation of a Toolkit for Building Fault-Tolerant Distributed Applications in Large Scale Networks", PhD. Thesis, EPFL, Lausanne, 1996.

[Moser94] L.E. Moser, P.M. Melliar-Smith, V. Agrawala, "Processor Membership in Asynchronous Distributed Systems", *IEEE Trans. on Parallel and Distributed Systems, vol. 5, #5*, 1994, pp.459-473.

[Peterson89] L.L. Peterson, N.C. Buchholz, R.D. Schlichting, "Preserving and Using Context Information in Interprocess Communication", *ACM Trans. on Computer Systems, vol. 7, #3*, 1989, pp.217-246.

[Pham92] H. Pham, "Fault-Tolerant Software Systems. Techniques and Applications", IEEE Computer Society Press, 1992.

[Singhal94] M. Singhal, N. G.Shivaratri, "Advanced Concepts in Operating Systems", McGraw-Hill, 1994.

[Skeen81] D. Skeen, "Non-Blocking Commit Protocols", *Proc. ACM SIGMOD Intern. Conf. On Management of Data*, 1981, pp.219-228.

[Schneyder92] M. Sneider, "Self stabilization", ACM Computing Surveys, 1992

[Tanenbaum91] A.S. Tanenbaum, M.F. Kaashoek, "Group Communication in the Amoeba Distributed Operating System", *Proceedings of 11th IEEE Intern. Conference on Distr. Comp. Sys.*, Arlington, 1991, pp.882-891.

[Tel94] G. Tel, "Introduction to Distributed Algorithms". Cambridge University Press, 1994, chapter 15.

[vanRenesse93] R. van Renesse, K. Birman, R. Cooper, B. Glade, P. Stepherson, "The Horus System", In *Birman & van Renesse: Reliable Distributed Computing with the Isis Toolkit*, IEEE Computer Society Press, 1993, pp.133-147.

[Verissimo91] P. Verissimo, L. Rodrigues, J. Rufino, "The Atomic Multicast Protocol (AMp)", In *D. Powell, "Delta-4: A Generic Architecture for Dependable Distributed Computing"*, Springer-Verlag, 1991, pp.267-294.

[Whetten94] B. Whetten, T. Montgomery, S. Kaplan, "A High Performance Totally Ordered Multicast Protocol", In *Lecture Notes in Computer Science #938*, Springer-Verlag, 1994, pp.33-57.

do uwzględnienia w swoim systemie prawnym istnienia społeczeństwa informacyjnego w najszerszym tego słowa znaczeniu.

Polski system prawny rozróżnia, jako przedmiot ochrony, informacje których treść może być uznana za tajemnicę państwową, służbową, tajemnicę przedsiębiorstwa (handlową), tajemnicę bankową, skarbową, tajemnicę korespondencji (komunikowania się).

Próby systematyzowania tajemnic, co do rangi ich ważności są nieporozumieniem. Nie można ustalić jednakowego kryterium pozwalającego dokonać zadowalającego uszeregowania. Jedyna systematyzacja mająca odczuwalne znaczenie, to systematyzacja warunkowana kryterium odpowiedzialności karnej. Odpowiedzialność ta nie może jednak być przesądzająca, ponieważ w wielu wypadkach bardziej odczuwalne będą skutki poniesionej odpowiedzialności cywilnej.

Podstawowymi źródłami polskiego prawa chroniącego informacje stanowiące tajemnice: państwową, służbową, przemysłową, korespondencji są:

- Konstytucja RP z 1952 r. (t.j. Dz.U. z 19976 r. nr 7 poz. 36)
- Ustawa z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej. (Dz.U. nr 40, poz. 271),
- Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. nr 47, poz. 211),
- Konwencja Paryska z 20.03.1883 r. o ochronie własności przemysłowej (wielokrotnie zmieniana, Polskę obowiązuje tekst sztokholmski (Dz.U. z 1975 r. nr 9, poz 52),
- Kodeks karny.

Inną potężną sferą informacji chronionej jest informacja intelektualna znajdująca ochronę w prawie autorskim, patentowym i wynalazczym oraz w ratyfikowanym przez Polskę Porozumieniu ustanawiającym Światową Organizację Handlu (WTO) z załącznikiem dotyczącym handlowych aspektów praw wolności intelektualnej (TRIPS) .

Wadą obowiązujących aktów prawnych jest to, że mimo zmiany ustroju politycznego i ekonomicznego Państwa, obowiązują one w wersji pierwotnej, nie były nowelizowane, nadto są trudno czytelne w związku z tym, że wydano szereg aktów wykonawczych niższej rangi poczynając od rozporządzeń, przez uchwały i zarządzenia na instrukcjach kończąc. Pozytywem jest, że można znaleźć akty prawne, z których usunięto obowiązujące początkowo klauzule „poufne" (np. zarządzenie nr 60/83 MSW w sprawie szczegółowych zasad i sposobu postępowania z wiadomościami stanowiącymi tajemnicę państwową i służbową - nie publikowane).Sądzić należy, że istnieją ciągle jakieś niepublikowane akty prawne dotyczące postępowania z tajemnicą państwową. Nie można uznać aktów prawnych nie publikowanych za obowiązujące. Mają one charakter norm jedynie indywidualnie obowiązujących, ten krąg osób, który został z nimi zapoznany i zobowiązał się do ich przestrzegania.

Wymienione wyżej Konstytucja i Kodeks karny doczekały się nowych tekstów - w sferze tu omawianej, nowych redakcji.

Obowiązująca Konstytucja w art. 87 ust. 2 stwierdza: „Ustawa ochrania nienaruszalność mieszkań i tajemnicę korespondencji. Przeprowadzenie rewizji domowej dopuszczalne jest jedynie w przypadkach określonych ustawą." Uchwalony projekt konstytucji stwierdza w art. 49: „Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony."

Dużo pojemniejszym jest użyte w projekcie konstytucji określenie „tajemnica komunikowania się" niż poprzednio: „tajemnica korespondencji". Informacje przesyłane sieciami komputerowymi nie były uważane za korespondencję i nie mogły korzystać z ochrony prawnej takiej, jak korespondencja. Obecnie, konsekwentnie, użyto podobnych określeń w zmienionym kodeksie karnym (jeszcze nie obowiązującym). W obecnie obowiązującym stanie prawnym jesteśmy dość bezsilni wobec sprawcy winnego naruszania informacji nie przeznaczonych dla niego, przesyłanych drogą komputerową. Wynika to z użytego w kodeksie karnym określenia

Przedsiębiorcami, w rozumieniu ustawy, są osoby fizyczne, osoby prawne oraz jednostki organizacyjne nie mające osobowości prawnej, które prowadząc chociażby ubocznie, działalność zarobkową lub zawodową uczestniczą w działalności gospodarczej. Adresatami ustawy są wszystkie podmioty prowadzące działalność gospodarczą. W tym kręgu znajdują się na przykład: wszystkie spółki, przedsiębiorstwa państwowe, prowadzące działalność gospodarczą fundacje, stowarzyszenia i partie polityczne, jednostki badawczo-rozwojowe, prowadzące działalność gospodarczą osoby fizyczne. Zastosowanie ustawy o znk będzie niemożliwe w stosunku do tych wszystkich podmiotów, które nie występują nawet ubocznie w obszarze działalności gospodarczej.

Ustawa ma zastosowanie także do zagranicznych osób fizycznych i prawnych, kiedy wynika to z umów międzynarodowych obowiązujących Polskę lub z zasady wzajemności.

Tajemnica przedsiębiorstwa

Przepisem ustawy o znk, regulującym istotę zakazu ujawniania informacji będących tajemnicą przedsiębiorstwa jest art. 11 ust. 1. „Czynem nieuczciwej konkurencji jest przekazywanie, ujawnianie lub wykorzystywanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej, jeżeli zagraża istotnym interesom przedsiębiorcy."

Za tajemnicę przedsiębiorstwa ustawa uznaje nie ujawnione do wiadomości publicznej informacje:

- techniczne,
- technologiczne,
- handlowe,
- organizacyjne

przedsiębiorstwa , co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności. Zakres dyscyplin, których może dotyczyć tajemnica przedsiębiorstwa, jest w ustawie określony wyczerpująco. Z tego względu, żadna informacja, która nie ma charakteru technicznego, technologicznego, handlowego lub organizacyjnego nie może być uznana za tajemnicę przedsiębiorstwa. Nie będzie też można uznać za stanowiącą tajemnicę przedsiębiorstwa informacji, która będzie sprzeczna z prawem, zasadami współżycia społecznego lub dobrymi obyczajami (np. metody oszukiwania kontrahentów, czy konsumentów).

Naruszenie tajemnicy przedsiębiorstwa może wystąpić w dwóch postaciach:

- zdrady tajemnicy przedsiębiorstwa,
- szpiegostwa gospodarczego.

Warunkiem odpowiedzialności karnej za zdradę tajemnicy przedsiębiorstwa jest wystąpienie łączne trzech przesłanek:

A) podjęcie przez przedsiębiorcę niezbędnych działań w celu zachowania poufności informacji. Przedsiębiorca musi zadbać o to, by określić rodzaje informacji stanowiące jego tajemnicę i w sposób wyraźny poinformować o poufności krąg osób upoważnionych do dostępu do nich. Nie może mieć miejsca domyślanie się, że informacja jest poufna. Muszą być także określone warunki służące ochronie informacji. Dla celów dowodowych najlepiej jest sporządzić odpowiednie dokumenty, w których będą wymienione informacje poufne i określone osoby dopuszczone do nich. Z drugiej strony przedsiębiorca musi doprowadzić do tego, by osoba postronna nie mogła dotrzeć do owych informacji bez podjęcia w tym kierunku szczególnych starań. Przedsiębiorca troszczy się o to, by wiadomość utrzymać w tajemnicy. Właściwą troską przedsiębiorcy jest także pewne zabezpieczenie przed dostępem osób nieuprawnionych w trakcie ich przekazywania osobom uprawnionym. Nie ma żadnych przeszkód prawnych do stosowania

karnej. Można będzie wówczas rozważać zasadność rekompensaty materialnej wynikającej z przepisów prawa cywilnego.

C) ujawnienie tajemnicy przedsiębiorstwa innej osobie lub wykorzystanie we własnej działalności.

Zdrada tajemnicy przedsiębiorstwa i szpiegostwo gospodarcze (art. 23 ustawy o uzp) zagrożone są karą pozbawienia wolności do lat 2, lub karą ograniczenia wolności albo karą grzywny (od 100 do 25.000 zł). Ściganie przestępstw nieuczciwej konkurencji następuje na wniosek pokrzywdzonego.

Typowym wykorzystywaniem informacji stanowiących tajemnice przedsiębiorstw jest ich podstępne lub wręcz nielegalne gromadzenie i odpłatne udostępnianie przez tzw. wywiadownie gospodarcze (także banki informacji gospodarczej). Korzystanie z informacji wywiadowni nie jest zabronione, może jednak w niektórych sytuacjach powodować odpowiedzialność cywilną w granicach określonych w art. 18 ustawy o znk.

Podstawę tej odpowiedzialności (ex delictu) stanowią:

przekazanie, ujawnienie, wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa,

lub ich nabycie od osoby nieuprawnionej jeżeli zagraża to istotnym interesom przedsiębiorstwa (art.11 ust. 1).

W razie dopuszczenia się czynu nieuczciwej konkurencji, przedsiębiorca, którego interes został zagrożony lub naruszony, może żądać:

1) zaniechania niedozwolonych działań,
2) usunięcia skutków niedozwolonych działań,
3) złożenia jednokrotnego lub wielokrotnego oświadczenia odpowiedniej treści i w odpowiedniej formie,
4) naprawienia wyrządzonej szkody,
5) wydania bezpodstawnie uzyskanych korzyści.

Z roszczeniami wymienionymi wyżej (art.18 ustawy o znk) może występować pokrzywdzony oraz krajowe lub regionalne organizacje ochrony praw konsumentów lub interesów przedsiębiorców.

Uwagi końcowe

Obowiązująca ustawa o zwalczaniu nieuczciwej konkurencji oceniana jest, jako nowoczesny akt prawny, dostosowany do prawa krajów członkowskich Unii Europejskiej. Taką samą ocenę ma ustawa o prawie autorskim i prawach pokrewnych. Istnieje jednak poważna luka w obu tych unormowaniach, charakterystyczna zresztą dla całego prawodawstwa Unii. Te akty prawne nie regulują problemów związanych z ochroną twórców i informacji zamieszczanych w tzw. bazach danych, w szczególności jeśli chodzi o wolności osób i przedsiębiorstw w zakresie dostarczania produktów i usług informatycznych w systemie „on line". Polska ustawa o zwalczaniu nieuczciwej konkurencji nie daje żadnych podstaw do tego, by uznać za czyn nieuczciwej konkurencji pobieranie - bez zgody twórcy - (*extraction*) części lub całości cudzej bazy danych lub powtórne wykorzystywanie takiej bazy danych (*re-utilization*). Jedynie obowiązujące jest w tym wypadku prawo autorskie, które chroni wykorzystane w bazie danych utwory (literackie, muzyczne, plastyczne itp.). Nie ma w tej materii wypracowanej dyrektywy europejskiej. Czynione są próby opracowania jednolitej zasady. Sprowadzają się one ostatnio do tego, że wszelkie informacje umieszczane w bazach danych muszą honorować już istniejące prawa do informacji, w szczególności nie mogą naruszać praw autorskich. Sam twórca bazy danych, w

PRZESTĘPSTWA POPEŁNIANE Z WYKORZYSTANIEM SPRZĘTU I SIECI KOMPUTEROWYCH

mł. insp. Andrzej Karp

Samodzielna Sekcja ds. Przestępczości Komputerowej, Analiz i Logistyki
Biura ds. Przestępczości Gospodarczej KGP w Warszawie

I. KOMPUTER JAKO NARZĘDZIE DO POPEŁNIANIA PRZESTĘPSTW

Definicja i podział przestępstw komputerowych

Rozwój cywilizacyjny świata i związany z nim postęp techniczny - w okresie zaledwie kilkunastu ostatnich lat - spowodował rewolucję w zakresie gromadzenia, przetwarzania, wymiany danych i informacji niemal we wszystkich dziedzinach życia społecznego, politycznego i gospodarczego.

Elektroniczne systemy gromadzenia i przetwarzania danych stanowią obecnie bazę operacyjną dla większości rozwiniętych działań w sferze bankowości, taktycznych i strategicznych operacji wojskowych, jak i w sferze pokojowego podboju kosmosu.

Możliwość wielostronnego, a nawet nieograniczonego - jak się wydaje - zastosowania sprawia, iż elektroniczne systemy, opracowane dla nich programy operacyjne i wprowadzone do nich zbiory informacji wymagają ochrony całego systemu, jak i poszczególnych jego elementów. Chodzi w szczególności o ochronę zbiorów danych zgromadzonych w komputerze, obiegu informacji w systemie połączeń komputerowych, ochronę programów komputerowych, a zwłaszcza zawartej w nich własności intelektualnej. Znaczenie tej ochrony było wielokrotnie przedmiotem międzynarodowego zainteresowania, zwłaszcza w sytuacji Polski, w której jeszcze do niedawna brakowało w tym zakresie jasnego określenia przedmiotu i zakresu ochrony własności intelektualnej. Postęp jaki w Polsce dokonał się w tej dziedzinie, wynika z jej aspiracji i gotowości włączenia się do międzynarodowej współpracy oraz faktycznego wywiązania się z przyjętych zobowiązań (Układ Europejski ustanawiający stowarzyszenie pomiędzy Rzeczpospolitą Polską a Wspólnotą Europejską).

Wśród zachowań związanych z informatyką, które wymagają (precyzyjnej) penalizacji można wyróżnić działania dotyczące:

1 - prawidłowego obiegu informacji,
2 - uprawnień do programów komputerowych.

W pierwszej grupie chodzi o czyny godzące bezpośrednio w oprogramowanie, system komputerowy i przechowywane dane. W ramach drugiej grupy występują naruszenia praw autorskich do programów komputerowych oraz związanych z tym praw pokrewnych. Chodzi tu o przestępstwa naruszania praw autorów, producentów i użytkowników oprogramowania.

W literaturze zwraca się uwagę, że pojęcie **„przestępstwo komputerowe"** jest bardzo pojemne i nieostre, co prowadzi do tego, że w jego zakres może wchodzić zarówno kradzież informacji z komputera, zmiana lub niszczenie danych komputerowych, jak również fizyczne zniszczenie komputera i współpracującego z nim sprzętu.

Wymienione wyżej przestępstwa ścigane są w zależności od swojego charakteru na podstawie przepisów zawartych w kodeksie karnym tj. w oparciu o następujące art. kk.:

a) 173 - rozpowszechnianie pornografii i inne przestępstwa o charakterze seksualnym, zwłaszcza za pomocą Internetu,
b) 199-202 - zagarnięcie mienia; kradzież komputerów lub jego składowych, mniej oczywiste - włamanie do sieci bankowej, „zakupy" przez sieć na podstawie sfałszowanych danych, podszywanie się pod legalnego użytkownika w Internecie w celu zagarnięcia mienia lub też kradzież impulsów telefonicznych z TP S.A. (poważny problem w krajach zachodnich),
c) 212 i 220 - zniszczenie mienia; uszkodzenie (świadome lub nie) systemu komputerowego, nielegalne wprowadzanie do systemów komputerowych specjalnych programów tzw. wirusy komputerowe, bomby logiczne, konie trojańskie, robaki komputerowe,
d) 260 i 264 - ujawnienie informacji objętych tajemnicą państwową lub służbową, poprzez np. skopiowanie danych, przesłanie pocztą elektroniczną, faksem komputerowym itp.,
e) 265 - 268 - fałszerstwo, uszkodzenie lub zniszczenie dokumentu i inne; współczesne drukarki kolorowe umożliwiają wykonanie doskonałych podróbek o rozdzielczości prawie drukarskiej,
f) 270 & 1 - publiczne lżenie wyszydzanie lub poniżenie Narodu Polskiego, Rzeczypospolitej Polskiej, jej ustroju lub naczelnych organów; prowadzenie np. list dyskusyjnych,
g) 270 & 2 - publiczne pochwalanie faszyzmu lub jakiejkolwiek jego odmiany,
h) 272 - publiczne nawoływanie do waśni na tle narodowościowym, etnicznym, rasowym lub wyznaniowym albo publiczne pochwalanie takich waśni,
i) 274 & 1 - publiczne lżenie, wyszydzanie lub poniżanie grupy ludności albo poszczególnej osoby z powodu jej przynależności narodowościowej, etnicznej lub rasowej.

Rozważając powyższą problematykę należy mieć także na uwadze karne przepisy pozakodeksowe, a zwłaszcza art. 119 i 119a ustawy z dnia 22.03.1991 roku „Prawo o publicznym obrocie papierami wartościowymi i funduszach powierniczych (wykorzystanie informacji stanowiących tajemnicę zawodową lub informacji poufnych w obrocie papierami wartościowymi) oraz art. 23 ustawy z dnia 16.04.1993 roku o zwalczaniu nieuczciwej konkurencji (ujawnianie tajemnicy przedsiębiorstwa).

Dość jednoznacznie są natomiast w Polsce chronione dwie kategorie czynów znajdujących się na liście minimalnej Komitetu Ekspertów Rady Europy, a mianowicie bezprawne kopiowanie, rozpowszechnianie lub publikowanie programów komputerowych prawnie chronionych (art. 115-118 ustawy z dnia 4 lutego 1994 roku o prawach autorskich i prawach pokrewnych) oraz bezprawne kopiowanie topografii półprzewodników (art.42 i 43 ustawy z dnia 31.10.1992 roku o ochronie topografii układów scalonych).

Oszustwa komputerowe

W pojęciu kryminalistyki oszustwa stają się bardziej atrakcyjne niż przestępstwa tradycyjne takie jak kradzieże itp. częściowo z powodu mniejszego ryzyka odpowiedzialności karnej, a częściowo z powodu potencjalnie dużo większych zysków. Większość oszustw popełnianych przy użyciu komputerów jest inna niż popełnianych w tradycyjnych systemach opartych „o papier". Poza tym mniejsze jest ryzyko wykrycia, a większe możliwości „zarobienia" ogromnych pieniędzy. Wskutek tego oszustwa komputerowe są obecnie atrakcyjną formą działalności przestępczej i jest prawdopodobne, że sytuacja ulegnie pogorszeniu ponieważ coraz większa liczba podmiotów gospodarczych rezygnuje z tradycyjnego prowadzenia księgowości na korzyść księgowości komputerowej.

każdego posiadacza rachunku jest zbyt mała, żeby mogła być zauważona. Jednakże małe kwoty pomnożone przez wiele tysięcy rachunków i wiele tysięcy transakcji dają w rezultacie oszustwo pokaźnych rozmiarów. Ten sposób działania wymaga od sprawcy znacznej wiedzy informatycznej. Stąd sprawców tego rodzaju przestępstw typować należy spośród twórców oprogramowania lub informatyków z poszkodowanej instytucji. Należ zwrócić również uwagę na włamywaczy do systemów komputerowych.

- **manipulacja wynikiem** (output manipulation), zwana często manipulacją urządzeniami wyjścia - wejścia. Polega ona na wykorzystywaniu ogólnie dostępnych peryferii komputerowych i systemów w celu dokonania przestępstwa. Klasycznymi przykładami takich działań są przestępstwa za pomocą terminali elektronicznych (np. bankomatów). Najczęściej ujawnianymi typami takich czynów są fałszerstwa danych zawartych na pasku magnetycznym karty, co pozwala posługiwać się przestępcy kartą bez widocznego ingerowania w dane na niej zawarte oraz tzw. „wstukiwanie" transakcji. ???

Wskazana wyżej grupa przestępstw jest trudna do ścigania. Niezbędne jest współdziałanie organów procesowych i poszkodowanego , który nie zawsze jest zainteresowany w ujawnianiu słabości własnego systemu komputerowego z uwagi na obawę utraty zaufania klientów.

Do dochodzenia tego typu oszustw muszą być zastosowane te same posunięcia co do pozostałych oszustw, z tym że istnieją dodatkowe trudności w uzyskiwaniu dowodów. Funkcjonariusze policji, prokuratura oraz sądy są dobrze przygotowane do uzyskiwania dowodów w tradycyjny sposób w postaci dokumentów, ale nie z elektronicznymi danymi. W swojej pracy winny oprzeć się w decydującej mierze o wyspecjalizowanych ekspertów (biegłych) z zakresu informatyki.

Fałszerstwa komputerowe

Wyróżnić należy dwa przejawy (aspekty) tego typu przestępstw:

- **klasycznych; jako komputerowe fałszerstwo dokumentów, gdzie komputer, oprogramowanie i peryferia są narzędziem do fałszowania dokumentów;**

Dynamiczny rozwój techniki komputerowej oraz oprogramowania powoduje, że praktycznie nie ma w obecnej chwili klasycznego dokumentu który nie mógłby być skopiowany za jego pomocą.

Jeszcze nie tak dawno dokonywanie fałszerstw było stosunkowo drogie ze względu na duży koszt zakupu sprzętu niezbędnego do dokonywania tego typu przestępstw. Obecnie wysokiej klasy oprogramowanie oraz wysokiej klasy urządzenia takie jak skanery i kolorowe drukarki (laserowe, atramentowe) są stosunkowo tanie.

Przestępcy komputerowi wykorzystują tę sytuację i obecnie są w stanie wykonać bardzo wiarygodne kopie czeków bankowych, umów kredytowych, dokumentów stwierdzających tożsamość, polis ubezpieczeniowych, dyplomów akademickich i innych znaczących dokumentów. Problemem w tej chwili dla sprawcy może być jedynie odpowiedni papier oraz złamanie jego zabezpieczeń technicznych np. wtopiony pasek lub znak hologramu, znak wodny, odpowiednia struktura . Przestępstwo takie , obecnie nie nastręcza szczególnych trudności dowodowych i jest obecnie często ujawniane i identyfikowane.

jako fałszerstwo dokumentów elektronicznych (niepapierowych), polegające na wprowadzaniu zmian w utworzonych i przyjętych dokumentach elektronicznych (księgi podatkowe i handlowe, kartoteki, ewidencje, remanenty, listy) lub też innych elektronicznych nośnikach informacji (np. zmiana zapisu na ścieżce magnetycznej karty płatniczej czy identyfikacyjnej).

Wirusy komputerowe są to programy o złych intencjach, które są tworzone w celu modyfikacji lub niszczenia danych lub też zakłócania pracy całych systemów komputerowych (muszą mieć nosiciela).

Niektóre wirusy są niegroźne i jedynie wypełniają przestrzeń na dysku, inne jednak mogą przejąć kontrolę nad komputerem i doprowadzić do katastrofalnych skutków. Motywy wprowadzania wirusów przez przestępców są bardzo zróżnicowane. Niektórzy przestępcy popełniają ten rodzaj przestępstwa aby pokazać swoje umiejętności w zakresie programowania. Zdarzają się jednak bardziej poważne przyczyny popełniania tego rodzaju przestępstw. Jedną z takich przyczyn może być niechęć „pirata komputerowego" do konkretnej osoby lub organizacji lub też , co zdarza się coraz częściej chęć szantażowania ofiary.

J. Hruska w swojej książce „Wirusy komputerowe i ochrona antywirusowa" wymienia potencjalnych twórców programów destrukcyjnych. Są nimi z reguły:

a) piraci komputerowi (hackerzy), dla których komputer staje się uzależnieniem podobnym do narkomanii i którzy poprzez stworzenie wirusa, chcą pokazać swoje zdolności,
b) studenci i uczniowie, którzy stworzenie wirusa traktują jako wyzwanie intelektualne,
c) niezadowoleni pracownicy, którzy w ten sposób chcą zemścić się na pracodawcy,
d) twórcy oprogramowania, którzy poprzez wprowadzenie np. bomby logicznej pragną zabezpieczyć się przed zwolnieniem z pracy lub też żądają określonych gratyfikacji,
e) członkowie organizacji terrorystycznych, które jak np. włoskie Czerwone Brygady wymieniają destrukcję systemów komputerowych w swoich manifestach. Twierdzono, że wirus Jeruzalem został napisany przez sympatyków OWP, lecz przeczy temu wiele autorytatywnych badań. Jedyną oznaką wiążącą wirus z OWP jest data wyzwolenia (13.piątek) pokrywająca się z ostatnim dniem istnienia państwa palestyńskiego.

Większość zgłaszanych ostatnio usterek sprzętu wywołują następujące wirusy:

Form	Cascade	Yankee Doodle
Ping Pong	Keypress	Joshi
Stoned	Telefonica	Michaelangelo
Hallowen	Omicron	Exebug

Najbardziej znanym jest wirus Form. Chociaż wirus ten wywołuje tylko efekt dźwiękowy „bib" w czasie naciskania klawiszy klawiatury, to koszt wyczyszczenia zainfekowanego systemu (doprowadzenie do poprzedniej postaci) jest znacznym wydatkiem dla firmy i wynosi ok. 25.000 funtów angielskich.

Po upadku żelaznej kurtyny, a nawet jeszcze podczas ostatnich lat komunizmu, wiele nowych wirusów wydostało się na świat z dawnego bloku wschodniego. W szczególności Bułgaria udowodniła, że ma bardzo płodnych programistów. Wiele wskazywało na bułgarskie „fabryki wirusów". THE DARK AVENGER to przezwisko autora wielu szatańskich wirusów, często zawierających szczególnie uciążliwe procedury destrukcyjne. Nie jest znana osoba kryjąca się pod tym pseudonimem' najprawdopodobniej mieszka on w Sofii i jest dawnym studentem Uniwersytetu w tym mieście.

W roku 1992 przewidywano, że na całym świecie powstaje w każdym miesiącu około 2000 nowych wirusów. W roku 1993 liczba ta miała zwiększyć się do około 5000 na miesiąc. Te dane okazały się przesadzone. Aktualnie w przybliżeniu powstaje od 100 do 180 wirusów miesięcznie. Oczywiście większość z tych wirusów nie jest naprawdę nowymi wirusami, tylko odmianami starszych.

informatyczny albo celowe zwirusowanie systemu komputerowego, jak i w skutek niedbalstwa lub lekkomyślności, np. w wyniku błędu hackera lub też zaniechania procedur nadzorujących sieć komputerową (monitoringu) przez pracownika odpowiedzialnego. Sabotaż komputerowy często jest połączony z szantażem komputerowym, gdzie sprawca w zamian za spełnienie jego warunków, najczęściej finansowych, gotów jest odstąpić od sparaliżowania systemu komputerowego w sobie znany sposób.

Należy ponadto zwrócić uwagę na poważne następstwa, jakie mogą wywołać zaburzenia w pracy systemów komputerowych i telekomunikacyjnych w wielu dziedzinach życia społecznego, które w coraz większym stopniu są uzależnione od niezakłóconego funkcjonowania techniki komputerowej. Z tego właśnie powodu w wielu krajach przepisy prawne przewidują kary również dla nieumyślnych sprawców zablokowania funkcji systemów informatycznych i telekomunikacyjnych.

„Wejście" (włamanie) do systemu komputerowego przez osobę nieuprawnioną - hacking

Jest to czyn polegający na przełamaniu przez osobę nieupoważnioną systemu informatycznego i spowodowanie paraliżu tego systemu tzw. hacking komputerowy. Hacking w żargonie informatycznym jest potocznym wyrażeniem służącym do opisania praktyk mających na celu zdalne atakowanie systemu komputerowego poza bazą sieciową. Natomiast słowo „hacker" w tymże żargonie stało się międzynarodowym określeniem osoby, która włamując się do sieci komputerowej, pokonuje zabezpieczenia w postaci kodów i haseł broniących dostępu do zgromadzonej i przetwarzanej informacji. Niektórzy hackerzy po dokonaniu włamania do systemu pozostawiają pewnego rodzaju wizytówki identyfikacyjne na zaatakowanym komputerze, zazwyczaj sprośną informację jako sposób poinformowania administratora, że jego system zabezpieczeń został złamany. Często ten rodzaj działalności jest prowadzony bez politycznych lub kryminalnych intencji, ale w wielu przypadkach dane zostają zniszczone i w tych przypadkach rezultaty hackingu mogą być katastrofalne.

Penetrowanie przez hackerów systemów informatycznych za pośrednictwem połączeń telekomunikacyjnych jest dziś zjawiskiem o zasięgu międzynarodowym, rozmaicie ocenianym w aspekcie jego szkodliwości i wywołującym zróżnicowane reakcje ustawodawców w poszczególnych krajach. Szkodliwość działania sprawców nieuprawnionego wejścia do systemu komputerowego wynika z faktu, że samo wejście do takiego systemu jest podstawą innych czynów przestępczych i kryminalizacja takiego zachowania ma oddziaływanie prewencyjne. FBI szacuje roczne straty na skutek ataków elektronicznych na 7,5 mld USD rocznie, a raport Departamentu Obrony USA stwierdza, że 88 % ich komputerów było penetrowane. Na włamanie narażone są praktycznie wszystkie sieci, zarówno mające dostęp z zewnątrz (poprzez INTERNET, modem, pakiet sieciowy itp..) jak i sieci zamknięte. Dane amerykańskie wskazują także, że ok. 70 % udanych kradzieży z sieci komputerowych nastąpiła w wyniku penetracji przez pracowników firmy korzystających z systemu komputerowego lub we współpracy z nim. Takie ataki są o wiele łatwiejsze i trudniej wykrywalne. Co więcej, o ile ataki zewnętrzne są w wielu przypadkach wykonywane dla zabawy, o tyle ataki wewnętrzne są dokonywane ze znacznie większą determinacją i zazwyczaj nie służą zabawie. Rozwój międzynarodowych sieci komputerowych i włączanie się ogromnej rzeszy prywatnych użytkowników do sieci INTERNET potęguje skalę zagrożeń. Już w tej chwili ujawniane są próby i udane przypadki włamań zgłaszane przez administratorów sieci w Polsce, a także próby włamań do systemów komputerowych w Polsce z terenu USA oraz udane włamania do systemów w jednym z krajów Europy z terenu Polski.

W literaturze przedmiotu podaje się przykład pirata komputerowego (hackera), który po zaatakowaniu systemu komputerowego dużej firmy ubezpieczeniowej zaszkodził temu systemowi do tego

chronę praw autorskich i patentowych (art. 42 i 43 ustawy z dn. 31.10.1992 roku o ochronie topografii układów scalonych Dz.U. nr 100, poz. 498).

Proponowane zmiany w nowym kodeksie karnym

W systemie polskiego prawa brak jest odrębnych (za wyjątkiem prawa autorskiego) przepisów regulujących odpowiedzialność za szkody wyrządzone przez czyny przestępne, dokonywane z wykorzystaniem komputera. W tej instytucji osoby za dokonanie takich czynów odpowiedzialne mogą być ukarane jedynie w oparciu o ogólne przepisy prawa.

Przepisy Kodeksu karnego powstały w czasie (1969 rok), gdy zagadnienia przestępczości związanej z systemami komputerowymi nie wymagały szczegółowej regulacji, stąd też brak przepisów odnoszących się wprost do tej sfery przestępczości. Brak odrębnej dyspozycji nie wyłącza jednak odpowiedzialności karnej, gdyż kodeks karny jest na tyle elastyczny, że pozwala na ściganie niemal wszystkich czynów patologicznych, umownie nazywanych przestępstwami komputerowymi. Nie ma przy tym znaczenia, jakim środkiem popełniono przestępstwo.... Spowodowanie np. śmierci człowieka czy zagarnięcie mienia jest ścigane bez względu na to, jakim narzędziem zostało popełnione. Może to być także sprzęt komputerowy.

Nowe typy przestępstw związanych z rozwojem nowoczesnej techniki cyfrowej zawiera projekt kodeksu karnego, przygotowany przez Komisję do Spraw Reformy Prawa Karnego.

Przepisy dotyczące przestępczości komputerowej, oprócz przepisów w zbliżonej formie istniejących obecnie, rozmieszczone zostały w kilku rozdziałach projektu, zależnie od przedmiotu ochrony, m.in. w rozdziale dot. przestępstw przeciwko ochronie informacji (art. 270 - 274 projektu), przestępstw przeciwko wiarygodności dokumentów (art. 275, 282 projektu), czy przestępstw przeciwko mieniu (art. 292 projektu). Przedmiotem ochrony tajemnicy (w tym tajemnicy korespondencji) jest wyraźnie wymienione bezprawne pozyskiwanie informacji uzyskane przez przełamanie elektronicznego, magnetycznego lub innego szczególnego zabezpieczenia wiadomości. Ochrony tej dotyczy także przepis „typizujący zachowanie polegające na zakładaniu lub posługiwaniu się urządzeniem podsłuchowym, wizualnym, lub innym urządzeniem specjalnym w celu uzyskania cudzej informacji bez uprawnienia" (art. 272,273).

W tym samym rozdziale projektu, art. 270 i 271 autorzy przewidują odpowiedzialność osób, które wbrew przepisom ujawniają cudzą tajemnicę, z którą zapoznały się podczas wykonywania obowiązków zawodowych, działalności publicznej, społecznej, gospodarczej lub naukowej. Przepis ten ma szczególne znaczenie w sytuacji, gdy większość danych opracowań i innych informacji dotyczących osoby lub jej działalności znajduje się w komputerowych bazach danych, a co za tym idzie wymaga szczególnej ochrony prawnej.

Odrębny typ przestępstwa dotyczy „zakłócenia lub uniemożliwienia gromadzenia lub przekazywania informacji o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji lub funkcjonowaniu administracji państwowej, przez niszczenie zapisu informacji na nośniku komputerowym , ich uszkodzenie lub zmiany, zniszczenie nośnika tej informacji lub jego wymianę albo też niszczenie urządzenia służącego automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji, które jest nazwane sabotażem komputerowym. (art. 274).

W przestępstwach przeciwko mieniu przewidziana jest odpowiedzialność karna osoby, która w celu osiągnięcia korzyści majątkowej przez ukształtowanie programu komputerowego, włączanie do pamięci komputera niewłaściwych lub niepełnych informacji albo przez inne oddziaływanie na przetwarzanie informacji wpływa na wynik opracowania i powoduje szkodę majątkową innej osobie

BEZPIECZEŃSTWO INFORMACJI I SIECI TELEKOMUNIKACYJNYCH A WIRTUALNA RZECZYWISTOŚĆ

Andrzej Zienkiewicz

Definicje :

Wirtualny - mogący zaistnieć, (teoretycznie) możliwy[1].

Telekomunikacja - przesyłanie informacji pomiędzy punktami nadania i odbioru określonymi przez użytkownika, bez zmiany formy i treści pomiędzy punktami nadania i odbioru.

Bezpieczeństwo - stopień pewności (prawdopodobieństwo) przesłania informacji pomiędzy punktami nadania i odbioru i tylko pomiędzy tymi punktami w oczekiwanym czasie.

Internet - ogół różnych sieci teleinformatycznych połączonych pomiędzy sobą w skali krajowej i globalnej przy pomocy protokołu telekomunikacyjnego IP (Internet Protocol).

Informacja - każdy czynnik, dzięki któremu ludzie lub urządzenia automatyczne mogą bardziej sprawnie, celowo działać. Przeciwieństwem jest dezinformacja.

W referacie zawarte są refleksje na temat skutków jakie dla bezpieczeństwa informacji i sieci stanowi stan świadomości użytkowników i operatorów sieci w relacji do rzeczywistości. Z rozlicznych badań wynika, że około 90% wszelkich zagrożeń bezpieczeństwa stanowi człowiek użytkujący sieć jak i operujący tą siecią. Z tego powodu stan jego świadomości jest decydujący dla bezpiecznego korzystania z sieci.

Globalna sieć Internetu jest bardzo złożona strukturalnie i technologicznie. Tak naprawdę nie jest znana nigdzie jego struktura. Również zasięg Internetu obejmującego większość cywilizowanego świata nie jest znany, chociażby z powodu nieustannego rozwoju. Dla uproszczenie rzeczywistości , na użytek masowy zostało przyjęte określenie *globalnej wioski.* Świetne na użytek propagatorski określenie oswaja Internet, czyni go bliskim, swojskim i zrozumiałym. Jednak Internet nie jest *wioską, w której* mieszkają sami swoi, gdzie rządzi przyjazny sołtys, gdzie wszyscy się znają i wzajemnie kontrolują. W rzeczywistości Internet jest mrocznym, nieznanym do końca żywiołem, bez jasnych reguł i egzekucji praw, żywiołem, w którym działają zarówno dobrzy (nam przyjaźni) jak i źli (nasi wrogowie). Jak każdy żywioł Internet jest do wykorzystania, niesie wiele korzyści dla wszystkich, zarówno dobrych jak i złych. I tylko świadomi faktu, że Internet **nie jest** *globalną wioską* mogą w miarę bezpiecznie wykorzystywać jego bezsprzeczne zalety.

Globalny system telekomunikacyjny wymaga w miarę jednolitego języka porozumiewania się. Nie chodzi tu tylko o same słowa, ale przede wszystkim o zakres pojęć. Dla purystów tego rodzaju zjawisko, przewaga języka angielskiego w wydaniu międzynarodowym, unifikacja pojęć stanowię istotne zagrożenie kulturowe oraz zmniejszenie szans ludzkości na przetrwanie wobec zmniejszenia zdolności przystosowawczych wynikających z bogactwa różnorodności. Jednak taka unifikacja jest ceną jaką trzeba zapłacić za możliwość działania w skali globalnej. Natomiast są inne zagrożenia bardziej konkretne i dotyczące naszego polskiego społeczeństwa. Szybka wymiana

[1] Por. Słownik Wyrazów Obcych PWN - wydanie XVII 1993 r.

podział na dziedziny EDU dla edukacji, COM dla zastosowań komercyjnych, GOV dla administracji, MIL dla zastosowań militarnych okazał się wkrótce niewydolny. Wprowadzono zatem kod regionu (w Polsce województwa). Jednak do dziś system nie jest jednolity i globalnie niejasny. Nie uporządkowano totalnie prawa do adresu czy to na zasadzie pierwszeństwa lub prawa do określonego znaku. Dopiero toczące się procesy sądowe uprzytomniły skalę problemu i możliwych z tego powodu naruszeń cudzych praw i zwykłych nadużyć. I znowu mamy tu istotną różnicę pomiędzy prawie powszechnym przeświadczeniem jak powinno i mogłoby być, a rzeczywistością. Stan niejasności ułatwia podszywanie się pod kogoś, uzyskiwanie korzyści z korzystania z czyjegoś dobrego imienia, szkalowanie przy pomocy symulowania kogoś innego lub rozpowszechniania fałszywych informacji w nie swoim imieniu itp.

W środkach masowego przekazu, na przykład w telewizji, na pokazach firmowych widzimy łatwość i szybkość z jaką uzyskuje się informacje multimedialne z całego świata poprzez sieci telekomunikacyjne. Tak mogłoby *teoretycznie być,* gdyby ..... Dr Tim Kelly na Inetnational Telecommunication Union Colloquy : Information highways : "Between dream and reality", Neuchatel, 3-5 April 1997 w referacie Secrets and lies on the Internet strawersował skrót WWW jako World Wide Wait. Możliwości generowania i odbioru informacji poprzez komputer multimedialny, a takim jest większość obecnie instalowanych komputerów osobistych, jest bardzo duża i poza nielicznymi wyjątkami przekracza możliwości systemów transmisyjnych. W skali globalnej niedobór mocy przesyłania wynosi wiele tysięcy lub dziś już prawdopodobnie wiele milionów razy. W obecnych technikach przysyłania informacji takich przepustowości nie da się zapewnić nawet jeśli nie stałby na przeszkodzie brak środków finansowych. Być może problem komunikacji rozwiąże nowa generacja sieci światłowodowych, być może zapotrzebowanie na łączność będzie rosło szybciej niż rozwój technologii przesyłania. Dziś *wirtualny Internet* zaciemnia obraz rzeczywistości i łudzi, że nie potrzebna jest pomysłowość i nakłady w celu ograniczania ujemnych zjawisk wynikających z globalnej niewydolności sieci. Istnieje konieczność ochrony swoich sieci i zastosowań przed inwazją ogólnego Internetu niosącego szereg nieoczekiwanych zagrożeń.

W referacie wprowadzającym Pana Machalskiego podano informację, że Unia Europejska zaleca, aby duże bazy danych określić jako "zastrzeżone" czyli ograniczyć do nich powszechny dostęp. Nie wymaga spostrzegawczości spostrzeżenie, że dla tak zwanego "białego wywiadu" zbiór informacji zawartych w szeroko rozumianym Internecie jest nieprzebraną skarbnicą wiedzy, możliwą do precyzyjnej i dyskretnej obróbki. Oczywiście dla szeregu entuzjastów Internetu zrzeszonych i niezrzeszonych w sieciach działają sami "święci" wobec czego każde ograniczanie dostępu do informacji, każda odpłatność, każdy wymóg formalny grozi wręcz kulturową zapaścią narodu. Jeżeli oddzielić *wirtualną rzeczywistość* od faktów nic z tej argumentacji nie pozostaje. Sieci telekomunikacyjne, w tym i Internet, stanowią kolejny krok ewolucyjny niosąc za sobą dodatkowe możliwości, ale i dodatkowe zagrożenia. Mocno nagłaśniana pornografia, pedofilia itp. są propagandowo nośne, natomiast ich znaczenie jest marginalne. Rzeczywiste zagrożenie stanowi *wirtualna rzeczywistość*, w której wychowuje się coraz liczniejsze grono młodzieży. Młodzież ta będzie jednak musiała kiedyś zmierzyć z rzeczywistym a nie wirtualnym światem i może w tym starciu mieć bardzo ograniczone szanse. Ale takie same argumenty padały w czasie wprowadzania chociażby telewizji, ponieważ problem leży nie w narzędziu, ale jego wykorzystaniu.

Inne zagrożenie dla bezpieczeństwa informacji wynika z przeniesienia tradycyjnych metod i zjawisk politycznych do tak zwanej cyberprzestrzeni. Zjawisko to było opisane swojego czasu w tygodniku Time i po przetłumaczeniu w Gazecie Wyborczej. Tradycyjnie organizowanie dowolnego lobby było trudne, zgromadzenie grupy zwolenników kosztowne i prawie niemożliwe. Dziś takie tradycyjne zjawiska spotyka się w postaci różnych manifestacji, gdzie jakaś głośna grupa czegoś się domaga, przeciw czemuś protestuje. Już przekaz telewizyjny czyni z demonstracji zjawisko publiczne, które bez tego przekazu byłoby społecznie nie zauważalne. Koszty jednak demonstracji

temat wspaniałości Internetu oraz korzyści z handlu, który tylko przez polskie zaniedbanie nie istnieje. Jednostronna informacja prowadzi do powstania w wyobraźni klientów obrazu rzeczywistości, która mogłaby być, ale niestety jeszcze jej nie ma.

Największym zagrożeniem bezpieczeństwa sieci jest *budżet*. Wszystkie działania na rzecz bezpieczeństwa kosztują, trzeba na nie mieć pieniądze, których zawsze brak. Naturalną tendencją jest pokusa zaoszczędzenia na bezpieczeństwie, a *może się uda ?*. Niestety tak jest, że koszty muszą ponosić wszyscy, nieszczęście spotyka niektórych. Usilna propaganda, przedstawiająca różne *wirtualne rzeczywistości i wirtualne korzyści* nie sprzyja rozsądnej ekonomice sieci. Wymuszane są w różny sposób świadczenia poniżej wartości lub byle jakie. Nie ma i nie może być w skali masowej pełnej świadomości czym są sieci telekomunikacyjne, jakie przynoszą korzyści, ale i jakie niosą zagrożenia. Na masową świadomość mogą oddziaływać tak zwane środki masowego przekazu, jednak właśnie te środki są szczególnie odpowiedzialne za tworzenie *wirtualnego świata* sieci telekomunikacyjnych. W takim przypadku konieczne są dyrektywne działania organów odpowiedzialnych za tworzenie polityki bezpieczeństwa oraz tworzenie specjalnych oaz podwyższonego bezpieczeństwa dla bardziej świadomych użytkowników. Zresztą te oazy już się tworzą czego dowodem jest dynamiczny rozwój sieci korporacyjnych. Bowiem do tego czasu nowoczesne sieci telekomunikacyjne, w tym szczególnie Internet, były zauważane. ale w niewielkim stopniu wykorzystywane przez organizacje, które rozumieją powody, dla których bezpieczeństwo informacji i sieci musi być zachowane. Dotyczy to przede wszystkim świata administracji oraz biznesu. Wydaję się, że kończy się epoka radosnej twórczości, niestety uzyskanie środków na bezpieczeństwo sieci będzie ogromnie trudne. Może to zaowocować sytuacją, w której masowy użytkownik sieci, w tym przede wszystkim młodzież, będzie spotykać się wyłącznie z *wirtualnym światem* Internetu dostępnym przez "darmowy" telefon nabijający kabzę operatorów telefonicznych, dla których stopień wykorzystania zainstalowanej infrastruktury technicznej jest najważniejszy.

Wszystko to co napisałem to tylko nieliczne przykłady wskazujące na istnienie problemu. Tak jak i na świecie podstawowy wysiłek musi być skierowany na zmianę świadomości społecznej, która niestety została jednostronnie i fałszywie ukształtowana. W pewnym zakresie pomoże tu i odpowiednie prawodawstwo. Wiadomo jednak, że prawo tylko wtedy jest naprawdę skuteczne, jeżeli spotyka się z przeważającym poparciem społecznym.

Mam nadzieję, że tych parę refleksji skłoni czytelników i słuchaczy referatu do przemyśleń i gorącej dyskusji w czasie panelu.

Warszawa maj 1997 rok

(także na rynku polskim) Należy jednak pamiętać, iż oceny takie poza elementem subiektywizmu, są wykonane dla potrzeb i z uwzględnieniem specyfiki lokalnego rynku, mogą one być jedynie składnikiem oceny całkowitej i ewentualnych rekomendacji dotyczących stosowania badanych produktów bądź technologii w warunkach docelowych.

2. Ocena wiarygodności rozwiązania

Warunkiem uzyskania właściwej oceny wydaje się być przetestowanie konkretnych narzędzi wybranych we wstępnej fazie - w warunkach docelowych. Podejście takie jest oczywiście czaso- i praco chłonne. Należy jednak pamiętać że elementy ochrony sieci nie są „towarem z półki" i właściwy ich dobór w konsekwencji wart jest dodatkowego wysiłku jaki należy włożyć dla uzyskania ich rzetelnej oceny. Minimalizację nakładów związanych z testami branych pod uwagę rozwiązań, można uzyskać poprzez tworzenie układów testowych w skali mikro (w stopniu pozwalającym na ocenę). Zalecane jest także izolowanie ich od „normalnej sieci" podlegającej ciągłej eksploatacji. Porównanie wyników testów w ramach tych samych funkcjonalnie elementów ochrony pozwala na wyłonienie wąskiej już grupy produktów, która może być poddana dalszej, wnikliwej ocenie.

3. Dążenie do certyfikacji w polskich warunkach

W obecnym stanie uregulowań prawnych w dziedzinie zasad i kryteriów oceny technologii podwyższających bezpieczeństwo sieci komputerowych brak jest wykrystalizowanych form i ścieżek certyfikacji pozwalających na autorytatywne potwierdzenie oraz rekomendująca konkretnyh produktów czy technologii, a także gwarancji ich skuteczności, jak również wysokiego stopienia odporności kryptograficznej. Jest wysoce pożądane aby także w naszym kraju wytworzyła się praktyka (procedury) poddawania produktów ocenie i certyfiakacji. Sytuacja taka nie wyklucza jednak uzyskiwania niezależnych ocen od krajowych instytucji naukowych posiadających nie tylko stosowne zaplecze, ale także wybitnych ekspertów w dziedzinie szeroko rozumianej ochrony systemów.

4. Wypracowanie założeń wdrożenia wybranych elementów bezpieczeństwa

Opisane wyżej etapy procesu doboru i pozyskiwania, a także wynikająca z niech późniejsza eksploatacja wybranych elementów bezpieczeństwa, pozwalają na uszeregowanie ich w kolejności stanowiącej pewien wspólny, ogólny algorytm postępowania. Oto on:

- rozpoznanie własnych potrzeb,
- dobór elementów bezpieczeństwa,
- instalacja pilotowa,
- plan modyfikacji programu bezpieczeństwa,
- ocena przydatności,
- faza wstępnej eksploatacji,

Aspekt techniczny

- Wymaga zastosowania odpowiednich rozwiązań w zakresie ochrony sieci.

Aspekt Organizacyjny

- Wymaga bezwzględnego przestrzegania ustalonych procedur.

6.1. Rozwiązania w zakresie uwierzytelniania

Przykładem przeprowadzonej pod kierunkiem NASK opisanej wyżej procedury pozyskania produktu jest wdrożenie systemu jednokrontych haseł firmy Security Dynamics.

Zespół Ochrony Sieci NASK w wyniku prowadzonych od początku 1995 roku prac badawczo-wdrożeniowych przeprowadził szereg testów i zgromadził dokumentację w zakresie wykorzystania technologii jednokrotnych haseł w szeroko pojętym obszarze sieci teleinformatycznych. Prace te, mające charakter pionierskich w skali kraju, zaowocowały konkretnymi wdrożeniami. Na bazie tych wdrożeń wypracowane zostały wzorce technologiczne bezpiecznego systemu uwierzytelniającego użytkownika w oparciu o hasła jednokrotnego użycia. Technologie te zostały ocenione i pozytywnie zaopiniowane przez, współpracującą stale z NASK, Wyższą Szkołę Oficerską Wojsk Łączności zajmującą się problemami bezpieczeństwa w sieciach teleinformatycznych.

Jednym z podstawowych wymagań systemu, jest zapewnienie skutecznego mechanizmu weryfikacji użytkowników w czasie procedury uwierzytelniania w sposób zapewniający odpowiedni poziom wiarygodności.

- **Systemy tradycyjne**

Tradycyjne systemy uwierzytelniania oparte o statyczne identyfikatory nie zapewniają zadowalającego poziomu bezpieczeństwa. Statyczne hasło może zostać odgadnięte lub podsłuchane.

- **Systemy dynamicznego identyfikatora**

W systemach dynamicznego identyfikatora uwierzytelnianie opiera się na zweryfikowaniu użytkownika na podstawie dwóch informacji:

a) tego co użytkownik posiada (kartę jednokrotnych haseł)

b) tego co użytkownik pamięta (osobisty numer identyfikacyjny - PIN)

Ad **a)**
Karta jednokrotnych haseł jest elektronicznym, inteligentnym urządzeniem wielkości karty kredytowej wyświetlającym użytkownikowi co kilkadziesiąt sekund nowy ciąg cyfr stanowiący dynamiczny identyfikator ważny tylko w tym czasie. Generacja jednokrotnego hasła oraz funkcjonowanie karty są oparte na dwóch podstawowych zasadach:

- Synchronizacji czasu (ang. time synchronization),

Jest to połączenie wyżej wymienionych elementów w jeden działający system wraz z przetestowaniem i stworzeniem dokumentacji.

Doświadczenia eksploatacyjne

Produkt firmy Security Dynamics: ACE Server wraz kartami SecurID odznacza się niezależnością od platformy telekomunikacyjnej i sprzętowej oraz skalowalnością (system może działać zarówno w małych kilkunastoosobowych biurach, jak i w rozległych instalacjach obejmujących od kilkudziesięciu do kilkuset tysięcy użytkowników). Liczba produktów programowych i sprzętowych posiadających support dla SecurID stale rośnie dzięki czemu rozwiązanie to jest de facto światowym standardem w zakresie uwierzytelniania za pomocą jednokrotnych haseł. System jest prosty w obsłudze i zarządzaniu. Nie pociąga za sobą narzutu dla jego użytkownika w postaci dodatkowych, skomplikowanych i uciążliwych procedur związanych z eksploatacją. Użytkownik systemu SecurID w ramach nadanych mu uprawnień może uzyskać bezpieczny dostęp do dużej ilości komputerów pamiętając tyko jedeno statyczne hasło (PIN) Zdecydowanie ułatwia to prace w przypadku konieczności zdalnego dostępu do dużej ilości maszyn lub rozległych struktur sieciowych. Użytkownicy systemu szybko przyzwyczaili się do korzystania z kart i wysoko ocenili korzyści wynikające z wdrożenia systemu. W celu spełnienia warunku niezależnej oceny produkt był poddany procesowi ewaluacji dokonanej przez eskpertów.

6.1.2. Uwierzytelnianie oparte o rozwiązania firmy Lintel Security

Drugim rozwiązaniem firmowym testowanym wspólnie z WSOWŁ było rozwiązanie belgijskiej Frimy Lintel Security.

Elementy rozwiązania:

a) Karta dostępu (token)

Tak jak w opisanym wyżej rozwiązaniu (SDI) każdy użytkownik otrzymuje kartę. Jest to inteligentna karta wyposażona w procesor z wyświetlaczem wielkości karty kredytowej. Zawiera ona dodatkowo klawiaturę numeryczną.

b) Serwer uwierzytelniania

Jest to oprogramowanie działające na istniejącym lub dedykowanym serwerze z systemem Novell. Pozwala ono na weryfikację użytkownika legitymującego się kartą i PIN-em. Oprogramowanie serwera wymaga odpowiedniej platformy sprzętowej w postaci komputera o mocy zależnej od liczby obsługiwanych użytkowników.

c) Oprogramowanie typu klient

Jest to oprogramowanie instalowane na serwerze (lub serwerach) potrzebne do zapewnienia komunikacji pomiędzy aplikacjami lub procedurami, a modułem serwera uwierzytelniania.

d) Zagadnienia organizacyjne i wdrożenie muszą spełniać wymagania identyczne jak dla systemu Security Dynamics.

zapewniając przy użyciu kryptografii bezpieczną transmisje pomiędzy dwoma odległymi siecami. Szczegółowe cechy produktu zależą od wybranej wersji.

Elementy rozwiązania:

a) Sprzęt

Wymagania :

- Platforma typu Sun SPARC
- System operacyjny SunOS 4.1.3 lub Solaris 2.3 (i wyższe)

b) Oprogramowanie

W oprogramowaniu można wyróżnić następujące moduły:

- Inspection module
- Router control module

W rozbudowanej wersji (network security center) system pozwala na zintegrowane zarządzanie routerami.

Doświadczenia eksploatacyjne

Od momentu wejścia na rynek (połowa 1994 roku) pakiet zyskał sobie opinie godnego zaufania, stabilnego rozwiązania zapewniającego właściwy poziom bezpieczeństwa. Jest on szeroko stosowany na świecie przez średnie i duże prywatne przedsiębiorstwa, telekomunikację, instytucje rządowe, duże stacje telewizyjne, a także świat finansów.
Pozyskane w czasie testów doświadczenia wykazują, że oprogramowanie daje się łatwo zintegrować z systemem uwierzytelniania firmy Security Dynamics - SecurID. Posiada także zadawalające tempo przetwarzania informacji (ang. performance). Dopracowany pod względem graficznym interface pozwala na łatwe definiowanie zasad filtrowania serwisów; jednak konfiguracja mechanizmów NAT w opraciu o istniejącą dokumentacje, okazała się przedsięwzięciem trudnym i stanowiła niemiłą przeciwwagę do klarownego i intuicyjnego interfejsu graficznego modułu zarządzania. Ogólna ocena przydatności rozwiązania potwierdza wysoką ocenę rynkową produktu.

6.3. Szyfrowanie danych

Wprowadzenie

Jednym z podstawowych problemów wynikających z przesyłania informacji poprzez sieci publiczne jest ich bezpieczeństwo. Podstawową metodą zapewnienia poufności danych jest ich szyfrowanie przy wykorzystaniu mocnych kryptograficznie algorytmów. Może ono być realizowane na wiele różnych sposobów, za pomocą różnych urządzeń, algorytmów i w różnych warstwach modelu ISO/OSI.

dzierżawionych czy X.25. System KryptoLan zapewnia także sprzętową dystrybucję kluczy poprzez sieć.

Elementy systemu KryptoLan

System składa się z inteligentnych szyfratorów-brydży zapewniających szyfrowanie sesji pomiędzy dowolnymi adresami IP w sieci korporacyjnej (w zależności od konfiguracji szyfrowanie odbywa się w warstwie 2 modelu OSI - np. Ethernet /LAN lub w warstwie 3 w przypadku sieci WAN). W skład systemu wchodzi także (opcjonalnie) urządzenie pełniące rolę serwera kluczy (CKS). Szyfratory porozumiewają się z serwerem kluczy w celu dystrybucji kluczy szyfrowych. Czas ważności klucza jest ustalany przez administratora systemu.

Główne cechy urządzeń

Głównym elementem systemu jest urządzenie KLB1002 z modułami szyfrującymi KM3 (dla sieci WAN) i KM2 (dla sieci LAN). W przypadkach stosowania technologii dla rozbudowanych struktur sieciowych zalecane jest stosowanie urządzeń CKS (Cntralized Key Server). Urządzenia te są odpowiedzialne za generacje i bezpieczną dystrybucje kluczy wymienianych podczas procedury nawiązywania sesji, a także dają możliwość wykonywania zmian w istniejącej konfiguracji oraz ułatwiają zarządzanie i nadzór co w przypadku sieci rozległych jest czynnikiem istotnym. Urządzenia mogą być monitorowane poprzez SNMP (MIB II).

Opinia o produkcie

KryptoLan firmy SECTRA jest specjalizowanym systemem stosowanym do ochrony transmisji w sieciach teleinformatycznych. Moduł szyfrujący dla potrzeb wewnętrznego rynku został wykonany pod kierunkiem TELII (Swedish Telecom). Szyfrowanie w wersji eksportowej oparte jest o algorytm Triple DES. System jest zaimplementowany w wielu instalacjach na terenie Skandynawii.

6.3.3. CISCO IOS

Wprowadzenie

Inną koncepcją zapewnienia bezpieczeństwa transmisji danych jest wykorzystanie mechanizmów szyfrowania zaimplementowanych na routerach amerykańskiej firmy CISCO Systems. Może one być realizowane w zależności od wersji urządzenia, sprzętowo (dla wyższych wersji sprzętu) lub programowo. Dostępna wersja systemu IOS 11.2 zawiera oprogramowanie szyfrujące wykorzystujące algorytm DES o długości klucza 40 bitów. Jest ono stosowane dla routerów 25xx przy minimalnych wymaganiach 8 MB pamięci flash i 4 MB pamięci DRAM, a także dla routerów 4500, 4500M i 4700M przy wyższych wymaganiach w zakresie pamięci (4 MB Flash, 16-32 DRAM, 4 MB Shared) . Oprogramowanie szyfrujące zawierające dłuższe klucze (patrz Tabela w pkt. 4.2 artykułu *„Wprowadzenie do technologii powdyższających ....”*) jest obecnie dostępne po uzyskaniu licencji od Departamentu Handlu USA.

Doświadczenia eksploatacyjne

System pozwala na tworzenie bezpiecznych sieci korporacyjnych, a także selektywne szyfrowanie pomiędzy wskazanymi adresami IP. Dużą zaletą rozwiązania jest możliwość definiowania, dla par adresów IP (pomiędzy którymi transmisja ma być szyfrowana), także numerów portów (usług)

PROBLEMATYKA ZWIĄZANA Z REALIZACJĄ WIDEOKONFERENCJI DLA URZĘDÓW ADMINISTRACJI PUBLICZNEJ.

Andrzej Maciej Skrzeczkowski

Naukowa i Akademicka Sieć Komputerowa NASK, ul. Bartycka 18, 00-716 Warszawa
E-mail: askrz@nask.pl

Wstęp

Przekazy obrazu i dźwięku są technicznie możliwe już od dawna. Pojawia się więc pytanie, co nowego jest w pojęciu wideokonferencji? Spróbujmy prześledzić to na przykładach. Załóżmy, że wykonane zostało połączenie pomiędzy dwoma punktami (przekaz obrazu i dźwięku). Z punktu widzenia użytkownika taki przekaz jest niczym innym jak dodaniem obrazu do telefonu. Czy jest to już wideokonferencja? Wydaje się, że tak. Bardzo uproszczona i ograniczona, ale jednak umożliwiająca „konferowanie na wizji". Taką transmisję będę dalej nazywał wideoprzekazem.

Czym w takim razie może być „pełna" wideokonferencja? Powinna ona umożliwiać rozmowę wielu osobom, z zapewnieniem kontaktu fonicznego i wizyjnego. Rozwiązanie tego zadania wymaga zapewnienia odpowiednich mechanizmów sterujących (decydujących np. o tym, który obraz jest widoczny u odbiorców). Dodatkowo podczas prowadzenia wideokonferencji przydatna jest możliwość przekazu i wspólnej pracy nad dokumentem. Z punktu widzenia urzędów administracji państwowej niezwykle ważna jest problematyka związana z zapewnieniem odpowiedniego poziomu bezpieczeństwa przekazu. Ważne jest także, aby system wideokonferencyjny działał niezawodnie i był prosty w obsłudze.

Takim postulatom jest w stanie podołać dopiero współczesna technika. Osiągane obecnie szybkości łączy przy jednoczesnym rozwoju współczesnej informatyki dają możliwość zestawienia wideokonferencji o odpowiedniej jakości i użyteczności.

Zespół pracowników NASK był organizatorem lub współorganizatorem kilku pokazów mających na celu zaprezentowanie wideokonferencji jej przyszłym użytkownikom ze sfery administracji publicznej. Pozwoliło to na zebranie wielu doświadczeń i ujawniło problemy z jakimi należy się zmierzyć przystępując do wdrażania systemów wideokonferencyjnych w tych specyficznych przecież warunkach.

Problemy z którymi się stykaliśmy można podzielić na dwie grupy: techniczne i organizacyjne. W takiej właśnie kolejności postaram się je omówić

Problemy techniczne.

Przy organizacji wideokonferencji stawiamy sobie przede wszystkim dwa pytania techniczne: jakimi dysponujemy łączami i jakim dysponujemy sprzętem? Odpowiedź na te pytania pozwala przewidzieć jakość zestawianej transmisji.

Łącza mogą mieć nie tylko różną przepustowość, ale także różnić się ze względu na zastosowaną technologię. Najprostsze połączenie - kanał cyfrowy - jest obecnie rozwiązaniem

dokumenty oraz możliwość wspólnej pracy nad dokumentem przy użyciu komputera (łącze danych dla dzielonych aplikacji).

Istnieje wiele sposobów realizacji miksowania wideokonferencji. Jako przykłady można podać system podziału ekranu między rozmówców, pokazywanie obecnie mówiącej osoby, pokazywanie osoby wybranej ręcznie przez operatora czy dowolne kombinacje tych sposobów. Wybór jednego z nich zależny jest od charakteru wideokonferencji i od indywidualnych upodobań jej uczestników.

Sprzęt do wideokonferencji w zastosowaniach dla urzędów administracji publicznej musi być odpowiednio wyposażony, realizować połączenia w jednolitych standardach, pozwalać realizować konferencje dla wielu stanowisk (np. 49). Ważne jest także, aby urządzenia te miały estetyczny wygląd i były proste w obsłudze.

Przy wyborze sprzętu dodatkowo należy zwrócić uwagę na to, jakie wprowadza on opóźnienia. Czasy poniżej 0,1 sekundy pozwalają prowadzić w zasadzie niezakłóconą rozmowę. Czasy dłuższe powodują nieprzyjemny efekt oczekiwania na odpowiedź rozmówcy, co sprawia wrażenie, że nasz partner w rozmowie nas nie słucha.

Osobną kwestię stanowi przesyłanie dźwięku. Jest to główny nośnik informacji podczas wideokonferencji i dlatego od jego jakości zależy w dużej mierze powodzenie przekazu. Największym problemem jest tu echo i sprzężenia. Ich eliminacja jest możliwa za pomocą odpowiednich algorytmów działania sprzętu oraz przez precyzyjne rozmieszczenie źródeł dźwięku w pomieszczeniach. Należy się także wystrzegać stosowania dodatkowych systemów przesyłania fonii, takich jak radiotelefony czy aparaty przywoławcze.

Problemy organizacyjne.

Organizacja wideokonferencji dla urzędów administracji publicznej jest zadaniem dość trudnym. Wygląda ona inaczej przy konferencjach podczas których wygłaszane są kolejno referaty, a inaczej gdy przewidywana jest dyskusja. Należy także uwzględniać wymogi protokolarne, wymogi poufności i indywidualne upodobania rozmówców.

Pierwszą rafą organizacyjną są pomieszczenia w których odbywają się wideokonferencje. Powinny one być dostosowane wielkością do ilości rozmówców, mieć odpowiednią infrastrukturę techniczną (zasilanie, linie transmisyjne), dzienne albo w ciepłych barwach oświetlenie, dobrą akustykę oraz zapewniać estetyczne tło dla przekazu wizyjnego. Dobranie takich pomieszczeń bywa kłopotliwe szczególnie ze względu na oświetlenie i akustykę. Gdy należy zorganizować połączenia w dużej sali bądź w gabinecie roboczym to problem dodatkowo narasta.

Kolejnym problemem jest ustalenie sposobu umówienia i obsługi wideokonferencji. Problem nie jest mały, bo dla maksymalnej użyteczności omawianego rodzaju łączności ilość osób uczestniczących w przedsięwzięciu jako obsługa powinna być minimalna. Ideałem byłoby, gdyby w czasie trwania wideokonferencji nie musiał być obecny nikt z obsługi. Jak rozwiązać ten problem? Pytanie to pozostaje ciągle otwarte.

Do problemów organizacyjnych należy także zaliczyć fizyczne zabezpieczenie pomieszczeń i łączy. Powinno być ono odpowiednie do charakteru prowadzonych rozmów.

PROBLEMY ROZLICZEŃ W SIECIACH TELEINFORMATYCZNYCH DOŚWIADCZENIA NASK

Andrzej Zienkiewicz

1. Wprowadzenie

Projektując i wdrażając systemy rozliczeń w NASK braliśmy pod uwagę wiele czynników. Najważniejsze w nich to:

- Konieczność możliwie uzasadnionego podziału kosztów utrzymania sieci pomiędzy abonentów z zachowaniem równych praw dla abonentów.

- Realność dokonania rozliczeń w oparciu o możliwe pomiary czy ograniczenia wykorzystania zasobów sieci poprzez abonentów.

- Ekonomia rozliczeń w rozumieniu adekwantych nakładów na rozliczenia stosownie do uzyskiwanych efektów.

Aby jednak przeprowadzić odpowiednie rozważania musimy dokonać analizy systemów telekomunikacyjnych, z którymi NASK się spotyka.

2. Analiza problemu

Coraz więcej osób korzysta z sieci teleinformatycznych nie znając tajników technologii, coraz mniej jest zauroczonych nową techniką, zorientowanych w tej technice entuzjastów. Sądzimy, że nadszedł czas ponownego przypomnienia pewnych ogólnych cech technologicznych różnych usług telekomunikacyjnych oraz wynikających z tego konsekwencji użytkowych. Skłania nas do tego rosnąca liczba reklamacji i pretensji zgłaszanych w wyniku nierealizownia oczekiwań, które w określonych technikach przesyłania nie mogą być spełnione.

Najogólniej usługi telekomunikacyjne możemy podzielić na połączeniowe (connection oriented) oraz bezpołączeniowe (connectionless). Pierwsze przed realizacją usługi wymagają nawiązania połączenia z odbiorcą, drugie takiego nawiązania nie potrzebują. Do pierwszych należy powszechnie znana usługa telefoniczna, ISDN (Integrated Service Data Network), a także połączenia w protokołach HDLC (Highlevel Data Link Control), Frame Relay czy ATM (Asynhronous Transfer Mode) na poziomie łącz logicznych czy X.25 na poziomie sieci. Do drugich należą transmisja radiowa, telewizyjna, a także Ethernet czy FDDI (Fiber Distributed Data Interface) na poziomie łącz logicznych oraz IP (Internet Protocol) na poziomie sieci.

Świadczenie usług w technikach połączeniowych zawsze jest poprzedzone nawiązaniem połączenia. W tym czasie sprawdzana jest możliwość uzyskania kanału fizycznego czy logicznego (istnienie i brak zajętości) oraz dostępność urządzenia końcowego, poprzez które będą świadczone usługi. W przypadku usług telefonicznych jest to sprawdzenie możliwości zestawienia kanału galwanicznego oraz najczęściej odpowiednich kanałów cyfrowych oraz dostępności aparatu końcowego. W przypadku usług ISDN sprawdzana jest możliwość zestawienia kanału cyfrowego oraz dostępność kanału w stacji końcowej. Brak możliwości zestawienia kanału sygnalizuje sygnał zajętości, brak dostępności stacji końcowej brak zgłoszenia tej stacji, np. nikt nie podnosi słuchawki telefonicznej. Sterowanie przepływem informacji w obu przypadkach przejmują użytkownicy, w przypadku telefonu rozmówcy.

wszystkim pozwala na przewidywanie czasu nadania strumieni informacji w określonym czasie. Z tego powodu ATM jako pierwszy protokół przesyłający pakiety informacji nadaje się do transmisji danych wymagających izochronizmu. W kanałach tworzonych przez ATM można przesyłać rozmowy telefoniczne, ruchomy obraz np. video konferencji oraz dane. Jednak podobnie jak we Frame Relay protokół ATM obsługuje warstwę łącz logicznych i zawsze łączy ze sobą uprzednio zdefiniowane punkty. Samo połączenie poprzez ATM nie zapewnia możliwości pracy i przesyłania w sieci otwartej. Do tego są potrzebne protokoły takie jak X.25 czy IP.

Przesyłanie informacji bez uprzedniego nawiązania połączenia jest w swojej istocie proste, jednak w zasadniczy sposób ogranicza możliwości operatora w zapewnieniu odpowiedniej jakości usługi. Większość problemów związanych z jakością przesyłania musi rozwiązać odbiorca i nadawca informacji. Ponieważ nie nawiązuje się połączenia, wobec tego nie istnieje nic takiego jak logiczny kanał przesyłania w sieci telekomunikacyjnej, Jeżeli takiego kanału nie ma, nie można kontrolować poprawności przepływu informacji, ani potwierdzać poprawność odbioru oraz sygnalizować zajętość kanału czy odbiornika. Niemożliwe jest również odzyskiwanie pakietów czy ramek, ponieważ nie ma informacji o ich poprawnym czy niepoprawnym odbiorze. Oczywiście cały czas opisujemy możliwości protokołów komunikacyjnych, które oferuje sieć i jej operator. Stacje końcowe abonenta sieci mogą, oczywiście w ramach nawiązanej sesji, uzupełnić niedostatki działania protokołów sieciowych, ale dzieje się to poza obszarem działania operatora. Wymaga to dodatkowych umiejętności po stronie abonenta lub korzystania z wyspecjalizowanej obsługi lub doradztwa.

Operator radiowy czy telewizyjny może starać się o zapewnienie możliwie silnego sygnału, specjalne kodowanie, właściwe rozmieszczenie stacji nadawczych itp. Nie ma możliwości sterowania przepływem informacji do abonenta, usuwania zakłóceń terenowych czy atmosferycznych, nie ma wpływu na zakłócenia. Zapewnienia właściwego odbioru dokonuje odbiorca działający w konkretnych warunkach. On musi zapewnić odbiornik odpowiedniej klasy zarówno o odpowiednim zakresie pasm odbiorczych, odpowiednich systemach eliminacji zakłóceń itp. Rola operatora polega na rozgłaśnianiu informacji, do których dostęp zapewnia abonent we własnym zakresie.

W sieciach informatycznych bezpołączeniowych procesy przebiegają podobnie, jakkolwiek media przesyłowe narzucają tu specyficzne rozwiązania i cechy użytkowe.

W sieci Ethernet (ISO 802.3) informacja w postaci ramki nadawana jest do wszystkich podłączonych do nośnika szerokopasmowego. Ramka posiada adres odbiorcy ograniczony do jednej sieci. Odbiorca po stwierdzeniu, że ramka jest adresowana do niego ją odbiera, w przeciwnym przypadku pomija. Ponieważ na ten sam nośnik może nadawać wielu nadawców, pojawia się problem rozwiązywania kolizji. Każdy nadawca informacji jednocześnie odbiera informacje z nośnika. Jeśli w czasie nadawania kodu początkowego (preamble), co równa się czasowi propagacji sygnału w sieci o ściśle ograniczonej wielkości, zaobserwuje pojawienie się informacji obcej zaprzestaje nadawania. Oczywiście drugi nadawca zrobi to samo. Obaj oczekują przez okres różny dla wielu stacji i rozpoczynają nadawanie od nowa. Taki sposób postępowania powoduje, że protokół zapewnia znośne usługi w sieci zapełnionej do około 15% przy standardowym wykorzystaniu protokołu. Tym samym efektywna szybkość sieci o przepustowości technicznej 10 Mbps wynosi do około 2 Mbps. Rzeczywiste wielkości są zależne od ilości i sposobu pracy urządzeń dołączonych do sieci, długości ramki itp. czynników, niezależnych od protokołu przesyłania. Jak łatwo zauważyć działanie tego rodzaju sieci jest w dużej części przypadkowe, zależne od chwilowych spiętrzeń transmisji, sposobu pracy oraz ilości urządzeń przyłączonych czyli czynników zewnętrznych w stosunku do działania samej sieci.

Podobnie dzieje się w sieci FDDI, gdzie prawo nadawania jest najczęściej regulowane przekazywaniem znacznika. Jednak brak kanałów logicznych, nie mylić z kanałami uprzywilejowanymi, nie zapewnia pewności transmisji. Wspólnie przez wszystkich

głosu i obrazu. Wadą przejściową jest przystosowanie do pracy w sieciach szybkich, w zasadzie od 155 Mbps w górę, na które nie wszędzie jest zapotrzebowanie, konieczność pracy na szybkich łączach cyfrowych, których jest mało oraz ograniczenie funkcji do tworzenia kanałów logicznych i małe pole adresowe ograniczające wielkość sieci. Pakiet (cell) według protokołu ATM składa się z 5 bajtów nagłówka oraz 48 bajtów informacji, czyli około 10% przesyłanej informacji traci się na sterowanie - reszta może być efektywnie wykorzystana co jest statystycznie wynikiem niezłym, bowiem pamiętać trzeba zawsze o różnicy pomiędzy statystyczną długością pakietów a ich wielkością maksymalną. Nawet przy pakietach długości maksymalnej 1 KB rzeczywiste długości są niewielkie.

Protokół Ethernet oraz protokół FDDI są przeznaczone dla sieci lokalnych lub wydzielonych. Ich znaczenie w sieci rozległej jest niewielkie. Z tego powodu nie będą tu omawiane. Można tylko wspomnieć, że protokół ATM pozwala rozdzielić sieć Ethernet i FDDI w taki sposób, że może być użytkowana jako całość. Często przyzwyczajeni do wolnego działania sieci podzielonej bridge'ami zaskoczeni jesteśmy ilością kolizji w sieci zapominając że szybkość przesyłania ATM jest większa niż w sieci Ethernet.

Protokół IP przeznaczony do sieci globalnej jest obecnie najpopularniejszy wśród użytkowników sieci. Jego podstawową zaletą jest prostota oraz masowość zastosowania. Jednak dla operatora sieci jest on źródłem poważnych kłopotów, które wynikają z jego cech takich jak:
- niemożność ustalenia kto jest inicjatorem przesyłania informacji (nie mylić z nadawcą, który jest zawsze znany),
- niemożność zagwarantowania pewności przesłania wobec tworzenia się losowych kolejek pakietów do przesłania, które w przypadku przepełnienia nie przyjmują kolejno odbieranych pakietów powodując ich gubienie,
- trudność ochrony kanałów przesyłania, które są zmienne.

Protokół ten stwarza szczególnie wysokie wymagania dla abonenta, który musi zapewnić kontrolę przesyłania w zakresie szybkości, zachowania sekwencji oraz odzysku utraconej informacji. Do tego abonent musi sam chronić się przed wykorzystywaniem swoich zasobów przez innych abonentów, jeśli nie chce ponosić konsekwencji pracy innych abonentów na swoich instalacjach komputerowych. Stoi to w zasadniczej sprzeczności z popularnością Internetu i wobec tego słabym przygotowaniem abonentów do tego rodzaju działań. Porównując protokół X.25 oraz IP można zauważyć że Internet wymusza na abonencie wykonywanie funkcji komunikacyjnych stanowiących integralne funkcje protokołu X.25.

Dla przykładu w sieci Internet użytkownicy często korzystają z możliwości ściągania na swój komputer zbiorów danych, programów, stron WWW i tym podobne. Inicjujący pracę użytkownik nadaje stosunkowo niewiele informacji inicjującej, natomiast jego partner wysyła duże ilości pakietów w odpowiedzi na akcję inicjującą. Obserwacja ruchu na poziomie sieciowym nie pozwala na ustalenie, który z partnerów odpowiada, za wywołany ruch w sieci. W innym przypadku abonent ściąga do siebie informacje z serwera przyłączonego do szybkiej sieci, nadającego z duża szybkością zbiory bez sterowania szybkością nadawania na przykład przez nadawanie znaczników i potwierdzanie odbioru. Jeśli przepustowość połączeń w kierunku odbiorcy maleje, to znaczna część przesyłanej informacji przepełni kolejki na urządzeniach przełączających i będzie zgubiona. Jeszcze inaczej może się zdarzyć, że kilku użytkowników sieci rozproszonych po świecie zechce mieć w tym samym okresie czasu dostęp do abonenta nie dysponującego odpowiednio przepustowym torem łączności, prawdopodobne wtedy jest przepełnienie kolejek i zgubienie części informacji. Jak widać protokół IP nie zawiera mechanizmów zapewniających jakość przesyłania. Przeciwdziałanie może być tylko ogólne, polegające na podnoszeniu jakości i przepustowości sieci w ogóle.

Najlepiej dostosowany do taryfikacji jest protokół X.25 powstający przy udziale organizacji telekomunikacyjnych. Ponieważ jest nawiązywane połączenie można ustalić inicjującego. Zhierarchizowany adres zawiera w pierwszej części trzycyfrowy znormalizowany kod kraju,

połączeń poprzez sieci dwóch czy więcej operatorów rozliczenia wykonuje się indywidualnie. Zachowana musi być jednak zasada jednolitego płacenia za kanał niepodzielony. Abonent nie może ponosić konsekwencji podziału swojej linii ponosząc opłaty do i od granicy działania operatorów co istotnie podnosiłoby opłaty, ponieważ opłata jest degresywnie powiązana z długością kanału.

W sieci ATM na razie problem nie istnieje, ponieważ nie został postawiony. W jedynym przypadku sieci ATM operatora NASK i operatora ICM nie ma jeszcze kanałów poprzez dwie sieci. Jeśli takie zapotrzebowanie wystąpi rozliczenia powinny być takie same jak w przypadku sieci Frame Relay.

Największe problemy rodzi rozliczenie operatorów Internetu, który jest największą działającą siecią, ale był tworzony dla zupełnie innych celów niż obecnie realizowane. Zwrócenie uwagi na interesy abonentów jest tu szczególnie ważne i z tego powodu, że to abonent musi sam chronić się przez skutkami połączeń i oddziaływań abonentów innej sieci, ponieważ protokół IP nie posiada odpowiednich mechanizmów. Najważniejsza dla abonenta jest konieczność ponoszenie opłat za działanie abonenta innej sieci oraz zapewnienie kontroli efektywnego przepływu informacji.

Nie ma na świecie jednego modelowego sposobu rozliczeń operatorskich. Na ogół panuje zasada, że „mniejszy" płaci za dołączenie „większemu". W Polsce nie ma jeszcze wypracowanego systemu rozliczeń i powstanie on najprawdopodobniej w wyniku negocjacji pomiędzy operatorami z uwzględnieniem opinii i reakcji abonentów.

Sprawa rozliczeń międzyoperatorskich staje się jednak coraz bardziej pilna. Z tego też względu zdecydowaliśmy się na zaproponowanie systemu rozliczania się za ruch krajowy innym operatorom dołączonym do sieci NASK, którzy posiadają własne łącza międzynarodowe.

Oczywistym jest, że przesłanie informacji poprzez dwie sieci różnych operatorów kosztuje więcej niż przesłanie tylko w ramach jednej sieci. Zwiększony ruch, będący wynikiem połączenia obu sieci, może w przyszłości spowodować obniżkę jednostkowych kosztów przesyłania u obu operatorów, ale w konkretnym miejscu i czasie koszt będzie większy. Wypowiadane czasami opinie na temat kompensacji wzajemnych opłat, które przy zbilansowanym ruchu prowadzą do kalkulacyjnego zaniku kosztów są ekonomicznie błędne. Przenoszą one rozwiązania z innych sieci, przede wszystkim X.25, i z innych systemów rozliczeń na grunt Internetu i tworzą pozór, że przy pomocy odpowiedniej manipulacji rozliczeniami można uniknąć kosztów wynikających z ponoszonych opłat, co oczywiście jest nonsensem.

W sieci Internet, praca odbywa się bez zestawiania połączeń (connectionless), na zasadzie przesyłania oddzielnie adresowanych datagramów. Posiada to wielorakie konsekwencje, z których najważniejszymi są:

- niemożność ustalenia kto jest inicjatorem przesyłania informacji (nie mylić z nadawcą, który jest zawsze znany),
- niemożność zagwarantowania pewności przesłania wobec tworzenia się losowych kolejek pakietów do przesłania, które w przypadku przepełnienia nie przyjmują kolejno odbieranych pakietów powodując ich gubienie,
- trudność ochrony kanałów przesyłania, które są zmienne.

Wydawałoby się, że rozwiązaniem problemu ustalania inicjatora sesji transmisji może być tunelowanie IP poprzez protokół X.25 przynajmniej na styku międzyoperatorskim. Daje to jednak fatalne skutki techniczne i ekonomiczne. Każdy nadchodzący z dowolnej strony datagram otwiera nowe połączenie, pakiety IP dzielone są na mniejsze po 128 B - szybkość dramatycznie spada, opłaty gwałtownie rosną a i tak nie wiadomo kto zainicjował transmisję sesji a nie datagramu.

W sieci Internet użytkownicy często korzystają z możliwości ściągania na swój komputer zbiorów danych, programów, stron WWW i tym podobne. Inicjujący pracę użytkownik nadaje stosunkowo niewiele informacji inicjującej, natomiast jego partner wysyła duże ilości pakietów w odpowiedzi na akcję inicjującą. Obserwacja ruchu na poziomie sieciowym nie pozwala na ustalenie, który z

- punkt przyłączenia sieci znajduje się zawsze na terenie abonenta, podczas gdy przy samej usłudze Frame Relay może znajdować się na porcie sieci NASK,

- usługa obejmuje również utrzymanie oraz ewentualnie dzierżawę urządzenia przyłączającego (routera) na terenie abonenta.

Usługa Frame Relay, świadczona łącznie z UBN (Unisource Business Networks), przekracza granice kraju i obejmuje rutynowo kraje skandynawskie oraz część Europy obsługiwaną poprzez UNISOURCE, a po uzgodnieniu dowolny, osiągalny kraj na świecie. Przy świadczeniu usługi transgranicznej z zasady poszerza się jej zakres o analizę i ewentualne zmodyfikowanie instalacji klienta, zestawienie i wyposażenie łącza oraz stały serwis polegający na utrzymaniu całości połączenia w sprawności.

Dla abonentów grupowych, z którymi zawiera się umowy lub porozumienia łączne, nie tworzy się cennika. Postępowanie jest indywidualne i polega na określeniu kosztów udostępnianej infrastruktury oraz podzieleniu tego kosztu pomiędzy abonentów. Stosuje się tu dwa odmienne kryteria. Dla sieci Frame Relay podstawą podziału jest najczęściej suma przepustowości CIR udostępnianych kanałów logicznych. Dla sieci ATM, która jest z zasady multimedialna stosuje się podział według pasma dostępu.

NASK oferuje połączenia do dwóch sieci otwartych X.25 oraz IP. W pierwszym przypadku zasady taryfikacji są znane, powszechnie akceptowane i stosowane. System rozliczeń między operatorskich jest unormowany w skali międzynarodowej i regułowany odpowiednimi umowami dwu i wielostronnymi. W tym zakresie cennik NASK nie odbiega co do istoty od cenników innych operatorów.

NASK pierwszy udostępnił usługi IP (Internet Protocol) w Polsce oraz pierwszy tworzył cenniki w tym zakresie. Nadal sądzimy, że mamy w tym zakresie największe możliwości oraz doświadczenia dobre i złe. Status NASK pozwala nam na elastyczne zachowania, na które operator wielki, angażujący wielkie kapitały, typu Telekomunikacja Polska SA, nie może sobie pozwolić. Nasz potencjał intelektualny, organizacyjny i ekonomiczny wykorzystujący niewielki, ale bardzo zróżnicowany kapitał pozwala na podejmowanie znacznego ryzyka w poszczególnych rodzajach działalności, bez większego ryzyka dla całości przedsiębiorstwa.

Dla abonentów drobnych dołączonych poprzez komutowane linie telefoniczne, które istotnie ograniczają możliwości abonenta NASK stosuje opłaty ryczałtowe za 29 godzin dostępu w ciągu miesiąca plus opłaty za czas dodatkowy. Praktycznie wszyscy abonenci mieszczą się w limicie i nawet ci, którzy zamówili początkowo dostęp nielimitowany z tego się wycofali. Dla abonentów łączących się ze skrzynkami pocztowymi poprzez linie telefoniczne innych operatorów (TP SA) NASK stosuje nadzwyczajną obniżkę cen do 60% pełnej usługi. NASK nie dopuszcza dostępu do sieci bez posiadania stałego adresu, conajmniej skrzynki pocztowej. Taka usługa świadczona na przykład przez TP SA opłacana jest przez ceny impulsów telefonicznych, co w przypadku NASK nie jest dostępne.

Dla abonentów większych NASK stosuje opłatę połączoną z wielkością ruchu całkowitego generowanego w sieci przez abonenta. Zasada ta, atakowana powszechnie przez środki masowego przekazu, ostała się pomimo wielu wad. Jej podstawową zaletą, że najlepiej dzieli koszty utrzymania sieci pomiędzy abonentów, zapewnia relację opłat z usługami, co daje środki na zapewnienie rozwoju sieci proporcjonalnie do potrzeb oraz daje świadomemu abonentowi wykonanie rachunku opłacalności korzystania z usług telekomunikacyjnych. Jest ona atakowana przede wszystkim przez tych, dla których taki rachunek jest niewygodny lub zagrażający ich interesom. W wyniku globalnych nacisków w cenniku NASK pojawił się wariant opłaty za pasmo

obejmującej limit ruchu oraz skutki jego przekroczenia w pierwszym miesiącu ograniczające się do powiadomieniu abonenta o fakcie. Powiadomiony abonent może ograniczyć ruch lub odpowiednio zmienić parametry umowy z operatorem.

Od czasu, gdy NASK był jedynym operatorem Internetu w Polsce pozostał zwyczaj nie pobierania opłat za utrzymanie usługi DNS (Domain Network Service). Pobierana opłata związana była jedynie z wprowadzeniem adresów i nazw do serwera. Dzisiaj, kiedy NASK jest jednym z wielu dostarczycieli usług Internetowych, w sieci NASK odbywa się znaczący ruch związany z obsługą obcych abonentów. Ponieważ ruch ten odbywa się na koszt abonentów NASK, wprowadzono nowość w postaci opłaty za utrzymanie serwisu dla abonentów innych operatorów.

NASK do tego czasu nie specjalizuje się w usługach związanych z WWW. Ten dział rozliczeń dopiero w przyszłości będzie musiał być potraktowany bardziej serio, o ile oczywiście NASK zdecyduje się na świadczenie usług w szerszym zakresie.

Warszawa maj 1997 r.

Opłata za ruch

Przeciwstawieniem wariantu ryczałtowego jest obciążanie abonenta na podstawie zarejestrowanego ruchu (słowo „zarejestrowany" zostało użyte świadomie, by nie przesądzać z góry, jaki rodzaj ruchu będzie brany pod uwagę przy taryfikacji).

Istotną cechą tego wariantu jest bezpośrednie przeniesienie na abonenta kosztów związanych z rosnącym ruchem.

Nie sposób w tym momencie pominąć problemy związane z pomiarem ruchu w Internecie. Jak wiadomo protokół IP jest bezpołączeniową usługą telekomunikacyjną tj.nie zestawia kanałów przesyłu pomiędzy nadawcą i odbiorcą przekazu, a także nie sprawdza ich zajętości. W efekcie może następować utrata części przesyłanej informacji, powodując rozbieżność pomiędzy statystykami ruchu abonenta i operatora. W praktyce przyjmuje się, że zajętość łącza nie powinna przekraczać 30 %. Nie jest także możliwe prześledzenie, kto inicjuje transfer; mankament o dużym znaczeniu w epoce rozwoju WWW.

Przy wyborze rodzaju ruchu stanowiącego podstawę obciążania abonentów zwykle stosowane są następujące warianty:

- ruch przychodzący
- ruch wychodzący
- ruch całkowity - nadawca i odbiorca płacą po połowie za ruch,

Opłaty mogą być naliczane za ruch bez rozróżniania (ruch nieważony), bądź też zróżnicowane w zależności od tego, czy jest to ruch lokalny, krajowy, czy też zagraniczny (ruch ważony).

Pierwszy z nich może być mierzony w jednym punkcie na styku z abonentem. Drugi natomiast wymaga pomiaru w trzech punktach, a mianowicie na styku z siecią międzynarodową, na styku z siecią krajową

Każdy z wariantów powoduje inny rozkład obciążeń : abonenci udostępniający swoje zasoby w postaci np. baz danych zyskują najbardziej przy opłatach za ruch przychodzący.

Istotnym uwarunkowaniem decydującym o sposobie rozliczania ruchu zagranicznego jest fakt że USA nie płacą za przyłączenie się do „reszty świata"- za ruch zagraniczny obciążany jest więc wyłącznie krajowy uczestnik transferu. Prezentowany poniżej wariant opłaty za ruch całkowity jest więc dostosowany do tej sytuacji.

SYMULACJA

Do symulacji wykorzystano bazę danych abonentów zawierającą informacje n.t. wygenerowanego ruchu całkowitego w rozbiciu na lokalny, miejski oraz zagraniczny oraz ruch przychodzący i wychodzący w analogicznym podziale.

Podstawą symulacji jest założenie, że niezależnie od wybranego wariantu taryfikacji przychód NASK pozostaje na niezmienionym poziomie. Zmienia się jedynie rozkład płatności pomiędzy abonentami.

- 1MB ruchu zagranicznego = 4MB ruchu krajowego = 8 MB ruchu lokalnego (porównaj z cennikiem NASK)

Jest to logiczna konsekwencja solidarnego podziału kosztów między abonentów krajowych i lokalnych oraz całkowitej opłaty za ruch zagraniczny.

3. **Ruch przychodzący nieważony**

Podstawa obliczeń: Suma opłat za ruch dzielona przez sumę nieważonego ruchu przychodzącego.

Całkowita opłata za ruch (PLN)	**789163**
Nieważony przychodzący ruch (MB)	**888360**
Opłata jednostkowa (PLN/MB)	**0,89**

4. **Ruch przychodzący ważony**

Obliczenia jak w p.3, z uwzględnieniem wag ruchu.

Całkowita opłata za ruch (PLN)	**789163**
Ważony ruch przychodzący (MB)	**458749**
Opłata jednostkowa (PLN/MB)	**1,72**

Oba warianty opłat za ruch przychodzący mogą spotykać się z zarzutem, że abonent musi płacić za ruch przesłany do niego bez jego woli (przykład „bombardowania" pocztą elektroniczną). Obawy te są praktycznie nieuzasadnione, jako że gros ruchu stanowią obecnie strony WWW „ściągane" przez abonentów.

5. **Ruch wychodzący nieważony**

Wariant ten zamieszczony został głównie dla ilustracji. Jest on bowiem nieefektywny ekonomicznie ze względu na konieczność pokrywania w całości kosztów ruchu zagranicznego przez abonentów krajowych . Napotyka na problemy związane ze zbilansowaniem *ex ante* kosztów informacji (głównie WWW) ściąganej przez abonentów krajowych z przychodami opartymi o ruch od nich wychodzący.

Całkowita opłata za ruch (PLN)	**789163**
Ruch wychodzący nieważony (MB)	**855770**
Opłata jednostkowa (PLN/MB)	**0,92**

Aneks

Wyliczenie - wariant dotychczasowy

Nr klienta	przepływność	Ruch lokalny	R.krajowy	R.zagraniczny	R. całk.nieważony	R.całk.ważony	ABONAMENT	PONAD ABONAM	TOT.OPŁ.
1	10000	795213	43414	46484	885111	156739	3600	176567	180167
2	10000	159711	35022	54851	249584	83570	3600	106010	109610
3	2000	776	41911	44364	87051	54939	1050	70041	71091
4	10000	9302	19932	26574	55808	32720	3600	40921	44521
5	512	5608	6215	11437	23260	13692	750	17325	18075
6	2000	4239	4589	9189	18017	10866	1050	13628	14678
7	128	0	14341	4528	18869	8113	2400	9744	12144
8	512	1660	4653	7559	13872	8930	750	11230	11980
9	128	0	5817	6380	12197	7834	2400	9387	11787
10	512	385	3812	6396	10593	7397	750	9268	10018

Ruch przychodzący (IN) oraz wychodzący (OUT) w MB

	Ruch_całkowity		Ruch_krajowy		Ruch_zagraniczny		Ruch lokalny		Ruch ważony	
	IN	OUT	IN	OUT	IN	OUT	IN	OUT	IN	OUT
1	312449	572661	16116	27298	26692	19792	269642	525570	102160	164834
2	201146	48436	19958	15063	37476	17375	143712	15998	83383	28906
3	33222	53829	35714	40624	17780	28767	0	0	35636	49079
4	20368	35439	5245	14687	8994	17580	6129	3173	13149	25716
5	14759	8499	2846	3369	7965	3471	3947	1660	10375	5570
6	16102	1914	3882	706	8381	808	3839	400	11282	1261
7	13752	5115	9883	4457	3869	658	0	0	8811	2887
8	4302	9568	963	3690	2459	5100	881	779	3160	7139
9	9171	3025	3851	1966	5320	1059	0	0	7246	2042
10	3728	6863	826	2985	2226	4170	676	0	2808	5663

Opłata wg. symulowanych wariantów

	Ryczałt	R.całk.nieważony	Przych.nieważ.	Przych.waż	Wych.nieważ.	Wych.waż
1	45432	399019	277560	175740	528089	365831
2	45432	112516	178685	143439	44667	64155
3	9086	39244	29512	61303	49640	108926
4	45432	25159	18094	22619	32681	57074
5	2326	10486	13111	17848	7838	12362
6	9086	8122	14304	19407	1765	2798
7	582	8506	12216	15157	4717	6406
8	2326	6254	3822	5436	8824	15845
9	582	5499	8147	12464	2790	4532
10	2326	4775	3312	4831	6329	12567

- usługi przetwarzania danych
- systemy rozsiewcze telewizyjne, radiowe i danych
- procesy rozproszone.

W relacji usługodawca - klient istotną rolę w rozwoju usług multimedialnych odgrywa terminal użytkownika. Należy się spodziewać, że w okresie kilku, kilkunastu lat terminal sieciowy użytkownika zostanie zunifikowany. W tym celu konieczne jest opracowanie standardowego styku opartego o ideę sieci wirtualnej. Umożliwi on świadczenie usług multimedialnych przez wszystkie sieci dostępowe i tranzytowe w ten sam sposób. Obserwowany jest trend do wdrażania w sieciach tranzytowych standardu ATM. Przy zachowaniu różnorodności interfejsów sieci dostępowych (ISDN, xDSL, łącza radiowe, łącza telewizji kablowej, dedykowane łącza cyfrowe) należy się spodziewać realizacji usług o zbliżonej jakości.

Można przedstawić wizję sieci szerokopasmowej , w której możliwe będzie kreowanie sieci wirtualnych udostępniających usługi multimedialne w sposób niezależny od lokalizacji usługodawcy i klienta. Duży wpływ na ostateczną formę oferowanych usług będą miały wdrożenia realizowane obecnie w sieci Internet.

3. Transmisja sygnałów muiltimedialnych

Usługi multimedialne charakteryzują się dużym zapotrzebowaniem na pasmo i w przypadku usług czasu rzeczywistego wrażliwością na fluktuacje opóźnienia. Wymagania stawiane sieciom do transmisji danych niosących dźwięk i obraz są inne niż do transmisji danych komputerowych. Najtrudniejsze w realizacji są transmisje multimedialne realizowane w czasie rzeczywistym, związane z przesyłaniem ruchomego obrazu.

Podstawowe parametry sieci transmisji danych to:

- dostępne pasmo (ang. Bandwidth),
- czas opóźnienia (ang. Latency),
- fluktuacje opóźnienia (ang. Jitter).

Czas opóźnienia i fluktuacje opóźnienia są dobrze zdefiniowane dla sieci z komutacją łączy. W sieciach z komutacją pakietów opóźnienie i fluktuacje opóźnienia kompensuje się przez inteligentne buforowanie sygnału. Kompensacja jest możliwa jeżeli pasmo wymagane dla transmisji jest znacznie mniejsze od dostępnego pasma kanału transmisyjnego.

Zmniejszenie zapotrzebowania na pasmo realizuje się przez kompresję cyfrowych sygnałów wizji i fonii przed wprowadzeniem ich do kanału transmisyjnego. Zalecanym standardem do zastosowań w kompresji sygnałów wizyjnych jest MPEG 2 (opracowany przez Motion Picture Expert Group). System kodowania sygnałów wizyjnych jest zdefiniowany dla różnych algorytmów wybierania obrazów:

- dla telewizji o dużej rozdzielczości obrazu HDTV,
- dla telewizji konwencjonalnej,
- dla telewizji o małej rozdzielczości obrazu.

Określa on zasady kodowania sygnałów wizyjnych z użyciem różnych metod kompresji, wykorzystujących:

- dyskretną transformację kosinusoidalną,
- prognozowanie,
- kompensację ruchu.

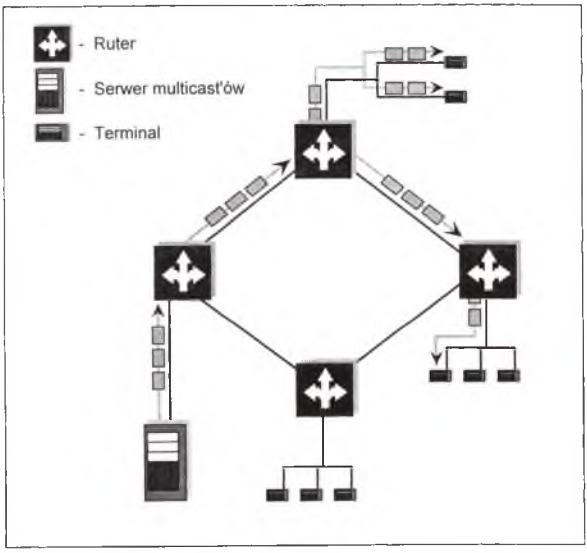
Strumień danych potrzebny do przesłania programu telewizyjnego zależy nie tylko od rodzaju wybierania, lecz również od rodzaju programu. Przykładowe wielkości strumienia danych po kompresji MPEG 2 w zależności od rodzaju programu dla telewizji konwencjonalnej przedstawiono w *Tabeli 1.*

protokołami wyboru trasy (ang. routing), nie mogą sprostać wymaganiom stawianym przez usługi multimedialne.

Realizacja transmisji multimedialnych w Internecie związana jest z powstaniem nowych protokołów i technik transmisji danych. Rozwój Internetu ewoluuje w kierunku zapewnienia gwarantowanej jakości transmisji (Quality of Service).

W Internecie wykorzystywane są różne mechanizmy obniżające wpływ nierównomiernej transmisji, dużych opóźnień i małej szerokości pasma na jakość transmitowanego sygnału wizji i fonii. Aplikacje wykorzystują w tym celu buforowanie i kompresję sygnału.

W celu zminimalizowania wykorzystania pasma stosuje się mechanizm rozsiewczego rozsyłania ramek jednocześnie do wszystkich odbiorców *(Rys. 1).* Ramki multicast'owe są powielane przez rutery tylko na drodze do wybranej grupy użytkowników. Zarządzanie tym procesem realizowane jest przez protokół IGMP (ang. Internet Group Management Protocol) W procesie wyboru trasy (ang. routing) wykorzystywany jest jeden z protokołów: DVMRP (ang. Distance Vector Multicast Routing Protocol), MOSPF (ang. Multicast Open Shortest Path First) lub PIM (ang. Protocol Independent Multicast). Przykładem sieci wykorzystującej transmisję multicast'ową jest sieć MBONE, w której realizowane są usługi rozsiewcze TV/Radio, oraz usługi telekonferencyjne. Sieć ta nie gwarantuje utrzymania parametrów QoS.



Rys. 1. Przykład realizacji transmisji multicast'owej

Dla zapewnienia odpowiedniej jakości transmisji sygnałów wizji i fonii powstają nowe protokoły sieciowe. Przykładem może być protokół wyboru trasy RSVP (ang. Resource Reservation Protocol) opracowywany w USC Information Sciences Institute USA, który umożliwia utrzymanie stałych parametrów transmisji takich jak : pasmo i opóźnienie sygnału. Obecnie dostępna jest wersja 14 tego protokołu pracująca w systemach zgodnych z UNIX'em. Można spotkać implementacje tego protokołu w niektórych ruterach. Aby wykorzystać właściwości protokołu RSVP konieczna jest interakcja ruterów z terminalami, pomiędzy którymi realizowana jest transmisja o gwarantowanych parametrach .

DETEKCJA INFORMACJI UŻYTECZNEJ W SIECIACH KOMPUTEROWYCH

Waldemar E. Grzebyk, Jarosław M. Janukiewicz

Naukowa i Akademicka Sieć Komputerowa
Zakład Telekomunikacji
50-327 Wrocław, ul. Janiszewskiego 7/9, tel./fax: 219529

1. Wprowadzenie

Detekcja informacji użytecznej jest to proces fizyczny mający na celu odtworzenie sygnału źródłowego z sygnału, który wydostaje się na zewnątrz urządzenia jedną z dróg:

- przez sprzężenia pojemnościowe (składowa elektryczna pola elektromagnetycznego),
- przez sprzężenia indukcyjne (składowa magnetyczna pola elektromagnetycznego),
- przez wypromieniowanie fali elektromagnetycznej,
- przez sprzężenia galwaniczne (prąd płynący w przewodach).

Współczesne metody detekcji skrajnie słabych sygnałów obarczonych szumami i zakłóceniami o dużej intensywności umożliwiają wykrycie sygnałów o poziomach mniejszych o ponad 40 dB od poziomu szumów cieplnych w obwodach elektrycznych. W systemach teleinformatycznych detekcja transmitowanych sygnałów jest możliwa dzięki emisji wielu składowych widma transmitowanego sygnału.

W Zakładzie Naukowym Telekomunikacji NASK prowadzone są prace dotyczące określenia możliwości detekcji informacji użytecznej oraz sposobów minimalizacji rozpraszania elektromagnetycznego w sieciach komputerowych. W artykule przedstawiono wyniki tych prac oraz wnioski z przeprowadzonych badań.

2. Analiza rozpraszania elektromagnetycznego pod względem charakterystyk czasowych i częstotliwościowych

Ze względów czasowych można rozróżnić rozpraszanie elektromagnetyczne:

- ciągłe,
- krótkotrwałe (zwane także zakłóceniami impulsowymi lub trzaskami radioelektrycznymi).

Rozpraszanie ciągłe w urządzeniach stanowiących elementy sieci komputerowych może być związane z pracą zasilaczy, układów zegarowych, układów synchronizacji i odchylania monitora.

Rozpraszanie krótkotrwałe jest na ogół związane z różnego rodzaju operacjami przełączania wewnątrz urządzeń lub sterowania urządzeniami zewnętrznymi. Można tu wyróżnić operacje przesyłania bloków danych do i z pamięci, sterowanie pracą drukarek, pamięci dyskowych itd.

Pod względem charakterystyk częstotliwościowych (widmowych) można rozróżnić dwie zasadnicze klasy rozpraszania elektromagnetycznego:

- rozpraszanie wąskopasmowe
- rozpraszanie szerokopasmowe.

Te ostatnie można podzielić na rozpraszanie o widmie:

- ciągłym - np. związane z iskrzeniem, ulotem w układzie wysokiego napięcia w monitorze),
- prążkowym - związane z kolejnymi harmonicznymi przebiegów okresowych (np. sygnały zegarowe i synchronizujące) lub przebiegów sinusoidalnych zniekształconych na elementach nieliniowych.

Rozpraszanie wąskopasmowe w sensie pojedynczych częstotliwości praktycznie w urządzeniach cyfrowych nie występuje.

promieniowania ciał niebieskich, Słońca, Ziemi, odległych wyładowaniami atmosferycznych, emisji odległych służb radiowych i oddziaływania odległych urządzeń energoelektrycznych. Wszystkie źródła zakłóceń fluktuacyjnych współdziałają w podobny sposób w wytwarzaniu ciągłego w czasie procesu stochastycznego, który daje w efekcie nieprzerwany szum. Proces ten jest na ogół stacjonarny i ergodyczny.

3.1.2. Ochrona przed zakłóceniami w torze pomiarowym

Przed zakłóceniami energetycznymi i pochodzącymi od urządzeń nadawczych oraz radiolokacyjnych widmo elektromagnetyczne powinno być chronione na drodze administracyjnej za pomocą odpowiednich norm krajowych i międzynarodowych. Normy te nakładają na użytkowników obowiązek stosowania urządzeń zapewniających spełnienie wymogów kompatybilności elektromagnetycznej. Przed zakłóceniami impulsowymi zabezpieczamy się stosując odpowiednie rozwiązania układowe i technologiczne (np. zastosowanie filtrów i ograniczników w odbiornikach). Przed szumem fluktuacyjnym ze względu na zjawiska, które go wywołują, kanał przesyłowy tym sposobem nie może być zabezpieczony. Jedyną drogą jest poszukiwanie systemów, które by mogły osłabić zakłócający wpływ szumu fluktuacyjnego.

Sygnał elektryczny niosący wiadomość użyteczną przedstawia dla odbiorcy proces losowy. Proces ten może być ziarnisty lub ciągły w sensie wartości jednego lub kilku parametrów sygnału. Sam fakt, że przebieg jest losowy nie może być przeszkodą w bezbłędnym odbiorze przekazywanej wiadomości, dopóki nie zostanie on skażony niekontrolowanymi zniekształceniami i zakłóceniami na drodze przesyłowej Skutek zniekształceń i zakłóceń jest taki, że w systemach cyfrowych zostaje odebrany nie ten element zbioru skończonej ilości wiadomości, który był nadany w rzeczywistości, a w systemach ciągłych odebrany przebieg nie odpowiada ściśle nadanemu. W tych warunkach powstaje problem stworzenia takiego układu odbiorczego, który by w sposób najlepszy poddawał obróbce odbierane sygnały, w sensie zapewnienia granicznie osiągalnej wierności odbioru nadanej wiadomości. Taki układ nazywamy odbiornikiem optymalnym.

3.2. Metody pomiaru

Warunkiem powtarzalności i porównywalności wyników pomiarów jest:

- stacjonarność procesów zachodzących w badanym źródle rozpraszania informacji użytecznej,
- jednoznaczne określenie metod pomiarowych. .

Poziom rozpraszania informacji użytecznej zależy od warunków pracy badanego urządzenia lub systemu takich jak:

- warunki propagacyjne,
- temperatura otoczenia,
- napięcie zasilania itp.

Pomiarów należy więc dokonywać w ściśle określonych warunkach, w miarę możliwości odpowiadających warunkom normalnej eksploatacji badanego urządzenia, systemu. Dla uzyskania poprawnych wyników pomiarów konieczne jest wyeliminowanie wpływu zakłóceń zewnętrznych, lub sprowadzenie ich do poziomu odpowiadającego warunkom normalnej eksploatacji badanego źródła rozpraszania informacji użytecznej

Zasady przeprowadzania pomiarów określają odpowiednie normy i zalecenia dotyczące kompatybilności elektromagnetycznej

W Europie Zachodniej podstawę w dziedzinie kompatybilności elektromagnetycznej stanowi wytyczna (ang. directive) 89/336/EEC opublikowana w Oficjalnym Dzienniku Unii Europejskiej (ang. Official Journal on the European Union). Na podstawie tej wytycznej wraz z uzupełnieniem 92/31/EEC oraz na bazie normy CISPR 22 (ang. Internacional Special Committee of Radio Interference) powstał harmonizowany standard EN 550022 (tzn. zwierający harmonizowane procedury testowe i wzorce odniesienia). Określa on wartości graniczne oraz opisuje metody

3.2.2. Pomiar mocy promieniowanej

Zamiast pomiaru natężenia pola można zastosować równoważne metody laboratoryjne. Dla urządzeń, których wymiary są małe w stosunku do długości fali promieniowanych zakłóceń, została opracowana metoda pomiaru mocy zakłóceń. W przypadku tego typu urządzeń głównym źródłem promieniowania jest przewód sieciowy lub sygnałowy, w którym rozchodzi się składowa niesymetryczna prądu zakłóceń. Do pomiaru mocy zakłóceń stosuje się specjalne urządzenie pomocnicze tzw. cęgi absorpcyjne lub cęgi prądowe. Metoda polega na pomiarze natężenia prądu zakłóceń płynącego przez znaną impedancję obciążenia w warunkach dopasowania. Funkcje układu dopasowującego spełnia odpowiedniej długości przewód sygnałowy. Kompensowana jest w ten sposób składowa urojona impedancji, nie ma jednak możliwości dopasowania składowych rzeczywistych impedancji źródła i obciążenia.

W praktycznej realizacji powyższej metody impedancję obciążenia stanowią cęgi absorbcyjne lub cęgi prądowe. Poprzez przesuwanie cęgów wzdłuż przewodu sygnałowego można skompensować składową urojona impedancji. Pomiaru prądu w.cz. dokonuje się miernikiem zakłóceń bezpośrednio na wyjściu cęgów.

Wartość napięcia zmierzonego w położeniu odpowiadającym pierwszemu maksimum wskazań (po uwzględnieniu współczynnika korekcyjnego dla danych cęgów) określa moc badanego źródła zakłóceń. Cęgi absorbcyjne są kalibrowane przy znanym obciążeniu w jednostkach mocy.

4. Analiza metod detekcji informacji użytecznej w sieciach komputerowych

Przy analizie procesu detekcji informacji użytecznej możemy zdefiniować dwa pojęcia kanału podstawowego i kanału podsłuchującego. Pierwszym pojęciem określamy drogę, którą sygnał powinien być przesyłany, drugie pojęcie określa drogę, którą sygnał wydostaje się na zewnątrz kanału podstawowego.

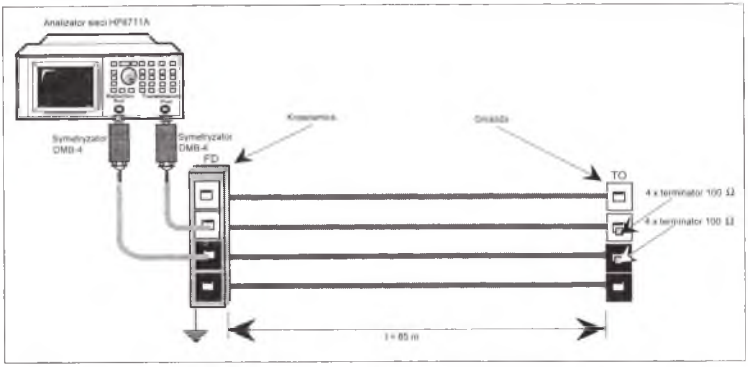
Pierwszym etapem analizy metod detekcji informacji użytecznej w sieciach komputerowych jest określenie potencjalnych źródeł sygnału użytecznego. Potencjalnymi źródłami informacji ze względu na możliwość detekcji w sieciach komputerowych są:

- monitory ekranowe komputerów (informacja na monitorach wyświetlana jest w postaci jawnej),
- okablowanie (informacja przesyłana w kablach jest w postaci sygnałów elektrycznych o znanej strukturze ramek).

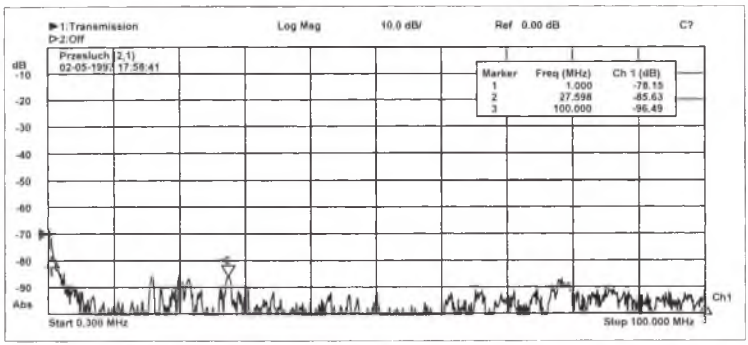
Monitory ekranowe komputerów są źródłem niepożądanego promieniowania elektromagnetycznego związanego głównie z obwodami odchylania oraz z treścią obrazu na ekranie. Promieniowanie to rozciąga się w bardzo szerokim zakresie częstotliwości. Może ono być odebrane z dość znacznej odległości od źródła. Po odpowiedniej obróbce (m.in. wzmocnieniu, filtracji, zmianie fazy) istnieje realna możliwość odtworzenia obrazu na innym monitorze ekranowym. Schemat blokowy przykładowego systemu detekcji przedstawiono na Rys. 1.

Kable miedziane stosowane w sieciach komputerowych są również źródłem promieniowania elektromagnetycznego związanego z transmisją sygnałów elektrycznych. Promieniowanie elektromagnetyczne zajmuje zakres częstotliwości zależny od stosowanej techniki transmisyjnej (Ethernet, FastEthernet, ATM). Znajomość charakterystyki transmitowanych sygnałów, zjawisk zachodzących podczas propagacji fal elektromagnetycznych stwarza realną możliwość odtworzenia sygnału źródłowego. Schemat blokowy przykładowego systemu detekcji przedstawiono na Rys. 2 .

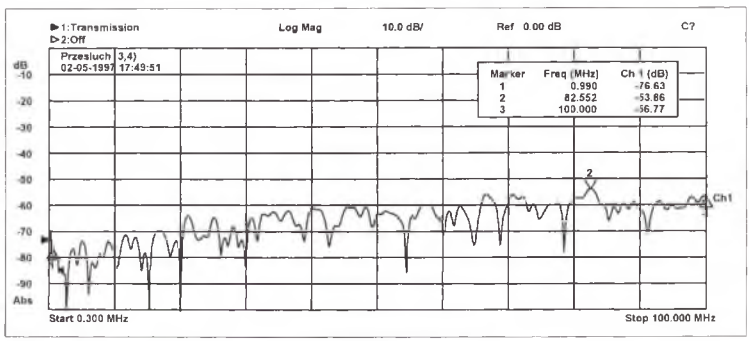
Packard *(Rys. 3)*, które zostały powtórzone w układzie wykorzystującym typowy tester okablowania strukturalnego PentaScanner 350 firmy Microtest *(Rys. 6)*.



Rys. 3. Schemat układu pomiarowego z wykorzystaniem analizatora sieci HP8711A

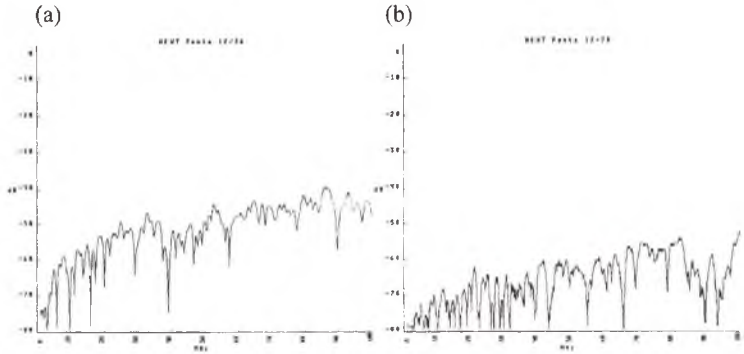


Rys. 4. Poziom przesłuchu zmierzony analizatorem HP8711A pomiędzy parami 12 i 12 w dwóch różnych kablach ekranowanych (S/UTP)



Rys. 5. Poziom przesłuchu zmierzony analizatorem HP8711A pomiędzy parami 12 i 12 w dwóch różnych kablach nieekranowanych (UTP)

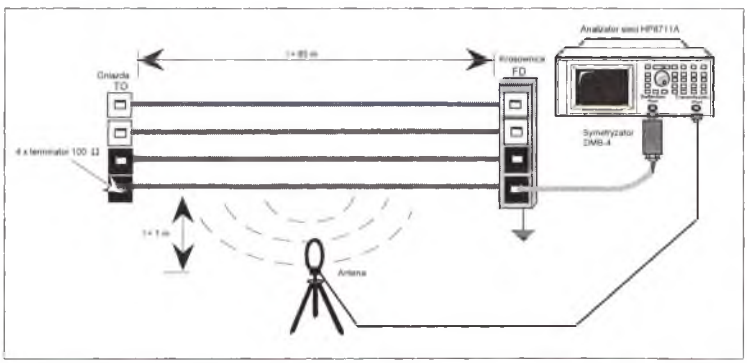
Pomiar przyrządem PentaScanner 350 miał na celu określenie przydatności testerów okablowania strukturalnego do wstępnych pomiarów emisyjności „skrętki". Dokonano pomiaru



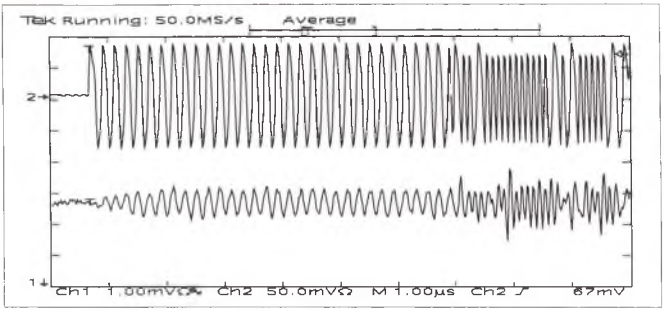
Rys. 8. Poziom przesłuchu zmierzony testerem PentaScanner 350 pomiędzy:
(a) - parami 12 i 36 w tym samym kablu nieekranowanym (UTP)
(b) - parami 12 i 12 w dwóch różnych kablach nieekranowanych (UTP)

5.2. Pomiary charakterystyk tłumienności sygnału użytecznego anteną w otoczeniu instalacji kablowej sieci

Badania przeprowadzono w tej samej instalacji okablowania strukturalnego co pomiary przesłuchów. Pomiaru charakterystyk tłumienności sygnału użytecznego w kanale podsłuchującym dokonano przy pomocy aktywnych anten pomiarowych, magnetycznej BBH-1100/A i elektrycznej ADA-120/A firmy Antenna Research Associates, oraz analizatora sieci HP8711A *(Rys. 9).* Sygnał wyjściowy z analizatora sieci HP8711A, był podawany przez układ dopasowujący DMB-4 na parę w przewodzie ekranowanym i nieekranowanym.



Rys. 9. Schemat układu do pomiary charakterystyk tłumienności w kanale podsłuchującym



Rys. 12. Preambuła ramki typu Ethernet zmierzona oscyloskopem:
w kablu nieekranowanym (UTP) - przebieg na górze wykresu,
w kanale podsłuchującym - przebieg na dole wykresu

6. Metody minimalizacji rozpraszania elektromagnetycznego w sieciach komputerowych

Chcąc minimalizować rozproszenie elektromagnetyczne informacji użytecznej z punktu widzenia ochrony przed niepożądaną detekcja należałoby redukować poziomy emitowanej informacji.

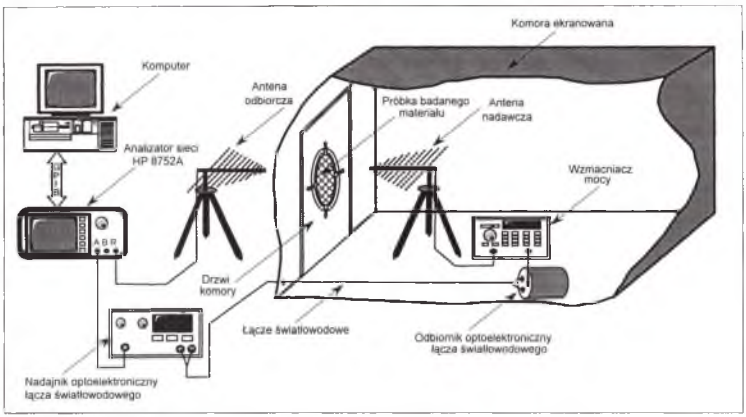
Posługując się wszystkimi najważniejszymi sposobami redukcji rozproszenia elektromagnetycznego - takimi jak ekranowanie, uziemianie, filtracja, izolowanie, dobór kabli - nie można zazwyczaj w pełni wyeliminować rozproszenia elektromagnetycznego informacji użytecznej. Może ono być jedynie zminimalizowane do pewnego poziomu. Jednym z podstawowych środków zmniejszania przenikania rozproszenia elektromagnetycznego jest ekranowanie.

Skuteczność ekranowania zmienia się wraz z częstotliwością sygnału, strukturą geometryczną ekranu, rodzajem ekranowanego pola, kierunkiem jego padania i polaryzacją. Ponieważ nie zawsze istnieje możliwość zastosowania metalowego (drogiego i trudnego w instalacji) ekranu, trwają poszukiwania nowych materiałów ekranujących np.: domieszkowanych tworzyw sztucznych, wielowarstwowych folii, tapet, tkanin oraz dzianin.
Waga tej problematyki sprawia, że ciągle prowadzone są badania nad optymalizacją technik ekranowania oraz doskonaleniem metod pomiarów jego skuteczności.
Zakład Naukowy Telekomunikacji NASK przy współpracy z Instytutem Telekomunikacji i Akustyki Politechniki Wrocławskiej (ITA PWr.) prowadzi badania dotyczące skuteczności tłumienia rozpraszania elektromagnetycznego przez materiały ekranujące. Wspólnie został opracowany projekt stanowiska pomiarowego. Na podstawie projektu powstało w Laboratorium Kompatybilności Elektromagnetycznej ITA PWr. stanowisko pomiarowe.

6.1. Ekranowanie w sieciach komputerowych

W sieciach komputerowych ekranowane mogą być obwody, elementy, kable, kompletne urządzenia lub wręcz całe pomieszczenia z wyposażeniem sieciowym. Osłona ekranująca działa najskuteczniej, jeśli jest szczelna (klatka Faraday'a), a napięcia zasilające są doprowadzone poprzez filtry dolnoprzepustowe. W urządzeniach stanowiących elementy sieci komputerowych ekrany metalowe są stosowane w wykonaniach specjalnych. W urządzeniach komputerowych ogólnego przeznaczenia, dostępnych na rynku, powszechnie są stosowane obudowy plastykowe. Do tych konstrukcji opracowano liczne technologie zapewniające ekranujące właściwości takich obudów. Między innymi:

- metalizowanie,



Rys. 14. Stanowisko do pomiaru skuteczności ekranowania

Badany materiał jest dociskany do kołnierza czterema szybkomocującymi przyciskami z siłą ok. 400 kG. Na stanowisku pomiarowym można badać próbki materiałów zakrywających przestrzeń pomiarową otworu o średnicy 30 cm. W przypadku próbek o mniejszych wymiarach, jest stosowany pierścień redukujący. Zmniejszenie przestrzeni pomiarowej obniża dynamikę pomiaru.

Szczegółowe warunki pomiaru zawarte zostały w tabeli 1. Umowną granicę pomiędzy strefą bliską i daleką uzyskuje się dla częstotliwości:

- 37,5 MHz - dla odległości 1,3 m anteny nadawczej od badanej próbki,
- 159 MHz - dla odległości 0,3 m anteny nadawczej od badanej próbki.

Przy odległości 5 cm praktycznie zawsze znajdujemy się w strefie pola bliskiego.

Tabela 1

	Składowa elektryczna E			Składowa magnetyczna H	
Częstotliwość	1 ÷ 30 MHz	70 ÷ 250 MHz	300 MHz ÷ 1 GHz	100 Hz ÷ 1 MHz	1÷ 30 MHz
Antena odbiorcza	prętowa, dł. 1 m	szerokopasmowa	logarytmiczna szerokopasmowa	o średnicy 12 cm (*)	ramowa o średnicy 30 cm
Antena nadawcza	prętowa, dł. 1 m	szerokopasmowa	logarytmiczna szerokopasmowa	o średnicy 12 cm (*)	ramowa o średnicy 30 cm
L1	30 cm	30 cm	30 cm	5 cm	30 cm
L2	30 cm	1,3 m	1,3 m	5 cm	30 cm

(*) antena jak w załączniku 5 do PN-86/E-06600

6.4. Przykładowe wyniki pomiarów.

Na opisanym powyżej stanowisku pomiarowym prowadzone są badania skuteczności (tłumienności) ekranowania różnych typów materiałów ekranujących:

- wykonanych z metali amorficznych,
- wykonanych z włókien modyfikowanych metalami lub ich związkami (np. miedzią, siarczkami miedzi),
- wykonanych z włókien modyfikowanych ferromagnetykami.

Jako przykład przedstawiono wyniki pomiarów dwóch typów materiałów:

- folii aluminiowej *(Rys. 15),*

(Rys. 12) wykazał, że już niewielka obróbka sygnału mierzonego pozwala na stwierdzenie jakiego rodzaju informacja jest przesyłana w sieci.

Podczas badań dokonano również porównania jakości sieci wykonanych z kabli typu skrętka ekranowana i nieekranowana. Oceniając różnice pomiędzy instalacją ekranowaną i nieekranowaną *(Rys. 10)* można stwierdzić, że emisyjność okablowania nieekranowanego jest wyższa niż okablowania ekranowanego. Przy **poprawnie wykonanych instalacjach** system ekranowany zapewnia większy „margines bezpieczeństwa" utrudniający możliwość detekcji informacji użytecznej niż system nieekranowany. Nawet poprawnie wykonana instalacja okablowania nie gwarantuje, że system będzie spełniał warunki na poziom emisyjności zapewniający odpowiednią protekcję informacji użytecznej. Wpływ na kompatybilność systemu mają wszystkie komponenty składające się na sieć. W sieci ekranowanej brak ciągłości ekranu może spowodować, że ekran zamieni się w antenę. W sieci nieekranowanej niezrównoważenie względem ziemi nadajnika lub odbiornika w karcie sieciowej spowoduje, że poziom emitowanej energii elektromagnetycznej drastycznie wzrośnie.

Ponieważ typowe rozwiązania sieci strukturalnych nie gwarantują odpowiedniego stopnia protekcji, istotne jest ekranowanie całych systemów. Ekranowanie pola magnetycznego jest dużo trudniejsze niż pola elektrycznego. Do ekranowania pół elektrycznych i fal płaskich należy stosować materiały przewodzące. Do ekranowania pół magnetycznych należy stosować materiały ferromagnetyczne. Odpowiednio dobrane materiały ekranujące w postaci dzianin i folii mogą być alternatywą dla stalowych klatek przy ekranowaniu urządzeń lub pomieszczeń.

8. Literatura

[1] Hołownia J., "Współczesne problemy kompatybilności elektromagnetycznej sprzętu komputerowego", Raport nr I-28/SPP - 008/86 Instytutu Telekomunikacji i Akustyki Politechniki Wrocławskiej, Wrocław 1986.

[2] Ott H.W., "Metody redukcji zakłóceń i szumów w układach elektronicznych", WNT, Warszawa 1979.

[3] White D.R.J., "EMI Control Methodology and Procedures", Don White Consultants Inc., Gaineswille, USA.

[4] MIL-STD-252, „Military Standard Attenuation Measurements for Enclosures, Electromagnetics Shielding for Electronic Test Purposes, Method of", United States Goverment Printing Office, Washington 1956.

2.1 Charakterystyka danych zarządzania

Można wyróżnić trzy kategorie danych przechowywanych w MIB: dane konfiguracyjne, dane sterujące i dane pomiarowe.

- *Dane konfiguracyjne* są kolekcją statycznych lub rzadko modyfikowanych informacji o bieżącej konfiguracji sieci. Opisują one na przykład: topologię sieci, łącza (ang. trunks), przełącznice (ang. switches), usługi sieciowe (ang. network services) lub klucze kodowania danych. Ze względu na złożoną strukturę sieci dane konfiguracyjne również charakteryzują się dużą złożonością strukturalną. Ta kategoria danych jest podstawą dla zarządzania konfiguracją sieci, kontrolą dostępu i usługami sieciowymi.

  Dla rozbudowanych rozległych sieci komputerowych wolumen danych konfiguracyjnych może osiągać rozmiar do kilku gigabajtów. Większość danych konfiguracyjnych jest składowana w MIB w momencie inicjacji systemu i jest modyfikowana w odpowiedzi na takie zdarzenia jak dodanie (lub usunięcie) nowego węzła sieci, połączenia lub usługi sieciowej.

- *Dane sterujące* są kolekcją danych opisujących bieżące nastawy parametrów umożliwiających strojenie sieci. Do tej grupy danych należą na przykład parametry określające maksymalne przepływy dla poszczególnych łączach, proporcje podziału obciążenia sieci na wyjściach przełącznic lub tablice marszrutyzacji. Oprócz bieżących nastaw parametrów, ta kategoria danych obejmuje również alternatywne zestawy nastaw dla różnych obciążeń i konfiguracji sieci. Na przykład MIB może zawierać dwa zestawy nastaw: dla obciążenia dziennego i nocnego.

  Dane sterujące są wykorzystywane do zarządzania wydajnością pracy i obsługą awarii sieci. W związku z tym, dane te mogą być modyfikowane wielokrotnie w ciągu dnia w celu uwzględnienia charakteru *ruchu* w sieci lub występujących awarii.

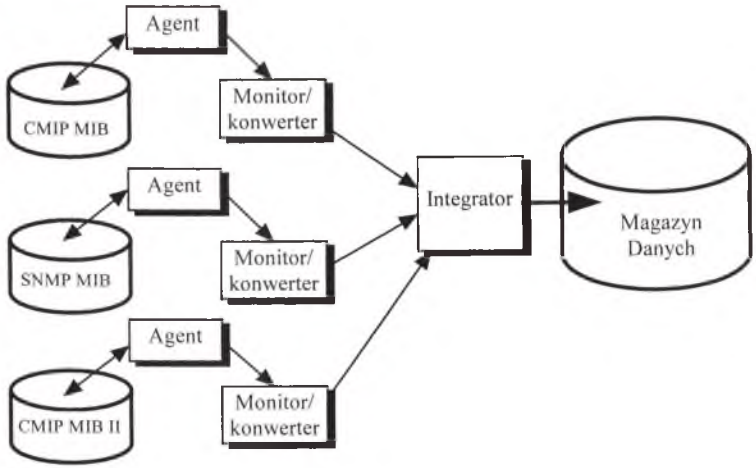
- *Dane pomiarowe* opisują dynamicznie zmieniający się stan sieci. Przykładem takich danych są długości kolejek na poszczególnych węzłach sieci, stany łączy lub współczynniki retransmisji danych. Wszystkie te dane są zbierane przez procesy monitorowania sieci. Są one podstawą do określenia stopnia wykorzystania i operacyjnej jakości sieci. Dane pomiarowe są podstawowymi danymi wejściowymi dla modułów zarządzania wydajnością pracy sieci, obsługą awarii i rozliczaniem obsługi klientów sieci. Szacuje się, że w rozbudowanych sieciach wolumen danych pomiarowych może przyrastać o 20 do 30 gigabajtów dziennie.

  Dane pomiarowe można podzielić na dwie grupy ze względu na niezbędny czas ich utrzymywania w bazie danych. Do danych trwałych, to jest danych, które powinny być utrzymywane przez okres wielu tygodni lub miesięcy, należą informacje o sumarycznym obciążaniu sieci przez poszczególnych klientów, o próbach naruszenia autoryzacji dostępu lub innych sytuacjach alarmowych. Z kolei do danych krótkotrwałych, to jest utrzymywanych w ciągu godzin lub pojedynczych dni, należy zaliczyć dane opisujące dynamiczną charakterystykę pracy sieci. W danym momencie oprócz bieżącego zbioru danych pomiarowych powinny być utrzymywane również historyczne wersje tych danych, dla celów analizy efektywności pracy systemu oraz częstotliwości i typów występujących w nim awarii.

2.2 Architektura systemu gromadzenia danych

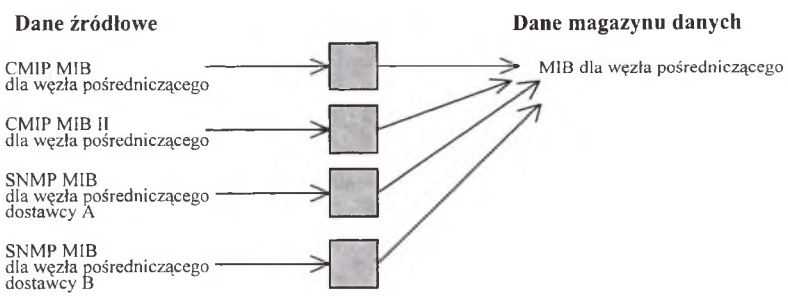
Architektura systemu gromadzenia danych w oparciu o technologię magazynowania danych obejmuje:

- **Źródłowe bazy danych**, którymi są w tym wypadku bazy informacji zarządzania związane z poszczególnymi urządzeniami sieciowymi. Formaty fizyczne, logiczne i pojęciowe poszczegól-



2.3 Fizyczna i logiczna konwersja danych źródłowych

Informacje zarządzania związane z różnymi elementami sieci komputerowej, pochodzącymi często od różnych dostawców, różnią się sposobem prezentacji na poziomie fizycznym, logicznym i pojęciowym. Bezpośrednie odwoływanie się do tych danych przez procesy zarządzania wymaga nieustannej translacji między różnymi standardami reprezentacji. Zastosowanie magazynu danych pozwala na sprowadzenie tych danych źródłowych do wspólnej reprezentacji przed ich wykorzystaniem przez procesy zarządzania.



3. Procesy zarządzające

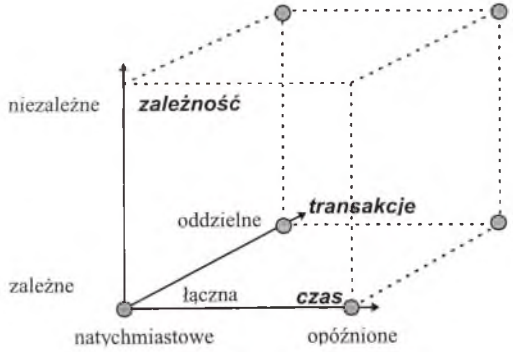
Zadaniem procesów zarządzających jest wykrywanie niepoprawnej i nieefektywnej pracy sieci, a następnie informowanie o tym operatorów sieci lub autonomiczne podejmowanie akcji, które poprzez zmianę nastaw parametrów sterujących lub konfiguracyjnych sieci doprowadzą do poprawy jej działania. W tym drugim wypadku będziemy mówili o ***aktywnych procesach zarządzania***. Aktywność procesów zarządzających przejawiająca się w ingerowaniu w nastawy parametrów sieci, zwalnia operatorów sieci z bezustannej dyspozycyjności i pozwala na skrócenie czasu reakcji proce-

dwóch kolejnych fazach. W fazie pierwszej następuje wykrycie zdarzenia i opcjonalna weryfikacja dodatkowych warunków związanych ze zdarzeniem. W fazie drugiej wykonywana jest druga część weryfikacji. W wypadku pomyślnej weryfikacji z obydwu faz następuje odpalenie skojarzonej ze zdarzeniem akcji.

Dostępnych jest wiele schematów powiązania modelu zarządzania obsługą zdarzeń a modelem zarządzania transakcjami. Schematy te są tworzone przez określenie związków między dwoma fazami przetwarzania zdarzeń. Mogą zachodzić między nimi trzy relacje:

- **Czasowa** - określająca czy fazy przetwarzania zdarzeń następują bezpośrednio jedna za drugą, czy są przesunięte w czasie. W tym drugim wypadku druga faza jest przesuwana do momentu zakończenia transakcji w ramach, której wystąpiło dane zdarzenie. Podczas definiowania operacji wyzwalanych opcje te są dostępne poprzez słowa kluczowe: *immediate* i *deferred*.
- **Transakcyjna** - określająca czy akcja zdefiniowana w danej procedurze wyzwalanej będzie fragmentem tej samej transakcji, w której wystąpiło zdarzenie uaktywniające procedurę wyzwalaną, czy dla tej akcji zostanie utworzona oddzielna transakcja. Opcja pierwsza jest domyślna, a druga jest dostępna za pomocą słowa kluczowego *separate*.
- **Zależności** - określająca czy w wypadku gdy akcja jest uruchamiana jako oddzielna transakcja, zakończenie tej transakcji ma być zależne od zakończenia transakcji w ramach, której wystąpiło zdarzenie uaktywniające procedurę wyzwalaną. Opcje te są dostępne za pomocą słów kluczowych: *dependent* i *independent*.

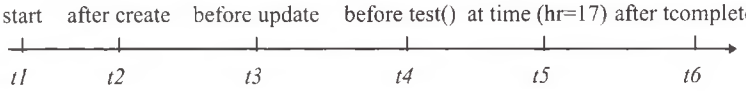
Kombinacje wartości powyższych relacji wyznaczają różne schematy aktywności procedur wyzwalanych. Zostało to zilustrowane na rysunku poniżej. Osie układu współrzędnych odpowiadają poszczególnym relacjom, natomiast wyznaczone przez określone wartości tych relacji węzły sześcianu odpowiadają różnym schematom aktywności.



Na kolejnym rysunku przedstawiono grafy przepływu sterowania dla wybranych schematów aktywności procedur wyzwalanych.

3.1.3 Operatory rachunku zdarzeń

Narzędziem do definiowania zdarzeń jest *rachunek zdarzeń*. Pozwala on na definiowanie zdarzeń złożonych. Rachunek zdarzeń jest zbiorem operatorów działających na historii zdarzeń danego obiektu, która jest sekwencją zdarzeń logicznych związanych z obiektem. Z każdym zdarzeniem logicznym jest związany znacznik czasowy, określający moment wystąpienia zdarzenia. W historii danego obiektu znaczniki te są unikalne, to znaczy nie ma dwóch zdarzeń o tych samym znaczniku. Początek historii każdego obiektu jest określony przez hipotetyczne zdarzenie *START*, które występuje tuż przed pierwszym zdarzeniem w historii tego obiektu. Rysunek poniżej przedstawia przykładową historię obiektu.



Można wyróżnić następujące kategorie operatorów rachunku zdarzeń:

- **Operatory logiczne**, umożliwiają definiowanie sumy, iloczynu i negacji logicznej zdarzeń. Na przykład definicja: *AFTER CREATE OR BEFORE DELETE*, oznacza zdarzenie złożone, które dla danej historii występuje w punkcie *t2*; a zapis: *NOT AFTER CREATE*, jest opisem zdarzenia złożonego występującego w punktach: *t3*, *t4*, *t5* i *t6*.

- **Operatory sekwencyjne** umożliwiają definiowanie zdarzeń złożonych jako sekwencji zdarzeń. Do tej kategorii należą operatory: SEQUENCE, PRIOR, RELATIVE i FIRSTAFTER. Operator SEQUENCE opisuje sekwencje zdarzeń, które nie mogą być przedzielone żadnymi innymi zdarzeniami. Na przykład, zdarzenie: *SEQUENCE(AFTER CREATE, BEFORE UPDATE)* wystąpiło w przykładowej historii obiektu w punkcie *t3*, ale zdarzenie: *SEQUENCE(AFTER CREATE, BEFORE TEST( ))*, w tej samej historii nie wystąpiło.

  Z kolei operatory PRIOR i RELATIVE nie wymagają by podane w niej zdarzenia występowały bezpośrednio po sobie, stąd zdarzenie: *PRIOR(AFTER CREATE, BEFORE TEST( ))*, występuje w naszej historii w punkcie *t4*.

  Operator *FIRSTAFTER* jest operatorem trzy-argumentowym. Dwa pierwsze argumenty określają wymaganą sekwencję zdarzeń, natomiast trzeci argument wskazuje zdarzenie, które nie może przedzielić tej sekwencji. Dla przykładu, zdarzenie: *FIRSTAFTER(AFTER CREATE, BEFORE TEST( ), AFTER TCOMPLETE)* ma miejsce w historii obiektu w punkcie *t*, ponieważ w historii obiektu wystąpiła sekwencja zdarzeń: *AFTER CREATE, BEFORE TEST( )*, nie przedzielona zdarzeniem *AFTER TCOMPLETE*.

- **Operatory powtarzalne** umożliwiają opis n-tego wystąpienia danego zdarzenia - operator *CHOOSE*, lub każde n-te wystąpienie zdarzenie - operator EVERY. Zdarzenia: *CHOOSE(3, AFTER TCOMLETE)* i *EVERY(5, AFTER TCOMLETE)* w podanej historii jeszcze nie wystąpiły.

Istnieje możliwość dowolnego zagnieżdżania podanych operatorów.

3.2 Przykładowa implementacja procesów zarządzania w oparciu o aktywną bazę danych

W ramach prac nad zastosowaniem aktywnych baz danych do implementacji procesów zarządzania sieciami komputerowymi, przeprowadzono eksperymenty z dwoma aktywnymi bazami danych: relacyjną bazą danych ORACLE i obiektową bazą danych ODE.

```
        AFTER UPDATE && przepustowość = 0
            ==> Alarm( );
};

Łącze::Łącze ( )
{
    ...
    SpadekPrzepustowości ( );
    BrakPołączenia ( )
}
```

Drugi przykład dotyczy bazy danych ORACLE. Model aktywności tej bazy danych oraz zbiory klas zdarzeń i operatory są dużo uboższe niż w systemie ODE. W związku z tym pełna implementacja aktywnych procesów zarządzania jest w tym wypadku bardziej złożona. Przykład ten obejmuje automatyczna reakcję systemu na spadek przepustowości o ponad 50% na jednym z łączy opisanych w relacji *Łącza*. Język definicji procedury wyzwalanej jest zgodny ze opracowywanym standardem SQL3.

```
CREATE TRIGGER SpadekPrzepustowości
    AFTER UPDATE OF przepustowość ON Łącza
    FOR EACH ROW
    WHEN (new.przepustowość/old.przepustowość < 0,5)
BEGIN
    Rekonfiguracje.Przełącz(old.id_łącza);
END;
```

4. Podsumowanie

Podstawą efektywnego zarządzania złożonymi sieciami komputerowymi są aktywne procesy zarządzania wyręczające operatorów sieci w monitorowaniu i rekonfiguracji sieci w odpowiedzi na pojawiające się awarie i zmiany obciążenia sieci. Konstrukcja aktywnych procesów zarządzania jest zadaniem złożonym koncepcyjnie i technicznie. Wiele mechanizmów niezbędnych do realizacji tego przedsięwzięcia znajduje się dopiero w fazie badań. Osiągnięcie celu aktywnego zarządzania wymaga zastosowania mechanizmów opracowywanych w dziedzinach magazynów danych i aktywnych baz danych.

Przeprowadzony w ramach prac badawczych NASK eksperyment polegający na implementacji prototypu aktywnego systemu zarządzania potwierdził możliwość wykorzystania do tego celu aktywnych bazy danych i wybranych technik magazynowania danych. Eksperyment przeprowadzono z wykorzystaniem dwóch systemów baz danych: ORACLE i ODE. Pierwszy z nich jest produktem komercyjnym wspomagającym budowę magazynu danych, ale o ograniczonych mechanizmach aktywności. Drugi jest systemem prototypowym o znacznie szerszych możliwościach tworzenia procesów aktywnych .

RDN jest jednym z atrybutów opisujących hasło, posiadającym szczególne znaczenie. Atrybuty mają postać zdefiniowaną jako para

(attributeType, attributeValue)

W przypadku zwykłych atrybutów dopuszcza się wielowartościowość w przypisaniu wartości typowi. Tak więc informacja dotycząca hasła jest umieszczona w postaci nieuporządkowanego zbioru atrybutów. Właściwa nazwa hasła – DN (*Distinguished Name*) powstaje przez konkatenację wszystkich nazw wyróżnionych prowadzących od korzenia drzewa (*root* reprezentujący poziom „Świat") do bieżącego elementu, czyli jest uporządkowaną sekwencją RDNów.

2.2. X.500 na arenie międzynarodowej

Usługa X.500 ma charakter międzynarodowy, udostępnia dane gromadzone w krajowych zasobach oraz informację z baz funkcjonujących w zaangażowanych w projekt instytucjach na całym świecie (europejskie przedsięwzięcie X.500, zwane NameFLOW-Paradise jest obecnie koordynowane przez DANTE). Fakt współdzielenia zasobów narzuca istotne uwarunkowania odnośnie ich postaci. Z jednej strony niezbędne jest zapewnienie możliwości umieszczania w bazie informacji zgodnie z narodowymi wymaganiami odnośnie stosowanego alfabetu, okrojenie danych ze znaków diakrytycznych znacznie obniża, a często wręcz dewaluuje ich jakość. Z drugiej strony należy brać pod uwagę, że informacja często jest odczytywana przez zagranicznych użytkowników, którym należy zagwarantować właściwą postać danych (chociażby dlatego, żeby ich wyprowadzenie nie spowodowało pojawienia się na ekranie „krzaczków"). Standard X.500 przewiduje umieszczanie w danych znaków spoza 7. bitowej strony kodowej ASCII, w tym przypadku stosuje się telekomunikacyjny standard kodowania T.61, w którym litery z akcentem są umieszczane jako sekwencje (kod akcentu, litera), a znaki specjalne mają swoje kody. T.61 obejmuje większość stosowanych w Europie typów kodowań, w szczególności Latin-2. Problem właściwego wyprowadzenia takiej informacji należy do stosowanego interfejsu użytkownika X.500.

Międzynarodowy projekt rekomenduje zalecenia dla krajowych administratorów baz X.500 ([2]). Mówi się w nich o postaci danych, głębokości zagnieżdżania informacji oraz stosowanych nazwach wyróżnionych. Jednym z problemów jest używanie wieloskładnikowych RDNów, czyli stosowanie kilku atrybutów do określenia nazwy wyróżnionej. Narzuca to dodatkowe wymagania na programy dostępowe, ale jest dobrym rozwiązaniem w przypadku, gdy np. w instytucji pracują dwie osoby o takim samym nazwisku i imieniu, poprzez dodanie do opisu dodatkowego atrybutu (np. personalTitle, czy UserId) można uzyskać wymaganą unikalność. Odnośnie nazewnictwa zalecenia stwierdzają, że należy stosować oficjalne nazwy instytucji i oddziałów, skróty czy nazwy popularne mogą stanowić uzupełnienia nazwy podstawowej. Osoby powinny być umieszczane, z kolei, pod „popularnymi" nazwami, tak by wyszukanie ich w danych było łatwe i naturalne. Międzynarodowy projekt dopuszcza stosowanie znaków T.61 w wartościach atrybutów, ale zaleca się nie stosowanie T.61 w DNach, czyli nazwach haseł. Wymóg ten jest podyktowany brakiem odpowiedniej platformy sprzętowo-programowej do zapewnienia właściwej postaci prezentacji danych.

2.2. Rodzaje zapytań w bazie X.500

Do najpopularniejszych operacji wykonywanych przy dostępie do zasobów X.500 Directory należy przeglądanie i wyszukiwanie. Przeglądanie (*browsing*), oznacza, że użytkownik wyprowadza informację dostępną na określonym poziomie i na jej podstawie decyduje o kolejnych działaniach (przejście do nowego poziomu, odczyt hasła, itp.). W tym przypadku drzewiasta struktura bazy umożliwia prosty dostęp do zasobów. Wyszukiwanie polega na podaniu wzorca informacji interesującej użytkownika danych i na jego podstawie rozpoczęciu procesu przeszukiwania. Ta sytuacja prowadzi zazwyczaj do przedstawienia serii wyników, uznanych za potencjalnie właściwe. W obu przypadkach jako rezultat pojawia się lista DNów lub fragmentów DNów (od bieżącego poziomu),

Załóżmy, że mamy do czynienia z hasłem reprezentującym Politechnikę Poznańską. RDN w przypadku stosowania typowego opisu ma postać („o" jest skrótem atrybutu organizationName):

o=Politechnika Poznanska

natomiast przy wieloskładnikowym RDNie, można w celu uzyskania prawidłowej polskiej formy nazwy obok międzynarodowej zdefiniować:

o=Politechnika Poznanska%polishorganizationName={T.61}Politechnika Pozna\c2nska

W tej sytuacji użytkownicy dysponujący tradycyjnymi interfejsami dostępowymi otrzymywaliby nazwę w postaci nieczytelnej, ponieważ atrybut polishorganizationName, znany wyłącznie w polskim pilocie, zostanie zastąpiony postacią w standardzie ASN.1 (*Abstarct Syntax Notation*), stosowanym do wewnętrznego opisu klas obiektów i atrybutów w bazie. Nie jest więc to metoda dobra.

Wobec tego wykorzystano istotną cechę bazy w standardzie X.500 – rozszerzalność, która daje możliwość lokalnego rozbudowywania typów haseł umieszczanych w zasobach, poprzez dodanie nowych klas obiektów oraz pozwala wprowadzać specyfikacje nowych typów atrybutów. Polski projekt bazuje na stosowaniu tablic klas obiektów i atrybutów zawierających dodatki w postaci definicji nowych polskich kłas obiektów oraz typów atrybutów (praca [1] szczegółowo omawia ten temat w rozdziale 4). Atrybuty przenoszące informacje, które powinny występować w języku narodowym mają swoje lokalne odpowiedniki. I tak, w przypadku osoby, poza atrybutem commonName mamy polishcommonName, dla instytucji obok organizationName występuje polishorganizationName. Jeden z atrybutów, o nazwie polishRDN, z założenia jednowartościowy, ma znaczenie specjalne ponieważ zawiera prawidłową polską nazwę hasła. Opisując operacje wyszukiwania i listowania zasobów X.500 Directory zwróciliśmy uwagę na fakt otrzymywania wyników w postaci nazw wyróżnionych – DNów „trafionych" haseł. W celu poprawnej prezentacji rezultatu lokalnemu użytkownikowi konieczne jest dokonanie przez interfejs użytkowy przemapowania na właściwą polską nazwę. Aby odwzorowanie to było jednoznaczne należy zagwarantować istnienie unikalnej nazwy, pełniącej rolę polskiego RDNu. Nazwa ta dotyczy poziomu, na którym element występuje, aby pokazać poprawną, lokalną formę DNa konieczne jest również odczytanie atrybutów polishRDN dla każdego poziomu powyżej bieżącego.

Tak zaprojektowany model wydaje się jedynym logicznym rozwiązaniem, ale niestety prowadzi do istotnych nieefektywności w procesie wyszukiwania danych. Po operacji wyszukiwania występuje szereg odczytów atrybutu przenoszącego lokalną nazwę, ich ilość jest zależna od głębokości poddrzewa. W praktyce, koszty tej techniki może zminimalizować stosowanie pamięci podręcznej (*cache*), w której składowane są dokonane przemapowania DNa na polski RDN. Oczywiście, im większa pamięć podręczna, rośnie szansa znalezienia odpowiedniego przemapowania w *cache*'u. Taka funkcjonalność została przez nas zaimplementowana w *gateway*'u WWW-X.500, programie dającym dostęp do zasobów X.500 z dowolnej przeglądarki WWW i pracującym zgodnie z umieszczonym wyżej opisem (http://x500.uni.torun.pl:8888).

4. Uniwersalny model dostosowania bazy X.500 do pracy wielojęzycznej

W podejściu ogólnym, przeznaczonym do stosowania w dowolnym kraju, proponujemy zastosowanie atrybutu localizedRDN do przenoszenia prawidłowej nazwy w języku narodowym, analogicznie inne atrybuty nazywane byłyby localizedcommonName, localizedorganizationName itp. Ponieważ tradycyjnie RDNy stosują nazwy lokalne w postaci poddanej transliteracji, a nazwy angielskie umieszczane są jako kolejne wartości atrybutu i często trudne do odfiltrowania, właściwe byłoby używanie atrybutu internationalRDN, zawierającego nazwę w języku angielskim. Tak zorganizowany system może być stosowany w sytuacjach, gdy nie jest potrzebne dysponowanie nazwami lokalnymi w kilku językach. Tymczasem wiele państw jest zainteresowanych oferowaniem w

[7]. Punktem wyjściowym działalności tej grupy było stwierdzenie, że usługi informacyjno-adresowe rozwijają się stosunkowo mało intensywnie na skutek wielu niejednoznaczności i utrudnień wynikających z przyjętego w X.500 systemu nazywania obiektów.
Jako najistotniejsze wady wymienia się:

1. często występujące powielanie się nazw na bieżącym poziomie DIT – stwarza to konieczność stosowania wieloskładnikowych nazw, które są przede wszystkim mało czytelne, ale również długie, co znacznie obniża efektywność,
2. model nazewnictwa X.500 przyjmuje stosowanie nazw instytucji w hierarchii drzewa informacji, tymczasem na świecie istnieją ograniczenia związane z prawem publikowania nazw oficjalnych, które są zastrzeżone, mówi się o konieczności formalnego rejestrowania (stworzono nawet jednostki odpowiedzialne za administrowanie), w efekcie utrudnione jest wprowadzanie informacji o osobach, ponieważ brakuje odpowiedniej struktury hierarchicznej; z opisanymi problemami nie mamy obecnie do czynienia w Polsce,

Członkowie grupy IDS zajmują się zagadnieniem nazewnictwa w kontekście stosowania obecnie w Internecie dwóch typów usług katalogowych (*directory services*): X.500 oraz LDAP. LDAP (*Lightweight Directory Access Protocol*) z uproszczonego protokołu dostępowego do zasobów X.500 urósł do roli samodzielnego standardu Internetu, definiującego metody dostępu do baz katalogowych. Aktualnie istnieją już implementacje tego standardu, a wiele znanych firm, jak Netscape, Microsoft, IBM ma w swoich produktach wbudowaną obsługę LDAP. LDAP stosuje metodę „*bottom-up*" do tworzenia zasobów, tzn. samodzielne bazy łączą się w globalną strukturę, podczas gdy w modelu X.500 mamy do czynienia z typową konstrukcją „*top-down*", gdzie drzewo informacji jest budowane od góry i brak pośredniczącego ogniwa zaburza rozwój gałęzi.

Proponowane przez grupę IDS zmiany w systemie nazewnictwa są prawdziwą rewolucją, ale zostały tak zaplanowane, by mogły zostać bez problemów wdrożone w systemach opartych na X.500 oraz LDAP. Nowe ustalenia zostały przygotowane pod kątem Internetu, definiują sposób nazywania użytkowników, urzędów poświadczających (*Certification Authorities*) oraz aplikacji. Zakłada się pozostanie przy drzewiastej konstrukcji informacji, ale zaleca się stosowanie schematu nazw przyjętego w Internecie, tzn. domenach internetowych (DNS – *Domain Name System*) oraz adresów pocztowych zgodnych z RFC822. Jako zaletę tego rozwiązania wymienia się m.in. łatwiejszą lokalizację serwerów LDAP czy X.500. Nowy typ drzewa informacji może współistnieć z tradycyjnym, co jest istotne, w przypadku niemożliwości usytuowania osób w gałęzi internetowej. Według sugestii grupy IDS hasła rodzaju instytucja powinny posiadać nazwę RDN, powstającą na podstawie wartości przypisanej wyróżnionemu atrybutowi domainComponent (zamiast dotychczasowego organizationName), natomiast w odniesieniu do osób należy stosować userId (zamiast common name).

Rozwiązanie to likwiduje, opisywane szeroko w poprzednich rozdziałach, kłopoty w przypadku występowania znaków spoza kodów ASCII w DNie. Oczywiście pozostaje problem udostępniania pozostałych informacji w języku lokalnym. Należy również podkreślić, że model umieszczania osób w poddrzewie Internetu jest obecnie trudny do wprowadzenia jako podstawowy w Polsce, ponieważ posiadanie adresów internetowych nie jest jeszcze rzeczą powszechną, natomiast baza X.500 ma służyć jako książka adresowo-informacyjna środowiska naukowo-akademickiego, nie polskiego Internetu.

Trudno przewidzieć losy przedstawionej propozycji, ale można spodziewać się, że zostanie ona pozytywnie przyjęta wśród aktywistów Internetu. O tym, że istnienie tego typu struktury jest praktyczne świadczyć może m.in. fakt, że w polskim projekcie X.500 gałąź internetowa pojawiła się w ubiegłym roku. Jej powstanie było związane z naszymi pracami nad wykorzystaniem X.500 do przechowywania kluczy publicznych PGP oraz PEM. Przechowuje ona wskazania (aliasy) do haseł w drzewie instytucji oraz dane tych osób, które dysponują adresami e-mail, a nie mogą zostać przypisane do instytucji. Najistotniejszą zaletą istnienia poddrzewa zgodnego ze strukturą internetową jest ułatwienie procesu wyszukiwania na podstawie adresu e-mail.

OCHRONA BAZY DANYCH X.500 ORAZ JEJ WYKORZYSTANIE DLA POTRZEB BEZPIECZNEJ POCZTY ELEKTRONICZNEJ

Maja Górecka *Maja.Gorecka@cc.uni.torun.pl*

Tomasz Wolniewicz *twoln@hpc.uni.torun.pl*

Naukowa Akademicka Sieć Komputerowa NASK

Bartycka 18, 00-716 Warszawa

Referat składa się z dwóch części.

W pierwszej omawiamy zagadnienia związane z zabezpieczeniami samego systemu X.500. Baza danych, która służy do przechowywania danych osobowych i może być wykorzystywana jednocześnie jako system dla celów wewnętrznych instytucji i jako system informacyjny na zewnątrz, musi być wyposażona w odpowiednie mechanizmy zabezpieczeń. Istotny jest zarówno mechanizm selekcji uprawnionych użytkowników, jak i system określenia uprawnień do konkretnych zasobów. Mechanizmy te, stosunkowo proste we wcześniejszych implementacjach, zostały bardzo istotnie rozbudowane w standardzie X.500 '93.

Druga część referatu jest poświęcona zastosowaniu bazy X.500 do celów wspierania bezpiecznej (szyfrowanej i sygnowanej) wymiany informacji. Omawiamy w niej rozwiązania zaimplementowane w ramach naszych prac rozwojowych w NASK.

Zakładamy, że czytelnik posiada pewną wiedzę na temat systemu X.500, dokładniejsze informacje można znaleźć w szeregu opracowań [7]. Bardzo dobrym źródłem informacji jest również książka D. Chadwicka [2]

Bezpieczeństwo w bazie X.500

Autentykacja

Autentykacją nazywamy metody identyfikacji osoby lub procesu komputerowego ubiegającego się o dostęp do pewnych zasobów. Autentykację stosuje się na ogół dla celów autoryzacji, tj. przydzielania bądź ograniczania dostępu do pewnych zasobów, niekiedy jednak autoryzacja ma na celu jedynie zbieranie danych o użytkownikach systemu, w celach statystycznych albo na użytek identyfikacji osób dokonujących prób nieuprawnionego dostępu.

Standard X.500 [1] a dokładniej X.509) określa trzy poziomy autentykacji: prosty, chroniony i silny.

- Poziom prosty (simple) zakłada, że hasło użytkownika przechowywane jest w bazie X.500. Nie określa się sposobu zabezpieczenia samego hasła, to znaczy algorytmu szyfrowania itp. Istotą tego poziomu autentykacji jest założenie, że użytkownik dowiązujący

- group (określenie — wyliczenie — grupy obiektów mających dane prawa dostępu),
- prefix (wszystkie obiekty znajdujące się w pewnej gałęzi drzewa, na przykład wszyscy pracownicy danej instytucji),
- other (wszyscy)

Prawa dostępu przechowywane są w atrybutach accessControlList na przykład:

```
acl = other # read # entry
acl = self # write # entry
acl = other # compare # attributes # userPassword
acl = prefix # c=pl@o=UMK # read # attributes # telephoneNumber
```

Administrator serwera zarządzającego pewnym zbiorem danych ma zawsze nieograniczony dostęp do wszystkich danych. Jest to oczywiście uzasadnione faktem, że administrator może modyfikować dane bezpośrednio na dysku.

Przechowywanie informacji autoryzacyjnej na poziomie każdego hasła jest bardzo przejrzyste, ale równocześnie dosyć uciążliwe, gdy trzeba dokonać zmiany obiektu, który ma mieć dostęp do znacznej ilości haseł (na przykład zmiany osoby odpowiedzialnej za pewien podzakres danych w ramach instytucji prowadzącej serwis X.500). Łatwo wówczas o pomyłki. Fakt, że administrator serwera nie musi być jawnie wpisany do każdego hasła jako osoba o uprawnionym dostępie, pozwala uniknąć modyfikacji bazy w momencie zmiany administratora.

QUIPU wprowadziło dodatkowo atrybuty dziedziczone, pozwalające na przykład na wprowadzenie adresu na poziomie instytucje i spowodowanie, ze pojawia się on jako domyślny u każdego pracownika tej instytucji. System atrybutów dziedziczonych nie daje się jednak stosować do accessControlList. Jak widać z opisanych metod, oddelegowanie administratorów odpowiedzialnych za określone fragmenty poddrzewa zlokalizowanego na jednym serwerze jest stosunkowo skomplikowane.

Standard '93

Standard w wersji '93 wprowadza bardzo rozbudowany system ochrony dostępu do danych. Jak wspomnieliśmy powyżej, mnogość możliwych metod (przy jednoczesnej opcjonalności ich implementowania) powoduje, że obecnie nie ma pewności jakie fragmenty faktycznie są podtrzymywane przez dany produkt X.500. Ma to bardzo istotne konsekwencje dla replikacji danych. Zreplikowanie danych chronionych w określony sposób na serwerze innego producenta, może oznaczać, że dane te nie będą chronione w ogóle, jeżeli drugi serwer nie podtrzymuje metody autoryzacji zastosowanej w pierwszym. Niestety nie określono sposobów reakcji na takie sytuacje serwera, który przejmuje dane. Implementatorzy X.500 radzą zatem, aby nie dopuszczać replikacji danych chronionych pomiędzy różnymi implementacjami serwera X.500

Podstawową nowością w standardzie '93 jest ścisłe określenie obszaru zarządzanego. Punkt drzewa informacyjnego, będący wierzchołkiem obszaru zarządzanego pozwala na umieszczenie w drzewie specjalnych obiektów (subentries), które mają znaczenie wyłącznie w administrowaniu systemem, a które pozwalają na określenie, na przykład praw dostępu do odpowiednich fragmentów drzewa. (W istocie standard pozwala wyróżniać specjalne podobszary drzewa w ramach których stosuje się autoryzacje — Access Control Specific Area — ale dla uproszczenia nie będziemy o nich wspominać.) W nowym standardzie można nadawać prawa dostępu dla każdej operacji (read,

podmioty, zarówno certyfikowane jak i certyfikujące, są identyfikowane za pomocą *nazw wyróżnionych* tworzonych zgodnie z hierarchiczną strukturą X.500.

W oparciu o standard X.509 określono standard PEM (Privacy Enhanced Mail) [3-6]. PEM poza formatem wymienianej informacji definiuje strukturę instytucji wystawiających certyfikaty. Podstawowe znaczenie dla systemu bezpieczeństwa opartego o certyfikaty ma struktura wzajemnie poświadczających się urzędów. Na to, aby system, taki jak PEM, działał sprawnie potrzebne jest spełnienie dwóch warunków:

1. klucze publiczne identyfikujące podmioty biorące udział w wymianie informacji, muszą być powszechnie i łatwo dostępne,
2. musi istnieć absolutna pewność, że klucze są istotnie związane z podmiotami, które je wykorzystują.

Drugi warunek zapewnić może tylko system urzędów certyfikacji, pierwszy wymaga utworzenia szeroko dostępnych baz danych.

Ponieważ standard X.509 stosuje nazewnictwo zgodne z bazą X.500, baza ta jest naturalnym miejscem do przechowywania informacji wymaganej dla sprawnego funkcjonowania PEM. Certyfikaty ze swojej natury są *bezpieczne*, a zatem przechowywanie ich nie wymaga, aby baza była dobrze zabezpieczona. Podmiana klucza jest wykluczona, możliwe jest jedynie jego skasowanie. Ta własność certyfikatów może być wykorzystana do zabezpieczenia samej bazy X.500, kiedy to certyfikaty, a nie hasła, są podstawą autentykacji użytkowników.

Polski projekt wspomagania bezpiecznej poczty

Powody powstania systemu

Systemy oparte o certyfikaty X.509 zaczynają być coraz bardziej popularne, wykorzystuje je na przykład przeglądarka Netscape. Z drugiej strony w zakresie poczty elektronicznej w Internecie przeważa zdecydowanie system PGP. W celu zapewnienia wsparcia takiej wymiany informacji zaprojektowaliśmy i zaimplementowaliśmy system certyfikacji i publikacji kluczy oparty o polską strukturę X.500.

Zaproponowany przez nas system może zostać wdrożony niewielkim nakładem środków, ponieważ bazuje na już istniejących strukturach — sieci serwerów X.500.

System zakłada zdalny kontakt z użytkownikiem poprzez lokalnych administratorów, rozproszenie zbioru danych, ale centralizację funkcji tworzenia certyfikatów. Taki system zapewnia na początku maksimum efektywności i minimum kosztów, przy jednoczesnej prostej skalowalności w przyszłości.

Certyfikaty użytkowników, w postaci sygnowanych kluczy PGP oraz certyfikatów X.509, przechowywane będą w bazie X.500 dając prosty i szeroki dostęp wszystkim zainteresowanym. Jednocześnie istnieje możliwość funkcjonowania systemu w oparciu o opłaty subskrybcyjne osób przechowujących certyfikaty w bazie.

Zastosowanie bazy X.500 do gromadzenia certyfikatów powinno mieć równocześnie efekt podniesienia atrakcyjności samej bazy i poprawienia aktualności przechowywanych w niej danych. Osoby przechowujące certyfikaty w bazie będą miały jednocześnie możliwość potwierdzenia swojej tożsamości, a co za tym idzie ułatwioną metodę wprowadzania poprawek do danych w bazie.

rozwikłania aliasu połączoną z operacją odczytu. Jest to znacznie bardziej efektywne od przeszukania.

- Modyfikacja polskiego interfejsu WWW do bazy X.500 w celu ułatwienia odzyskiwania kluczy PGP. Interfejs został wzbogacony o możliwość korzystania z gałęzi domenowej w celu zwrócenia albo samego klucza, albo pełnej informacji o osobie odpowiadającej danemu adresowi elektronicznemu.
- Utworzenie oprogramowania wspomagającego prace CUC. Przygotowano zestaw programów narzędziowych współpracujących z systemami PGP i SecuDE umożliwiających tworzenie certyfikatów PEM i podpisywanie kluczy PGP. Narzędzia te generują w wyniku dane dla skryptów, które automatycznie modyfikują zawartość bazy X.500. Ponieważ wprowadzanie i modyfikacje danych w bazie X.500 leży poza kompetencjami CUC niezbędne było przygotowanie systemu, który byłby bardzo prosty w obsłudze i nie wymagał przeszkolenia osób obsługujących delegatury.

Do przygotowania pozostaje jeszcze sporządzenie narzędzi wspomagających użytkownika w szybkim uzyskiwaniu informacji z bazy X.500. w chwili obecnej konieczne jest korzystanie z interfejsu WWW i samodzielne kopiowanie uzyskanego klucza PGP.

Literatura

[1] Data Networks and Open System Communications: *Directory*, ITU-T Recommendations X.500-X.525

[2] David Chadwick, *„Understanding X.500 Directory"*, 1994

[3] J. Linn, Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedure, Request for Comments RFC1421

[4] S. Kent, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, Request for Comments RFC1422

[5] D. Balenson, Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers, Request for Comments RFC1423

[6] B. Kaliski, Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services, Request for Comments RFC1424

[7] Raporty i prace na temat projektu X.500 w Polsce

http://ocelot.uni.torun.pl/raporty_pl.html

Struktura i zasady działania

Jak wspomniano, system oparty jest o obecnie istniejąca strukturę X.500. Jednostkę tworzącą certyfikaty nazwaliśmy Centralnym Urzędem Certyfikacyjnym (CUC). Zadaniem CUC jest wystawianie certyfikatów w oparciu o dane przesłane przez delegatury. CUC jest jedynym punktem certyfikacji, co oznacza, że możliwa jest bezpośrednia weryfikacja każdego certyfikatu znajdującego się w systemie. Na CUC spoczywa znaczna odpowiedzialność, gdyż skompromitowanie jego klucza oznaczałoby konieczność unieważnienia wszystkich certyfikatów. Z tego powodu CUC musi dysponować absolutnie bezpiecznym systemem komputerowym (bez kontaktu z siecią). W praktyce, z powodów oszczędności, zrealizowane to jest w oparciu o wymienny dysk komputerowy zawierający system operacyjny, łącznie ze wszystkimi narzędziami potrzebnymi do certyfikacji kluczy.

CUC jest przygotowany do wystawiania zarówno certyfikatów w standardzie PGP jak i PEM. W obecnej fazie certyfikaty PEM tworzone są na podstawie kluczy PGP i mają znaczenie pomocnicze (w przeciwieństwie do podpisanych kluczy PGP zawierają stemple czasowe i okresy ważności).

Pewność, że certyfikat jest faktycznie związany z konkretną osobą lub instytucją ma znaczenie absolutnie podstawowe. Z tego powodu wymagane jest osobiste przedstawienie klucza do certyfikacji z odpowiednim potwierdzeniem tożsamości. Niemożliwe jest aby każda osoba pragnąca umieścić w bazie swój certyfikat kontaktowała się bezpośrednio z CUC, ustanowione zostały zatem delegatury CUC stowarzyszone z administratorami lokalnych serwerów X.500. Do zadań delegatury należy potwierdzenie tożsamości użytkownika, ewentualne zawarcie umowy i pobranie abonamentu, a następnie wysłanie otrzymanego od użytkownika klucza do certyfikacji. Przesłanie to musi nastąpić w sposób wykluczający sfałszowanie informacji. Wykorzystywana będzie w tym celu poczta PGP. Należy przy tym podkreślić, że bezpieczeństwo kluczy delegatur jest również bardzo istotne, gdyż skompromitowanie klucza może doprowadzić do tego, że CUC poświadczy nieprawdziwy klucz, ale możliwa jest częsta zmiana kluczy delegatur, a skompromitowanie klucza może co najwyżej oznaczać konieczność zweryfikowania certyfikatów wystawionych w pewnym okresie czasu przez jedną delegaturę.

CUC stosuje zestaw narzędzi, które po utworzeniu certyfikatów przygotowują informację w postaci plików wsadowych, tak że wprowadzenie danych do bazy X.500 jest automatyczne. Wprowadzenia tych danych dokonuje delegatura opiekująca się odpowiednim serwerem X.500.

Systemy wspomagające

W ramach prac przygotowujących system do wdrożenia wykonano między innymi:

- Zaprojektowanie nowych atrybutów przeznaczonych do przechowywania kluczy PGP i wygenerowanie odpowiednich tablic systemowych dla oprogramowania QUIPU.
- Zaprojektowanie struktury gałęzi X.500 zgodnej ze strukturą domenową Internetu. Utworzenie takiej gałęzi było niezbędne w celu szybkiego odnajdywania klucza PGP na podstawie adresu e-mail. Standardowa struktura drzewa X.500 wymagałaby dokonania skomplikowanego przeszukania w zakresie całej Polski. Takie przeszukanie angażowałoby znaczne zasoby i z pewnością byłoby czasochłonne. System gałęzi domenowej tworzy poddrzewo na kształt drzewa DNS, na którego liściach umieszczone są atrybuty typu uid określające elektroniczny adres. Obiekty te są aliasami do odpowiednich punktów właściwego drzewa X.500, a w pewnych przypadkach, gdy trudno jest wprowadzić osobę do głównego drzewa, mogą to być również prawdziwe hasła opisujące osoby. Gałąź domenowa jest rodzajem indeksu ze względu na atrybut adresu poczty elektronicznej. Odszukanie osoby ze względu na jej adres oznacza w tej sytuacji jedynie operacje

modify, list, search. add, itd.). Dopuszcza się także określenie wymaganego poziomu autentykacji, potrzebnego dla określonego typu dostępu, na przykład można sobie wyobrazić, że operacja odczytu chroniona jest jedynie prostą autentykacją, ale operacja modyfikacji będzie wymagała silnego poświadczenia tożsamości. Rozbudowano również opis zbioru użytkowników, którym można nadawać prawa dostępu, najbardziej istotne jest dodanie użytkowników z pewnego spójnego obszaru drzewa, jest to system zbliżony do „prefix", ale znacznie bardziej rozbudowany. Standard przewiduje również różne poziomy ochrony w zakresie błędów zwracanych przez system. Można dopuścić, aby system informował, że szukana informacja istnieje, ale nie ma do niej dostępu, albo też zachowywał się identycznie jak gdyby informacja nie istniała.

Poza ochroną poddrzew nadal możliwa jest ochrona poszczególnych haseł poprzez atrybuty zawarte w samym haśle.

Dopuszczenie do dostępu do danego hasła wymaga sprawdzenia, w jakich obszarach kontroli dostępu dane hasło się znajduje, dla każdego takiego obszaru konieczne jest sprawdzenie czy dany użytkownik na prawo dostępu czy nie, widać zatem, że przy skomplikowanych systemach sprawdzenie i zezwolenie na dostęp może być operacją znacznie obciążającą system. Niezbędne jest, aby brać to pod uwagę w momencie gdy definiuje się system zabezpieczeń. Implementacje serwerów '93 dostarczają specjalnych narzędzi do konfiguracji i testowania systemów ochrony danych, przyjmuje się, że konfigurowanie bezpośrednie jest zbyt skomplikowane.

Potwierdzenie prawdziwości wyników

Standard '93 przewiduje możliwość potwierdzania wyników operacji na bazie X.500 poprzez ich elektroniczne podpisywanie. W tym celu konieczne jest wyposażenie serwerów w klucze szyfrujące. Stosowanie opcji podpisywania powinno być istotne gdy odpowiedź z bazy X.500 ma kluczowe znaczenie. Na przykład baza X.500 może zarządzać fizycznym dostępem do pomieszczeń, w zależności od bezpieczeństwa sieci łączącej serwer X.500 z systemem dostępu, podpisywanie wyniku może być uzasadnione lub nie.

Ochrona przesyłanych danych

Należy podkreślić, ze standard X.500 '93, pomimo zdefiniowania bardzo wyrafinowanych metod ochrony przed niepowołanym dostępem, nie definiuje żadnej metody ochrony samych danych w czasie transmisji (a wiec ich szyfrowania). Wydaje się to znacznym niedociągnięciem i należy oczekiwać, ze kolejne wersje standardu zostaną odpowiednio rozbudowane.

Wykorzystanie bazy X.500 do celów autentykacji

Standard X.509

System X.500 od początku swojego powstawania był pomyślany jako wsparcie systemów bezpiecznej wymiany informacji i autentykacji obiektów. Podstawy takiego systemu opisuje standard X.509 wprowadzając określenie *certyfikatu*. W myśl tego standardu certyfikatem nazywa się klucz publiczny obiektu (osoby, systemu komputerowego, instytucji itp.) zaopatrzony atrybutami daty wystawienia i okresu ważności i następnie podpisany elektronicznie przez inny obiekt. Podstawowy związek pomiędzy X.509 a definicją bazy X.500 polega na nazewnictwie obiektów. Wszelkie

się do bazy podaje swoje dane (nazwę wyróżnioną) oraz hasło. Informacje te są następnie przesyłane przez sieć bez żadnych zabezpieczeń.

- Poziom chroniony (protected) zakłada, podobnie jak poprzednio przechowywanie hasła w bazie, różnica polega na przesyłaniu hasła w sposób zaszyfrowany dodatkowo wzbogacony stosowaniem stempla czasowego. W ten sposób hasło nie może być ani rozszyfrowane ani przechwycone w postaci zaszyfrowanej i ponownie wysłane w celu włamania.

Poziom silny (strong) stosuje metodę klucza publicznego. W bazie X.500 przechowywany jest certyfikat (a więc poświadczony klucz publiczny) użytkownika. System ,wysyła użytkownikowi *wyzwanie*, czyli tekst zaszyfrowany jego kluczem publicznym. System wspierający użytkownika ma za zadanie rozszyfrować wyzwanie i odesłać je systemowi autentykacji. Poprawne rozszyfrowanie oznacza, że użytkownik jest w posiadaniu odpowiedniego klucza, a zatem jest tym, za kogo się przedstawia.

Autoryzacja

Autoryzacja dostępu określa zakres danych które są udostępniane konkretnym użytkownikom. Oczywiście zagadnienie to jest ściśle związane z autentykacją. Zagadnienia związane z autoryzacją zakładają, że autentykacją użytkownika zajmuje się osobny podsystem i mogą co najwyżej wymagać, aby dostęp do pewnych zakresów danych był poprzedzony odpowiednią metodą autentykacji.

QUIPU i standard '88

Autorzy standardu X.500 '88 nie zdefiniowali w ogóle zagadnień związanych z autoryzacją dostępu, sprawą tą zajął się dopiero standard w wersji '93. Ponieważ autoryzacja w pewnym zakresie była niezbędna, implementatorzy musieli wprowadzać swoje własne metody, fakt, który stał się dosyć uciążliwy w momencie ogłoszenia oficjalnej wersji standardu. Prawdopodobnie nacisk implementatorów spowodował, że standard '93 ma niezwykle rozbudowane metody autoryzacji dostępu, tak że większość stosowanych już metod może się obecnie pojawić jako implementacja fragmentu standardu. Niestety to oznacza jednocześnie, że różne implementacje X.500 mogą stosować zupełnie niekompatybilne metody związane z autoryzacją.

Zaimplementowanie autoryzacji było niezbędne chociażby dla potrzeb administrowania bazą, wymagającego sprawdzenia tożsamości administratora. Autentykacja typowo oparta była o metodę prostą lub chronioną, ale w każdym przypadku przewidywała, że baza X.500 będzie przechowywała hasło administratora. To z kolei oznaczało, że konieczne jest specjalne traktowanie atrybutu jakim jest hasło, tak aby umożliwić porównanie, ale nie odczyt.

Oprogramowanie QUIPU, będące fragmentem ostatniego, publicznie dostępnego pakietu Isode 8.0, implementowało dwie pierwsze metody autentykacji (prostą i chronioną) oraz własną metodę autoryzacji.

Autoryzacja w QUIPU zakładała, że informacja o dostępie do hasła (entry) jest przechowywana w samym haśle. System zakłada możliwość chronienia zawartości hasła (lub pojedynczego typu atrybutu) w operacjach:

- odczytu
- modyfikacji
- porównania

W zakresie upoważnionych użytkowników dopuszczano cztery poziomy:

- self (obiekt opisywany danym hasłem),

6. Podsumowanie

Prowadzone w ramach polskiego projektu X.500 prace nad dostosowaniem funkcjonalności bazy do potrzeb krajowych użytkowników pozwoliły nam dogłębnie przeanalizować problematykę nazewnictwa obiektów w rozproszonym systemie informacyjnym. Działania te przyniosły również praktyczny efekt – realizację zaprojektowanego modelu, poprzez rozbudowanie tablic obiektów i atrybutów oraz implementację interfejsów użytkowych. Obecnie, wszystkie eksploatowane w Polsce serwery X.500 pracują w oparciu o zmodyfikowane oprogramowanie obsługi zasobów X.500 i wiele ośrodków oferuje dostęp do zasobów X.500 przez polski *gateway* WWW-X.500. Tematyka internacjonalizacji X.500 Directory i innych systemów informacyjnych jest obecnie popularna, dzięki czemu nasze prace mogły być prezentowane i dyskutowane na arenie międzynarodowej, a proponowane rozwiązania są przyjmowane z zainteresowaniem, ponieważ ich implementacja jest stosunkowo prosta i nie wymaga ingerencji w moduły systemowe. Śledząc prace standaryzacyjne widzimy, że w przyszłości większość potrzeb związanych z dostępem wielojęzycznym do zasobów zostanie pokryta przez oprogramowanie podstawowe, jednak zdobyte doświadczenie z pewnością w wielu sytuacjach będzie owocowało.

7. Literatura

[1]M. Górecka, T. Wolniewicz, „Dostosowanie bazy X.500 do specyfiki języka lokalnego", materiały konferencyjne, Miedzeszyn'96

[2]M. Górecka, T. Wolniewicz, *„Use of national languages in X.500 Directory"*, konferencja robocza *CEN/TC304 Providing Multilingual support in middleware: Implementing the Universal Character Set ISO 10646 in European Information Society*, Bled, Słowenia, listopad 1996.

[3]P. Barker, S. Kille, T. Lenggenhager, „Naming and Structuring Guidelines for X.500 Directory Pilots", RFC 1617, 1994

[4]P. Barker, *„X.500 Index DSAs"*, NameFLOW-Paradise Paper, June 1995

[5]D. Chadwick. *„IndeX.500"*, DANTE IN PRINT, No.19, May 1996

[6]Draft Amendments for Context to ITU-T Recommendation X.500 (1993)

[7]*„Naming Plan for an Internet Directory Service"*, IDS Working Group, INTERNET-DRAFT (draft-ietf-ids-dirnaming-01.txt), March 12, 1997

[8]Raporty i prace na temat projektu X.500 w Polsce
http://ocelot.uni.torun.pl/raporty_pl.html

zasobach X.500 informacji wielojęzycznej (np. francuski i niemiecki). Wówczas w proponowanym przez nas modelu niezbędne są rozszerzenia, polegające na przyjęciu założenia, że atrybuty lokalne oraz localizedRDN są wielowartościowe, a każda wartość charakteryzuje się tym, że na początku łańcucha występuje kod języka. Jednocześnie przyjmuje się, że jeśli istnieje wartość localizedRDN dla danego języka, to istnieją też odpowiednie wartości atrybutów w tej wersji językowej. Tego typu system wymaga oczywiście właściwie przygotowanego interfejsu użytkownika, co nie jest zadaniem łatwym, ponieważ różnorodność możliwych sytuacji przypisań atrybutów jest duża.

5. Międzynarodowe prace nad nazewnictwem w X.500 Directory

5.1. Dalsze prace standaryzacyjne zespołu ITU-T

Obecnie trwają, w ramach ITU-T oraz grup roboczych, prace nad internacjonalizacją X.500 Directory. Planowane jest dodanie tzw. kontekstu (*context*) informacji umieszczanej w zasobach X.500, poprzez specyfikacje nowej składni atrybutów przenoszących nazwy. Proponowane rozszerzenia mają wpływ na większą część standardu. Uzupełnienia ukazały się w postaci nieoficjalnych szkiców (Draft Amendments [6]), formalnie zostaną ogłoszone w standardzie X.500'97.

Podstawową zmianą jest dodanie flagi do atrybutu w celu możliwości interpretacji jego wartości. Przewiduje się, że interfejsy użytkowe (DUA – *Directory User Agent*) będą dostarczały informację, jakiego kontekstu oczekują w odpowiedziach.

O takim rozwiązaniu wspominaliśmy opisując możliwości analizowane przez nas w fazie projektowania systemu. Również nasza propozycja globalnego systemu wielojęzycznego uwzględnia stosowanie znaczników informacji w atrybutach. Jednak z powodu ograniczenia zasięgu niezbędnych zmian do programów użytkowych, nie przewidywaliśmy zmiany składni, interpretacja wartości należałaby do interfejsu DUA.

Propozycje wprowadzenia kontekstu informacji implikują konieczność modyfikacji podstawowych operacji, wykonywanych na zasobach X.500, jak read, search, list, compare, add entry, modify entry. Odnośnie nazewnictwa uzupełnienia do standardu wprowadzają nową definicję nazwy wyróżnionej (DN) – dotychczas każde hasło miało dokładnie jedną wartość DN, nowa specyfikacja określa, że hasło ma minimum jedną nazwę wyróżnioną. Jeżeli dostępne są liczne RDNy, rozróżnialne przez kontekst, hasło ma wiele DNów, które interpretowane są na podstawie znacznika kontekstu. Wykonywanie operacji wyszukania czy listowania, może przenosić w argumentach interesujący zleceniodawcę kontekst, co spowoduje otrzymanie wyników w odpowiedniej postaci.

„*Draft Amendments for Context*" są, jak się wydaje, kompletne. Pozostaje więc zatwierdzenie standardu i implementacja w pakietach X.500. Trudno określić jak długo potrwa dostosowanie oprogramowania do zapewniania internacjonalizacji, ale z pewnością pojawienie się takich produktów będzie istotnym przełomem w działalności X.500. Oczywiście dochodzi do tego kwestia dostępu do oprogramowania. Od jesieni ubiegłego roku firma Isode, będąca autorem stosowanego w polskim projekcie pakietu IC zaniechała udzielania bezpłatnej licencji ośrodkom akademickim, aby korzystać z oprogramowania należy opłacić roczną subskrypcję. Przyjęcie i implementacja proponowanego przez nas nazewnictwa pozwoli wykorzystywać dostępny publicznie pakiet Isode-8.0, modyfikacje byłyby wcielone w przygotowane interfejsy użytkowe, które w dużej mierze są już gotowe, więc na efekt końcowy nie trzeba by czekać długo.

5.2. Działania standaryzacyjne grupy roboczej IETF

Bardzo istotne są prace dotyczące nazewnictwa w bazach typu katalogowego, prowadzone przez grupę roboczą IDS (*The Integrated Directory Services*) pracującą w ramach IETF (*Internet Engineering Task Force*). Ważnym dokumentem podsumowującym jest INTERNET-DRAFT z marca 1997

co wobec wymogu stosowania 7. bitowych łańcuchów ASCII dla nazw wyróżnionych oznacza, że w bezpośredniej formie wynik ten nie zadowoli lokalnego użytkownika.

3. Dostosowanie bazy X.500 do lokalnych potrzeb

3.1. Cel

Przystosowanie zasobów X.500 do potrzeb lokalnych użytkowników oznacza pełną obsługę języka narodowego, a więc:

1. nazwy atrybutów muszą być prezentowane w języku narodowym,
2. wartości atrybutów dotyczące haseł lokalnych (czyli polskich, w przypadku krajowej bazy) pojawiają się w języku narodowym, o ile użytkownik nie zadecydował inaczej,
3. wynik operacji wyszukania, czy listowania jest zwracany w języku lokalnym (DNy muszą zostać skonwertowane do lokalnych nazw),
4. interfejsy użytkowe powinny akceptować stosowane strony kodowe (ISO-Latin-2, czy Windows-1250),
5. należy uwzględnić wprowadzanie łańcuchów zawierających znaki diakrytyczne (we wzorcach itp.).

Z punktu widzenia użytkowników zagranicznych muszą być spełnione następujące warunki:

1. RDNy występują jako łańcuchy ASCII, w odniesieniu do znaków diakrytycznych stosuje się transliterację,
2. hasła, w szczególności te umieszczone na wyższych poziomach drzewa informacji, powinny zawierać podstawowe informacje również w języku angielskim.

3.2. Rozwiązanie przyjęte w polskim projekcie

Zaprojektowane w polskiej usłudze X.500 funkcje dostosowujące bazę do potrzeb polskich użytkowników musiały uwzględnić następujące realia:

1. usługa X.500 w Polsce działa w oparciu o oprogramowanie Isode (ogólnodostępny pakiet Isode-8.0 lub wersja rozwijana przez firmę Isode – IC), implementujące standard X.500'88 (najnowsza edycja IC obsługuje również X.500'93),
2. ponieważ zasoby polskiej bazy X.500 są udostępniane w serwisie światowym, nie jest możliwa ingerencja w moduły systemowe, np. niedopuszczalna jest zmiana składni (*syntax*) atrybutów przechowujących nazwy,
3. modyfikacje systemu mogą dotyczyć wyłącznie interfejsów użytkowych, nie programów obsługi bazy.

Popularną praktyką w projekcie NameFLOW-Paradise jest stosowanie wielowartościowych atrybutów, pozwala to umieścić jako nazwę dodatkową, obok łańcucha w kodzie ASCII, pełną wersję, z uwzględnieniem znaków T.61. Następnie interfejsy użytkowe powinny dopuszczać odfiltrowywanie interesujących użytkownika wartości. Zakres takich zastosowań, w sytuacji, gdy wartości nie posiadają znaczników identyfikujących jest utrudniony. Poniższy przykład obrazuje trudności przy stosowaniu nazywania haseł poprzez zbiór par (attributeType, attributeValue).

NAZEWNICTWO OBIEKTÓW W ROZPROSZONEJ MIĘDZYNARODOWEJ BAZIE X.500

Maja Górecka
Maja.Gorecka@cc.uni.torun.pl

Tomasz Wolniewicz
twoln@hpc.uni.torun.pl

Naukowa Akademicka Sieć Komputerowa NASK
Bartycka 18, 00-716 Warszawa

1. Wstęp

Referat opiera się na prowadzonych przez nas pracach nad dostosowaniem informacyjno-adresowej bazy X.500 do przechowywania prawidłowych polskich nazw. Sposób implementacji tego zadania został szczegółowo opisany w ubiegłorocznym referacie, przedstawionym w Miedzeszynie [1]. Obecnie zajmiemy się omówieniem problemów, na jakie napotkaliśmy w trakcie pracy nad zagadnieniem, na tle specyfiki modelu X.500. Wszelkie trudności były związane z przyjętym w standardzie X.500 sposobem nazywania elementów umieszczanych w bazie X.500 oraz zaleceniami międzynarodowego projektu odnośnie nazewnictwa [2]. Opracowanie w skrócie przedstawia istotne dla poruszanego tematu cechy standardu X.500 i ich wpływ na wykonywane zadanie adaptacji bazy do polskich potrzeb. Opisujemy polskie rozwiązanie oraz proponowany na jego podstawie projekt rozwiązania ogólnego, które mogłoby zostać zastosowane w krajach wielojęzycznych. Omawiamy również działania na arenie międzynarodowej, zmierzające do zwiększenia funkcjonalności X.500 w zakresie nazewnictwa. Temat polskich rozwiązań dotyczących wielojęzyczności X.500 Directory był przez nas prezentowany w listopadzie 1996 podczas konferencji *„CEN/TC304 Providing Multilingual support in middleware: Implementing the Universal Character Set ISO 10646 in European Information Society"*, proponowane podejście ogólne zostało przyjęte z zainteresowaniem. Planujemy przeprowadzenie testu pracy systemu międzynarodowego opartego na tym modelu, do współpracy zgłosili się przedstawiciele Danii i Słowenii.

2. Specyfika bazy X.500

2.1. Model informacyjny

Struktura informacji przechowywanej w bazie X.500 ma istotne znaczenie w przypadku implementacji zagadnienia wielojęzyczności.

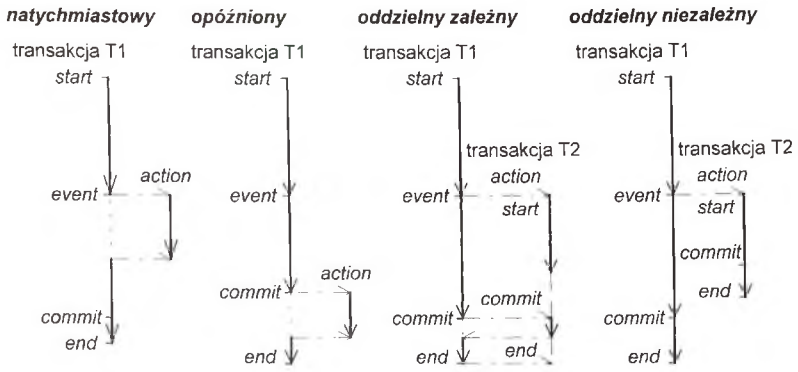
X.500 Directory to rozproszona baza danych o bardzo szerokim zakresie. W celu zapewnienia takich własności jak: proste metody zarządzania tego typu zasobami, jednoznaczne nazewnictwo obiektów oraz łatwość wyszukiwania danych zdecydowano się definicję bazy X.500 jako struktury hierarchicznej, zwanej potocznie drzewem informacyjnym DIT (*Directory Information Tree*). Ustalając postać zasobów wykorzystano powszechne relacje między elementami umieszczanymi w bazie (np. osoba pracuje w oddziale należącym do instytucji usytuowanej na poziomie kraju). Element, zwany dalej hasłem (*entry*) wprowadzany do bazy X.500 umieszczony jest w odpowiednim poddrzewie informacyjnym, wynikającym z jego asocjacji do istniejącej w DIT informacji. Hasło na danym poziomie DIT uzyskuje unikalną nazwę wyróżnioną – RDN (*Relative Distinguished Name*).

Poniżej przedstawiono przykłady procedur wyzwalanych, które realizują aktywne zarządzanie siecią komputerową. Pierwszy przykład dotyczy bazy danych ODE. Obejmuje on fragmenty definicji dwóch klas: *SiećKomputerowa* i *Łącze*. Definicje te obejmują deklaracje monitorowanej zmiennej wystąpienia *przepustowość*, nagłówki metod realizujących modyfikacje nastaw i rekonfiguracje sieci, oraz definicje procedur wyzwalanych: *PrzełączNaDzień*, *PrzełączNaNoc*, *SpadekPrzepustowości* i *Brak-Połączenia*. Procedury *PrzełączNaDzień* i *PrzełączNaNoc* powodują automatyczną reorganizację sieci w określonych godzinach, w celu uwzględnienia zmiany obciążenia sieci w różnych okresach dnia. Procedura wyzwalana *SpadekPrzepustowości* wykrywa zdarzenie spadku przepustowości łącza poniżej 10% na okres 5 minut, i przeprowadza w takim wypadku rekonfigurację sieci.. Zdarzenie *BrakPołączenia* przesłanie odpowiedniej informacji na konsolę operatorską.

```
class SiećKomputerowa {
private:
        ...
public:
        SiećKomputerowa ( );
        boolean KonfiguracjaDzienna ( );
        boolean KonfiguracjaNocna ( );
        ...
trigger:
        PrzełączNaDzień ( ) : perpetual separate independent
                at time( HR=7, M=30 )
                        ==> KonfiguracjaDzienna ( );
        PrzełączNaNoc ( ) : perpetual separate independent
                at time( HR=19, M=30 )
                        ==> KonfiguracjaNocna ( );
};

SiećKomputerowa::SiećKomputerowa ( ) {
        ...
        PrzełączNaDzień ( );
        PrzełączNaNoc ( );
}

class Łącze {
private:
        float przepustowość;
        ...
public:
        boolean Przełącz(Łącze);
        void Alarm (Status );
        ...
trigger:
        SpadekPrzepustowości ( ) : perpetual separate dependent
                firstAtfter ( AFTER UPDATE && przepustowość < 10,
                AFTER TIME ( M=5 ),
                AFTER UPDATE && przepustowość > 10)
                        ==> Przełącz (this);
        BrakPołączenia ( ) : perpetual immediate
```



3.1.2 Klasy zdarzeń

Zdarzenia rozpoznawalne przez aktywną bazę danych mogą należeć do jednej z wielu klas zdarzeń. Poniżej przedstawiono wykaz klas zdarzeń i odpowiadających im identyfikatorów, dostępnych w prototypowej aktywnej obiektowej bazie danych ODE firmy AT&T.

1. Zdarzenia związane ze stanem obiektu w bazie danych:
   a. utworzenie obiektu: *AFTER CREATE*;
   b. usunięcie obiektu: *BEFORE DELETE*;
   c. modyfikacja, odczyt lub dowolny dostęp do obiektu: *{BEFORE | AFTER} UPDATE , READ , ACCESS* ;
2. Zdarzenia związane z uaktywnieniem metody obiektu: *{BEFORE | AFTER} nazwa_metody*;
3. Zdarzenia związane ze zmianami stanu transakcji:
   a. rozpoczęcie transakcji: *AFTER TBEGIN*;
   b. punkt zatwierdzenia transakcji: *AFTER TCOMPLETE*;
   c. zatwierdzenie transakcji: *AFTER TCOMMIT*;
   d. wycofanie transakcji: *{BEFORE | AFTER} TABORT*;

1. Zdarzenia temporalne:
   d. określony moment czasu: *AT TIME (timestamp);*
   e. po upływie czasu: *AFTER TIME (interval);*
   f. periodycznie co określony czas: *EVERY TIME (interval)*;
5. Zdarzenia zdefiniowane przez użytkownika: *{BEFORE | AFTER} nazwa_zdarzenia*.

Podane powyżej zdarzenia należą do zbioru tak zwanych *zdarzeń elementarnych*. Ze zdarzeniami elementarnymi można kojarzyć *zdarzenia logiczne*, mówimy wtedy o tak zwanych zdarzeniach logicznych. Zdarzenia logiczne pozwalają na śledzenie stanów danych. Na przykład zdarzenie: „spadek przepustowości łącza poniżej wartości 10%"; można wyspecyfikować dla danego obiektu, następująco: *AFTER UPDATE && przepustowość < 10*, co spowoduje, że po każdej modyfikacji tego obiektu będzie weryfikowany warunek: *przepustowość < 10*.

su zarządzania. Ponadto, procesy zarządzające mogą zostać rozszerzone o procedury symulacyjne, które pozwolą w krótkim czasie na określenie optymalnych działań dla poprawienia pracy sieci.

Implementacja aktywnych procesów zarządzania może zostać zrealizowana jako zbiór aplikacji klasycznej, nieaktywnej bazy danych. Zadaniem aplikacji byłoby w tym wypadku bezustanne monitorowanie stanu bazy danych zawierającej informacje zarządzania, w celu wykrycia stanów świadczących o nieefektywnej pracy sieci. Alternatywnym rozwiązaniem jest implementacja procesów zarządzania jako *wyzwalanych procedur* (ang. trigger) aktywnej bazy danych. Rozwiązanie to w porównaniu z poprzednim charakteryzuje się szeregiem zalet:

- cykliczne monitorowanie stanu bazy danych jest zastąpione monitorowaniem ściśle określonych zdarzeń co oznacza mniejsze obciążenie i co za tym idzie większą wydajność systemu;
- systemowy mechanizm monitorowania wybranych zdarzeń i *wyzwalania* skojarzonych z nimi akcji upraszcza znacznie implementację aktywnych procesów zarządzania;
- istnieje możliwość zastosowania różnych modeli powiązań mechanizmu monitorowania zdarzeń z modelem zarządzania transakcjami;
- zdarzenia i model uaktywniania procedur wyzwalanych są definiowane w sposób deklaratywny, co znacznie ułatwia to proces tworzenia i utrzymywania procesów zarządzania;
- system zarządzania ma budowę modułową: warstwa monitorowania stanu bazy informacji zarządzania jest logicznie oddzielona od warstwy odpowiedzialnej za modyfikacje i rekonfigurację sieci.

3.1 Aktywne bazy danych

Aktywność bazy danych jest realizowana przez dodatkowy moduł programowy, na którego wejście podany jest strumień zdarzeń. Do zbioru rozpoznawanych zdarzeń należą zdarzenia elementarne: zachodzące w systemie bazy danych, zdarzenia czasowe i zdarzenia zgłaszane przez użytkownika, oraz zdarzenia złożone, które są kompozycją zdarzeń elementarnych. Aktywna baza danych musi realizować funkcje związane z monitorowaniem zdarzeń, wartościowaniem dodatkowych warunków skojarzonych ze zdarzeniami i wyzwalanie zdefiniowanych przez użytkowników akcji. Niektóre z tych akcji mogą generować nowe zdarzenia, które dodawane są do wejściowego strumienia zdarzeń. Ogólna architektura aktywnej bazy danych została przedstawiona na rysunku poniżej.

3.1.1 Schematy aktywności bazy danych

Powszechnie przyjętym modelem aktywnej bazy danych jest tak zwany dwufazowy model ECA (ang. Event(i)-Condition(i,ii)-Action(ii)). W modelu tym przetwarzanie zdarzeń odbywa się w

nych źródłowych baz danych mogą różnić się między sobą, w zależności od przyjętego standardu baz informacji zarządzania i dostawcy konkretnego urządzenia.

- **Agentów**, są to moduły programowe odpowiadające za dostęp do baz informacji zarządzania Moduły te są skojarzone z poszczególnymi urządzeniami. Są one jedynym legalnym środkiem odczytu i modyfikacji danych zarządzania.
- **Moduły monitorowania i konwersji danych** źródłowych, których zadaniem jest monitorowanie zmian danych w bazach informacji zarządzania oraz konwersji różnych formatów danych do wspólnego formatu przyjętego w centralnym magazynie danych. Procesy monitorowania mogą pracować zarówno w trybie powiadomieniowym, oczekując na sygnał od agenta o zmianach danych lub w trybie cyklicznego odczytu bazy informacji zarządzania.
- **Moduł integratora** realizujący funkcje integracji danych źródłowych do postaci akceptowalnej przez schemat centralnej bazy informacji zarządzania ulokowanej w magazynie danych. Dane przechowywane w magazynie danych mogą różnić się schematem pojęciowym od danych przechowywanych w poszczególnych źródłowych bazach danych. Zazwyczaj są to dane bardziej przetworzone, na przykład do wartości sumarycznych, średnich itp. Wyznaczenie nowych wartości tych danych wymaga często od modułu integratora ponownego dostępu do w ogólności wielu źródłowych baz danych, dla pobrania wszystkich niezbędnych danych źródłowych. Ten sposób modyfikacji danych w magazynie danych jest nazywany modyfikacją przyrostową (ang. incremental view). Ze względu na asynchroniczny charakter uaktualniania danych w magazynie danych w stosunku do ich modyfikacji w źródłowych bazach danych niezbędne jest zastosowanie odpowiednich algorytmów gwarantujących spójność tych danych.
- **Magazyn danych** pełniący rolę centralnej bazy informacji zarządzania Dane przechowywane w magazynie nie są zwykłą kopię danych źródłowych. Dane przechowywane w źródłowych bazach danych zarządzania mają charakter operacyjny. Są to dane niezbędne dla lokalnego zarządzania danym urządzeniem. Z kolei, dane składowane w magazynie danych są podstawą dla globalnego zarządzania siecią. Są to więc dane silnie przetworzone. Mają one zazwyczaj charakter wielowymiarowy. Wymiarami danych zarządzania są na przykład: czas, lokalizacja urządzenia lub warstwa architektury sieci.

  Efektywne przetwarzanie danych zarządzania wymaga zastosowania specyficznych struktur danych, takich jak: pliki kratowe, R-drzewa lub indeksy bitowe. Struktury te przyśpieszają jednoczesne wyszukiwanie danych w wielu wymiarach.

AKTYWNE ZARZĄDZANIE SIECIAMI KOMPUTEROWYMI

Jerzy Brzeziński, Tomasz Koszlajda
{Jerzy.Brzezinski | Tomasz.Koszlajda}@cs.put.poznan.pl

1. Wprowadzenie

Współczesne sieci komputerowe charakteryzują się wysoką dostępnością, i dużą złożonością mierzoną liczbą połączonych węzłów, oraz różnorodnością urządzeń komunikacyjnych i protokołów sieciowych. Efektywne zarządzanie takimi sieciami w zakresie obsługi awarii i optymalizacji pracy sieci, wymaga szybkiego podejmowania decyzji dotyczących modyfikacji architektury lub parametrów konfiguracyjnych sieci. Realizacja efektywnego zarządzania sieciami komputerowymi wymaga rozwiązania dwóch podstawowych problemów: zapewnienia szybkiego dostępu do aktualnej informacji o globalnym stanie sieci oraz zautomatyzowania procesu zarządzania.

Dostęp do aktualnej informacji o globalnym stanie sieci jest podstawą do podejmowanie racjonalnych i trafnych decyzji dotyczących rekonfiguracji lub zmiany parametrów sieci. Tymczasem bazy informacji zarządzania (MIB) związane z poszczególnymi elementami sieci pozwalają jedynie na ustalenie stanu ograniczonych fragmentów sieci. Dopiero zebrane i przetworzone informacje z wszystkich tych elementów pozwolą na określenie globalnego stanu sieci i ustalenie przyczyn niskiej wydajności sieci lub na wykrycie awarii. Wiąże się to z koniecznością zastosowania centralnej bazy informacji o stanie sieci. Predestynowanym rozwiązaniem dla implementacji centralnej bazy informacji zarządzania jest technologia *magazynów danych*.

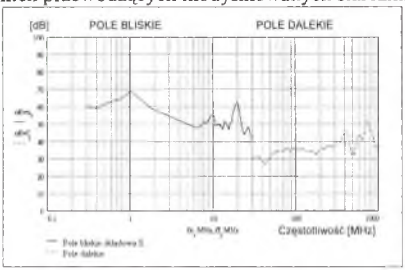
Efektywne zarządzanie wymaga szybkiego wykrywania niepoprawnej i nieefektywnej pracy sieci oraz szybkiej modyfikacji parametrów sterujących lub konfiguracji sieci mającej na celu poprawę jej działania. Dla zagwarantowania dużej efektywności procesu zarządzania wymagana jest pełna automatyzacja tego procesu. Automatyzacja ta powinna obejmować procesy monitorowania stanu sieci, procesy decyzyjne, których celem jest ustalenie optymalnych nastaw parametrów sterujących i konfiguracji sieci dla danego obciążenia sieci, oraz realizację działań rekonfiguracji sieci do wyznaczonego stanu optymalnego. Rola operatorów sieci powinna zostać zredukowana do ogólnego nadzoru nad procesem zarządzania. Technologią, która w istotny sposób upraszcza realizację w pełni autonomicznych procesów zarządzania są mechanizmy oferowane przez *aktywne bazy danych*.

W niniejszym artykule przedstawiono koncepcję zastosowania do implementacji procesów zarządzania sieciami komputerowymi technologii magazynów danych i aktywnych baz danych. Rozdział drugi artykułu zawiera przegląd problemów związanych z konstrukcją systemu gromadzenia informacji o stanie sieci komputerowej z wykorzystaniem magazynu danych. W rozdziale trzecim przedstawiona została problematyka aktywnych baz danych. Ostatni rozdział zawiera podsumowanie artykułu.

2. Baza danych zarządzania

Baza danych zarządzania (MIB) zawiera dane opisujące stan oraz stałe i modyfikowalne parametry zasobów sieciowych podlegających procesowi zarządzania. Na bazę tę składają się dane związane z poszczególnymi elementami sieci, przeznaczone do lokalnego zarządzania tymi elementami, oraz dane zawierające sumaryczne informacje o globalnym stanie sieci.

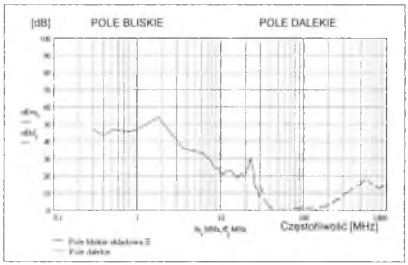
- cienkiej dzianiny z włókien przewodzących modyfikowanych siarczkami miedzi *(Rys. 16).*

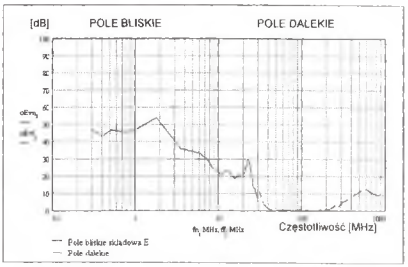


Rys. 15. Tłumienność ekranowania folii aluminiowej

Wyniki pomiarów przedstawiono w postaci wykresów na których zamieszczono charakterystyki tłumienności ekranowania dla strefy pola bliskiego i strefy pola dalekiego. W przypadku dzianiny, która w odróżnieniu od folii aluminiowej posiada własności kierunkowe tłumienia ze względu na układ włókien, pomiary wykonano dla dwóch położeń próbek:

- poziomego położenia pasa materiału,
- pionowego położenia próbki.





Rys. 16. Tłumienność ekranowania dzianiny zmierzona dla:
(a) - poziomego ustawienia próbki,
(b) - pionowego ustawienia próbki

Na wykresach nie jest prezentowana wartość tłumienności ekranowania dla składowej magnetycznej pola elektromagnetycznego, obydwa materiały wykazywały tłumienność bliską zeru.

7. Uwagi i wnioski

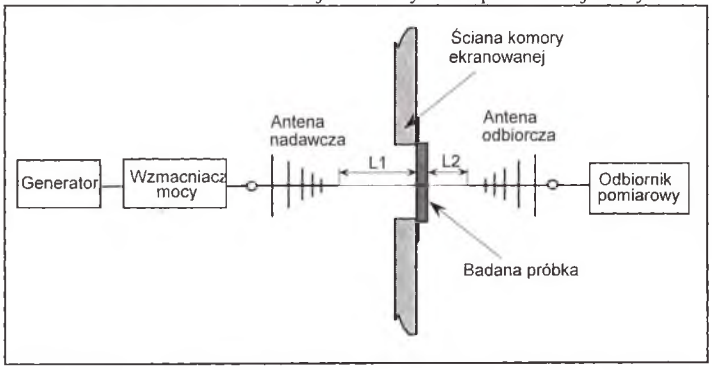
Przeprowadzone badania mały na celu wykazanie możliwości detekcji informacji użytecznej w sieciach komputerowych. Bazując na metodach pomiarowych zalecanych przez normy dotyczące kompatybilności elektromagnetycznej, wskazano sposoby realizacji systemów detekcji informacji użytecznej. Przeprowadzono badania metodami obwodowymi i polowymi pozwalające na oszacowanie dynamiki układów do detekcji informacji użytecznej. Z pomiarów wynika, że w typowych sieciach wystarczająca jest dynamika urządzeń pomiarowych rzędu 100 dB *(Rys. 4, Rys. 5, Rys. 10).* Laboratoryjne przyrządy pomiarowe posiadają dynamikę wystarczającą do realizacji systemów detekcji informacji. Ze względu na złożone charakterystyki tłumienia w kanale podsłuchującym (np. *Rys. 10*) do realizacji regenaratora sygnału konieczne jest wykonanie zestawu filtrów, dostosowanych do pasma sygnału źródłowego. Pomiar w dziedzinie czasu metodą polową

- natryskiwanie i malowanie obudów pokryciami przewodzącymi,
- stosowanie przewodzących mas plastycznych do tłoczenia obudów,
- stosowanie elastycznych tkanin przewodzących wykonanych z metalizowanych włókien, połączonych z masą plastyczną w procesie tłoczenia obudowy,
- wykorzystanie samoprzylepnych folii nakładanych na obudowę.

Coraz częściej, w zastosowaniach specjalnych, ekranowane są całe pomieszczenia. Ze względów praktycznych i ekonomicznych, niezmiernie rzadko wykonuje się ekranowanie w postaci stalowej klatki Faraday'a. Jako materiał ekranujący stosuje się natomiast tapety wykonane z tkanin przewodzących z włókien modyfikowanych metalami lub ich związkami. Najprostszym sposobem sprawdzenia skuteczności ekranowania rozpraszania elektromagnetycznego takich materiałów jest pomiar charakterystyk częstotliwościowych tłumienia.

6.2. Metody pomiaru skuteczności ekranowania materiałów ekranujących

Metodyka pomiaru tłumienia elektromagnetycznego przez pomieszczenia ekranowane została opracowana w 1956 roku w Stanach Zjednoczonych dla potrzeb wojskowych.

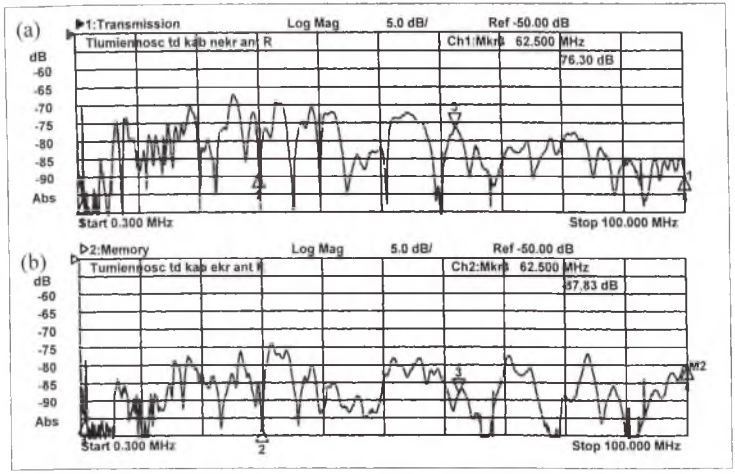


Rys. 13. Schemat układu pomiarowego do badania skuteczności ekranowania materiałów wg. MIL-STD-285

Opis metodyki został zawarty w normie MIL-STD-285. Norma ta wraz z późniejszymi uzupełnieniami obowiązuje do dziś. Procedura pomiaru skuteczności ekranowania badanych materiałów jest analogiczna jak pomiar tłumienia elektromagnetycznego przez pomieszczenia ekranowane. W komorze ekranowanej wykonywany jest otwór o wymiarach ok. 1m x 1m, który przesłaniany jest materiałem ekranującym *(Rys. 13).*

6.3. Stanowisko do pomiaru skuteczności ekranowania materiałów ekranujących

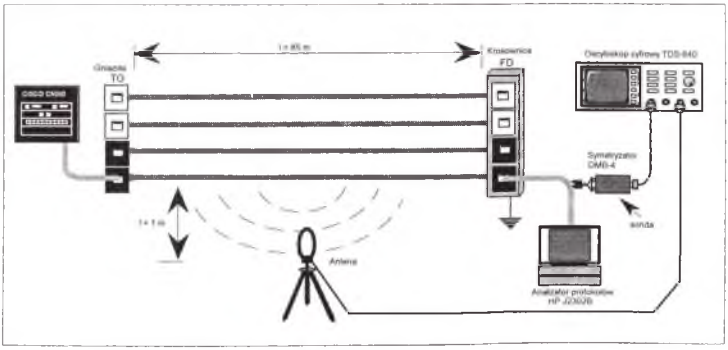
Stanowisko pomiarowe wykonano na bazie komory ekranowanej o wymiarach 4,24 x 6 m *(Rys. 14).* Obszar pomiarowy w kształcie koła o średnicy 30 cm został wykonany w postaci otworu w drzwiach komory. Otwór ten zakończony został stalowym kołnierzem. W kołnierzu umieszczono podwójną spiralną uszczelkę wykonaną ze stali nierdzewnej, zapewniającą bardzo dobry kontakt eklektyczny z badanymi próbkami materiałów.



Rys. 10. Charakterystyki tłumienności w kanale podsłuchującym zmierzone anteną BBH-1100/A dla: (a) - kabla nieekranowanego (UTP)
(b) - kabla ekranowanego (S/UTP)

5.3. Sprawdzenie możliwości detekcji informacji użytecznej przez kanał podsłuchujący

W celu weryfikacji możliwości detekcji informacji użytecznej z kanału podsłuchującego przeprowadzono pomiary pola wokół instalacji okablowania strukturalnego w dziedzinie czasu. Sygnał źródłowy w postaci ramek typu Ethernet był generowany z analizatora protokołów HP J2302B do kabla instalacji sieciowej połączonego z innym urządzeniem sieciowym. Zastosowano antenę BBH-1100/A podłączoną do oscyloskopu cyfrowego TDS 640 firmy Tektronix. Pomiar synchronizowano sygnałem ramki Ethernet mierzonym przez sondę różnicowo prądową.

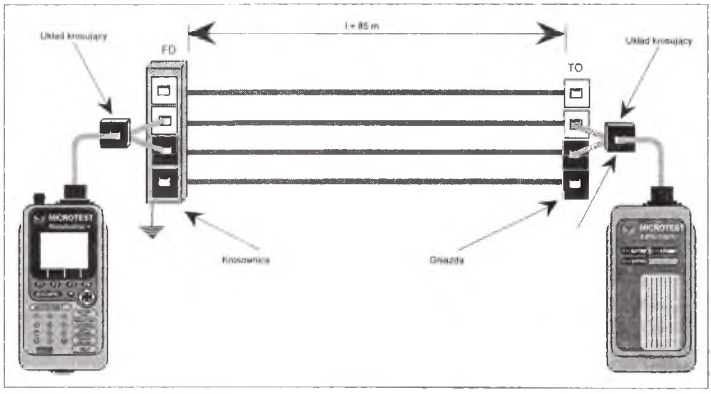


Rys. 11. Schemat układu pomiarowego sygnału w torze detekcji

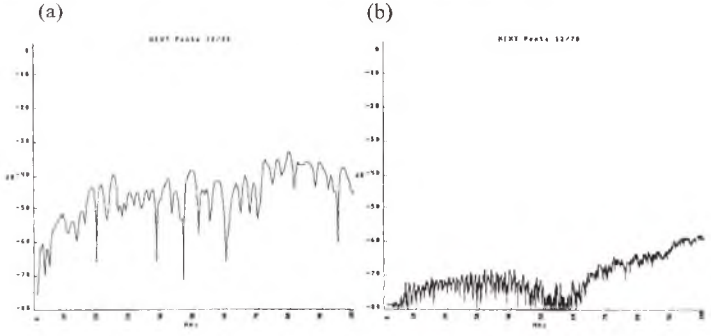
poziomu przesłuchów pomiędzy parami w tym samym kablu oraz pomiędzy parami w różnych kablach .

Pomiary przesłuchów w tym samym kablu wykonano testerem PentaScanner 350. Pomiar ten był weryfikowany poprzez pomiar analizatorem sieci HP8711A dla wybranych par. Pomiary przesłuchów pomiędzy kablami wykonano zarówno analizatorem sieci HP8711A i testerem PentaScanner 350.

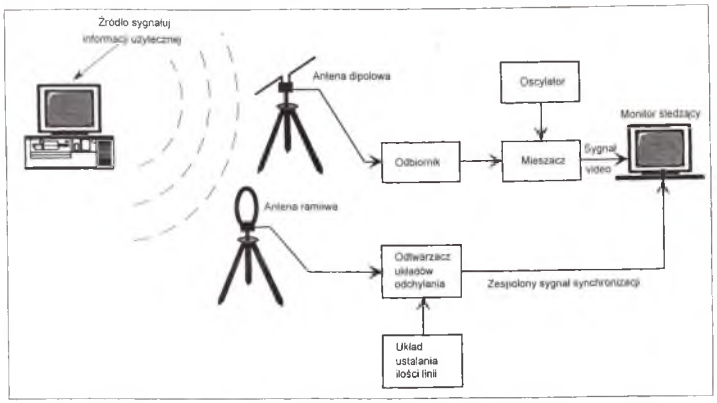
W przypadku pomiaru analizatorem sieci HP8711A, sygnał wyjściowy i wejściowy był podawany przez układy dopasowujące (100 Ω / 50 Ω) DMB-4 firmy EG&G o bardzo dobrym zrównoważeniu względem masy (powyżej 50 dB) w całym mierzonym paśmie częstotliwości (300 kHz - 100 MHz). Wszystkie pary przewodów były zakończone obciążeniem dopasowanym o impedancji 100 Ω.



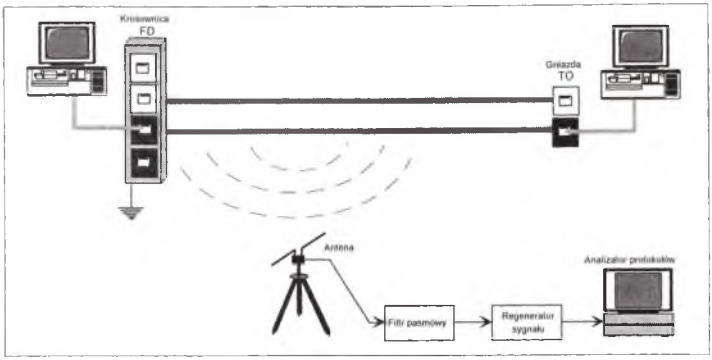
Rys. 6. Schemat układu pomiarowego z wykorzystaniem miernika PentaScanner 350



Rys. 7. Poziom przesłuchu zmierzony testerem PentaScanner 350 pomiędzy:
(a) - parami 12 i 36 w tym samym kablu ekranowanym (S/UTP)
(b) - parami 12 i 12 w dwóch różnych kablach ekranowanych (S/UTP)



Rys. 1. Przykład systemu detekcji informacji użytecznej z monitora komputerowego



Rys. 2. Przykład systemu detekcji informacji użytecznej z okablowania sieci komputerowej

5. Badania rozpraszania elektromagnetycznego instalacji sieci komputerowych

Miarą możliwości detekcji informacji użytecznej mogą być charakterystyki tłumienia w kanale podsłuchującym. Przykładem takich charakterystyk są:

- wielkości przesłuchów mierzone w funkcji częstotliwości wewnątrz kabla i pomiędzy kablami instalacji sieciowej,
- tłumienność rozpraszanego sygnału użytecznego w funkcji częstotliwości, mierzona anteną w otoczeniu instalacji kablowej sieci.

W celu sprawdzenia możliwości detekcji informacji użytecznej z typowych - stosowanych w sieciach strukturalnych - torów symetrycznych, nazywanych zazwyczaj „skrętką" przeprowadzono pomiary obydwu wymienionych rodzajów charakterystyk tłumienia.

5.1. Badanie przesłuchów w torach symetrycznych

Badania przeprowadzono w instalacji okablowania strukturalnego wykonanej z czterech kabli typu „skrętka" (dwa kable typu UTP kategorii 5 i dwa kable S/UTP kategorii 5) prowadzonych równolegle na odcinku ok. 85 m. Kable ekranowane uziemiono po stronie krosownicy (FD). Pomiary przeprowadzono przy pomocy analizatora sieci HP8711A firmy Hewlett

pomiaru charakterystyk interferencji radiowych urządzeń techniki informatycznej. W Polsce podstawowe zagadnienia dotyczące kompatybilności elektromagnetycznej zawarto w trzech normach opracowanych w latach osiemdziesiątych

- **PN-80/T-01005** - Przemysłowe zakłócenia radioelektryczne. Nazwy i określenia podstawowe.
- **PN-86/E-06600** - Automatyka i pomiary przemysłowe. Kompatybilność elektromagnetyczna urządzeń. Ogólne wymagania i badania.
- **PN-89/E-06251** - Przemysłowe zakłócenia radioelektryczne. Techniczne urządzenia informatyki. Dopuszczalne poziomy zakłóceń. Wymagania i badania.

Techniczne urządzenia informatyki IT (ang. Information Technology) można traktować jako potencjalne źródła informacji użytecznej, którą możemy poddać detekcji. Problem detekcji informacji użytecznej jest ściśle związany z poziomem emisyjności źródeł informacji użytecznej. Metody pomiarowe zalecane przez powyższe normy mogą mieć zastosowanie w określaniu metodyki detekcji i ochrony przez detekcją.

3.2.1. Pomiary natężenia pola zakłóceń

Wartość natężenia pola wyznacza się na podstawie pomiaru napięcia U doprowadzonego do wejść miernika z anteny pomiarowej korzystając z następującej zależności

$$E\ [\mu V/m] = K\ [1/m] * U[\mu V] \qquad (1)$$

lub

$$E\ [dB\mu V] = K\ [dB] + U\ [dB\mu V] \qquad (2)$$

przy czym: E - natężenie pola elektromagnetycznego,
K - współczynnik antenowy,
U - napięcie mierzone na wyjściu anteny

Pomiarów dokonuje się zwykle na specjalnych poligonach pomiarowych. Metody pomiarowe opisane są dokładnie w normach (CISPR 22, PN-89/E-06251, EN 550022).
W każdym punkcie przestrzeni pole jest wypadkowa działania fali bezpośredniej i odbitej. Jeżeli spełnione są warunki

$$l>2L \text{ oraz } l>3\lambda \qquad (3)$$

przy czym: l - odległość anteny od elementu promieniującego,
L - największy wymiar liniowy elementu promieniującego,
λ - długość fali.

to pomiary wykonuje się w strefie dalekiej. Stosunek natężenia pola E/H jest wtedy stały i wynosi

$$E/H=120*\pi \qquad (4)$$

W zakresie częstotliwości mniejszych od 30 MHz wykonywanie pomiarów w strefie dalekiej jest w praktyce utrudnione. W tym zakresie mierzy się obie składowe pola elektromagnetycznego w określonym punkcie w strefie bliskiej lub pośredniej. Niejednorodność pola powoduje, że wyniki nie pozwalają oszacować wartości pola w innych punktach przestrzeni. Dla częstotliwości większych od 30 MHz przyjmuje się, że składowa elektryczna mierzona w odległości co najmniej 10 m od źródła charakteryzuje wystarczająco i jednoznacznie promieniowanie źródła Podczas pomiarów, nie jest znana charakterystyka promieniowania i polaryzacja mierzonego sygnału. W celu określenia największej wartości natężenia pola, pomiarów dokonuje się przy rożnych polaryzacja, kierunkach i wysokościach zawieszenia anteny.

Normy dopuszczają przeprowadzenie badań w miejscu zainstalowania u użytkownika. Pomiary zaleca się wykonywać na granicy terenu wydzielonego. Jeżeli badane urządzenie jest zainstalowane w odległości mniejszej niż 10 m od granicy terenu, pomiary zaleca się wykonywać na zewnątrz terenu w odległości 10 m od badanego obiektu. Normy dopuszczają również pomiary z mniejszych odległości.

3. Metody pomiaru rozpraszania elektromagnetycznego urządzeń komputerowych (normy i zalecenia)

3.1. Zakłócenia w torze pomiarowym

Sygnał emitowany przez źródło sygnału informacji użytecznej może ulec zakłóceniu na drodze do anteny pomiarowej tzn., podczas rozpraszania elektromagnetycznego informacji użytecznej widmo emitowanego sygnału może zostać zaburzone w skutek obecności niepożądanych przebiegów elektrycznych rożnego pochodzenia.

Rozpatrując system detekcji i miejsce i w którym sygnał zostaje zakłócony, za miejsce powstawania zakłóceń możemy przyjąć jeden z czterech elementów tego systemu:

- źródło informacji użytecznej,
- tor emisji,
- odbiornik (detektor).

3.1.1. Typy zakłóceń

Zakłócenia powstałe w źródle sygnału informacji użytecznej, wywołane procesem przetwarzania wiadomości pierwotnej w wiadomość wtórną, przypisujemy sygnałom rozpraszanym przez źródło w torze emisji. Do tego rodzaju zakłóceń zaliczamy:

- zniekształcenia nielinearne i intermodulacyjne,
- przydźwięki,
- szum cieplny,
- szum śrutowy,

Rozpraszany sygnał jest funkcją czasu.

W torze emisji sygnał może ulec zniekształceniom przez zakłócenia typu multiplikatywnego i addytywnego zewnętrznego..

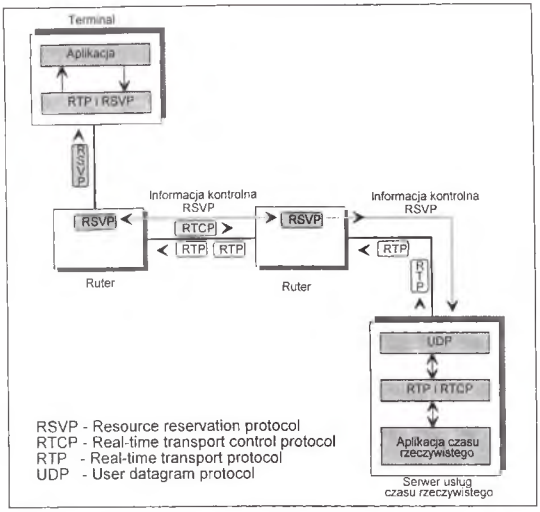
Zakłócenia multiplikatywne są spowodowane rozpraszaniem energii, związanym z propagacją fali w środowisku określonym przez tłumienność w funkcji częstotliwości. Tłumienność ze względu na niejednorodność i niestacjonarność środowiska oraz wielodrogowość propagacji jest również funkcją czasu i miejsca.

Zakłócenia addytywne zewnętrzne wywołane są przez przebiegi elektryczne związane z pracą urządzeń elektroenergetycznych (zakłócenia energetyczne) lub wywołane wyładowaniami atmosferycznymi (zakłócenia atmosferyczne), emisjami służb telekomunikacyjnych (zakłócenia od radiostacji), promieniowaniem elektromagnetycznym ciał niebieskich (zakłócenia kosmiczne) itp. Jeżeli widma tych zakłóceń (lub ich cześć) leżą w torze emisji sygnału informacji użytecznej, dodają się do widma sygnału.

W odbiorniku podobnie jak to ma miejsce w źródle sygnał jest zniekształcony przez zakłócenia multiplikatywne związane ze wzmocnieniem lub tłumieniem sygnału i przez zakłócenia addytywne wewnętrzne.

Można dokonać klasyfikacji zakłóceń addytywnych dzieląc je na:

- **harmoniczne** - o ograniczonym widmie częstotliwości, wywołane głównie przez służby telekomunikacyjne. Szerokość widma zazwyczaj nie przekracza szerokości widma sygnału odbieranego;
- **impulsowe** - o ograniczonym czasie trwania, pochodzące np. od bliskich wyładowań atmosferycznych, od iskrzenia styków, przebiegów elektrycznych itp. Czas trwania pojedynczego impulsu zakłócającego jest znacznie krótszy od długości elementu sygnału, lecz jego energia może być stosunkowo duża;
- **fluktuacyjne** - nie ograniczone w czasie i częstotliwości. Wywołane wewnętrznymi zakłóceniami urządzeń elektronicznych, takimi jak szum cieplny, szum śrutowy, szum pochodzący od



Rys. 2. Przykład realizacji łącza wirtualnego w sieci IP dla transmisji multimedialnej z wykorzystaniem protokołów RTP i RSVP.

W trakcie opracowania jest protokół RTP (ang. Real Time Transport Protocol), który stanowi warstwę transportową dla przesyłania sygnałów czasu rzeczywistego *(Rys. 2).*

5. Podsumowanie

Duże zapotrzebowanie na usługi multimedialne będzie czynnikiem stymulującym integrację różnych sieci w jeden spójny system telekomunikacyjny, który może być nazwany **globalnym systemem multimedialnym**.

Czynnikiem integrującym będzie zunifikowany terminal użytkownika współpracujący ze stykiem do multimedialnej sieci wirtualnej. Istniejące różnice technologiczne w stosowanych systemach transmisyjnych zostaną ukryte, poprzez zdefiniowanie protokołów pracujących w sieciach wirtualnych. Nie jest możliwe w ciągu najbliższych kilkunastu lat wprowadzenie homogenicznego systemu transmisji (np. tylko BISDN z ATM) dla globalnego systemu multimedialnego.

Warunkiem powstania systemu globalnego z połączenia usług w różnych sieciach telekomunikacyjnych i teleinformatycznych jest ujednolicenie parametrów jakości usług (QoS).

Tabela 1.

Rodzaj programu telewizji konwencjonalnej	**Strumień danych po kompresji MPEG 2**
Obraz szerokoekranowy	6 Mb/s
Obraz zawierający szybki ruch	4 Mb/s
Obraz z programu informacyjne	2 Mb/s
Film	2÷3 Mb/s

W systemie MPEG 2 przyjmuje się, że aby zapewnić dobrą jakość odtwarzanego w odbiorniku obrazu, do transmisji sygnału wymagane są prędkości bitowe jak w *Tabeli 2.*

Tabela 2.

System	**Prędkość bitowa**
Duża rozdzielczość	24÷32 Mb/s
Podwyższona rozdzielczość (jakość studyjna)	ok. 9 Mb/s
Rozdzielczość konwencjonalna (odpowiadająca PAL/SECAM)	4,5÷6 Mb/s
Mała rozdzielczość obrazu (odpowiadająca VHS)	ok. 1,5 Mb/s

MPEG 2 stosowany jest w telewizji cyfrowej (ang. Digital Video Broadcasting) i zalecany do stosowania w sieci ATM. W sieci ATM MPEG 2 jest zdefiniowany dla warstwy adaptacyjnej AAL1 (zalecenia europejskie) i dla AAL5 (zalecenia amerykańskie).

W Europie problemami normalizacji w dziedzinie multimediów zajmuje się głównie ETSI (European Telecommunications Standards Institute). W zakresie norm międzynarodowych główną rolę odgrywa ITU-T.

4. Multimedia w Internecie

Sieć komputerowa Internet z zasady swojego działania jest siecią z komutacją pakietów. Do niedawna była ona wykorzystywana wyłącznie do przesyłania danych komputerowych. Obserwowany w ostatnich latach rozwój sprzętu komputerowego pozwolił na realizację usług związanych z transmisją ruchomego obrazu i dźwięku. Rozwój aplikacji a w szczególności World Wide Web stał się przyczyną zwiększenia zapotrzebowania na nowe usługi.

Pasmo, opóźnienie sygnału, fluktuacje opóźnienia, to parametry krytyczne dla transmisji ruchomych obrazów i fonii. Wartości tych parametrów decydują o jakości transmisji QOS (ang. Quality of Service) oferowanej przez sieć.

Dostępne pasmo kanału transmisyjnego określa maksymalną szybkości transmisji. Opóźnienia decydują o jakości usługi szybkiej wymiany informacji. Fluktuacje czasu opóźnienia wpływają na płynność i synchronizację przesyłanej informacji. Z tego względu zaawansowane usługi multimedialny pracujące w czasie rzeczywistym, takie jak np. video na żądanie, wymagają dedykowanego kanału transmisyjnego o zadanych parametrach QOS. Parametry takiego kanału użytkownik może zmieniać w zależności od rodzaju wykonywanej aktualnie usługi. Sieć Internet nie posiada możliwości rezerwacji kanału o żądanych parametrach transmisyjnych. Stosowane do niedawna techniki transmisyjne w sieciach lokalnych, miejskich i rozległych z tradycyjnymi

REALIZACJA SIECI WIRTUALNYCH I TRANSMISJI MULTIMEDIALNYCH

Waldemar E. Grzebyk, Jarosław M. Janukiewicz

Naukowa i Akademicka Sieć Komputerowa
Zakład Telekomunikacji
50-327 Wrocław, ul. Janiszewskiego 7/9, tel./fax: 219529

1. Wstęp

W okresie ostatnich dwóch lat w sieciach „zadomowiły" się dwa pojęcia sieci wirtualne i multimedia. Obydwa mają długą historię lecz ostatnio wraz z szybkim rozwojem sieci transmisji danych nabrały dużego znaczenia i znalazły wymiar praktyczny. Przez sieci wirtualne rozumiemy struktury komunikacyjne (zazwyczaj w warstwie drugiej lub trzeciej wg. ISO OSI) tworzone w obrębie innych sieci posiadające cechy sieci fizycznych. Użytkownik zazwyczaj postrzega sieć wirtualną poprzez standardowy interfejs i parametry transmisji określone przez przepustowość, opóźnienia i fluktuacje opóźnienia. Ukryta jest przed nim wewnętrznej struktura sieci. Połączenia w sieci wirtualnej mogą stanowić ekwiwalent łącza znanego z tradycyjnych systemów telekomunikacyjnych, jeżeli zostaną zapewnione określone parametry transmisji.

Celem niniejszego opracowania jest przedstawienie wybranych rozwiązań i trendów w rozwoju sieci z usługami multimedialnymi.

2. Trendy i kierunki rozwoju sieci z usługami multimedialnymi

Transmisje multimedialne to połączenie transmisji obrazu, dźwięku i danych w dowolnych kombinacjach w celu realizacji takich usług jak telekonferencje, wideo konferencje, telefonia, systemy rozsiewcze foniczne i wizyjne. Cechą oczekiwaną współczesnych sieci transportowych i dostępowych jest możliwość dynamicznego udostępnienia łącza o ustalonych parametrach dla potrzeb transmisji multimedialnych. Rolę sieci transportowych i dostępowych mogą spełniać np. Internet lub sieć szerokopasmowa. W chwili obecnej obserwujemy gwałtowny rozwój usług multimedialnych. Najczęściej dla potrzeb multimediów adaptowana jest i rozwijana rodzina protokołów Internetowych. Wraz z rozwojem sieci zbudowanych zgodnie ze standardem ATM pojawiają się implementacje systemów transmisji, które wykorzystują właściwości ATM w zakresie usług multimedialnych. Znane są rozwiązania systemów telekonferencyjnych dla sieci typu Frame Relay. Dobrze zdefiniowane są systemy telekonferencyjne wykorzystujące ISDN.

Dynamicznie rozwijające się usługi i aplikacje multimedialne wymagają prac normalizacyjnych i regulacyjnych pozwalających na współpracę różnych systemów telekomunikacyjnych i teletransmisyjnych. Obecnie wiodącą rolę w telekomunikacji i teletransmisji odgrywają co najmniej cztery rodzaje takich systemów:

- klasyczne sieci telekomunikacyjne,
- telewizja kablowa,
- telefonia komórkowa,
- Internet.

Można zaobserwować trend do oferowania tych samych usług, wśród których można wymienić:

- rozmowy telefoniczne,
- transfer obrazów w czasie rzeczywistym,
- pocztę elektroniczną,
- dostęp do dokumentów multimedialnych,
- wideo na życzenie
- usługi wideo interakcyjne

6. **Ruch wychodzący ważony**

Patrz uwagi w pkt.5.

Całkowita opłata za ruch (PLN)	**789163**
Ruch wychodzący nieważony (MB)	**355576**
Opłata jednostkowa (PLN/MB)	**2,22**

Przykłady wyliczenia opłat w oparciu o różne warianty taryfikowania dla wybranych abonentów zawiera Aneks.

Wariant ryczałtowy

Kalkulacja opłat w niniejszym wariancie dokonywana jest w następujący sposób. Sumę opłat według cennika NASK dzieli się przez łączną przepływność portów wszystkich abonentów, w efekcie otrzymując jednostkową opłatę za kbps portu klienta. Całkowita należność od abonenta jest wówczas iloczynem powyższej opłaty jednostkowej i przepływności portu.

Opłata całkowita (PLN)	**872001**
Łączna przepływność (kbps)	**191936**
Opłata jednostkowa (PLN/kbps)	**4,54**

Czynnikiem powstrzymującym NASK przed stosowaniem ryczałtu jest m.in. fakt, że środki na opłacenie korzystania przez środowisko naukowe i akademickie są ściśle określone i jakikolwiek przyrost ruchu nie zostałby opłacony ; ww. środowisko charakteryzuje duża dynamika wzrostu ruchu.

Warianty opłaty za ruch

O ile podstawą symulacji w wariancie opłaty ryczałtowej była suma opłat z tytułu abonamentu i wygenerowanego ruchu, o tyle w niżej zaprezentowanych wariantach ujmuje się 2/3 abonamentu stanowiące w przybliżeniu „opłatę" za bezpłatny limit jednostek przeliczeniowych (JP) ruchu oraz kwotę należną za ruch ponad abonament. Przyjmuje się, że 1/3 abonamentu zależna od przepływności portu pozostaje bez zmian.

1. **Ruch całkowity nieważony**

Dane do taryfikacji otrzymuje się sumując bez ważenia ruch całkowity lokalny, krajowy i zagraniczny a następnie dzieląc przezeń całkowitą opłatę z tytułu ruchu (p.Warianty opłaty za ruch).

Całkowita opłata za ruch (PLN)	**789163**
Całkowity ruch nieważony (MB)	**1750533**
Opłata jednostkowa (PLN/MB)	**0,45**

2. **Ruch całkowity ważony**

Stosowany obecnie przez NASK . Wyliczenia jak w p.1 po zważeniu ruchu krajowego i lokalnego.

Ogólnie rzecz biorąc ruch zagraniczny ma się do krajowego i lokalnego jak 4:2:1. Takie są też wagi dla ruchu przychodzącego i wychodzącego.

Dla ruchu całkowitego wagi związane z poszczególnymi rodzajami ruchu są następujące:

ANALIZA ROZLICZEŃ ABONENTÓW NASK W RÓŻNYCH WARIANTACH CENNIKOWYCH

Marcin Pragłowski

Naukowa i Akademicka Sieć Komputerowa NASK, ul.Bartycka 18, 00-716 Warszawa

E-mail: marcin@nask.pl

Wstęp

Przedmiotem niniejszego referatu jest symulacja rozliczeń NASK z abonentami przeprowadzona w oparciu o możliwe do zastosowania warianty taryfikacji na podstawie danych za ruch zarejestrowany w marcu b.r. Dane dotyczą abonentów podłączonych łączem stałym.

WPROWADZENIE

Metody taryfikacji

Wśród obecnie stosowanych w świecie metod taryfikowania za korzystanie z sieci Internet rysuje się zasadniczy podział na :

- opłaty ryczałtowe w zależności od przepływności portu
- opłaty w zależności od zarejestrowanego ruchu

Wybór wariantu zależy od uwarunkowań oddziałujących na dostarczyciela (providera) Internetu.

Ryczałt

Jeżeli operator ma wysokie koszty stałe związane z utrzymaniem infrastruktury telekomunikacyjnej, wówczas jest bardziej skłonny do wyboru wariantu opłaty ryczałtowej, łatwiejszej w rozliczeniu lecz mogącej powodować niezrównoważony dodatkowymi wpływami finansowymi wzrost ruchu w sieci. Tego typu sytuacja jest akceptowalna dla operatorów telekomunikacji tradycyjnej, których infrastruktura jest wykorzystywana w niewielkim stopniu (kilka do kilkunastu procent w Europie Zachodniej).

Niezależnie od tego, co zostało powiedziane wcześniej, wariant ryczałtowy stosowany jest również przez operatorów korzystających głównie z infrastruktury nie będącej w ich posiadaniu; należy mniemać, że krok ten jest podyktowany koniecznością dostosowania do cen stosowanych przez operatorów tradycyjnych.

Rodzi się wówczas zagrożenie rozziewem pomiędzy zobowiązaniami z tytułu opłat za wykorzystanie infrastruktury (naliczanymi na bazie transferowanego ruchu, czasu trwania transferu, bądź odległości) a należnościami od abonentów (ryczałt). Ponadto zmiana liczby abonentów i generowanego przez nich ruchu utrudnia konstruowanie cennika zapewniającego pokrycie kosztów oraz grozi nadmiernym obciążeniem sieci.

Korzyść z rozliczenia ryczałtowego zauważana przez abonenta to pewność, że opłata z tytułu korzystania z sieci Internet w danym okresie czasu zamknie się określoną kwotą.

dostępu do Internetu. Po upływie dłuższego czasu widać jej zasadnicze wady, przede wszystkim w postaci nierównego podziału kosztów oraz tworzeniu warunków do rywalizacji o pełne wykorzystanie pasma co dla jakości usług Internetowych jest zabójcze. Po zawarciu umów zbiorowych z podstawowymi abonentami korzystającymi z usług w oparciu o opłatę za pasmo, usługa zostanie zlikwidowana.

Opłata uwzględniająca ruch generowany przez abonenta ma jednak kilka wad. Chronologicznie pierwszą podnoszoną publicznie był zarzut pobierania opłaty za ruch przychodzący, którego abonent sobie nie życzy. Pomijając argumentację w okresie przejściowym trzeba zauważyć, że obecnie coraz popularniejsza jest metoda pobierania opłat tylko za ruch przychodzący. Drugą istną wadą metody przyjętej w NASK jest nieuwzględnienie istnienia równorzędnych operatorów krajowych. W cenniku przyjęto, że operatorowi zagranicznemu należy płacić, zgodnie z rzeczywistością i koszty tych opłat musi ponieść abonent. Natomiast operatorzy krajowi, analogicznie jak to jest w przypadku NASK w stosunku do operatorów zagranicznych, płacą NASKowi, wobec czego koszty te nie obciążają abonenta. W chwili pojawienia się operatora w postaci Telekomunikacji Polskiej SA, który wręcz odmówił opłat wykorzystując swoją siłę rynkową, powstał problem pokrycia kosztów pracy abonentów POLPAK T w sieci NASK. Dzisiaj problem ten jest rozwiązany prowizorycznie poprzez ograniczenie kanału dostępu do sieci POLPAK T i solidarna pokrywanie tego kosztu przez abonentów NASK. Niestety problem wzrostu kosztów wynikający z rozrastania się sieci, tym samym udostępniania coraz większych zasobów abonentowi nie daje się pominąć. Nie można zakładać, że operator każdej sieci uzyska taki przyrost opłat od abonentów, że rosnące koszty pokryje ze zwiększonych dochodów. Nawet jeśli tak się stanie odbędzie się to w zamian za należną abonentom obniżkę kosztów, co będzie dotyczyło również tych, którzy nie skorzystają z większych możliwości dostępu do zasobów połączonych sieci. Problem nie jest incydentalny, ponieważ, na przykład, również nowopowstającej sieci TEN34 opłata abonamentowa za przyłączenie do sieci rośnie w miarę przyłączania nowych abonentów. W przypadku niewielkiej ilości tych abonentów i w warunkach umowy grupowej jest to możliwe. Podstawą cennika to być nie może.

Jednak podstawowa wada tego typu rozliczeń kryje się w samej istocie Internetu. Internet gubi informacje. Skala tego zjawiska jest różna od kilku, normalnie kilkanaście, do kilkudziesięciu procent pakietów danych. Gubienie to jest zależne od szeregu czynników losowych, na który wpływ ma globalne zachowanie użytkowników sieci, oraz zachowania konkretnego abonenta, który nie uwzględnia lub nie chce uwzględnić istoty sieci Internet i jej konkretnych uwarunkowań lokalnych. Straty wynikające z faktu gubienia informacji mogą być uśrednione i wkalkulowane w cenę przesłania informacji. W takim przypadku możliwy byłby pomiar ruchu na styku z klientem kontrolowany dwustronnie. Jednak w tym przypadku konieczne byłoby uśrednienie ceny przesłania lub instalowanie systemów taryfikujących na każdym styku z klientami. Oczywiście kosztowałoby to duże pieniądze i podniosło istotnie ceny. Pomiar ruchu dokonywany jest w kilku wyróżnionych punktach: na styku z sieciami zagranicznymi, na styku z siecią krajową oraz na styku z instalacją abonenta. Ponieważ, jak poprzednio napisaliśmy, Internet gubi informacje, pomiary te się nie bilansują co rodzi niepokój oraz sprzeciwy. Jak pisaliśmy zaniechanie tego typu pomiarów i rozliczeń na ich podstawie prowadzi do uśrednienia cen, obciążenia wszystkich skutkami działania niektórych oraz nie skłania do rozsądnych działań abonentów. Przyjęty system rozliczeń jest niedoskonały, ale "najlepszy ze złych", ponieważ poprawnego systemu rozliczeń do tego czasu nie wynaleziono. Dopiero wprowadzenie zasadniczych zmian do IP może coś poprawić, powstaje jednak pytanie - czy będzie to nadal Internet ?

System opłat związanych z ruchem rodzi również skutki psychologiczne, szczególnie przy zmasowanych kampaniach w środkach masowego przekazu, powodujące, że cześć abonentów zachowuje się nie rozsądnie, nie wykorzystując nawet bezpłatnych limitów ruchu. Dla tych abonentów cennik wprowadza ofertę specjalną polegającą na wprowadzenie opłaty zryczałtowanej

partnerów odpowiada, za wywołany ruch w sieci. Inaczej sprawa się przedstawia przy rozpowszechnianiu informacji, pracy dialogowej itp. z tym, że stwierdzenie o niemożności ustalenia odpowiedzialnego za wywołany ruch jest nadal prawdziwa. W sieci operowanej przez NASK dla rozliczeń ruchu Internetowego przyjęto zasadę solidarnego pokrywania kosztów, to znaczy, że w każdym przypadku współpracy dwóch abonentów sieci NASK, pokrywają oni koszt przesłania solidarnie po połowie. De facto tak jest zawsze, bo w przypadku dzierżawy pasma czy kanału przesyłania zawsze płacą obaj partnerzy pracujący na dwóch końcach łącza. Zwracamy uwagę, że tak się dzieje w przypadku opłat za kanały Frame Relay i ATM to znaczy tam, gdzie nie można ustalić inicjatora transmisji. Nie wiąże się to również z systemem opłat / ryczałtowe, za pasmo czy za ruch/.

3. Rozliczenia i cenniki - doświadczenia NASK

Stworzenie odrębnego systemu dla każdej technologii telekomunikacyjnej jest zbyt pracochłonne w sieci stosunkowo niewielkiej o bardzo dużej różnorodności. Wobec tego nastąpiła redukcja problemu poprzez podzielenie usług na kilka grup, w ramach których stosuje się optymalne, systemy taryfikacji i rozliczeń Najogólniej mamy do czynienia z trzema grupami usług i abonentów.

- Usługi polegające na zapewnieniu abonentowi połączeń telekomunikacyjnych poprzez sieć NASK, w których abonent łączy się poprzez sieć tylko sam ze sobą. W tej grupie znajdują się również usługi dla abonentów zbiorowych.

- Usługi polegające na przyłączeniu abonenta do sieci otwartej. NASK zapewnia swoimi środkami usługi tylko w pewnym zakresie, w pozostałym usługi świadczą inni operatorzy, z którymi za świadczenie tych usług należy się rozliczyć.

- Wreszcie usługi mieszane, gdzie abonent korzysta zarówno z przyłączenia do sieci otwartej, jak i połączeń telekomunikacyjnych poprzez sieć NASK.

Ceny oferowane przez NASK składają się z dwóch składników: opłaty jednorazowej, która rekompensuje koszty związane z instalacją i udostępnieniem portu, oraz opłaty za utrzymanie usługi, która rekompensuje koszty bieżące utrzymania oraz rozłożone w czasie koszty zaangażowanych środków trwałych.

NASK oferuje połączenia telekomunikacyjne oparte na dwóch protokołach Frame Relay oraz ATM, być może w niedalekiej przyszłości poprzez łącza fizyczne. Dla abonentów pojedyńczych opracowane są cenniki dzierżawy kanałów zawierające dwa składniki: opłatę za dzierżawę portu dostępu oraz dzierżawę kanału logicznego. Zarówno port jak i kanał charakteryzowane są poprzez przepustowość, która może być asymetryczna. Dla sieci Frame Relay przepustowość kanału logicznego jest określana przez gwarantowane pasmo CIR oraz rozszerzone EIR, który w przypadku NASK stanowi dwukrotność CIR. NASK odpowiedzialnie traktując abonentów nie oferuje im połączeń z CIR równym zero, co oznacza, że abonent w przypadku awarii czy zapchania sieci nie ma de facto żadnych uprawnień i możliwości korzystania z usługi. W przypadku ATM przepustowość cennikowa jest określana jako odpowiednia cześć przepustowości portu.

Połączenie Frame Relay mają swoją odmianę w postaci usługi LAN INTERCONNECT, która różni się od poprzedniej dwoma cechami:

następnie kod rejonu telekomunikacyjnego i w pozostałości adres docelowego DTE. Pozwala to na obliczenie trzyczęściowej opłaty składającej się z opłaty za nawiązanie połączenia, opłaty za czas utrzymania kanału (VC Virtual Call) oraz opłaty za liczbę przesłanych segmentów (64 oktety) zawierającej opłatę uzależnioną od tego czy ruch jest lokalny, międzyrejonowy czy międzynarodowy. W ten sposób operator, do którego jest dołączony abonent może obliczyć całość należności za przesyłanie w sieci własnej oraz w sieciach innych operatorów, z którymi się następnie rozlicza.

Usługa w sieci Frame Relay polega na udostępnieniu kanału o gwarantowanej przepustowości. Nie ma nawiązywania połączenia, ponieważ jest ono zestawione na stałe (PVC Permanent Virtual Circuit). Kanał jest zestawiony pomiędzy dwoma lokalizacjami jednego lub dwóch płatników. Opłatę pobiera się solidarnie od obu, z których każdy płaci za port oraz gwarantowaną przepustowość przy czym opłata jest uzależniona od długości kanału logicznego.

Podobnie jest w sieci ATM, gdzie pobiera się solidarnie opłatę za oba porty oraz gwarantowaną przepustowość stanowiąca część przepustowości portu.

Największy problem stanowi taryfikacja w sieci Internet. Nie ma nawiązywania połączenia na poziomie sieci wobec czego nie można ustalić inicjatora transmisji, można tylko ustalić nadawcę i odbiorcę. Nie ma kanału logicznego, wobec tego pomiary ruchu mogą odbywać się tylko w charakterystycznych punktach sieci. Protokół nie gwarantuje jakości przesyłania wobec tego ceny muszą być ustalane brutto. Ponieważ nie jest znany inicjator przesyłania opłatę trzeba dzielić solidarnie pomiędzy nadawcę i odbiorcę. W takiej sytuacji najprostsze wydają się opłaty ryczałtowe lub za port przyłączenia. Poza ograniczonymi przypadkami, kiedy abonent ze względów technicznych ma limitowane możliwości pracy w sieci (połączenia telefoniczne) takie rozwiązanie zagraża wprost jakości pracy sieci, która może pracować znośnie pod kilkoma warunkami:
- łącza są wykorzystane nie więcej niż w jednej trzeciej,
- abonent w ramach sesji kontroluje przepływ informacji.

W przypadku opłaty ryczałtowej za port lub opłaty za pasmo motywacje abonenta są odwrotne, jeśli chodzi o wykorzystanie portu czy pasma, a obojętne w zakresie organizowania sesji zapewniającej jakość przesyłania. W efekcie sieć pracuje źle, a operator nie ma środków na jej usprawnianie. Obserwacja obciążenia sieci NASK prowadzi do wniosku, że każda przepustowość sieci jest w krótkim czasie zbyt mała. Na przykład ponad dwukrotne zwiększenie przepustowości łącz międzynarodowych wystarczyło na niecałe pięć miesięcy. Konieczne jest dalsze podnoszenie przepustowości co powoduje dalszy wzrost kosztów lub ograniczenie się abonentów. Tylko taryfikacja za ruch daje większe środki na rozwój proporcjonalnie do jego wzrostu jednocześnie motywując abonenta do rozsądnego korzystania z sieci.

Ogólnoświatowy system telekomunikacyjny oparty jest między innymi na systemie umów pomiędzy operatorami. Umowy takie są i chyba zawsze będą pod szczególną obserwacją urzędów antymonopolowych i innych organizacji chroniących konsumenta, bowiem mogą zawierać elementy podziału rynku i porozumień cenowych. Z tego powodu operatorzy muszą brać pod uwagę fakt utrzymywania sieci przez jej abonentów i we wszelkich uzgodnieniach rozliczeniowych muszą chronić swoich klientów. Z tego też powodu nie mogą przenosić ciężaru swoich uzgodnień na abonentów na przykład w myśl zasady wszystkim po równo.

W sieci X.25 problem rozliczeń i obciążeń abonentów jest najprostszy. Abonent wie za co płaci, od jego wyłącznej woli wynika zestawienie połączenia i wynikające z tego roszczenie do zapłaty, operator w sposób bezpośrednio jawny pobiera opłaty na rzecz innych operatorów. Ponieważ jednak system szczegółowych rozliczeń każdy z każdym jest zbyt pracochłonny ustala się w skali międzynarodowej stawki rozliczeniowe na tyle uzasadnione, że nie powodują istotnych dopłat i strat w eksploatacji sieci poszczególnych operatorów.

W sieci Frame Relay w zasadzie podstawowe opłaty pobiera jeden operator wobec czego problem rozliczeń międzyoperatorskich jest mniej istotny. W sporadycznych przypadkach tworzenia

wykorzystywany nośnik może być okresowo przepełniony. Cytowana jest często graniczna przepustowość efektywnie działającej sieci z protokołem FDDI jako 25% przepustowości teoretycznej. Odpowiednie sterowanie przepływem, buforowanie informacji itp. spoczywa na urządzeniach dołączonych do sieci czyli abonentach.

Protokoły Ethernet czy FDDI normują przesyłanie w warstwie łącz logicznych i tym samym przeznaczone są do obszarów lokalnych. Najpopularniejszym, robiącym największą karierę jest protokół sieci otwartych IP. W nawale informacji pozytywnych wynikających z łatwości stosowania pomija się bardzo istotne wady tego protokołu, zwłaszcza przy bezmyślnym jego stosowaniu. Bezsprzeczne są zalety tego protokołu dla użytkowników prostych stacji końcowych. Natomiast dla operatora stanowi on źródło nieustających zmartwień.

Realizacja protokołu IP polega na nadawaniu, przełączaniu i odbiorze datagramów, które tworzą odrębne pakiety z ogólnoświatowym adresem. Pakiety są nadawane bez sprawdzenia możliwości przesłania wynikającej z istnienia wolnej drogi do nadawcy. Podobnie się dzieje przy kierowaniu ich na poszczególne linie przy przechodzeniu przez urządzenia przełączające (routery) na całej drodze do odbiorcy. Łatwo zauważyć, że nadchodzące pakiety napływają nierównomiernie wobec czego są kolejkowane. Ponieważ kolejki mają ograniczoną wielkość zdarza się, ze są pełne. Nadchodzący pakiet trafiający na przepełnioną kolejkę jest gubiony (drop). Liczba gubionych pakietów zależy od średniego zapełnienia łącza. Przyjmuje się, że przy zapełnieniu łącza średnio w czasie całej doby w 30%, gubienie pakietów występuje sporadycznie i ich liczba nie jest wielka. Wynika to z tego, że statystyczne prawdopodobieństwo chwilowych spiętrzeń ponad możliwości łącza buforowanego kolejkami na urządzeniach przełączających jest małe. Zwracamy uwagą na prawdopodobieństwo, czyli zachowaniu się mierzonym statystyką. Oczywiście zachowania się sieci w konkretnym miejscu i czasie są inne. Wypełnienia kolejek jest zupełnie niezależne od systemu przesyłania i jest wynikiem działania abonentów dołączonych do wszystkich sieci na świecie w ramach globalnego Internetu. Dla operatora jest to działanie niesterowalne o charakterze losowym.

W dalszym ciągu przedstawimy zalety i wady wymienionych wyżej protokołów komunikacyjnych stosowanych w teleinformatyce oraz ich podstawowe przeznaczenie.

Jak pisaliśmy poprzednio protokół HDLC nie ma znaczącego zastosowania w usługach świadczonych abonentowi końcowemu. Stosowany jest jako warstwa łącz dla protokołów sieciowych X.25 oraz IP. Nie będziemy go tutaj szerzej omawiać.

Protokół X.25, jeszcze kilka lat temu podstawowy w usługach telekomunikacyjnych traci obecnie na znaczeniu. Mała długość pakietu, nadmiar informacji kontrolnej oraz mała szybkość przesyłania odsuwają jego zastosowania na peryferia sieci teleinformatycznych. Jednak podstawowe zalety tego protokołu jak możliwość efektywnej pracy na słabych łączach oraz przeniesienie podstawowej części procedur komunikacyjnych na urządzenia sieciowe i tym samym odciążenie komputerów dołączonych do sieci zapewniają mu trwałość użytkowania jako narzędzia komunikacji w sieciach rozległych.

Protokół Frame Relay służy do zestawiania logicznych linii przesyłania poprzez wiele urządzeń (węzłów) sieci. Może być wykorzystywany w sieciach o podwyższonej jakości, na traktach cyfrowych. Służy do zestawiania stałych połączeń na przykład wewnątrz jednej korporacji, wielozakładowego przedsiębiorstwa, banku itp. Jest to również dobry protokół do usprawniania przesyłania w sieci Internet, poprzez uporządkowanie dróg przesyłu o gwarantowanej jakości i przepustowości. W sieci NASK jest to podstawowy protokół przesyłania w szkielecie sieci (back bone). Jego wadą jest ograniczenie funkcji do tworzenia kanałów logicznych, ograniczone pole adresowania oraz wyższe wymagania jakości sieci podstawowej. Do czasu rozpowszechnienia się protokołu ATM, protokół Frame Relay w sieciach rozległych będzie podstawowy w warstwie logicznej sieci rozległych i lokalnych realizowanych na połączeniach cyfrowych.

Protokół ATM jest nadal w fazie rozwoju standardów, techniki i technologii. Jego podstawową zaletą jest duża przepustowość i uniwersalność pozwalająca na transmisję danych,

Usługi teleinformatyczne różnią się od poprzednich tym, że wobec uczestniczenia w przepływie urządzeń automatycznych organizuje się również kontrolę przepływu informacji. Kontrola ta jest różna w zależności od cech fizycznej sieci, przy pomocy której świadczy się usługi. Najsilniejsza w przypadku protokołu HDLC i X.25, najsłabsza przy protokole ATM. Omówimy ją w dalszej kolejności.

Protokół HDLC służy do zestawiania kanału logicznego i przesyłania ramek informacji tylko pomiędzy dwoma stacjami DCE (Data Circuit Equipment) lub stacją DCE i DTE (Data Terminal Equipment). Adresowanie w tym protokole jest ubogie, mocne mechanizmy nawiązywania i rozłączania połączenia wraz z jego odzyskiwaniem w przypadku zerwania, mechanizmy kontroli przepływu z numerowaniem ramek, sprawdzaniem kolejności, potwierdzaniem odbioru z jednoczesną informacją o gotowości odbioru lub jej braku wraz z mocnymi procedurami odzysku informacji poprzez retransmisję czy ponowne nadawanie. Sam protokół HDLC rzadko występuje jako podstawa świadczenia usług telekomunikacyjnych dla abonenta. Najczęściej jest stosowany łącznie z protokołami X.25 oraz IP jako narzędzie dla tworzenia logicznych kanałów przesyłania pomiędzy dwoma węzłami (DCE), na których następuje przełączanie na poziomie sieciowym. Protokół X.25 działający w warstwie sieci posiada możliwość adresowania w skali całego świata poprzez znormalizowany, zhierarchizowany system adresowania. Podobnie jak omówiony protokół posiada mechanizmy nawiązywania połączenia i jego rozłączania, mechanizmy kontroli przepływu i odzysku utraconej informacji tylko nieco słabsze od protokołu HDLC. Protokół X.25 i HDLC tworzą bardzo silne narzędzie przesyłania w skali całego globu przystosowane do pracy na liniach, które w całości lub częściach są słabszej jakości - jednostkowa stopa błędów 10 do minus trzeciej potęgi. Stosowane szybkości przesyłania przy użyciu tych protokołów nie przekraczają 64 kbps.

W miarę poprawy jakości sieci telekomunikacyjnych zauważono, że rozbudowane procedury kontroli są zbędne - statystycznie zmniejszają efektywność przesyłania informacji. Wobec tego zaproponowano protokół Frame Relay z uproszczonymi procedurami ochrony i z rozszerzoną możliwością adresowania. Przy pomocy tego protokołu można zestawić kanał logiczny poprzez wiele urządzeń DCE. Rozbudowane pole adresowania pozwala na tworzenie wielu połączeń logicznych w ramach ograniczonej sieci. Specjalny protokół NII (Network to Network Independed Interface) pozwala na łączenia kanałów logicznych różnych sieci w jeden dla abonenta łączny. Uproszczono procedury przepływu rezygnując z kontroli na stacjach pośrednich ograniczając się tylko do procedur podobnego typu jak HDLC tylko na stacjach końcowych. Wprowadzono pojęcie gwarantowanej przepustowości CIR (Commited Information Rate) traktowanej osobno dla każdego kierunku adresowania. Uzyskano w ten sposób narzędzie lepiej przystosowane do jakościowo lepszych, najczęściej cyfrowych, traktów przesyłania, pozwalające na uzyskiwanie efektywnych szybkości do 52 Mbps. Trzeba jednak pamiętać, że Frame Relay pozwala wyłącznie na zestawienia efektywnego połączenia dwóch stacji końcowych, coś w rodzaju inteligentnego drutu. Bez współdziałania protokołów warstwy sieciowej, typu X.25 czy IP, nie pozwala na swobodne uzyskiwanie połączeń w sieci teleinformatycznej. Po dodaniu dodatkowych procedur Frame Relay pozwala również na transmisję głosu w sieci teleinformatycznej jednak niskiej jakości z powodu braku izochronizmu. Niektóre firmy uzupełniają urządzenia Frame Relay o procedury i elementy gwarantujące izochroniczność i wtedy w pełni nadają się do przesyłania i głosu i w ograniczonym szybkością zakresie obrazu ruchomego.

Dla wielkich szybkości przesyłania w sieciach cyfrowych wykorzystujących trakty cyfrowe SDH (Synchronous Digital Hierarchy) został wprowadzony kolejny protokół ATM. W tym protokole zrezygnowano w ogóle z kontroli przepływu, wychodząc z założenia, że straty w sieci wynikające z błędów transmisji są znacząco mniejsze niż koszty przesłania informacji kontrolnej. Wprowadzono natomiast bardziej rozbudowany system tworzenia kanałów logicznych grupując je dodatkowo w ścieżki. Najistotniejszą nowością i cechą protokołu jest wprowadzenie stałej długości ramki (cell) o wielkości tylko 53 oktetów. Upraszcza to procedury nadania i odbioru, a przede

Problemy pojawiają się także podczas samej wideokonferencji. Konieczne jest wybranie osoby prowadzącej, która szczególnie przy większej ilości uczestników przyznawałaby prawo głosu oraz ustalenie sposobu zarządzania sprzętem (można np. automatycznie pokazywać osobę mówiącą, albo ustalić źródło obrazu ręcznie). Szczególnie uwidacznia się także konieczność przyzwyczajenia się użytkowników do nowego rodzaju łączności. Tylko wtedy można wykorzystać wszystkie jego zalety.

Podsumowanie.

Wideokonferencja jest nowym, bardzo wygodnym i ułatwiającym pracę systemem łączności. Jego wykorzystywanie jest nie tylko przejawem mody, ale także bardzo ważnym czynnikiem ułatwiającym podejmowanie właściwych decyzji i zwiększającym operatywność zarządzania. Ten rodzaj łączności pozwala na szybkie porozumienie osób na duże odległości (w granicach Polski lub nawet w relacjach międzynarodowych), umożliwiając pracę podobną do bezpośredniego spotkania.

Istnieje już stosunkowo dużo produktów umożliwiających organizację wideokonferencji na profesjonalnym poziomie. Wszystkie z zasygnalizowanych problemów technicznych nie są zbyt trudne do pokonania. Rozwiązanie problemów organizacyjnych wymaga włożenia pewnego wysiłku, a także najprawdopodobniej uczenia się na błędach.

Jedyne co jest potrzebne z punktu widzenia użytkownika to decyzja, że chcemy wykorzystywać ten nowy środek łączności. Tylko w ten sposób jesteśmy w stanie, pokonując problemy, znaleźć odpowiednie dla nas jego zastosowanie.

najbardziej popularnym. Pozwala on na przeprowadzenie transmisji z zachowaniem niezbędnej dla przekazu obrazu i dźwięku izochroniczności - zachowania relacji czasowych w sygnale (małe, stałe opóźnienie). Taki sposób transmisji ma jednak swoje wady. Wymaga on zestawiania każdorazowo kanału o stałej przepustowości. Z ekonomicznego punktu widzenia nie jest to więc rozwiązanie optymalne, choć przy zastosowaniu połączeń ISDN - czasami jedyne możliwe.

Najtańsze w realizacji jest wykorzystanie już istniejącego medium - łącza IP. Takie rozwiązanie nie może jednak dostarczyć (przynajmniej na razie) satysfakcjonującej jakości. Nie znane i zmienne opóźnienia oraz skomplikowana, czasochłonna obróbka sygnału nie pozwalają na inne niż amatorskie wykorzystanie połączenia tego typu.

Rozwiązaniem obecnie prawdopodobnie najlepszym jest użycie technologii ATM. Łączy ona w sobie możliwości przesyłu danych komputerowych i izochronicznego sygnału wideo. Możliwe jest tutaj dynamiczne przydzielanie pasma nawet w trakcie trwania połączenia. Szczególne znaczenie ma to przy przesyłaniu sygnałów skompresowanych, jednocześnie wymagających zmiennej przepustowości łącza i izochroniczności. Technologia ATM jest jednak stosunkowo droga. Można się wydawać dziwne, pozostaje jednak faktem, że w porównaniu z ceną łącz użycie tego sposobu transmisji jest zazwyczaj opłacalne.

Na jakość wideokonferencji decydujący wpływ ma przepustowość łącz. Połączenie daje się już uzyskać przy szybkościach 28,8 kbps - 64kbps. Taki przekaz, pomimo kompresji, nie jest jednak zadowalający. W jego efekcie oglądamy serię zmieniających niezbyt często obrazów, w dużej części niekompletnych i z dużym opóźnieniem. Przy szybkościach rzędu 128kbps - 384kbps przekaz jest już w miarę czytelny, chociaż występują w nim odczuwane jako zakłócenia śnieżenia sygnału oraz opóźnienia. Najlepsze efekty uzyskuje się przy przepływnościach rzędu 5Mbps - 20 Mbps. Obraz jest wtedy niemal idealny.

Z praktycznego punktu widzenia ważny jest też sposób zestawiania połączenia. Gdy mamy do czynienia z koniecznością organizowania wideokonferencji stale między tymi samymi punktami, to czas zestawiania nie jest wówczas ważny. Linii takiej po prostu się nie rozłącza. Gdy jednak chcemy łączyć się z wieloma różnymi osobami, to należy wykorzystać zestawiane łącza - ISDN lub ATM.

Dla administracji publicznej ważna jest poufność łącz. Można ją uzyskać stosując kilka metod zabezpieczeń:

1. Szyfrowanie transmisji na poziomie aplikacji bądź łącza algorytmem z kluczem o odpowiedniej długości. Ograniczenia eksportu wprowadzone przez USA powodują trudności w uzyskaniu sprzętu realizującego ten sposób zabezpieczenia.

2. Ochrona przed podsłuchem łącz. Można stosować połączenia wirtualne zestawiane różnymi drogami, zaszumianie łącz innymi transmisjami (jak w technologii ATM) i inne tradycyjne sposoby.

3. Ochrona przed podsłuchem elektromagnetycznym (pomieszczeń i łącz).

Odrębny problem stanowi wybór sprzętu do wideokonferencji. Oprócz wideoprzekazu powinien on też zapewniać odpowiednie miksowanie lub przełączanie obrazu i głosu do i od wielu rozmówców. Przydatna jest też możliwość przekazywania obrazu ze specjalnej kamery filmującej

sieciowych. Istotną cechą jest także możliwość definiowania czasu ważności kluczy sesyjnych (w zakresie od 1 minuty do 24 godzin). Parametr ten ma ogromne znaczenie dla wydajności pracy routera. Ustawienie zbyt krótkiego czasu ważności kluczy (key life) z uwagi na fakt generowania wszystkich kluczy w procesie głównym (foreground) powoduje bardzo znacze spowolnienie pracy routera. Dostępna obecnie wersja oprogramowania szyfrującego posiada status „early deployment release", z informacji producenta wynika że przyszłe jego wersje będą potrafiły przenieść generację kluczy do procesów tła (background), co w znacznym stopniu poprawi efektywność obsługi połączeń. Inne ograniczenia dotyczą ilości możliwych do zdefiniownia reguł szyfracji (do 300 tzw. Kryptomap dla routerów 25xx). Nie istnieje także mechanizm upraszczający dystrybucję kluczy tzw. Centrum dystrybucji kluczy.

7. PODSUMOWANIE

Opisane doświadczenia we wdrażaniu technologii podwyższających bezpieczeństwo sieci pozwalają przypuszczać że wzrastające wymagania w zakresie bezpieczeństwa oraz wyraźnie rysujące się tendencje na rynku produktów tego segmentu potwierdzą słuszność oceny i zasadność doboru przedstawionych elementów ochrony sieci.

Określmy więc zarys kryteriów bezpiecznego transferu danych.

Bezpieczny transfer danych

Najprościej poprzez bezpieczny transfer danych rozumiemy zapewnienie następujących, potwierdzonych kryptograficznie mechanizmów:

- **integralności**
- **niezaprzeczalności**
- **poufności**

6.3.1. Bezpieczna poczta

Przykładem zastosowania wymienionych wyżej mechanizmów może być bezpieczna poczta.(opis standardów bezpiecznej poczty znajduje się w części p.t. *Wprowadzenie do technologii podwyższających bezpieczeństwo sieci teleinformatycznych*). Popularny e-mail jest jedną ze sztandarowych usług sieciowych, dlatego też dla „poważnych" zastosowań istotne jest stosowanie mechanizmów jego ochrony. Doświadczenia wynikające z wdrożenia i korzystania z bezpiecznej poczty w standarcie PEM (Privacy Enhanced Mail) jak również dostępnym publicznie standardzie PGP (Pretty Good Privacy), pozwalają wyraźnie zaobserwować dominujące cechy obydwu rozwiązań.

PEM a PGP - doświadczenia eksploatacyjne

PEM pomimo posiadania mechanizmów certyfikacji oraz zgodności ze standardami sam nigdy nie zasłużył na miano szeroko rozpowszechnionego standardu. Przyczyn takiego stanu rzeczy jest prawdopodobnie wiele. Główną i kluczową wydaje się być istnienie na rynku (w sieci) innego, choć mniej doskonałego kontr-produktu - PGP. Główne cechy tego ostatniego to powszechna (darmowa) dostępność (istnieją także komercyjne wersje programu) dla większości platform, łatwość instalacji i korzystania, a także możliwość integracji z większością popularnych typów oprogramowania pocztowego, przy tych samych funkcjonalnie możliwościach. Doświadczenia w korzystaniu z bezpiecznej poczty w skali NASK-u potwierdziły światowe tendencje powodując w sposób naturalny migrację w stronę prostszego i przyjemniejszego w użyciu PGP.

6.3.2. Inteligentne urządzenia szyfrujące

Przykładem dedykowanego urządzenie szyfrującego połaczenia TCP/IP może być system KryptoLan szwedzkiej firmy SECTRA. KryptoLan jest kompleksowym rozwiązaniem sprzętowym pozwalającym na szyfrowanie danych sesji TCP/IP zarówno w odniesieniu do transmisji pomiędzy stacjami sieci lokalnej jak i odległych stacji rozległej sieci korporacyjnej. System zapewnia poufność i integralność, jest transparenty dla przesyłanych danych, nie ma także wyczuwalnego wpływu na parametry transmisji. Urządzenia szyfrujące umieszcza się w zależności od topologii sieci na styku z siecią rozległą lub w sieci lokalnej. System jest niewrażliwy na sposób transmisji danych i sprawdza się zarówno w odniesieniu do połączeń Frame Relay, linii

Doświadczenia eksploatacyjne

Propozycja rozwiązania bezpiecznego dostępu do sieci w oparciu o system uwierzytelniania firmy LINTEL SECURITY, zapewnia dużą elastyczność zastosowań i możliwość ścisłej integracji z całością systemu . Z założenia gotowy dostarczany produkt firmowy nie rozwiązuje żadnych konkretnych problemów. Wymaga on samodzielnego opracowania koncepcji zastosowania w konkretnych warunkach, w tym technologii jego wdrażania i użytkowania. Pozwala on także na zintegrowanie z istniejącymi lub planowanymi aplikacjami (środowiskiem użytkowania). Powyższe cechy produktu stanowią, że jego wdrażanie wymaga: praktycznego sprawdzenia funkcjonowania poszczególnych elementów zgodnie z firmową dokumentacją techniczną, oraz wypracowanie koncepcji wdrożenia. Taka koncepcja powinna zawierać nie tylko aspekty techniczne, lecz również organizacyjne, administracyjne i prawne.
Jedną z najbardziej istotnych cech stanowiących o przydatności rozwiązania jest możliwość uwierzytelniania użytkownika w odniesieniu do konkretnych aplikacji - pozyskane doświadczenia techniczne potwierdzają dużą elastyczność rozwiązania. Produkt był poddawany ocenie niezależnych ekspertów.

6.2. Ochrona styków międzysieciowych

Wprowadzenie

Co w rzeczywistości kryje się za coraz częściej przewijającym się w różnych okolicznościach, odmianach i osobach terminem *firewall* ?
Wśród wielu definicji tego zwrotu lub jego rzadko stosowanej polskiej wersji („Ściany Ogniowe") na uwagę zasługuje parę, z czego chyba najbardziej ta najprostsza i najkrótsza:

Firewall to system lub grupa systemów stanowiących ochronę styku, pomiędzy co najmniej dwoma sieciami.

Nie zależnie od definicji, istnienie narzędzia pozwalającego na kontrolowanie styku pomiędzy sieciami szczególnie gdy jedna z nich jest siecią publiczną jest z punktu widzenia bezpieczeństwa wymogiem kardynalnym.

6.2.1. Narzędzia ochrony styku pomiędzy sieciami

Przykładem narzędzia zapewniającego bezpieczny styk pomiędzy sieci jest pakiet Solstice Firewall-1 frimy Checkpoint (zaadaptowany także przez SunSoft). Oprogramowanie to jest instalowane na dedykowanym komputerze z systemem UNIX. Zapewnia ono możliwość logowania wszystkich zdarzeń, filtrowania pakietów, instalowania serwisów typu „proxy" (w tym także WWW). Posiada rozbudowany i łatwy interfejs graficzny. Umożliwia także „ukrycie" adresów komputerów w sieci wewnętrznej poprzez ich translację (dzięki zastosowaniu techniki <ang. Network Address Translation> w sieci „nie widać" rzeczywistych adresów stacji). System jest transparentny (nie widoczny dla użytkowników), nie powoduje odczuwalnych opóźnień, ma również wbudowaną obsługę opisanych wcześniej kart jednokrotnego hasła firmy Security Dynamics (SDI). Firewall-1 pozwala także na dodatkową współpracę z routerami firmy Cisco i Wellfleet. Produkt może być wykorzystywany do budowy tzw. Virtual Private Networks

- Pytanie - odpowiedź (ang. challange -response).

Ad **b)**
PIN pamiętany przez klienta posiadającego kartę stanowi dodatkowe zabezpieczenie w przypadku zagubienia karty lub jej kradzieży.
Klient składający zamówienie legitymuje się więc obiema informacjami: osobistym numerem identyfikacyjnym oraz dynamicznym identyfikatorem odczytanym przez użytkownika z posiadanej karty.

6.1.1. Uwierzytelnianie oparte o rozwiązania firmy Security Dynamics

Jednym z testowanych rozwiązań wykorzystujących technologie haseł jednokrotnego użycia było frimowe rozwiązanie Security Dynamics.

Elementy rozwiązania:

a) karty SecurID

Każdy użytkownik otrzymuje kartę SecurID. Na wyświetlaczu karty SecurID pojawia się dynamiczny identyfikator w postaci ciągu cyfr, który co kilkadziesiąt sekund zmienia swoją wartość. Identyfikator ten może być użyty tylko raz.

b) serwer uwierzytelniania

Jest to oprogramowanie działające w środowisku UNIX zapewniające weryfikację użytkownika legitymującego się kartą i PIN-em. Oprogramowanie ACE Serwera zawiera w sobie system bazodanowy Progress. Stanowi on nowoczesne środowisko dla przechowywania i dostępu do danych o użytkownikach, potrzebnych w procesie uwierzytelniania. Oprogramowanie serwera wymaga odpowiedniej platformy sprzętowej w postaci komputera o mocy zależnej od liczby obsługiwanych użytkowników.

c) oprogramowanie klient

Jest to oprogramowanie instalowane na stacjach dostępowych lub w przypadku systemu rozproszonego na serwerze sieciowym (np. Novell NetWare)

d) zagadnienia organizacyjne

Sprawą kluczową jest stworzenie dokumentu zawierającego procedury obsługi systemu uwierzytelniania. Opisują one sposób i warunki wydawania kart, inicjalizowania użytkownika w systemie, administrowanie programem zarządzającym serwerem uwierzytelniającym, postępowanie w sytuacjach nietypowych itp. Organizacja jest najważniejszym elementem wdrożenia. Część sprzętowa w postaci serwera i kart, nie będzie prawidłowo służył założonym celom jeśli nie zostanie stworzony właściwy opis technologiczny zaakceptowany w fazie projektowania, wdrożony i przestrzegany w fazie użytkowania systemu.

e) wdrożenie

- zarządzanie systemem bezpieczeństwa,
- **pełna integracja z pozostałymi elementami bezpieczeństwa.**

5. Wdrożenie

Po zakończonym sukcesem okresie testów należy rozpocząć wdrażanie rozwiązania. Przebiegać ono powinno w dających się wyróżnić głównych etapach:

- uruchomienie instalacji eksploatacyjnej
- ciągłe zbieranie doświadczeń
- modyfika programu bezpieczeństwa
- stała opieka dedykowanego personelu (ang. security oficer)

6. Doświadczenia we wdrażaniu technologii podwyższających bezpieczeństwo sieci

Wprowadzenie

W sieciach komputerowych niezawodna praca całego organizmu zależy od stosowania określonych procedur zapewniających bezpieczeństwo przez każdego kto ma dostęp do jakiegokolwiek elementu sieci. Poziom bezpieczeństwa zależy bowiem od najsłabszego miejsca w systemie zgodnie z zasadą "pięty achillesowej". Jak z tego widać należy mieć świadomość iż:

Konsekwencje zaniedbania jednego elementu bezpieczeństwa sieci zawsze uderzają w większym zakresie niż można początkowo przewidzieć.

Reguły bezpieczeństwa sieci mogą dotyczyć całej organizacji, określonej lokalizacji oraz zastosowanego systemu komputerowego (lub technologii).
Bezpieczeństwo sieci zależy od trzech kardynalnych aspektów:
fizycznego, technicznego oraz organizacyjnego.

Aspekt fizyczny jest ściśle związany z:

- Świadomością potrzeby i obowiązku bezpiecznego operowania zasobami przez wszystkich użytkowników (niezależnie od posiadanych uprawnień)
- Fizyczną ochroną dostępu do sieci,
- Ochroną fizyczną nośników informacji (kopie zapasowe, dokumentacja)
- Poziomem niezawodności usług.

DOŚWIADCZENIA WE WDRAŻANIU TECHNOLOGII PODWYŻSZAJĄCYCH BEZPIECZEŃSTWO SYSTEMÓW KOMPUTEROWYCH

Andrzej Chrząszcz - Zespół Ochrony Sieci

Naukowa i Akademicka Sieć Komputerowa NASK, ul. Bartycka 18, 00-716 Warszawa
e-mail: andrzej@nask.pl

Wstęp

Podlegające nieustannym zmianom środowisko, specyfika i charakter Internetu jako konglomeratu sieci, a także wyraźny kierunek komercyjny jego rozwoju wymuszają konieczność stosowania skutecznych mechanizmów, właściwych i wiarygodnych środków ochrony danych użytkowników oraz zapewnienia bezpiecznego styku z siecią rozległa.

1. Rynek produktów bezpieczeństwa sieci

Mnogość dostępnych na rynku technologii, istniejących rodzin i wariantów różnorodnych produktów podwyższających bezpieczeństwo sieci nie ułatwia właściwego ich doboru. Jak zatem go dokonać ? Nie ma tu oczywiście jednoznacznej recepty gwarantującej pozyskanie najbardziej właściwego i skutecznego zestawu technologii i narzędzi. Od czego więc zacząć ? Najbardziej uzasadnione (nie zależnie od rozmiaru i ilości użytkowników sieci) jest systemowe podejście do problemu bezpieczeństwa. Poniżej przedstawiono główne filary takiego podejścia :

- zdefiniowanie zasobów sieci podlegających ochronie,
- klasyfikacja informacji z uwzględnieniem typów nośników na jakich jest ona przechowywana,
- określenie zasad, ilości i rodzajów styków z siecią publiczną,
- ścisłe określenie potrzeb i związanych z nimi uprawnienie użytkowników do zasobów sieci (zarówno wewnętrznej jak i zewnętrznej)
- analiza ekonomiczna pozwalająca ocenić wartość informacji oraz możliwe do poniesienia nakłady finansowe związane z jej ochroną.

Założenia te stanowią zrąb znacznie szerszych wymagań ujętych w *programie bezpieczeństwa* (patrz pkt.6), o którego stworzeniu powinna pomyśleć każda firma korzystająca z sieci.

Dokładne określenie własnych potrzeb, wymagań i istniejących uwarunkowań stanowi wstęp do rozpoznania rynku i pozyskania stosownych produktów. Proces ten nie daje się jednak unifikować, zależny jest bowiem od rodzaju, przeznaczenia i umiejscowienia elementu bądź elementów bezpieczeństwa. Odnosi się to również do istniejących jak i przyszłych - dających się przewidzieć wymagań w zakresie poufności, dostępności, a także innych charakterystycznych zmiennych. We wstępnym etapie warto postarać się o możliwie wiarygodną ocenę poziomu technicznego, skuteczności i innych cech stanowiących o przydatności i wysokich walorach rozwiązania. Istnieje wiele wzorców, a także wiele organizacji pretendujących do miana niezależnych organów oceny

są wysokie, obserwator może przymierzyć się do skali zjawiska czyli posiada szereg środków weryfikacji, które czynią tego rodzaju zjawiska polityczne mało skutecznymi, zwłaszcza kiedy ilość demonstrujących jest w skali społeczeństwa znikoma. W cyberprzestrzeni mamy do czynienia z nowymi zjawiskami. Organizowanie form wypowiedzi jest znacznie prostsze, sięga do społeczności przekraczającej granice kraju, zbieranie wypowiedzi znacznie tańsze i czytelnikowi znacznie trudniej ocenić jak jest skala zjawiska. Na przykład organizowany protest jest tym skuteczniejszy im mniej respondenci wiedzą o co chodzi, do tego doskonali są respondenci zagraniczni, i tym skuteczniejsi im mniej jest zorientowany ten do kogo ten protest jest kierowany. Trzeba zdawać sobie sprawę , że wiele tysięcy wypowiedzi w Internecie tak naprawdę nic nie znaczy, ponieważ wypowiadająca się grupa stanowi ułamki promile ogółu społeczności. Nawet na niskich szczeblach użytkowników sieci spotyka się *wirtualny świat polityki*, szereg postaw, zachowań i frustracji , które nic są relatywne do rzeczywistości. Tego rodzaju zjawiska są przeciwieństwem informowania i stanowią bardzo poważne zagrożenie bezpieczeństwa informacji w sieciach telekomunikacyjnych.

W dzisiejszych czasach mówi się, że podstawowy wysiłek wywiadów na całym świecie jest skierowany na pozyskiwanie informacji mających znaczenie gospodarcze. Szczególnie cenne są tu informacje w zakresie postępu technicznego i nauki, których posiadanie zapewnia najwyższe korzyści czynne w postaci możliwości uruchomienia lub zaniechania własnej produkcji czy usług, oraz bierne w postaci możliwości optymalnego wyboru zakupu lub odrzucenia cudzej produkcji czy usług. Środowiska naukowe pierwsze zauważyły konieczność i celowość wykorzystania nowoczesnych sieci telekomunikacyjnych. I jednocześnie środowiska naukowe, zwłaszcza polskie wykazują tu największą niefrasobliwość. Traktują rzeczywistość telekomunikacyjną jako *globalną wioskę* przyjazną i własną. Być może tak się dzieje, że w środowisku naukowym telekomunikacja nie jest robiona przez naukowców tworzących wiedzę, ale przez ludzi z obrzeża nauki, którzy tworzą sobie własny wirtualny świat, w którym czują się dowartościowani ? Szczególnie zagrażające bezpieczeństwu są tendencje do łączenia działania ośrodków superkomputerowych, z założenia kupowanych dla obsługi najcenniejszych badań, z szerokim propagowaniem wiedzy i rozpowszechnianej informacji. Ambicje propagatora są całkowicie sprzeczne z koniecznością najwyższej ochrony przebiegu i wyników badań prowadzonych w ośrodkach superkomputerowych. Znowu zderzają się tu dwa światy, ten idealnego (teoretycznie możliwego) świata Internetu z rzeczywistością, która z natury od ideału jest odmienna.

Bardzo dynamicznie rozwija się handel poprzez sieci telekomunikacyjne, w tym przez Internet. Nawet w Stanach Zjednoczonych AP nie ma ustalonych praw, regulujących ten rynek. Rozwija się on na ryzyko stron w nim uczestniczących. Dla sprzedawców rynek ten jest masowy, poddający się obróbce statystycznej. Można bez większego ryzyka określić na przykład procent nieuczciwych klientów. Procent ten będzie w pewnych okresach czasu stabilny. To znaczy można sobie wkalkulować w marżę odpowiednie straty, zwłaszcza, że handel przez Internet jest korzystny, nie wymaga powierzchni sklepowych, magazynów itp. za to zwiększa obrót. Marża naliczana do towarów i usług sprzedawanych przez Internet i tak może być niska. Zresztą sprzedający przy większych zakupach może stosować wysyłkę za pobraniem, co naraża go tylko na utratę kosztów przesyłki, może tworzyć listy stałych klientów i dla nich tworzyć specjalne systemy identyfikacji. Dla klienta, zwłaszcza tego kupującego sytuacja nie jest już tak pewna. Podając swój numer karty narażam się na jego przechwycenie, obciążenie mnie kosztami za towar, który mnie nie odpowiada lub wreszcie obciążenie mnie zupełnie przypadkowe, którego sam doświadczyłem. Ryzyko dla klienta jest indywidualnie nieporównywalnie większe, zwłaszcza, że poddany manipulacji reklamowej klient jest swoiście uśpiony i zdaje sobie sprawy z zagrożeń własnego bezpieczeństwa i kieszeni. Żyje on w rzeczywistości, która mogłaby być i pewnie będzie, kiedy problemy handlu przez Internet zostaną rozwiązane. Dzisiaj, nawet w rozmowach z poważnymi polskimi firmami i bankami nie zauważamy pełnej świadomości rodzaju i wielkości zagrożenia bezpieczeństwa obrotu handlowego. Tym bardziej klient faszerowany przez publikatory jednostronnymi informacjami na

informacji, pomiędzy osobami zafascynowanymi Internetem prowadzi do powstawania swoistego świata pojęć. Do takich należą różnego rodzaju pojęcia jak środowisko na przykład naukowe, porozumienie osób nie posiadających innej osobowości prawnej niż własna osób fizycznych, uzgodnienia dokonywane bez posiadania prawa podmiotowego do tego rodzaju uzgodnień i tym podobne sprawy , które w żaden sposób nie dają się przełożyć na język prawa. W tradycyjnej wymianie informacji, zwłaszcza w tak konkretnych sprawach, otrzymuje się pismo, które jednoznacznie określa podmiot prawa, osobę upoważnioną do występowania w imieniu tego podmiotu, na ogół dosyć dobrze określony przedmiot pisma oraz inne znaki jak data, liczba dziennika itp. W Internecie tego nie ma. Konta są osobiste i nikt nie wymaga, ani nie sprawdza jakie uprawnienia podmiotowe ma osoba podpisująca się pod listem e-mail. Zresztą ten podpis to jest wyłącznie ciąg znaków wygenerowanych przez komputer odbierający informację. Nie ma pewności skąd pismo pochodzi, a jego przedmiot przedstawiany przez osoby przypadkowe najczęściej nadzwyczaj mętny., Jednak tego rodzaju wymiany informacji prowadzą do powstawania faktów, zapisanych w przeświadczeniu wymieniających informacje jako praworządne. Szczytem nieporozumienia jest przyjmowanie podobnych obyczajów przez urzędników państwowych nawet wysokiego szczebla czego przykłady chyba państwo znacie. W e-mail przesyłanym w powszechnie dostępnym Internecie, mamy polecenia o charakterze władczym, w pismach urzędnik państwowy udziela pełnomocnictw w imieniu podmiotu, którego nie ma, którego nikt nie reprezentuje, a który kreują tylko *wirtualna rzeczywistość* sieci telekomunikacyjnych Oczywiście nikt nie wie czy mamy tu do czynienia z naiwnością, świadomą manipulacją czy po prostu z bezradnością wobec wirtualnych faktów.

Doświadczenie zdecydowanej większości użytkowników obecnych, multimedialnych sieci telekomunikacyjnych wywodzi się z użytkowania telefonu. Spodziewa się, że podobnie jak w telefonie po wykręceniu numeru zgłosi się stacja końcowa, jeśli będzie obsłużona zostanie podniesiona słuchawka przez abonenta lub sztuczną sekretarkę, będziemy mogli sprawdzić czy z właściwym adresatem się komunikujemy, ewentualnie spowodować przywołanie adrestata i wreszcie wymienić informacje stale kontrolując przebieg wymiany. Użytkownicy sieci tego się spodziewają i w dużej części tego wymagają. Znowu mamy do czynienia z wirtualną rzeczywistością , która teoretycznie jest możliwa, ale która nie istnieje. W obecnych sieciach telekomunikacyjnych w dużej części zautomatyzowanych, przede wszystkim w Internecie, takich usług nie ma. Internet oparty jest na technikach rozgłaśniania (bezpołączeniowych), a nie na wymianie informacji po ustalonych kanałach z pełną kontrolą przepływu. Żeby zbliżyć się do wymiany informacji podobnej do telefonicznej trzeba uruchomić odpowiednie procedury w samym systemie telekomunikacyjnym lub obok tego systemu. Zresztą właśnie anarchiczna technologia była wybrana dla Interne dla *przetrzymania ataku atomowego* i była powodem niesłychanego powodzenia tej technologii. Potoczne poglądy na temat działania nowoczesnych sieci telekomunikacyjnych stanowią groźne zagrożenie bezpieczeństwa informacji i sieci telekomunikacyjnych.

W tradycji mamy utrwalony sposób adresowania, w którym na najwyższym poziomie hierarchicznym występuje kraj, potem jakaś struktura regionalna, następnie miasto (lub/i poczta), dzielnica i miejscowość, ulica lub wieś, numer domu i ewentualnie mieszkania. Wprowadzenie kodu adresowego zamienia włącznie część opisu tekstowego na wygodniejszy w obróbce cyfrowy. Sieci telefoniczne i telekomunikacyjne, oparte na technikach połączeniowych (np. X.25) ten model powielają. Analizując adres można odtworzyć układ regionalny, którego ten adres dotyczy. I znowu rewolucję spowodował tutaj Internet. Z analizy cyfrowego adresu Internetu nic nie wynika. Dopiero teraz próbuje się wprowadzać trochę porządku wprowadzając autonomiczne grupy adresowe, ponieważ urządzenia mające przełączać paczki informacji (routery) przestały być wydolne. Wprowadzony adres domenowy nieco porządkuje adresowania wprowadzając na końcu adresu jednolite oznaczenie kraju, co jednak nie dotyczy Stanów Zjednoczonych AP. Zalecany początkowo

(art. 292) oraz dla osoby która niszczy, uszkadza lub czyni niezdatnym do użytku cudzy zapis magnetyczny lub elektroniczny, lub bez upoważnienia zmienia jego treść (oszustwo komputerowe).

Art. 283 § 2 projektu, w tym samym rozdziale w odniesieniu do tego, co potocznie nazywa się kradzieżą programu komputerowego, wprowadza nowy typ przestępstwa „zbliżony do kradzieży", jako że czyn taki „nie polega na zaborze rzeczy (informacja nie jest rzeczą)" ani też „zabór" nie pozbawia osoby uprawnionej dalszego dysponowania programem, zatem „chodzi tu nie tylko o uzyskanie programu od jego autora, a więc uzyskanie dyspozycji osobistymi prawami autorskimi, lecz raczej innej osoby uprawnionej, dysponującej materialnymi prawami związanymi z danym programem".

Jak wynika z powyższego tekstu droga legislacyjna w dziedzinie przestępczości „komputerowej" została rozpoczęta i będzie ona w niedalekiej przyszłości pozwalać organom ścigania na skuteczne wykrywanie i zwalczanie tego typu zjawisk patologicznych.

Przestępczość komputerowa nie jest fikcją ani też odległą przyszłością. Na całym świecie, a obecnie i w Polsce gdzie wykorzystywanie systemów informatycznych stoi na wysokim poziomie, przestępczość komputerowa stanowi poważne, realne zagrożenie dla funkcjonujących w oparciu o systemy informatyczne instytucji. Należy mieć także na uwadze nieuchronny rozwój obrotu bezgotówkowego i wykorzystywanie kart kredytowych oraz bankomatów.

Powyższy materiał nie miał na celu pełnej prezentacji zagadnień związanych z przestępczością komputerową, miał natomiast zasygnalizować istniejący problem.

stopnia (zostały zniszczone pliki firm i pliki klientów), że koszt odzyskania straconych informacji wyniósł ok. 9,5 ml funtów angielskich.

Hackerzy często robią bardzo wiele, aby ukryć swoją działalność przestępczą. Zamiast dokonać bezpośredniego połączenia z docelowym systemem podłączają się do niego drogą okrężną. Czasami jest to robione na cudzy koszt w celu zaoszczędzenia własnych pieniędzy, ale często w celu utrudnienia wytropienia konkretnego hackera np. atak na system komputerowy w Kalifornii wymagał użycia czterech różnych sieci - PSTN, PSS, JANET oraz sieci INTERNET. Wykrycie tej działalności przez Policję angielską poprzez trzy sieci danych - INTERNET, JANET I PSS nie było zadaniem trudnym i wymagało kilka dni na zebranie niezbędnych danych. Trudności pojawiają się wtedy kiedy próbuje się wytropić tego typu działalność poprzez pierwszą gałąź - sieć telefoniczną.

Podczas prób śledzenia działalności hackerów pojawia się wiele trudności. Jakkolwiek hacker może być osobą bardzo wytrwałą w atakowaniu konkretnego urządzenia to zwykle poświęca tylko kilka minut na jeden atak. Należy pamiętać, że każdy hacker może podłączyć się także do konkretnego urządzenia poprzez różne „trasy". Dać to może błędne wrażenie, że jest w to zamieszanych więcej niż jedna osoba.

Nieuprawnione przechwycenie informacji - podsłuch komputerowy

Czyny te stanowią poważne zagrożenie dla systemów informatycznych. Współczesne techniki przechwytywania informacji są poważnym zagrożeniem dla systemów informatycznych. Dane komputerowe można bowiem przejmować zarówno z transmisji teleinformatycznych jak i w wyniku analizy fal elektromagnetycznych emitowanych przez sprzęt komputerowy (komputery, monitory, przewody itp.) oraz fal akustycznych generowanych przez drukarki. Pozwalają one bowiem na zdalne i nie pozostawiające śladów „podglądanie" (obserwowanie) bez wiedzy i zgody uprawnionego do dysponowania tymi informacjami. Współczesne metody detekcji skrajnie słabych sygnałów obarczonych szumami i zakłóceniami o dużej intensywności umożliwiają wykrycie sygnałów o poziomach mniejszych o ponad 40 dB od poziomu szumów cieplnych w obwodach elektrycznych (rozwiązaniem są klatki Faradaia). Detekcja jest to proces fizyczny mający na celu odtworzenie sygnałów źródłowych (informacji użytecznej) z sygnału wypromieniowanego przez urządzenie nadawcze i odebranego przez antenę. W systemach komputerowych detekcja transmitownych sygnałów jest możliwa dzięki emisji wielu składowych widma transmitowanego sygnału przenoszonego przez :

a) pole elektryczne (sprzężenia pojemnościowe),
b) pole magnetyczne (sprzężenia indukcyjne),
c) pole elektro magnetyczne (promieniowanie wysokiej częstotliwości),
d) przewody (sprzężenia galwaniczne).

Czyny te są „chlebem powszednim" służb specjalnych i sprowadzają się do analizy fal elektromagnetycznych emitowanych przez komputery, monitory i fal akustycznych wytwarzanych przez drukarki oraz przejmowania danych z transmisji teleinformatycznych.

Bezprawne kopiowanie topografii półprzewodników

Przez topografię półprzewodników rozumie się rozwiązanie polegające na przestrzennym, wyrażonym w dowolny sposób rozplanowaniu elementów, z których co najmniej jeden jest elementem aktywnym, oraz wszystkich lub części połączeń układu scalonego. W tym przypadku chodzi też o o-

Bomba logiczna, koń trojański i robak komputerowy

Bomba logiczna jest programem - instrukcją (programową instrukcją), która uruchamia się w określonym czasie lub w momencie gdy zostaną spełnione określone okoliczności (przeważnie przemyślnie wyrafinowanie - mogą nimi być czas, obecność lub nieobecność danych takich jak nazwa itp.). Wirus ten zazwyczaj uruchamia się jako pojedynczy atak na system (uruchamia się procedura niszcząca).

Bomby logiczne często są znajdowane w bardziej wymyślnych przypadkach przestępstw komputerowych. Ciekawy przypadek dotyczył programisty obsługującego listy płac. Aby zagwarantować sobie stałe zatrudnienie wprowadził on krótką sekwencję poleceń sprawdzających, czy jego nazwisko występuje na liście płac. Jeżeli tak było nic się nie działo. Lecz gdy nazwiska nie było (np. z powodu zwolnienia) pliki miały być skasowane oraz miały nastąpić inne zniszczenia. Ww. został zwolniony i nastąpiło niszczące działanie bomby. Dopiero po uzyskaniu obietnicy przywrócenia do pracy zgodził się wskazać bombę logiczną umieszczoną w programie. Nie był ścigany sądownie.

Bomby logiczne są często odkrywane w wirusach, w których wyzwolony jest ładunek użyteczny (który wywołuje efekty uboczne), gdy występują określone warunki. Wirus ITALIAN wprowadza skaczącą piłeczkę na ekranie tylko wtedy, gdy dostęp do dysku następuje w ciągu jednosekundowego odstępu na każde 30 minut.

Koń trojański jest rodzajem wirusa, który jest zamaskowanym dopuszczalnym (przyjaznym) program. Wykonuje on więcej czynności od wymienionych w jego specyfikacji i jest bardzo prawdopodobne, że zniszczy oprogramowanie i wszelkie dane w komputerze. Wirus ten po osiągnięciu określonego stanu wykonuje swoje nieautoryzowane funkcje podczas gdy główny program w którym zagnieżdżony jest koń trojański kontynuuje wykonywanie swoich zamierzonych funkcji.

Robak komputerowy jest podobny do wirusa, ale wytwarza swoje dokładne kopie w całości bez potrzeby istnienia programu nosiciela. Pojawia się w sieciach komputerowych i komputerach wielodostępnych, wykorzystując łączność między komputerami i między użytkownikami jako nośnik transmisji. Dla użytkowników systemów komputerowych różnice te mogą nie mieć znaczenia, jednakże z punktu widzenia kryminologicznego są stosunkowo istotne. W przypadku ujawnienia bomby logicznej lub konia trojańskiego bez uprzedniego zawirusowania systemu komputerowego sprawcy należy szukać wśród osób uprawnionych do zmiany systemu, natomiast krąg sprawców wprowadzenia wirusa lub robaka komputerowego może być praktycznie nieograniczony.

Zniszczenie danych lub informacji może więc dotknąć praktycznie każdego użytkownika sprzętu komputerowego, niezależnie od tego czy będzie to komputer jednostanowiskowy czy też pracujący w sieci.

Najbardziej znanym robakiem dużych komputerów był CHRISTMAS TREE WORM, który rozpowszechnił się szeroko na BITNET, Europejskiej Akademickiej Sieci Badawczej i wewnętrznej sieci IBM. Został on wypuszczony w 1987 roku i poza innymi efektami, sparaliżował światową sieć IBM. Robak ten gdy działa rysuje choinkę Bożonarodzeniową.

Sabotaż komputerowy

Celem działania sprawcy przestępstwa określonego mianem sabotażu komputerowego jest sparaliżowanie funkcjonowania systemu komputerowego lub telekomunikacyjnego. Może do niego dojść zarówno w wyniku działania sprawcy, np. poprzez podłożenie ładunku wybuchowego pod obiekt

Fałszerstwo dokumentów elektronicznych jest przestępstwem trudno wykrywalnym. Pewne pozytywne wyniki przynosi porównanie zawartości dokumentu papierowego z dokumentem elektronicznym. Wydaje się, iż ta grupa przestępstw ciągle czeka na swoje wykrycie. Istnieje pilna potrzeba opracowania taktyki ujawniania i ścigania tego rodzaju przestępstw oraz zorganizowania odpowiedniego zaplecza ekspertów i konsultantów. Z dotychczasowej praktyki wiadomo, że wiele podmiotów gospodarczych prowadzi podwójną księgowość, jedną oficjalną dla izb i urzędów kontroli skarbowej oraz drugą ukrytą dla zobrazowania rzeczywistego stanu finansowego firmy. W związku z powyższym wydaje się, iż działania służby ds. przestępczości gospodarczej i kryminalistyki muszą zostać w szerszym stopniu wyposażone w specjalne urządzenia umożliwiające zabezpieczenie materiałów dowodowych w postaci komputerowego zapisu danych na dyskach optycznych, ich dalszą analizę i przetworzenie do postaci ekspertyzy kryminalistycznej .

W polskich warunkach pewnym ograniczeniem możliwości fałszerza jest m.in. obowiązek przechowywania wydruków na nośniku papierowym z dokumentu elektronicznego m.in. dla potrzeb organów fiskalnych (zgodnie z ustawą o rachunkowości okres przechowywania dokumentów papierowych wynosi 5 lat).

- **Dystrybucja pornografii i innych zakazanych materiałów**

Wraz ze wzrostem popularności sieci INTERNET oraz niskich kosztów sprzętu komputerowego, osoby które wcześniej zajmowały się sprzedażą literatury pornograficznej „z pod lady" mogą sobie obecnie znacznie ułatwić życie. Zainstalowanie bazy komputerowej zdjęć pornograficznych i rozpowszechnianie ich na całym świecie jest obecnie stosunkowo tanie i łatwe do zrealizowania. Operacje tego typu są coraz trudniejsze do wykrycia i ścigania, w szczególności wówczas kiedy obraz może być zaszyfrowany i zapisany w zdalnej pamięci komputera w różnych obszarach kraju a nawet w innych krajach.

W literaturze przedmiotu oraz w materiałach Międzynarodowej Organizacji Policji Kryminalnej INTERPOL za przestępstwa komputerowe uznaje się poza przesyłaniem za pomocą sieci informatycznych materiałów pornograficznych, także przesyłanie materiałów rasistowskich. Używanie sieci komputerowych do celów komunikacyjnych przez zorganizowane grupy przestępcze jest również karane.

II.PRZESTĘPSTWA POPEŁNIANE PRZECIWKO KOMPUTEROM

Niszczenie danych lub programów komputerowych

Ataki na dane i programy komputerowe w celu ich zniszczenia lub modyfikacji należą do najczęściej popełnianych, a w każdym razie ujawnianych przestępstw komputerowych w krajach Europy Zachodniej. Tego typu przypadki zamachów na dane komputerowe notuje się również w Polsce. Dane komputerowe mogą być niszczone fizycznie (np. wymazanie z dyskietki przy pomocy magnesu lub wysadzenie w powietrze ośrodka obliczeniowego) lub też skomplikowaną metodą działań softwarowych. W tym drugim przypadku chodzi o wprowadzenie do systemu komputerowego specjalnego programu zwanego „wirusem" komputerowym , koniem trojańskim, bombą logiczną, robakiem komputerowym lub łańcuchem szczęścia.

Przestępstwa te są ponadto ubocznym wynikiem informatyzacji systemów bankowych, które coraz częściej oparte są na bezpapierowym obiegu dokumentów, teletransmisji danych i elektronicznym przelewie pieniądza. Koszty związane wyłącznie z oszustwami elektronicznymi, dotykającymi świat amerykańskiego biznesu w połowie lat osiemdziesiątych, oceniano na 100 mln USD rocznie. Wg źródeł FBI dzięki komputerom rocznie kradnie się około 3-5 mln dolarów. Badania przeprowadzone na początku lat 90-tych w Wielkiej Brytanii określiły roczne straty z powodu oszustw komputerowych na ponad 407 mln funtów szterlingów, przy czym jak stwierdzał raport, „okoliczności do nadużyć komputerowych nadal zwiększają się proporcjonalnie do technicznego postępu".

Najważniejszymi czynnikami sprawiającymi, że komputery nie są odpowiednio zabezpieczone przed oszustami to:

1. ogólny brak zrozumienia skomplikowanej technologii związanej z systemami komputerowymi przez dyrektorów i audytorów. Wskutek tego dane są faktycznie pod kontrolą kilku „zaufanych" pracowników, którzy posiadają niezbędną znajomość systemu,
2. dokumentacje i informacje, które normalnie byłyby trzymane w różnych miejscach są zgromadzone w jednym małym obszarze tzn. w komputerze; łatwiej jest zatem znaleźć dostęp do różnych części procedury księgowej bez wzbudzania podejrzeń,
3. system zabezpieczenia jest często zaniedbywany na korzyść szybkości i sprawności, szczególnie w przypadku dużej konkurencyjności rynku,
4. z powodu możliwości „zarobienia" ogromnych kwot, istnieje czasami pokusa wzięcia udziału w oszustwie komputerowym nawet przez zaufanych oraz innych uczciwych pracowników,
5. w przeciwieństwie do innych typów oszustw, oszust komputerowy bardzo rzadko pozostawia ślady identyfikujące takie, jak pismo odręczne i odciski palców,
6. instytucje prawne nie są tak dobrze wyposażone do zwalczania oszustw komputerowych jak do większości tradycyjnych przestępstw,
7. w przypadku zawiłych oszustw komputerowych łatwiej obronie poddać w wątpliwość zeznania poprzez zawikłanie (pogmatwanie) sprawy.

Najczęstszymi formami popełniania oszustw komputerowych są:

- **manipulacja danymi** (input manipulation), polegająca na wprowadzaniu nieprawdziwych danych w celu uzyskania nienależnych korzyści majątkowych. Forma ta jest najbardziej znana, gdyż nie wymaga od sprawcy żadnej szczególnej wiedzy lub umiejętności. Modyfikacji danych dokonują najczęściej operatorzy sprzętu, ale mogą dokonywać ich także osoby włamujące się do systemów komputerowych. Jak się ocenia w krajach wysoko rozwiniętych, w wyniku włamań do systemów komputerowych banków i towarzystw ubezpieczeniowych, straty ponoszone przez te podmioty w wyniku manipulacji danymi są wielokrotnie większe niż na skutek napadów i wymuszeń. W czasopiśmie COMPUTER CRIME z 1987 roku podaje się, że banki w USA w wyniku „tradycyjnych" napadów tracą średnio ok. 8000 USD, podczas gdy przeciętne oszustwa komputerowe „kosztują banki ok. 0,5 mln USD.
- **manipulacja programem** (software manipulation), polega na takim opracowaniu programu lub jego modyfikacji, by program wykonywał określone instrukcje niezależnie od operatora sprzętu. Czyli dla osoby z dobrą znajomością systemu możliwe jest zmodyfikowanie systemu w taki sposób, że będzie on sam, automatycznie, dokonywał oszustw. Najprostsza metoda znana jako Salami polega na braniu małych części z całości bez dostrzegalnego zmniejszenia ogólnego. Na przykład w systemie bankowym metoda ta mogłaby polegać na zaokrąglaniu „w dół" obliczanych odsetek i transferowaniu kwoty o którą suma jest zaokrąglona, na specjalne konto z którego pieniądze mogłyby być podejmowane. Sukces tej metody polega na tym, że kwota utracona przez

W piśmiennictwie fachowym określeniu „przestępstwo komputerowe" nadaje się z reguły szerokie znaczenie, obejmując nim wszelkie zachowania przestępne związane z funkcjonowaniem systemu elektronicznego przetwarzania danych, zarówno polegające na naruszaniu uprawnień do programu komputerowego, jak i godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz w całym systemie połączeń komputerowych a także w sam komputer. Przestępczość komputerowa może polegać również na wykorzystaniu istniejących systemów informatycznych do popełniania czynów zabronionych. W tym przypadku komputer staje się „narzędziem pracy" przestępcy.

Powołany w połowie lat osiemdziesiątych Komitet Ekspertów Rady Europy, którego raport stał się podstawą rekomendacji nr R (89)9 Komitetu Ministrów Rady Europy, wskazał formy zachowań związanych z wykorzystaniem komputera i systemu komputerowego, które winny być skryminalizowane w systemach prawnych państw członkowskich. Zostały one skatalogowane w dwóch listach - pierwszej (tzw. lista minimalna), zawierającej czyny wymagające kryminalizacji we wszystkich krajach członkowskich, a co za tym idzie ścisłej współpracy międzynarodowej pociągającej za sobą harmonizację ustawodawstw krajowych w zakresie ścigania przestępczości transgranicznej oraz drugiej (tzw. lista fakultatywna), obejmującej zachowania o mniejszym stopniu szkodliwości i nie wymagającej ścisłej współpracy międzynarodowej w zakresie ich ścigania i jurysdykcji.

Taki podział przestępstw komputerowych wynika z przyjęcia przez różne kraje, różnej interpretacji prawnej czynów. Minimalna lista czynów, uznanych jako szczególnie niebezpieczne przez Ekspertów Rady Europy to:

1. oszustwa związane z wykorzystaniem komputera,
2. fałszerstwa przeprowadzane za pomocą komputerowa,
3. niszczenie danych lub programów komputerowych,
4. sabotaż komputerowy,
5. nieuprawnione „wejście" (włamanie) do systemu komputerowego - hacking,
6. nieuprawnione przechwycenie informacji - „podsłuch" komputerowy,
7. bezprawne kopiowanie, rozpowszechnianie lub publikowanie programów komputerowych prawnie chronionych,
8. bezprawne kopiowanie topografii półprzewodników.

Na liście fakultatywnej Komitetu Ekspertów Rady Europy znalazły się:

1. modyfikacja danych lub programów komputerowych,
2. szpiegostwo komputerowe,
3. używanie komputera bez zezwolenia,
4. używanie prawnie chronionego programu komputerowego bez upoważnienia.

Polskie prawo nie przewiduje odrębnych typów przestępstw, skierowanych przeciwko systemowi komputerowemu. Naruszenia tego systemu mogą być ścigane tylko o tyle, o ile zachowania takie są stypizowane w ramach innych przepisów prawa.

W szerokim zakresie spenalizowane są natomiast zachowania naruszające prawa do programów komputerowych, co wynika z faktu, iż ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz.U. Nr 24, poz. 83) wprost uwzględnia te zagadnienia.

zakresie oryginalności pomysłu, co do utworzenia i metody utworzenia bazy (nie jej treści, na którą składają się utwory chronione prawem autorskim) traktowany być powinien, jako właściciel ustanawiający licencje na pobranie lub powtórne wykorzystanie istotnych części bazy danych. Tworzenie i korzystanie z baz danych w Polsce może nastręczać spore problemy prawne, które mogą być rozstrzygane obecnie na podstawie przepisów kodeksu cywilnego i w części prawa autorskiego.

Przypisy

1. Układ Europejski' ustanawiający stowarzyszenie między Rzecząpospolitą Polską z jednej strony, a Wspólnotami Europejskimi i ich państwami członkowskimi z drugiej strony - Dziennik Ustaw z 1994 r. nr 11, poz. 38.,
2. White paper . Preparation of the associated countries of Central and Estern Europe for integration into the internal market of the Union. Luxembourg, 1995.,
3. J. Barta, R. Markiewicz Ochrona informacji naukowej w świetle dyrektyw Unii Europejskiej o ochronie banków danych. „Informacja Naukowa w Krajach Unii Europejskiej - wybrane zagadnienia OPI 1997 r.,
4. J. Bęczkowski - Podstawy zabezpieczenia systemów informacyjnych w dużych organizacjach - NBP 1997r.,
5. M. Grabowska, A. Ogonowska Regulacja prawna informacji naukowej w Unii Europejskiej - „Informacja Naukowa w Krajach Unii Europejskiej - wybrane zagadnienia OPI 1997 r.,
6. M. Mozgawa Zwalczanie nieuczciwej konkurencji - Info-Trade Gdańsk 1997 r.,
7. P. Nachman Instytucja zakazu konkurencji w prawie polskim - Monitor Prawniczy 10/1996,
8. S.Zając Prawne i etyczne aspekty zabezpieczenia tajemnicy państwowej i służbowej przedsiębiorstwa - Instytut Łączności 1997 r.

w takich sytuacjach specjalnych kodów, szyfrów czy kryptogramów (prawdopodobnie istnieje nie publikowany akt prawny zakazujący stosowania kryptografii informacji stanowiących *tajemnicę państwową* - bez zgody UOP). W wypadku prowadzenia negocjacji z osobami postronnymi, przedsiębiorca powinien zabezpieczyć się - przed przystąpieniem do rozmów - wprowadzeniem odpowiednich klauzul o poufności przekazywanych informacji. W rozumieniu ustawy o znk chodzi o takie informacje - z woli przedsiębiorcy utrzymywane przed konkurencją w sekrecie - które zapewniają przedsiębiorcy pewne ułatwienia i korzyści i z tego powodu przedstawiają dla przedsiębiorcy określoną wartość.

B) ujawnienie innej osobie lub wykorzystanie we własnej działalności gospodarczej informacji stanowiących tajemnicę przedsiębiorstwa. Warunek ten dotyczy zarówno pracownika przedsiębiorcy, jak i innej osoby, która była zobligowana do poufności. Odnośnie do pracownika, ustawa stwierdza, że obowiązek zachowania tajemnicy ciąży na pracowniku w czasie całego zatrudnienia i w ciągu 3 lat po jego ustaniu. Czas ten może być określony przez strony inaczej. Na tle tego zapisu powstają wątpliwości, czy pracownik po zmianie zatrudnienia może wykorzystywać u innego pracodawcy wiadomości, w których posiadanie wszedł w poprzednim zakładzie i czy nie będzie wówczas podstawy do pociągnięcia go do odpowiedzialności z powodu dopuszczenia się czynu nieuczciwej konkurencji. Uznać należy, że w większości sytuacji chodzić będzie nie tajemnicę sensu stricto, a jedynie o nabyte umiejętności. Pracodawca, który uważa, że pracownik tak wiele się u niego dowiedział, iż nie powinien dzielić się informacjami z nowym pracodawcą, ma możliwość ustrzec się przed taką ewentualnością. Może mianowicie zawrzeć z pracownikiem umowę o zakazie podejmowania działalności konkurencyjnej. W umowie określa się okres obowiązywania zakazu konkurencji i wysokość odszkodowania, z tym, że nie może być ono niższe od 25% wynagrodzenia otrzymywanego przez pracownika przed ustaniem stosunku pracy przez okres odpowiadający okresowi obowiązywania zakazu konkurencji. Naruszenie zobowiązania wynikającego z klauzuli konkurencyjnej powoduje powstanie obowiązku naprawienia szkody. Czas zachowywania tajemnicy przedsiębiorstwa określony ustawą będzie obowiązywał jedynie w odniesieniu do informacji, w których posiadanie pracownik wszedł legalnie. W wypadku uzyskania takich informacji bezprawnie, czas ten ulegnie przedawnieniu na ogólnych zasadach określonych w kodeksie karnym.

C) wyrządzenie poważnej szkody przedsiębiorcy. Nie sposób określić, jaka szkoda jest poważna. W każdym indywidualnym wypadku będzie określana osobno. Celem prowadzenia działalności gospodarczej jest osiąganie zysków. Wyrządzenie zatem szkody bezpośrednio istotnie zmniejszającej takie zyski będzie mogło zostać uznane za szkodę poważną. Istotnym przy ustalaniu szkody będzie stosunek rozmiarów szkody do obrotów przedsiębiorstwa. Nie ma póki co żadnego orzecznictwa na ten temat, także nie było go w okresie międzywojennym na tle podobnej ustawy z 1926 r.

Odpowiedzialność karna odnosi się tylko do tych przypadków, gdy wystąpiła szkoda W wypadku braku takiej szkody i wystąpieniu jedynie zagrożeń istotnych interesów przedsiębiorcy, będzie można mówić o odpowiedzialności cywilnej.

Do stwierdzenia, że wystąpiło szpiegostwo gospodarcze muszą wystąpić łącznie 3 przesłanki:

A) podjęcia przez przedsiębiorcę niezbędnych działań zmierzających do zachowania poufności informacji,

B) bezprawne uzyskanie wiadomości stanowiących tajemnicę przedsiębiorcy. Jeżeli sprawca nabył informację legalnie (np. z wywiadowni gospodarczej), nie będzie ponosił odpowiedzialności

penalizującego czyn polegający na: „otwarciu bez uprawnienia zamkniętego pisma lub ukrywaniu albo niszczeniu cudzej korespondencji lub na podstępnym uzyskaniu przez sprawcę nie przeznaczonej dla niego wiadomości nadanej przy użyciu środków telekomunikacji" (art. 172 kk).

Tajemnica państwowa i służbowa

Co do przepisów ustawy o tajemnicy państwowej i służbowej, należy podkreślić, że ma ona ograniczony krąg adresatów. Określa generalnie, co może stanowić przedmiot tajemnicy państwowej, zobowiązując naczelne i centralne organy państwa oraz terenowe organy administracji państwowej stopnia wojewódzkiego do szczegółowego określania informacji stanowiących tajemnicę państwową. Obszar wiadomości objętych tajemnicą państwową jest bardzo szeroki, dotyczy wielu dziedzin życia i w zasadzie zawsze wiąże się z obronnością i bezpieczeństwem państwa oraz sprawami międzynarodowymi i innymi istotnymi ze względu na dobro i interes państwa. Ustawa obliguje do zachowania tajemnicy państwowej każdego, do czyjej wiadomości tajemnica dotarła. Zapis ten ma charakter ogólny i jako jedyny jest adresowany do nie określonego kręgu osób. Jest on poddawany licznym, rozmaitym krytykom, sprowadzającym się do tego, że przypadkowy dysponent informacji stanowiącej tajemnicę państwową nie może i nie powinien ponosić konsekwencji złego strzeżenia tajemnicy przez osobę do tego zobligowaną.

Co do tajemnicy służbowej regulowanej tą ustawą, uznaje się za nią „wiadomość nie stanowiącą tajemnicy państwowej, z którą pracownik zapoznał się w związku z pełnieniem swoich obowiązków w państwowej, spółdzielczej lub społecznej jednostce organizacyjnej, a której ujawnienie może narazić na szkodę interes społeczny, uzasadniony interes tej jednostki organizacyjnej lub obywatela". Z tej definicji wynika, że o tajemnicy służbowej można mówić jedynie w jednostkach organizacyjnych państwowych, spółdzielczych i społecznych. Informacje jednostek organizacyjnych innych niż wymienione nie korzystają z ochrony ustawy o tajemnicy państwowej i służbowej.

Czyny nieuczciwej konkurencji

W obecnym czasie, w związku z wprowadzeniem gospodarki wolnorynkowej koniecznym stało się uchwalenie ustawy gwarantującej ochronę konkurencji, zwalczającej konkurencję nieuczciwą. Takim aktem prawnym jest ustawa z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (ustawa o znk). Ustawa stwarza ochronę przed zachowaniami powszechnie uznawanymi za złe i naganne, które mogą zakłócić proces prawidłowego funkcjonowania konkurencji.

Czynem nieuczciwej konkurencji - zgodnie z art. 3 ust. 1 ustawy o znk - jest „działanie sprzeczne z prawem lub dobrymi obyczajami, jeżeli zagraża lub narusza interes innego przedsiębiorcy lub klienta". Czynami nieuczciwej konkurencji są w szczególności : wprowadzające w błąd oznaczenie przedsiębiorstwa, fałszywe lub oszukańcze oznaczenie pochodzenia geograficznego towarów albo usług, **naruszenie tajemnicy przedsiębiorstwa,** nakłanianie do rozwiązania lub niewykonania umowy, naśladownictwo produktów, pomawianie lub nieuczciwe zachwalanie, utrudnianie dostępu do rynku, a także nieuczciwa lub zakazana reklama. Ustawa o zwalczaniu nieuczciwej konkurencji nie podaje wyczerpującego katalogu czynów nieuczciwej konkurencji. Generalną zasadą - ocenianą w każdym wypadku indywidualnie - jest, że działanie to musi być sprzeczne z prawem lub (także!) dobrymi obyczajami, jeżeli zagraża lub narusza interes innego przedsiębiorcy lub klienta.

Ustawa reguluje zapobieganie i zwalczanie nieuczciwej konkurencji w działalności gospodarczej, w szczególności produkcji przemysłowej i rolnej, budownictwie, handlu i usługach - w interesie publicznym, przedsiębiorców oraz klientów, a zwłaszcza konsumentów.

OCHRONA TAJEMNICY PRZEDSIĘBIORSTWA W ŚWIETLE USTAWY O ZWALCZANIU NIEUCZCIWEJ KONKURENCJI

Maria Ziółkowska

Naukowa i Akademicka Sieć Komputerowa NASK, ul. Bartycka 18, 00-716 Warszawa,
E-mail:mariaz@nask.pl

Wstęp

Informacja zawsze była cennym dobrem ułatwiającym podejmowanie decyzji politycznych, gospodarczych, handlowych. Nigdy jednak bardziej niż obecnie nie zdawano sobie sprawy z tego, że szybka informacja, przekazywana bezpośrednio i w sposób zapewniający poufność ma wartość niewymierną. Rozwój techniki uczynił informację towarem, świadczenie usług informatycznych - potężną gałęzią przemysłu.

Informacja stała się jednym z najcenniejszych elementów umożliwiających rozwój wielu gałęzi życia. Rozwój nauki, techniki, rozwój gospodarki i handlu oraz przebieg procesów gospodarczych i ekonomicznych są w ogromnej mierze uzależnione od posiadania informacji, możliwości szybkiego jej wyselekcjonowania, pewności jej konfidencjonalności, możliwości skutecznego zabezpieczenia -formalnego i technicznego - przed dostępem osób niepożądanych.

Wśród różnych zjawisk rzutujących w ostatnim czasie na obraz życia społecznego i gospodarczego niebagatelną rolę odgrywają zmiany w traktowaniu informacji. Z jednej strony, chodzi tu o traktowanie informacji, jako swoistego towaru, z drugiej strony natomiast o rolę informacji w uzyskiwaniu efektów ekonomicznych w różnych gałęziach produkcji czy usług.

Te zmiany oraz idące z nimi w parze potrzeby, wymuszają określone reakcje w sferze metod zarządzania i organizacji oraz zabezpieczeń prawnych.

Źródła prawa ochrony informacji.

Wbrew dość powszechnej opinii, polskie prawo w sposób dość szczegółowy chroni informacje stanowiące tajemnicę państwową, służbową, tajemnicę przedsiębiorstwa, tajemnicę korespondencji.

Sposób prawnej ochrony oraz określenie przedmiotu ochrony w polskim prawie ulega i będzie musiał ulegać dalszym zmianom wynikającym z wejścia w życie (1.02.1994r.) „Układu Europejskiego ustanawiającego stowarzyszenie między Rzecząpospolitą Polską z jednej strony, a Wspólnotami Europejskimi i ich państwami członkowskimi z drugiej strony". Umowa ta reguluje stosunki między Rzecząpospolitą Polską, a Wspólnotami Europejskimi w okresie przejściowym, to jest do momentu wejścia w życie Układu Europejskiego, do czasu uzyskania przez Polskę pełnego członkostwa w Unii Europejskiej. Przewidziano na to 10 lat. W układzie Polska zobowiązała się między innymi do „zbliżenia istniejącego i przyszłego ustawodawstwa Polski do ustawodawstwa istniejącego we Wspólnotach. Polska podejmie najlepsze starania w celu zapewnienia zgodności jej przyszłego ustawodawstwa z ustawodawstwem Wspólnot." (art. 68).

W opublikowanej przez Komisję Europejską Białej Księdze (Luxemburg - 1995 r.) zawarty jest wykaz wymagań w stosunku do stowarzyszonych z Unią krajów Europy Centralnej i Wschodniej. Wśród priorytetowych zagadnień znalazły się m.in. sektor audiowizualny, telekomunikacja, własność intelektualna i ochrona danych personalnych. Polska jest zobligowana

3.4 Asynchroniczna replikacja danych

Replikacja asynchroniczna, w przeciwieństwie do synchronicznej, jest niewrażliwa na pewne awarie węzłów i środowiska komunikacyjnego. W przypadku jakiejkolwiek awarii nie następuje blokowanie przetwarzanie danych, których repliki są dostępne lokalnie. Własność ta została uzyskana kosztem rozluźnienia podstawowego modelu spójności. Z tego powodu asynchroniczna replikacja danych winna być stosowana z dużą ostrożnością i nie może znajdować zastosowania w takich dziedzinach jak: bankowość, systemy czasu rzeczywistego itp.

Ze względu na zbiór operacji udostępnianych przez mechanizm replikacji asynchronicznej, repliki dzielimy na: *tylko-do-odczytu* (*Read Only* -RO) i *odczyt-zapis* (*Read-Write* - RW). Repliki RO mogą być jedynie odczytywane, natomiast repliki RW mogą być również modyfikowane. Asynchroniczna modyfikacja kopii danych na różnych węzłach może spowodować trwałą utratę spójności danych. Z tego powodu asynchroniczna replikacja typu RW musi być wyposażona w mechanizm wykrywania i usuwania niespójności. Najczęściej wykorzystywaną techniką służącą do wykrywania niespójności jest porównanie obrazu danych sprzed i po modyfikacji. Do usuwania niespójności dostarcza się szereg standardowych procedur np.: odrzucenie lub zaakceptowanie konfliktowej transakcji w oparciu o etykietę czasową lub priorytet, zastosowanie arytmetyki komutatywnej itp. Niespójność może być również usunięta przez zdefiniowaną przez użytkownika transakcję kompensującą.

Technika replikacji asynchronicznej cieszy się dużą popularnością i została zaimplementowana w wielu produktach komercyjnych, np. Oracle7, Sybase10 i DB2.

4. Podsumowanie

Artykuł ten miał na celu zaprezentowanie najważniejszych problemów niezawodności systemów rozproszonych. Poruszone tematy nie wyczerpują oczywiście całego zagadnienia, jednak powinny być dobrą ilustracją złożoności problemów związanych z tolerancją uszkodzeń. Bieżący stan wiedzy pozwala na opracowanie mechanizmów niezbędnych do konstrukcji systemów odpornych na uszkodzenia. Pozostaje wierzyć, iż z dnia na dzień, coraz więcej takich systemów będzie do naszej dyspozycji.

Literatura:

[Agarwal92] D.A. Agarwal, P.M. Melliar-Smith, L.E. Moser, "Totem: A protocol for Message Ordering in a Wide Area Network", *In Proc. 1st ISMM International Conference on Computer Communications and Networks*, 1992.

[Amir92] Y. Amir, D. Dolev, S. Kramer, D. Malki, "Transis: A Communication Sub-System for High Availability", In *22nd Annual International Symposium on Fault-Tolerant Computing*, 1992, pp.76-84.

[Babaoglu95] ö. Babaoglu, R. Davoli, L. Giachini, M. Baker, "Relacs: A Communications Infrastructure for Constructing Reliable Applications in Large-Scale Distributed Systems", *In Proc. 28th International Conference on System Sciences*, 1995, pp. 612-621.

[Birman90] K. Birman, R. Cooper, T.A. Joseph, K. Marzullo, M. Makpangou, K. Kane, F. Schmuck, M. Wood, "The ISIS System Manual", DCS, Cornell University, 1990.

[Brzeziński95] J. Brzeziński, J-M. Helary, M. Raynal : Semantics of recovery lines for backward recovery in distributed systems, *Annales des Telecommunications*, vol. 50, no. 11-12, 1995 s. 877-887

kontynuowane na pozostałych maszynach. Rozwiązanie to w odróżnieniu od technologii serwerów zapasowych ze współdzielonym nośnikiem wykorzystuje wszystkie serwery w gronie do bieżącego przetwarzania. Rozwiązanie to wymaga synchronizacji działania systemów baz danych.

3.2 Zatwierdzanie transakcji w środowisku rozproszonym

Istotnym zagadnieniem dla niezawodnego przetwarzania transakcyjnego w środowisku rozproszonym jest zagwarantowanie atomowości operacji zatwierdzenia. Atomowość operacji zatwierdzenia rozproszonej transakcji zapewnia się przez wprowadzenie synchronizacji procesów realizujących tą operację na różnych węzłach środowiska przetwarzania. W scenariuszu realizacji rozproszonej transakcji bez synchronizacji operacji zatwierdzenia, w przypadku awarii procesu użytkownika w czasie trwania tej operacji może się okazać, że część transakcji na jednym węźle została zatwierdzona, a część na pozostałych węzłach została wycofana. Może się tak wydarzyć z tego powodu, że procedura odzyskania danych po awarii polega na wycofaniu wszystkich operacji, które nie zdążyły być zatwierdzone. Taki scenariusz jest w większości zastosowań nieakceptowalny, ponieważ narusza atomowość transakcji, jej podstawową własność.

Najpopularniejszym sposobem synchronizacji operacji zatwierdzenia rozproszonych transakcji wykorzystywanym przez systemy baz danych jest protokół dwufazowego zatwierdzania (*Two Phase Commitment* - 2PC)[Gray96]. Protokół ten opiera się na wprowadzeniu dwóch faz operacji zatwierdzenia. Pierwsza faza wymusza na wszystkich węzłach uczestniczących w rozproszonej transakcji deklaracji odnośnie możliwości zatwierdzenia transakcji. Przejście do kroku drugiego jest możliwe tylko w przypadku, gdy wszystkie węzły potwierdzą swą gotowość zatwierdzenia transakcji. W przypadku, gdy któryś z węzłów tego nie uczyni, transakcja jest wycofywana. W drugiej fazie, węzły zatwierdzają lokalne zmiany zrealizowane przez transakcję. Każdy etap zatwierdzenia transakcji jest trwale składowany w lokalnym dzienniku bazy danych na każdym z węzłów biorących udział w rozproszonej transakcji. Jeżeli awaria nastąpi przed dokończeniem pierwszej fazy realizacji protokołu, transakcja zostanie wycofana. Jeżeli awaria nastąpi w drugiej fazie, to na podstawie zapisu w dzienniku bazy danych lokalny, system bazy danych podejmie próbę skomunikowania się z innymi węzłami w celu ustalenia sposobu zakończenia transakcji.

Sterowanie protokołem 2PC może być realizowane na trzy sposoby:

- rozproszone,
- scentralizowane,
- hierarchiczne.

W sterowaniu rozproszonym wszystkie węzły biorące udział w transakcji kolektywnie ustalają moment przejścia z jednej fazy do następnej. Wadą tego rozwiązania jest duża liczba wymienianych komunikatów między węzłami. Ponadto, sterowanie to jest bardzo podatne na zablokowanie. Jeżeli w drugiej fazie 2PC ulegnie awarii jeden z węzłów, to wszystkie pozostałe węzły muszą zawiesić przetwarzanie zatwierdzanej transakcji, aż do usunięcia awarii.

Zcentralizowane sterowane eliminuje część tych wad. W tym przypadku spośród węzłów biorących udział w rozproszonej transakcji wybierany jest jeden węzeł zwany koordynatorem. Zadaniem tego węzła jest koordynowanie przechodzenia między fazami 2PC. Zablokowanie wykonania operacji zatwierdzenia może nastąpić tylko wtedy, kiedy awarii w drugiej fazie 2PC ulegnie koordynator. Wadą tego rodzaju sterowania jest duże obciążenie jednego węzła.

Na potrzeby sterowania hierarchicznego wyróżnia się jeden węzeł zwany koordynatorem globalnym i grupę współpracujących z nim węzłów zwanych koordynatorami lokalnymi. Hierarchia połączeń między nimi jest najczęściej ustalana na podstawie składni operacji wykonywanych w ramach transakcji. Rozwiązanie to obniża obciążenie jednego wyróżnionego węzła kosztem

je powielać. Systemy baz danych wykorzystują w tym celu mechanizmy: kopii zapasowych, kopii lustrzanej (*mirroring*) i macierzy dyskowych. Istotnym aspektem tolerancji awarii w systemach baz danych jest redundancja przetwarzania. Mechanizmy architektoniczne tych systemów, które mogą wspierać redundancję przetwarzania to serwery zapasowe, grona serwerów (*cluster*) i replikacja danych.

Architektura systemów baz danych nie obejmuje swoim zasięgiem redundancji komunikacji i całkowicie bazuje na usługach dostarczanych przez oprogramowanie komunikacyjne.

3.1 Odzyskiwanie danych

Ze względu na rozległość awarii w systemach baz danych wyróżniamy ich trzy rodzaje: awaria procesu użytkownika, awaria procesów systemowych (procesora) i awaria nośnika danych.

Awaria procesu użytkownika obejmuje jedynie aktywną transakcję realizowaną przez ten proces. Odzyskanie danych po awarii takiego procesu wymaga jedynie wycofania zmian wprowadzonych przez tą transakcję, aby zagwarantować atomowość transakcji, oraz zwolnienia zasobów systemowych (np.: blokady). Ponieważ transakcje są izolowane ich odtwarzanie jest całkowicie niezależne od stanu przetwarzania innych transakcji. Stąd w bazach odtwarzanie jest znacznie prostsze niż w przypadku ogólnego przetwarzania rozproszonego. W systemach baz danych wycofanie zmian jest wykonywane na podstawie utrzymywanego przez system, dziennika bazy danych (*database log*). Dziennik ten zawiera opis wszystkich operacji wykonanych przez transakcje (zarówno te, zatwierdzone jak i wycofane). Procedurę odzyskania danych po awarii procesu użytkownika zazwyczaj nadzoruje specjalny proces systemowy.

Awaria procesów systemowych wpływa na wszystkie aktywne transakcje w systemie oraz wszystkie rozproszone transakcje korzystające z danych nadzorowanych przez uszkodzony system. W tym przypadku do odzyskania danych niezbędne jest restartowanie systemu bazy danych. W czasie restartu system dokonuje wycofania wszystkich niezatwierdzonych transakcji, podobnie jak to ma miejsce w przypadku uszkodzenia procesu użytkownika. Ponadto, ze względu na buforowanie w pamięci operacyjnej operacji zapisu do bazy danych, odtworzenia mogą wymagać dane zmodyfikowane przez zakończone transakcje. W tym celu wykorzystuje się dane zawarte w dzienniku bazy danych.

Mechanizmy stosowane przez systemy baz danych gwarantują, że w przypadku niebizantyjskich awarii procesu użytkownika lub procesów systemowych udaje się odzyskać wszystkie zmiany na danych w bazie danych wykonane przez zatwierdzone transakcje i wycofać wszystkie zmiany niezatwierdzonych transakcji.

Ograniczenie skutków awarii nośnika danych wymaga odpowiednich środków. Podstawowym rozwiązaniem jest regularne wykonywanie kopii bezpieczeństwa. Pozwala ona na odzyskania wyników wielomiesięcznej lub nawet wieloletniej pracy z czasu wykonania ostatniej kopii. W wielu systemach informatycznych utrata danych z jednego dnia jest akceptowalna. Większość systemów baz danych wspiera wykonywanie gorącej kopii bezpieczeństwa (*hot backup*) w czasie normalnej pracy systemu, nie naruszając rytmu eksploatacji bazy danych.

Dla niektórych systemów informatycznych utrata wyników pracy rzędu jednego dnia nie jest jednak do zaakceptowania. W tym przypadku należy powielić na niezależnych nośnikach wszystkie strategiczne dane. Systemy baz danych wykorzystują mechanizm programowego utrzymywania kopii lustrzanej do powielania danych zawartych w dzienniku bazy danych. Nie powiela się za pomocą tego mechanizmu pozostałych danych systemu, gdyż to drastycznie obniżyłoby efektywność jego działania. W przypadku awarii jednego z nośników, na podstawie ostatniej kopii

2.3 Stabilizacja stanu systemu

Sporo pracy poświęca się ostatnio na opracowywanie takich algorytmów przetwarzania rozproszonego, które posiadają własność stabilizacji. System jest nazywamy samo-stabilizującym się, jeśli pomimo wystąpienia awarii potrafi w skończonej liczbie kroków sam (tzn. bez ingerencji z zewnątrz) powrócić do stanu poprawnego. System taki nie wymaga poprawnej inicjacji, dopuszcza dowolne przejściowe awarie (nawet Bizantyjskie) i adaptuje się do dynamicznych zmian topologii sieci. Niestety istnieją też poważne wady tego podejścia. Najważniejsze z nich to uwzględnienie tylko uszkodzeń przejściowych, brak możliwości wykrycia stabilizacji w dowolnym momencie i możliwa niespójność stanów poprzedzających ustabilizowanie się systemu. Szerokim polem zastosowań są tu m.in. protokoły komunikacyjne o podwyższonej niezawodności i sieci komputerowe ([Casavant94], [Schneider92], [Tel94]).

2.4 Replikacja

Niezawodność pracy systemu informatycznego można w naturalny sposób podnieść poprzez wprowadzenie redundancji sprzętu, usług i danych. Rozproszone systemy komputerowe są szczególnie predestynowane do implementacji koncepcji redundancji, poprzez replikację danych i procesów w różnych węzłach sieci. Powstałe w wyniku takiej replikacji systemy tolerujące uszkodzenia, są logicznym zbiorem pewnych grup procesów współpracujących ze sobą i komunikujących się za pomocą tzw. **komunikacji grupowej** lub **rozgłoszeniowej**. Przez grupową należy tu rozumieć komunikację typu jeden nadawca - wielu odbiorców komunikatu. Możliwość wystąpienia awarii łączy oraz asynchronizm komunikacji, wprowadzają zagrożenie, iż część procesów danej grupy może nie otrzymać wszystkich wiadomości, otrzymać wiadomości w różnej kolejności, a nawet wielokrotnie otrzymać te samą wiadomość. Te niepożądane zjawiska mogą doprowadzić do utraty spójności pracy systemu (np. niemożliwości rozwiązania problemu consensusu). Wymagana jest więc komunikacja, dysponująca takim mechanizmem synchronizacji pracy procesów, który gwarantuje odpowiednie **uporządkowanie wiadomości**. Realizacja spójnego uporządkowania wiadomości jest uzależniona od możliwości wykrycia uszkodzeń, a więc od rozwiązania następnego problemu - detekcji błędów (*faults detection*). Kolejnym ważnym problemem jest rozpad systemu na części (*partitions*), w wyniku takich uszkodzeń łączy, które prowadzą do rozdziału sieci. Jeśli mimo podziału sieci, istnieje jedna partycja, w której możliwy jest do osiągnięcia consensus (typowo ta skupiająca większość procesów) mówimy, że system zachowuje własność nadrzędnej partycji (*primary partition property*).

Jak wiadomo, podstawowe z wymienionych problemów, w tym problem consensusu czy detekcji błędów, są nierozwiązywalne w środowisku rozproszonym w pełni asynchronicznym [Fisher85]. Stąd w praktyce systemy powinny spełniać pewne dodatkowe założenia dotyczące synchronizacji komunikacji (np. maksymalne opóźnienia) lub dostępności mechanizmów detekcji błędów o określonych własnościach (*fault detectors*, [Chandra91]). Protokoły spójności mogą wymagać mechanizmów rozproszonego głosowania dynamicznego (*dynamic voting protocols*), które pozwalają na zebranie większości głosów pomimo uszkodzeń procesów-członków grupy.

Stosowane są w ogólności dwie metody replikacji:

- **aktywna replikacja**, w której proces klient komunikuje się ze wszystkimi członkami grupy serwerów;
- replikacja typu ***primary-backup***, w której proces klient komunikuje się tylko z wyróżnionym serwerem („nadrzędnym"), a on z kolei dba o aktualizację stanu replik zapasowych (czyli pozostałych procesów z grupy).

Aktywna replikacja wymaga pełnego uporządkowania wiadomości lub atomowego rozgłaszania i nie jest odporna na uszkodzenia typu Bizantyjskiego. Replikacja typu *primary-*

SYSTEMY ROZPROSZONE O PODWYŻSZONEJ NIEZAWODNOŚCI

Jerzy Brzeziński, Juliusz Jezierski, Michał Szychowiak

Instytut Informatyki
Politechnika Poznańska
{Jerzy.Brzeziński | Michal.Szychowiak | Juliusz.Jezierski}@cs.put.poznan.pl

Abstrakt. Wraz ze wzrostem złożoności rozproszonych systemów informatycznych i dynamicznego wzrostu ich zastosowań coraz częściej kluczowym problemem jest zagwarantowanie odpowiednio wysokiego stopnia niezawodności tych systemów. Artykuł ten prezentuje podstawowe problemy konstrukcji systemów rozproszonych o podwyższonej niezawodności obejmując zarówno aspekty badawcze, jak i rozwiązania stosowane w dostępnych na rynku systemach baz danych.

1. Wprowadzenie

W odpowiedzi na rosnące wymagania dotyczące niezawodności przetwarzania aplikacyjnego w środowisku rozproszonym, podjęto próbę realizacji rozproszonych systemów tolerujących uszkodzenia (*fault tolerant systems*). Aktualnie istnieje już pewna liczba takich systemów. Różnią się one rodzajem komponentów systemu odpornych na błędy, stopniem tolerancji uszkodzeń, czy sposobem osiągania niezawodności funkcjonowania. Niektóre systemy zakładają występowanie tylko błędów przejściowych (*transient failures*), inne zakładają uszkodzenia permanentne (*crash failures*), a jeszcze inne radzą sobie z oboma przypadkami. Istnieją systemy odporne na pojedyncze awarie łącz oraz takie, które akceptują nawet wielokrotny podział sieci na odrębne partycje. Niezawodność jest osiągana niekiedy poprzez specjalne rozbudowanie aplikacji o dodatkowe mechanizmy gwarantujące poprawną pracę nawet w przypadku wystąpienia awarii, i wówczas to warstwa aplikacyjna przejmuje na siebie odpowiedzialność za tolerancję uszkodzeń. O wiele wygodniejsze jednak, z punktu widzenia projektantów aplikacji i użytkowników systemów, jest dostarczenie odpowiedniej warstwy pośredniej, umożliwiającej odporne na uszkodzenia rozproszone wykonanie procesów. Warstwa taka, poprzez zastosowanie odpowiednich protokołów udostępnia warstwie aplikacyjnej gotowe usługi tolerancji uszkodzeń.

Tolerancja uszkodzeń jest dziś bardzo obszerną dziedziną, obejmuje m.in. takie zagadnienia jak: wycofanie operacji (*rollback*) i odzyskiwanie danych (*recovery*), maskowanie i ograniczanie skutków uszkodzeń (*fault masking, fault containing*), lokalne usuwanie uszkodzeń (*fault local mending*), protokoły rozproszonego głosowania (*voting protocols*) i zatwierdzania transakcji (*commit protocols*), czy algorytmy samo-stabilizujące się ([Casavant94], [Pham92], [Schneider92], [Singhal94], [Tel94]). Dużą popularność uzyskały w ciągu ostatnich lat systemy niezawodnej komunikacji grupowej (*reliable group communication*).

szyfrowane wartości w nowej dziedzinie. Szyfrowanie przez system bazy danych na poziomie nośnika jest zbyt kosztowne. Konieczność szyfrowania i odszyfrowywania informacji przy każdym zapisie i odczycie mogłaby drastycznie zmniejszyć efektywność bazy danych. Jedynym akceptowalnym rozwiązaniem jest szyfrowanie sprzętowe na poziomie sterownika dysku.

3.4 Obserwowanie użytkowników bazy danych

Istotnym mechanizmem systemów baz danych wspierającym bezpieczeństwo danych jest obserwowanie działań użytkowników. Za pomocą tego mechanizmu administrator może wykryć próby wykroczenia użytkowników poza swoje kompetencje oraz próby włamania się do systemu z zewnątrz.

Istnieje możliwość obserwowania użytkownika w trzech płaszczyznach: wykonania zlecenia SQL, wykorzystania przywileju systemowego oraz dostępu do określonego obiektu. Zakres zbieranej informacji we wszystkich płaszczyznach może być zawężony ze względu na: użytkownika, poprawność wykonanej operacji oraz krotność wykonanej operacji.

Wszystkie informacje zebrane w wyniku obserwacji są składowane w dzienniku obserwacji (*audit log*). Dziennik ten może być obiektem bazy danych, wówczas jest chroniony jak każdy inny obiekt w bazie danych i może być przeglądany za pomocą zleceń SQL. Dziennik obserwacji może być również składowany jako plik w systemie plikowym systemu operacyjnego, w tym przypadku jest chroniony przez system operacyjny i może być przeglądany za pomocą standardowych narzędzi. W przypadku, gdy dziennik jest obiektem bazy danych dostęp do niego również może być obserwowany.

Dziennik obserwacji zawiera informacje dotyczące: typu wykonanej operacji, użytkownika, wykorzystanych uprawnieniach, czasu i lokalizacji wykonanej operacji, statusu poprawności itp. W dzienniku obserwacji nie ma danych zmodyfikowanych przez obserwowane operacje. Jednakże zbieranie informacji o zmodyfikowanych danych może być w prosty sposób zaimplementowany korzystając mechanizmy wyzwalanych procedur (*trigger*).

4. Podsumowanie

Współczesny stan technologii informatycznych pozwala na zapewnienie rozproszonym aplikacjom i systemów zarządzania baza danych rożnych poziomów bezpieczeństwa Wybór odpowiednich mechanizmów konfrontuje kryteria ich sprawności, efektywności i ceny z faktycznymi potrzebami danego systemu informatycznego. Należy jednak pamiętać, iż problem bezpieczeństwa winien traktowany kompleksowo i angażować, w sposób starannie przemyślany i dokładnie zaplanowany, zarówno środki techniczne, jak i personalne i proceduralne. Tylko wówczas istnieje realna szansa zapewnienia bezpieczeństwa pracy całości systemu.

Literatura:

[Bellovin89] S.M. Bellovin, "Security Problems in the TCP/IP Protocol Suite" *Computer Communications Review*, 2(19) 1989, s.32-48.

[Braden89] R. Braden, "Requirements for Internet hosts-Communication Layers and Requirements for Internet Host's Communication Layers", RFC 1122, 1989.

[Chapman95] B.D. Chapman, E.D. Zwicky, *Building Internet Firewalls*, O'Reilly & Associates, Inc. Sebastopol, CA, 1995.

[Cheswick94] W.R. Cheswick, and S.M. Bellovin, *Firewalls and Internet Security*, Addison-Wesley, Reading, 1994.

Systemy baz danych wspierają również identyfikację użytkowników metodami biometrycznymi. W tym przypadku w bazie danych są przechowywane unikalne cechy biologiczne użytkowników np.: odcisk palca, kształt i kolor tęczówki oka, itp. Dane te są porównywane, w momencie żądania dostępu, z danymi przesłanymi z urządzeń pomiarowych.

Podobną rolę w ustalaniu tożsamości użytkowników może spełniać osobisty klucz identyfikacyjny, najczęściej w postaci karty magnetycznej lub elektronicznej np. SecurID.

Systemy baz danych do identyfikacji użytkowników w rozproszonych, heterogenicznych systemach informatycznych mogą wspierać się również na sieciowych usługach poświadczania tożsamości (*Network Authentication Services*), przykładowo: CyberSAFE Challenger, ICL Access Manager/SESAME, Kerberos, Bull ISM, DCE Security Services, itp.

3.2 Autoryzacja dostępu

Najczęściej wykorzystywane mechanizmy autoryzacji dostępu użytkowników do danych opierają się na uznaniowym modelu kontroli dostępu (*Discretionary Access Control*). Model DAC realizowany jest przez: przywileje systemowe, przywileje obiektowe oraz ochronę strukturalną i funkcjonalną danych.

Język kontroli dostępu dla relacyjnych baz danych został dobrze zdefiniowany w standardzie ANSI SQL92 Entry Level.

Przywileje systemowe opisują prawo wykonania operacji na systemie bazy danych, np. utworzenie użytkownika. Nadanie przywileju systemowego jest opisane następującą parą: przywilej, użytkownik; przykładowy zapis w języku SQL będzie wyglądał następująco: **GRANT** *CREATE USER* **TO** *KOWALSKI*. Przywileje systemowe mogą być nadawane jedynie przez administratora lub uprawnionego przez niego użytkownika.

Przywileje obiektowe odnoszą się do konkretnych obiektów, np. prawo odczytania danych z tabeli *pracownicy* należącej do Nowaka. Przywilej obiektowy opisany jest trójką: operacja, obiekt, użytkownik; przykładowo: **GRANT** *SELECT* **ON** *NOWAK.PRACOWNICY* **TO** *KOWALSKI*. Jedynie właściciel lub uprawniony przez niego użytkownik może nadawać przywileje obiektowe. Przywileju takiego nie ma administrator bazy danych.

Ochrona strukturalna opiera się na obiektach bazy danych zwanych perspektywy (*view*). Perspektywy umożliwiają zawężenie dostępu do wybranych informacji na podstawie zawartości i kontekstu danych. Perspektywy dają możliwość autoryzowania dostępu do danych w oparciu czasową dostępność danych, lokalizację użytkownika itp. Ponadto perspektywy umożliwiają kontrolę dostępu z ziarnistością pojedynczych rekordów. Takiej możliwości nie ma w standardowym modelu DAC.

Ochrona funkcjonalna wykorzystuje mechanizm składowanych w bazie danych funkcji i procedur. Użytkownik nie ma bezpośredniego dostępu do danych lecz jedynie do funkcji, które wykonują jedynie operacje przewidziane przez projektanta systemu. Przykładowo: użytkownik pełniący rolę pracownika personalnego posiada dostęp do funkcji *zatrudnij_pracownika*, *zwiększ_pensję* itp., nie musi mieć natomiast bezpośredniego dostępu do relacji *pracownicy*. Reguły ochrony w tym przypadku są zapisane w algorytmie procedury lub funkcji.

Do łatwiejszego zarządzania uprawnieniami standard SQL definiuje pojęcie roli. Rola jest to zbiór przywilejów przypisywany użytkownikom lub innym rolom. Jest to mechanizm zbliżony do mechanizmu grup w systemach operacyjnych.

Model ochrony danych DAC stanowi obowiązkową część poziomu ochrony C2.

Poufność informacji

Poufność ma ona gwarantować, że informacje będą obierane tylko przez osoby upoważnione. Podstawowym zagrożeniem dla poufności komunikacji jest podsłuch (monitoring). Może się on odbywać potencjalnie w każdym miejscu, przez które fizycznie przepływają nasze informacje, a więc zarówno we własnej sieci lokalnej, jak i w sieci rozległej. Istotnym problemem jest również swobodny dostęp do serwerów sieci lokalnych, stwarzający możliwość wtargnięcia intruza i odgadnięcie haseł użytkowników serwera. Dotyczy to zwłaszcza serwerów pracujących pod kontrolą systemu Unix, jest on bowiem dość powszechnie znany i szczególnie podatny na włamania.

Osobnym problemem, lecz nie pomijalnym, jest przypadkowy dostęp do pozostawionych aplikacji wykorzystujących poufne informacje.

Nienaruszalność informacji

Nienaruszalność ma gwarantować spójność informacji i chronić je przed dokonywaniem zmian przez osoby nieupoważnione oraz zapewniać by system zachowywał się w sposób przewidziany przez uprawnionych użytkowników.

Uwierzytelnianie użytkowników (*authentication*)

Z systemu informatycznego mogą korzystać tylko upoważnione osoby. Uwierzytelnianie jest procesem mający zapewnić, że osoby, które ubiegają się o dostęp do systemu, są rzeczywiście tymi, za które się podają. W sieci rozległej jest to w ogólności problem skomplikowany, lecz tym bardziej niezwykle istotny.

2.2 Ogólne zasady bezpieczeństwa

Świadomość

Najistotniejszym elementem ochrony danych jest świadomość zagrożeń. Dotyczy ona nie tylko stanowisk kierowniczych i administratorów sieci lokalnych, lecz również - i przede wszystkim - użytkowników. Świadomość problemów oraz mechanizmów ochrony danych i potrzeby ich stosowania jest niezbędna dla powodzenia jakichkolwiek prób zabezpieczenia systemu informatycznego. Należy pamiętać, że około 80% wszelkich naruszeń bezpieczeństwa danych pochodzi "od wewnątrz" i jest wynikiem mniej lub bardziej świadomego działania własnych pracowników.

Polityka ochrony informacji

Przede wszystkim należy oszacować, jak ważne są poszczególne dane (zasoby) dla nas i jaką wartość mogą one przedstawiać dla niepowołanych osób, a także na jakie straty zostaniemy narażeni w przypadku utraty tych danych lub chwilowej choćby niemożności korzystania z nich. Ta wiedza powinna być zebrana w postaci przemyślanej, powszechnie znanej polityki bezpieczeństwa, zarówno w zakresie lokalnym (sieci lokalnej), jak i globalnym. Musi ona zostać zaakceptowana i bezwzględnie przestrzegana na każdym szczeblu struktury systemu organizacyjnego.

Polityka bezpieczeństwa musi spełniać kryterium spójności pionowej i poziomej. Pierwsze dotyczy zachowania bezpieczeństwa w każdej warstwie systemu informatycznego ("w pionie"), tak aby dana warstwa (np. aplikacje) miała zagwarantowany wymagany poziom bezpieczeństwa z warstw niższych (np. komunikacyjnych). Drugie kryterium wymusza kompletność stosowanych zabezpieczeń na poziomie każdej z warstw z osobna, tak aby nie powstawały luki naruszające bezpieczeństwo całego układu.

MECHANIZMY BEZPIECZEŃSTWA W SYSTEMACH BAZ DANYCH

Juliusz Jezierski, Tomasz Koszlajda, Michał Szychowiak

Instytut Informatyki
Politechnika Poznańska
{ Juliusz.Jezierski | Tomasz.Koszlajda | Michal.Szychowiak }@cs.put.poznan.pl

Abstrakt. Wraz ze wzrostem złożoności infrastruktury sieciowej i często nieuniknionej konieczności łączenia lokalnych sieci komputerowych w sieć rozległą, komplikuje się problem zapewnienia bezpieczeństwa rozproszonego systemu informatycznego. Problem ten dotyczy całości systemu komputerowego danego przedsiębiorstwa czy instytucji - rozproszonych aplikacji, zasobów sieci lokalnej, mechanizmów administracji sieci. Artykuł ten prezentuje podstawowe problemy bezpieczeństwa oraz niezawodności systemów rozproszonych, z uwzględnieniem głównie aspektów teoretycznych i aktualnych trendów w rozwiązaniach praktycznych. Poruszane zagadnienia obejmują w szczególności poufność informacji i jej dostępność w systemach baz danych.

1. Wprowadzenie

Dzięki niezwykle intensywnemu postępowi technologii sieciowej, współczesne aplikacje mają okazję korzystać z bardzo szybkich łączy komunikacyjnych, wydajnych protokołów sieciowych i atrakcyjnych rozproszonych zasobów infrastruktury sieciowej. Palącym staje się jednakże problem bezpieczeństwa tej infrastruktury. Znaczenie tego problemu rośnie wraz ze wzrostem rozmiaru i złożoności struktury przestrzennej, liczby aplikacji oraz stopnia ważności przetwarzanych danych. Dla wielu organizacji i przedsiębiorstw ochrona informacji jest jednym z najważniejszych aspektów zarządzania współczesną infrastrukturą informatyczną. Dotyczy to zwłaszcza systemów rozproszonych baz danych oraz aplikacji pracujących w architekturze klient-serwer. Ochrona informacji angażować powinna więc wszelkie dostępne środki fizyczne, proceduralne, personalne i techniczne proporcjonalnie do wartości tych informacji.

1.1 Bezpieczeństwo danych

Każdy komponent systemu informatycznego jest narażony na mniej lub bardziej celowe działania naruszające poprawność jego funkcjonowania. Każda dana, do której istnieje dostęp może zostać niewłaściwie zmodyfikowana lub przekazana w niewłaściwe ręce. Praktycznie, cały czas jesteśmy narażeni na szereg niebezpieczeństw, od awarii zasilania, poprzez podsłuchiwanie i podszywanie się pod uprawnionych użytkowników, ataki wirusów, aż po włamanie i całkowitą destrukcję systemu. Podstawowym warunkiem zagwarantowania bezpieczeństwa jest opracowanie

Ilość styków z Internetem powinna być jak najmniejsza dla uzyskania łatwości zarządzania i kontroli bezpieczeństwa połączenia z Internetem.
Z tego względu wydaje się, iż optymalnym rozwiązaniem byłby jeden wspólny styk z Internetem dla wszystkich sieci administracji państwowej. Rozwiązanie takie daje maksimum bezpieczeństwa przy minimalnym nakładzie kosztów.

Przegroda na styku z Internetem (firewall)

Zakładajac jeden, wspólny styk z Internetem dla lokalnych sieci jednostek administracji należy zdefiniować funkcje bezpieczeństwa tego styku.
Infrastruktura styku , który realizowałby funkcje przegrody (firewall) powinna z punktu widzenia bezpieczeństwa spełniać następujące funkcje:

- filtrowanie pakietów na podstawie adresów źródłowych i docelowych oraz na podstawie rodzaju usługi,

- niezawodne i bezpieczne uwierzytelnienie użytkowników Internetu

- agenta zastępczego (proxy service) usług, które maja być dozwolone (np. telnet, ftp, WWW)

- zapis zdarzeń związanych z komunikacją wskroś przegrody
- opcjonalnie: translację adresów (Network AddressTranslation)
- odpowiednią przepustowość (performance)

Przegroda powinna być administrowana w sposób ciągły oraz dać możliwość pełnej analizy wchodzącego i wychodzącego ruchu pod kątem założonego programu bezpieczeństwa.

Filtrowanie

Filtrowanie zgodnie z założonym programem bezpieczeństwa zapewnia, iż żadne usługi lub połączenia , które nie są dozwolone w komunikacji pomiędzy siecią wewnętrzną a Internetem nie będą realizowane.
Dodatkowo przegroda na styku z Internetem powinna realizować funkcję Network Address Translation (NAT) w celu mapowania adresów z sieci wewnętrznej na adresy widoczne z zewnątrz (np. w celu ukrycia prawdziwych adresów).

Zastępstwo usług (proxy services)

Konstrukcja przegrody musi zapewniać także analizę odwołań użytkowników żądających konkretnych usług - żadne pakiety, które nie wpisują się w założony program bezpieczeństwa nie powinny być przepuszczane przez przegrodę.

Uwierzytelnienie

Powodzenie systemu ochrony jest zależne od właściwej technologii uwierzytelnienia użytkowników. Zaleca się stosowanie haseł jednokrotnego użycia co oznacza, że użytkownicy są wyposażeni w tzw. tokeny generujące hasła ważne tylko na jedno uwierzytelnienie. Jeden token może służyć użytkownikowi do uwierzytelniania na wiele urządzeń, do których dostęp został dlań zdefiniowany.

- często skutecznym wyjściem jest użycie specjalisty z zewnątrz dla pokonania barier świadomości potrzeby stosowania tych czy innych mechanizmów ochrony
- należy rozmawiać kolejno ze wszystkimi „nieprzekonanymi"
- należy unikać teoretyzowania
- zalecane jest ćwiczenie: postaw się w roli intruza
- pomyśl o zgrożeniach (z wewnątrz i z zewnątrz)
  spróbuj sobie wyobrazić czarny scenariusz (i tak pozostanie wiele rzeczy, które nie dają się przewidzieć)

W sytuacjach krytycznych tylko odtworzenie systemu z „czystych" kopii może dać pewność, że wyjściowa funkcjonalność zostanie przywrócona.
- jest rzeczą podstawową aby przewidzieć sposób na „recovery" - odtworzenie działającego systemu po nieprzewidzianych zdarzeniach

Bezwzględne kanony eksploatacji

W czasie pilotowej i docelowej eksploatacji istotne jest zapewnienie:

- stałego nadzoru i opieki nad przyjętym programem
- aby rezultaty stosowania przyjętych rozwiązań były właściwie spożytkowane
- aktualizacji
- kontroli czy wszystko zostalo uwzględnione ?

Realność zagrożenia

Trzeba bezwzględnie stwierdzić, iż zagrożenie jest realne.Brak przewidywania, testowania, świadomości, brak czasu na śledzenie pojawiających się metod ataku i ochrony oraz niedocenianie zagrożen zewnętrznych i wewnętrznych może być powodem przykrych niespodzianek -szczególnie w sieciach , które niejako z definicji powinny mieć podwyższony reżim ochrony.

Niektóre zagrożenia, mimo, że występują na dużą skalę - nie są przez wszystkich dostrzegane
Przykłady? Oto one:
trudno znaleść włamywacza, który nie czytałby publikacji (advisory) CERT/CC, AUSCERT lub CIAC
- jest natomiast spora liczba administratorów systemów (Intranet , Internet), którzy tego nie czytają
Samo „czytelnictwo" advisory nic wystarcza - liczy się wprowadzanie w życie sprawdzonych sposobów zabezpieczania się.
- włamywacze stosując narzędzia programowe dostępne w „hacker sites" stosują coraz to nowe typy ataków
- jeśli nie działasz szybko aby się zabezpieczyć możesz nie zdążyć...
- typowy administrator sieci ma wiele obowiązków na głowie
  - na zabezpieczanie się przed niewidzialnym wrogiem po prostu często nie ma czasu...

Internetowe sąsiedztwo

W Internecie wszyscy właściwie są sąsiadami. Jest to trywialna prawda - lecz często nie zauważana. Sasiedztwo to może być zaskakujaco negatywnym doświadczeniem jeśli nie zostaną podjęte skuteczne metody ochrony sieci dołączonych do tej sieci.

- Zapewnieniem integralności danych (konfiguracyjnych lub użytkownika) czyli zabezpieczeniem przed nieuprawnionymi zmianami
- Zapewnieniem dostępności danych i usług zgodnie z założonym programem
- Kontrolą dostępu do zasobów i pomieszczeń,
- Zdolnością oceny stanu bezpieczeństwa systemu na różnych odcinkach

Program bezpieczeństwa, a Internet

Wśród głównych serwisów podlegających ochronie należy wymienić:
- E-mail (poczta elektroniczna)
- FTP (przesyłanie plików)
- telnet (zdalny dostęp terminalowy)
- HTTP (klient WWW)
- HTTPD (serwer WWW)

Poczta elektroniczna.

Aby system poczty elektronicznej nie stanowił zagrożenia dla bezpieczeństwa systemu należy sobie odpowiedzieć na szereg podstawowych pytań w rodzaju:

- kto może posiadać konto i na jakiej zasadzie jest ono przyznawane?
- jakie prawa i obowiązki ciążą na użytkowniku konta?
- czy jest mechanizm weryfikacji ważności konta?
- czy korespondencja jest/powinna być szyfrowana ?
- czy istnieje (oraz czy musi istnieć) kopia zapasowa plików użytkownika na koncie?
- jakie są potencjalne luki bezpieczeństwa w zastosowanym systemie pocztowym?

FTP (File Transfer Protocol)

Jest to protokół pozwalający na przesyłanie dowolnych plików do i z sieci abonenta Internetu a dodatkowo (jak wszystkie protokoły internetowe) nie wolny od luk bezpieczeństwa. W związku z tym tak jak poprzednio istnieje wiele pytań, które muszą znaleść odpowiedź w programie bezpieczeństwa:

- kto i skąd ma dostęp do usługi ?
- czy istnieje możliwość weryfikacji ściąganego oprogramowania
- czy można ograniczyć dostęp do serwisu ?
- jakie środki należy przedsięwziąć by zwiększyć bezpieczeństwo użytkowania serwisu?

Telnet to z kolei najpopularniejszy protokół dostepu terminalowego do ogległych maszyn. W tym przypadku rownież pojawiają się określone pytania:

- kto i dlaczego potrzebuje dostępu do serwisu ?
- czy zastosować dodatkową ochronę (np. hasła jednokrotnego użytku) ?
- czy istnieje potrzeba/konieczność szyfrowanych sesji ?

HTTP jest bodaj najpopularniejszym protokołem internetowym ze wzgledu na rozwój usług typu WWW. Tu szczególnie ważne jest zaplanowanie:

Najskuteczniejszą metodą weryfikacji poziomów emisyjności i odporności systemu na narażenia elektromagnetyczne jest pomiar. Przeprowadzenie pomiarów jest wiarygodnym źródłem informacji na temat potrzeby ochrony systemu teleinformatycznego. Ze względu na fakt starzenia się instalacji, co pewien czas powinny być prowadzone pomiary weryfikacyjne.

7.Literatura

[1] Ott H.W., "Metody redukcji zakłóceń i szumów w układach elektronicznych", WNT, Warszawa 1979.

[2] White D.R.J., "EMI Control Methodology and Procedures", Don White Consultants Inc., Gaineswille, USA.

[3] Hołownia J., "Współczesne problemy kompatybilności elektromagnetycznej sprzętu komputerowego", Raport nr I-28/SPP - 008/86 Instytutu Telekomunikacji i Akustyki Politechniki Wrocławskiej, Wrocław 1986.

[4] Więckowski T.W., Badanie odporności urządzeń elektronicznych na impulsowe narażenia elektromagnetyczne, Prace Naukowe Instytutu Telekomunikacji i Akustyki Politechniki Wrocławskiej, Seria: Monografie, nr 37, Wrocław 1993.

- ekranować i filtrować,
- zmniejszać poziomy emitowanej informacji.

Chcąc zapewnić odporność systemu teleinformatycznego na narażenia elektromagnety-czne należy:

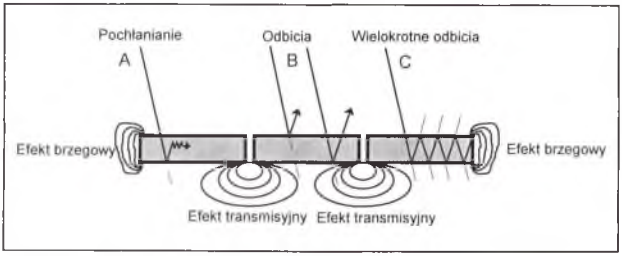
- stosować odpowiednie rozwiązania układowe i technologiczne podwyższające odporność,
- ekranować i filtrować.

5.1. Ekranowanie

Należy pamiętać, że nawet posługując się wszystkimi najważniejszymi sposobami redukcji rozproszenia elektromagnetycznego - takimi jak ekranowanie, uziemianie, filtracja, izolowanie, dobór kabli - nie można zazwyczaj w pełni wyeliminować rozproszenia elektromagnetycznego informacji użytecznej oraz zabezpieczyć systemu przed narażeniami elektromagnetycznymi. Może jedynie zminimalizowane do pewnego poziomu zarówno rozpraszaną przez system energię jak i narażenia elektromagnetyczne. Dwoma podstawowymi środkami zmniejszania przenikania energii elektromagnetycznej są: ekranowanie i uziemianie. Metody ekranowania i uziemiania są ściśle powiązane ze sobą.

W sieciach teleinformatycznych ekranowane mogą być kable lub kompletne urządzenia (komutatory, komputery, serwery, itp.). Skuteczność ekranowania zmienia się wraz z częstotliwością sygnału, strukturą geometryczną ekranu, rodzajem ekranowanego pola, kierunkiem jego padania i polaryzacją. Do podstawowych charakterystyk ekranów zaliczamy skuteczność ekranowania S_s (dB) i charakterystykę częstotliwościową tej skuteczności. Skuteczność danego ekranu przy określonej częstotliwości zależy zarówno od materiału i grubości ścianek konstrukcji ekranującej jak też od odległości miedzy powierzchnią ekranująca a źródłem promieniowania r [m].

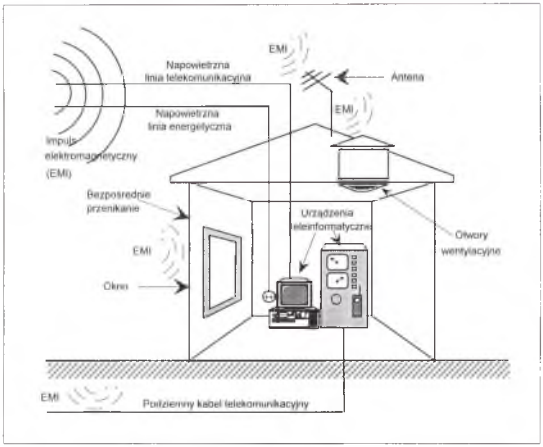
Oddziaływanie materiałów ekranujących na pole elektromagnetyczne zilustrowano na rysunku *(Rys. 7)*. Skuteczność ekranów idealnych (czyli w pełni jednorodnych, bez złącz szczelin i otworów) można obliczyć przy pomocy teoretycznych zależności matematycznych. Jednak rzeczywiste ekrany maja skuteczność znacznie mniejszą z powodu niejednorodności powierzchni ekranującej oraz przerw w powierzchni ekranującej. Charakterystyki ekranów rzeczywistych najłatwiej wyznaczyć na drodze pomiarów. Materiały o dużej przewodności są w stanie ograniczyć jedynie rozproszenie składowej elektrycznej pola elektromagnetycznego. Składowa magnetyczna pola wymaga stosowania materiałów o dużej przenikalności magnetycznej takich jak np. stal.



Rys. 7. Oddziaływanie materiału ekranującego na pole elektromagnetyczne

5.1.1. Ekranowanie urządzeń

Osłona ekranująca działa najskuteczniej, jeśli jest szczelna (klatka Faraday'a), a napięcia zasilające są doprowadzone poprzez filtry dolnoprzepustowe. W urządzeniach stanowiących elementy sieci teleinformatycznej ekrany metalowe są stosowane w wykonaniach specjalnych. W urządzeniach teleinformatycznych ogólnego przeznaczenia, dostępnych na rynku, powszechnie są



Rys. 6. Ilustracja sposobów oddziaływania impulsów elektromagnetycznych na obiekt teleinformatyczny

Ściany betonowe wnoszą tłumienie od 5 do 35 dB, zależnie od ich konstrukcji. Jeśli budynek jest ekranowany blachą stalową (klatka Faradaya), to tłumienie pola wzrasta do 50-100 dB. Ponieważ składowe impulsu o większych częstotliwościach są silniej tłumione, więc czas narastania impulsu wewnątrz impulsu wewnątrz budynku ulega wydłużeniu. Pole, które wniknęło do budynku indukuje w wewnętrznym okablowaniu prądu o natężeniu od 1 do 20 amperów. Dodatkowo na rozpatrywany obiekt teleinformatyczny oddziałują, przez linie zasilające, impulsowe zakłócenia powodowane przez zasilacze tyrystorowe, wyłączniki, zgrzewarki itp..

Z przedstawionych rozważań wynika, że są dwa sposoby oddziaływania zakłóceń impulsowych, zwłaszcza impulsów elektromagnetycznych, na urządzenie elektroniczne, a mianowicie:

- oddziaływanie pośrednie,
- oddziaływanie bezpośrednie

Przez oddziaływanie pośrednie rozumiemy oddziaływanie impulsów prądu lub napięcia na urządzenie elektroniczne, indukowanych przez impulsy elektromagnetyczne w liniach energetycznych, torach sygnałowych i antenach

Przez oddziaływanie bezpośrednie rozumiemy oddziaływanie impulsu elektromagnetycznego wprost na urządzenie.

4.2. Ocena odporności urządzeń na narażenia impulsowe

O wymaganiach stawianych urządzeniom i systemom pracującym w obecności impulsowych pól elektromagnetycznych lub narażonym na celowe oddziaływanie takich pól decyduje użytkownik. Wymagania te sprecyzowane są najczęściej w normach przedmiotowych. Używa się powszechnie przy tym trzech podstawowych pojęć, a mianowicie:

- odporność,
- podatność,
- wytrzymałość.

$$Epu = max \{ Epur, Epuc \} \quad (2)$$

oraz

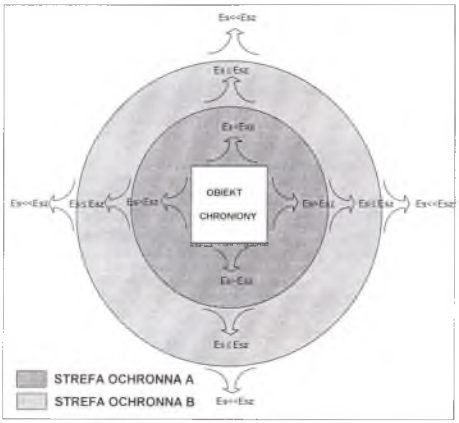
$$ps(f)\ [dB] = 20*log(Ed/Epu) + Ss\ [dB] = 20*log(Ed/Es) > 0\ [dB] \quad (3)$$

przy czym: *Epur - maksymalna dopuszczalna emisja promieniowana widma wiadomości przez urządzenie,*

Epuc - maksymalna dopuszczalna emisja przewodzona widma wiadomości.

Najistotniejsze elementy takiej instalacji decydujące o stopniu zabezpieczenia poufności informacji to *(Rys. 3)*:

- rozproszenie elektromagnetyczne wiadomości przez urządzenia, linie transmisyjne i zasilające systemu mniejsze niż dopuszczalny poziom *Epu*),
- strefa ekranowana o dostatecznie dużej skuteczności ekranowania systemu *Ss*,
- filtry o odpowiednio dużej skuteczności *Afs* na wejściach zasilających,
- izolatory minimalizujące możliwość rozproszenia elektromagnetycznego wiadomości przez linie transmisyjne.



Rys. 4. Podział obszaru na strefy ochronne wokół systemu bez skutecznej ochrony przed rozpraszaniem elektromagnetycznym informacji

W przypadku gdy nie jesteśmy w stanie zapewnić odpowiedniego stopnia protekcji systemu teleinformatycznego w obrębie obiektu chronionego, należy wyznaczyć strefy ochronne wokół tego obiektu *(Rys. 4)*. Powinny one obejmować obszar , w obrębie którego poziom natężenia pola elektromagnetycznego wypromieniowanego przez system teleinformatyczny nie będzie przekraczał dopuszczalnych poziomów. Ze względu na trudność oszacowania poziomu energii emitowanej przez system teleinformatyczny jako całość, rzeczywiste natężenia pola elektromagnetycznego w obrębie takiego systemu najłatwiej wyznaczyć na drodze pomiarów.

4.Odporność systemów teleinformatycznych na narażenia elektromagnetyczne

Narażenia elektromagnetyczne dzieli się na dwie zasadnicze grupy:

- pola elektromagnetyczne o charakterze ciągłym - powstające np. w wyniku pracy urządzeń nadawczych, pieców indukcyjnych, kuchni mikrofalowych.
- zakłócenia impulsowe - impulsy napięcia, prądu lub pola elektromagnetycznego.

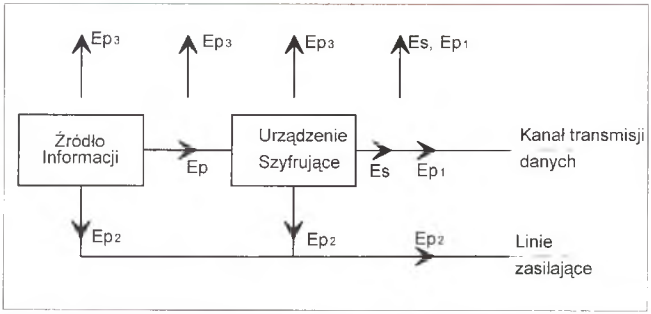
- linie zasilające układy scalone, zwłaszcza gdy układy pracują synchronicznie, np. bufory szyn i magistral, pamięci (prądy wieloamperowe);
- okablowanie wewnątrz urządzeń, np. płaskie taśmy wielożyłowe, skrętki, kable ekranowane, pojedyncze połączenia;
- korpusy urządzeń wykonane z materiałów przewodzących;
- zasilacze, zwłaszcza impulsowe;
- niezakończone obciążeniem linie sygnałowe i sterujące, np. do nieużywanych gniazd interfejsów;
- wszelkie przekaźniki, klucze, włączniki;
- połączenia sieciowe między urządzeniami;
- monitory ekranowe, zwłaszcza układy odchylania i zasilania lampy kineskopowej.

3.2. Ochrona informacji użytecznej przed niepożądaną detekcją

Minimalizacja rozproszenia elektromagnetycznego informacji użytecznej jest ściśle związana z jej detekcja i ma do spełnienia dwa zasadnicze zadania :

- ochrona przesyłanych i przetwarzanych informacji przed ich przekłamaniem lub zanikiem oraz przed niepożądanym dostępem,
- zapewnienie kompatybilności elektromagnetycznej urządzeń tzn. wypromieniowana przez te urządzenia energia nie powinna powodować zakłóceń w pracy innych urządzeń zarówno w ramach danego systemu (zakłócenia wewnątrzsystemowe), jak i innych systemów (zakłócenia międzysystemowe).

Ochrona informacji przed niepożądanym dostępem oprócz klasycznych form zabezpieczenia, takich jak zapobieganie nielegalnemu dostępowi do pamięci masowych i wydruków itp. wymaga minimalizacji rozproszenia elektromagnetycznego. Staje się to szczególnie konieczne, gdy instalacje obejmujące urządzenia łączone są w sieć. Podsłuch może być stosowany znacznie częściej niż to sobie wyobrażamy. Gdy istnieje dość duże rozproszenie w postaci pola elektromagnetycznego podsłuch stosować może każdy, kto zada sobie trud ustawienia anteny. Należy zatem ograniczyć rozproszenie elektromagnetyczne i szyfrować dane, tak aby stały się one niezrozumiale dla wszystkich, z wyjątkiem właściwego adresata.



Ep1 - niepożądane nałożenie składowych widma wiadomości na widmo zaszyfrowanego sygnału Es i zawartość tych składowych w widmie emisji przewodzonych i promieniowanych Es,
Ep2 - zawartość widma emisji wiadomości pierwotnej w liniach zasilających systemu,
Ep3 - promieniowanie widma emisji wiadomości pierwotnej przez obwody i linie źródła wiadomości i szyfratora.

Rys. 2. Schemat przetwarzania i transmisji wiadomości ze skutecznym jej szyfrowaniem i możliwymi drogami rozpraszania elektromagnetycznego wiadomości

Tabela 5.cd. Zakres norm stowarzyszonych z normą ***EN 50082-1; 1995***

Standard IEC	Standard europejski EN	Zakres
IEC 1000-4-11	EN 61000-4-11;1994	Sekcja 11: Spadki napięcia, krótkie zaniki i zmiany napięcia
-	ENV 50140;1993	Testowanie odporności na promieniowane zakłócenia elektromagnetyczne o częstotliwościach radiowych
-	ENV 50141;1993	Testowanie odporności na przewodzone zakłócenia elektromagnetyczne o częstotliwościach radiowych
-	ENV 50204;1995	Testowanie odporności na promieniowane zakłócenia elektromagnetyczne pochodzące od radiotelefoni cyfrowej

Tabela 6. Zakres norm stowarzyszonych z normą ***EN 50082-2; 1994***

Standard IEC	Standard europejski EN	Tytuł
IEC 50(161)	-	Międzynarodowy Słownik Elektrotechniczny Rozdział 161: Kompatybilność elektromagnetyczna
IEC 801-4	-	Kompatybilność elektromagnetyczna sprzętu pomiarowego i kontrolnego związanego z procesami przemysłowymi Sekcja 4:Wymagania dotyczące szybkich wyładowań elektrycznych
IEC 1000-4-2	EN 61000-4-2	Kompatybilność elektromagnetyczna (EMC) Część 4: Testowanie i techniki pomiarowe Sekcja 4:Wymagania dotyczące szybkich wyładowań elektrycznych
IEC 1000-4-8	EN 61000-4-8	Sekcja 8: Testowanie odporności na pola magnetyczne o częstotliwości zasilania
CISPR 11 (mod)	EN 55011	Wartości graniczne i metody pomiaru charakterystyk zakłóceń radiowych urządzeń przemysłowych , badawczych, i medycznych (ISM) pracujących w zakresie częstotliwości radiowych
CISPR 22:1985	EN 55022:1987	Wartości graniczne i metody pomiaru charakterystyk interferencji radiowych urządzeń techniki informatycznej
-	ENV 50140;1993	Testowanie odporności na promieniowane zakłócenia elektromagnetyczne o częstotliwościach radiowych
-	ENV 50141;1993	Testowanie odporności na przewodzone zakłócenia elektromagnetyczne o częstotliwościach radiowych

3. Detekcja i rozpraszanie elektromagnetyczne

Detekcja informacji użytecznej jest to proces fizyczny mający na celu odtworzenie sygnału źródłowego z sygnału, który wydostaje się na zewnątrz urządzenia

Pod pojęciem rozproszenia elektromagnetycznego informacji użytecznej urządzeń teleinformatycznych należy rozumieć energię wypromieniowaną przez te urządzenia.

Istnieją cztery drogi rozpraszania energii elektromagnetycznej (EM):

- przez sprzężenia pojemnościowe (składowa elektryczna pola EM),
- przez sprzężenia indukcyjne (składowa magnetyczna pola EM),
- przez wypromieniowanie fali elektromagnetycznej,
- przez sprzężenia galwaniczne (prąd płynący w przewodach).

Tabela 2

<table>
<tr><td>Kompatybilność elektromagnetyczna
Pomieszczenia i urządzenia</td><td colspan="2">Emisja</td><td colspan="2">Odporność</td></tr>
<tr><td rowspan="11">Powszechnego użytku,
komercyjne,
środowisko przemysłu lekkiego</td><td colspan="2">EN-50081-1;1992
Standard źródłowy</td><td colspan="2">EN 50082-1;1995
Standard źródłowy</td></tr>
<tr><td colspan="2">Normy szczegółowe stowarzyszone</td><td colspan="2">Normy szczegółowe stowarzyszone</td></tr>
<tr><td>Normy IEC</td><td>Normy EN</td><td>Normy EN</td><td>Normy EN</td></tr>
<tr><td>IEC 50(161)</td><td>-</td><td>IEC 50(161)</td><td>-</td></tr>
<tr><td>IEC 555-1</td><td>EN 60555-1</td><td>IEC 1000-4-2</td><td>EN 61000-4-2; 1995</td></tr>
<tr><td>IEC 555-2 (mod)</td><td>EN 60555-2</td><td>IEC 1000-4-4</td><td>EN 61000-4-4; 1995</td></tr>
<tr><td>IEC 555-3</td><td>EN 60555-3</td><td>IEC 1000-4-5</td><td>EN 61000-4-5; 1995</td></tr>
<tr><td>CISPR 14 (mod)</td><td>EN 55014</td><td>IEC 1000-4-8</td><td>EN 61000-4-8; 1993</td></tr>
<tr><td>CISPR 22 (mod)</td><td>EN 55022</td><td>IEC 1000-4-11</td><td>EN 61000-4-11; 1994</td></tr>
<tr><td colspan="2" rowspan="3"></td><td>-</td><td>ENV 50140; 1993</td></tr>
<tr><td>-</td><td>ENV 50141; 1993</td></tr>
<tr><td>-</td><td>ENV 50204; 1995</td></tr>
<tr><td rowspan="11">Środowisko przemysłu ciężkiego</td><td colspan="2">EN-50081-2;1993
Standard źródłowy</td><td colspan="2">50082-2;1994
Standard źródłowy</td></tr>
<tr><td colspan="2">Normy szczegółowe stowarzyszone</td><td colspan="2">Normy szczegółowe stowarzyszone</td></tr>
<tr><td>Standardy IEC</td><td>Standardy EN</td><td>Standardy IEC</td><td>Standardy EN</td></tr>
<tr><td>IEC 50(161)</td><td>-</td><td>IEC 50(161)</td><td>-</td></tr>
<tr><td>CISPR 11 (mod)</td><td>EN 55011</td><td>IEC 801-4</td><td>-</td></tr>
<tr><td>CISPR 14</td><td>EN 55014</td><td>IEC 1000-4-4</td><td>EN 61000-4-4</td></tr>
<tr><td>CISPR 22;1985 (mod)</td><td>EN 55022; 1987</td><td>IEC 1000-4-8</td><td>EN 61000-4-8</td></tr>
<tr><td colspan="2" rowspan="4"></td><td>CISPR 11 (mod)</td><td>EN 55011</td></tr>
<tr><td>CISPR 22; 1985</td><td>EN 55022; 1987</td></tr>
<tr><td>-</td><td>ENV 50140; 1993</td></tr>
<tr><td>-</td><td>ENV 50141; 1993</td></tr>
</table>

(mod) - modyfikacja standardu

KOMPATYBILNOŚĆ ELEKTROMAGNETYCZNA A BEZPIECZEŃSTWO INFORMACJI W SIECIACH TELEINFORMATYCZNYCH

Daniel J. Bem, Waldemar E. Grzebyk, Jarosław M. Janukiewicz

Naukowa i Akademicka Sieć Komputerowa
Zakład Telekomunikacji
50-327 Wrocław, ul. Janiszewskiego 7/9, tel./fax: 219529

1. Wprowadzenie

U progu XXI wieku informacja staje się najbardziej poszukiwanym i najlepiej chronionym towarem. Rozwój cywilizacyjny społeczeństw jest uzależniony od stopnia rozwoju systemów teleinformatycznych i telekomunikacyjnych. Szczególną rolę odgrywają urządzenia i systemy służące do przesyłania magazynowania i przetwarzania informacji. Wspólnie z systemami telekomunikacyjnymi są one integralną częścią złożonych systemów gospodarczych i kulturowych. Bezpieczeństwo i niezawodność systemów teleinformatycznych warunkuje rozwój i prawidłowe funkcjonowanie gospodarki narodowej.

Bezpieczeństwo systemów teleinformatycznych jest w dużej mierze uzależnione od dwóch podstawowych elementów:

- stopnia protekcji informacji użytecznej przed niepożądaną detekcją,
- odporności systemu na narażenia elektromagnetyczne.

Obserwuje się więc wzrastające zainteresowanie problematyką kompatybilności elektromagnetycznej. Pod pojęciem kompatybilności elektromagnetycznej systemu EMC (ang. Electromagnetic Compatibility) rozumiemy jego zdolność do poprawnej pracy w swoim otoczeniu. Kompatybilność elektromagnetyczna obejmuje dwa aspekty pracy systemu:

- emisyjność (ang. Emission) - poziom zakłóceń elektromagnetycznych generowanych przez wyróżniony system nie może zakłócać otoczenia,
- odporność (ang. Immunity) - wyróżniony system musi być odporny na pola występujące w środowisku elektromagnetycznym.

Wymagania dotyczące kompatybilności elektromagnetycznej urządzeń i systemów teleinformatycznych coraz częściej należą do kategorii wymagań podstawowych, takich jak odporność na narażenia mechaniczne i klimatyczne. W zastosowaniach specjalnych takich jak gospodarka narodowa oraz bezpieczeństwo i ochrona państwa, wymagany jest podwyższony poziom kompatybilności elektromagnetycznej systemów teleinformatycznych.

Podstawowym problemem staje się zrównoważenie wymagań dotyczących łatwego dostępu do zasobów przez uprawnionych użytkowników sieci teleinformatycznej i ochrona informacji przed niepowołanym dostępem, zakłóceniami lub zanikiem. Skala problemu zwiększa się wraz z lawinowo rosnącą liczbą instalacji. Na administratorze sieci spoczywa obowiązek zabezpieczenia sieci i jej zasobów. O ile dostrzegamy potrzebę stosowania mechanizmów zabezpieczeń przed nieuprawnionym dostępem wewnątrz sieci teleinformatycznej, to często nie zwracamy uwagi na:

- niebezpieczeństwo podsłuchu za pomocą odbioru promieniowania elektromagnetycznego od linii komunikacyjnych, terminali i innych urządzeń sieciowych,
- niebezpieczeństwo celowego zakłócania pracy sieci poprzez emisję narażeń elektromagnetycznych.

2. Europejskie standardy kompatybilności elektromagnetycznej

Na terenie Wspólnoty Europejskiej i krajów stowarzyszonych w EFTA (ang. European Free Trade Association) działa organizacja CENELEC (ang. European Committee for Electrotechnical Standardization) i w jej ramach kilka ciał zajmujących się kompatybilnością elektromagnetyczną , a

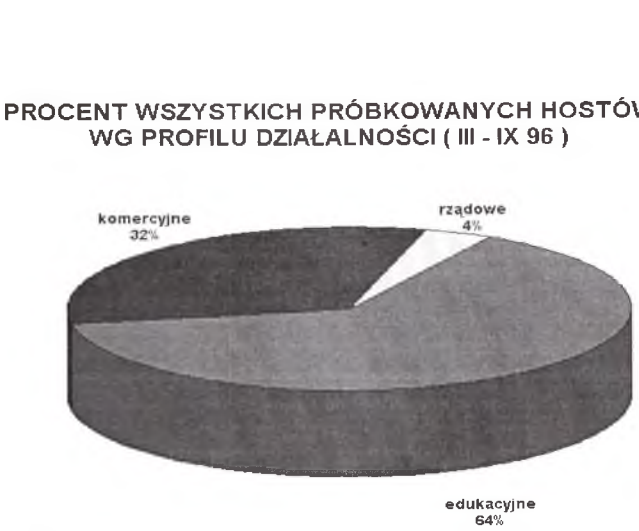


Diagram nr 2 ilustruje podział procentowy atakowanych komputerów wg. profilu działalności podmiotów do których te komputery należą.

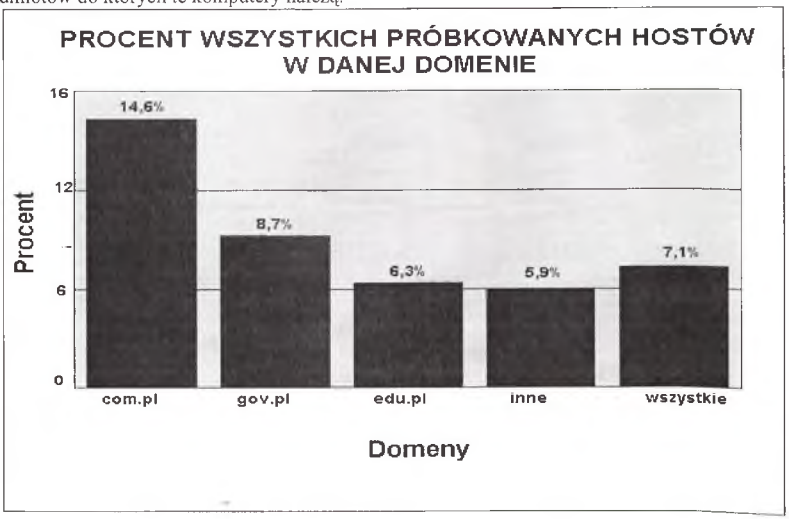


Diagram nr 3

Na diagramie nr. 3 zilustrowano proporcje próbkowanych hostów do ogólnej ilości zarejestrowanych hostow w danej domenie.

Kategoria "inne" odpowiada tej samej kategorii z diagramu nr. 1.

Oddzielną grupę stanowią działania związane z naruszeniem etykiety sieciowej (zwanej netykietą). Przykładami tego jest spamming i mail bombing. Można ten typ działalności podzielić na dwa rodzaje. Pierwszy to rozsyłanie materiałów reklamowych lub innych, które nie są zamawiane przez odbiorcę, drugi zaś to przesyłanie dużej ilości listów, lub mniejszej ale o większej zawartości, pod jeden wybrany adres. Ten drugi sposób niejednokrotnie może zablokować skrzynkę pocztową poszkodowanego i skutecznie utrudnić mu pracę i korzystanie z sieci. Pierwszy zaś może powodować np. dezorganizację jednej lub wielu list dyskusyjnych. Zdarza się także , że oba sposoby są wykorzystywane wspólnie.
Wśród przypadków zarejestrowanych przez CERT NASK były takie gdzie sprawca dokonywał spammingu w dużej mierze nieświadomie (nie wiedział do końca,że skutek jego działalności może być przykry dla wieluset użytkowników Internetu na całym świecie, którzy mogą dostać wieleniezamówionych przesyłek tej samej treści). Nie zawsze więc incydent mający swoje źródło w Polsce a odbijający się szerokim echem na całym świecie jest intencjonalnie zaplanowany co do skutków przez sprawcę (z resztą nie jest to nic niezwykłego od czasu incydentu Internet Worm z 1988 roku).
Mail bombing natomiast to już z reguły intencjonalne działanie intruza mające na celu utrudnienie pracy lub wręcz zablokowanie innemu użytkownikowi pracy w sieci. Spośród zarejestrowanych przez CERT NASK przypadków szczególnie uciążliwy był ten w czasie którego sprawca mail bombingu zarzucał skrzynki pocztowe pracowników firmy przeciwko której prowadził prywatną wojnę w Internecie dużą ilością przesyłek pokaźnej objętości. „Wojna" ta obfitowała także w przesyłanie i publikowanie przez sprawcę treści nieprzychylnych czy wręcz szkalujących daną firmę.

Proporcje geograficzne i typologiczne

W całym 1996 roku (licząc od marca) zgłoszenia incydentów z Polski stanowiły około 64%, pozostałe 36% to zgłoszenia z zagranicy. Można uznać, że w zgłoszeniach z Polski dominują informacje na temat konkretnych włamań i poczynionych szkód Zgłoszenia z zagranicy natomiast w większości dotyczyły przypadków skanowania sieci, spammingu (zarzucanie odbiorców ogromna ilością przesyłek), nienależytego używania USENET News (tzw. junk mails, wysyłanie zdjęć pornograficznych). Tego typu działania powodują szkody o charakterze szkód moralnych i faktu utrudniania pracy użytkownikom Internetu przez polskich użytkowników sieci. Były jednak również przypadki konkretnych włamań do komputerów za granicą przeprowadzone z Polski.

Na podstawie zgromadzonych danych CERT NASK przeprowadził analizę grupującą atakowane komputery w odpowiednie kategorie ze względu na domenę, w której zostały zarejestrowane. W ten sposób atakowane komputery w domenie .edu.pl a także komputery zarejestrowanie w domenach regionalnych należące do placówek akademickich (np. uczelnie wyższe niezależnie od ich charakteru - także uczelnie niecywilne) zostały ostatecznie zliczone w jednej grupie (umownie nazwaną : edukacja). Komputery z domeny .com.pl. a także należące do firm komercyjnych zarejestrowanych w innych domenach także zgrupowano (grupa: komercyjni). Z grupy tej wyodrębnioną klasę tzw. prowiderów (dostawców usług Internetowych). Trzecią grupę atakowanych komputerów stanowią hosty zarejestrowane w domenie .gov.pl. oraz innych instytucji administracji publicznej, państwowej (grupa: rządowe).

Rozpowszechnianie tego typu oprogramowania poprzez umieszczanie go na serwerach jest czynnością ze wszech miar naganną i nie powinno pozostać bez reakcji - przynajmniej w trybie administracyjnym.

Typologia ataków

- Ataki na systemy komputerowe w Internecie związane z Polską poprzez lokalizację źródła bądź celu mają różną wagę i zasięg. Jeśli weźmiemy pod uwagę tylko zdarzenia poważnie zagrażające lub naruszające bezpieczeństwo to w roku 1996 obok incydentów, w których zaangażowanych było kilka komputerów CERT NASK zanotował i obsłużył np. incydent, w którym próbkowano kilkanaście tysięcy komputerów w Polsce, z czego - zgodnie z posiadanymi informacjami tylko w kilku z nich zostały skutecznie przełamane zabezpieczenia przez intruza.

W owych masowych atakach intruzi posługują się wcześniej wspomnianymi skryptami i programami, które automatycznie wyszukują w sieci swoje potencjalne ofiary a następnie probują wykorzystać określoną słabość danego systemu (np. popularnego acz niebezpiecznego systemu rozproszonego NIS) w celu przechwycenia informacji przydatnych do włamania a następnie wykorzystania jej do samego włamania.

Jeżeli chodzi o typy ataków to najczęściej spotykano w okresie III - IX 96 (pierwszy okres sprawozdawczy CERT NASK) ataki poprzez :

- słabości systemów rozproszonych takich jak NIS,
- słabe hasła
- słabości HTTP (WWW)
- luki w oprogramowaniu (najczęściej sendmail).

W okresie X-XII 96 ataki najczęściej odbywały się poprzez:

- sniffing ,
- słabe hasła, (do tego celu używano często narzędzi skanujących),
- coraz częściej wykorzystywano niski poziom bezpieczeństwa stron World Wide Web.

Tradycyjne systemy haseł, które są pierwszym i często ostatnim elementem zabezpieczenia każdego współczesnego systemu komputerowego wielodostępnego nie stanowia już w tej chwili dostatecznego zabezpieczenia w obliczu rozpowszechnionej przez intruzów techniki sniffingu czyli podsłuchiwania haseł. Odgadnięcie (złamanie) zbyt prostego hasła lub też podsłuchanie statycznego hasła (które jest zbyt żadko zmieniane) jest w dalszym ciągu jedną z podstawowych technik wykorzystywanych przez włamywaczy. Praktycznie atak na hasła jest elementem prawie 100% ataków zarejestrowanych przez CERT NASK. Czasem jest to podstawowy element scenariusza włamania, czasem tylko jeden z kroków nieuprawnionych działań intruza - jednakże prawie zawsze jest to chętnie wykorzystywana słabość systemów.

Rosnąca popularność systemu WWW skutkuje także w pojawiających się coraz częściej atakach na serwery WWW poprzez wykorzystanie rozmaitych luk np. w programach CGI, języku Java i innych. Na serwerze WWW CERT NASK znajdują się kopie CERT /CC advisories oraz linki do zasobów udostępnianych przez inne zespoły.

ZESPOŁY REAGUJĄCE NA ZDARZENIA W SIECI - DOŚWIADCZENIA CERT NASK

Krzysztof Silicki

Naukowa Akademicka Sieć Komputerowa 00-716 Warszawa ul Bartycka 18.
e-mail: krzysiek@nask.pl

W roku 1996 kiedy formalnie zaczął swą działalność zespół CERT NASK zanotowano na całym świecie - Polska nie była tu wyjątkiem dużą liczbę zdarzeń zagrażających i naruszających bezpieczeństwo sieci Internet i jej użytkowników.

Zespół CERT NASK reagujący na zdarzenia naruszające bezpieczeństwo w sieci polskiego Internetu począwszy od marca roku 1996 rejestruje zdarzenia naruszające bezpieczeństwo oraz reaguje m.in. poprzez :

- oferowanie pomocy poszkodowanym,
- alarmowanie i ostrzeganie użytkowników i administratorów sieci wobec występujących zagrożeń i incydentów,
- szerzenie informacji podnoszącej wiedzę z zakresu problematyki bezpieczeństwa i ochrony
- prezentowanie statystyk zanotowanych incydentów.

CERT NASK w okresie marzec -grudzień 1996 zaprezentował dwukrotnie dane statystyczne W tym czasie zespół zanotował kilkadziesiąt poważnych incydentów o charakterze krajowym i międzynarodowym. Wśród tych zdarzeń były próby włamań do komputerów w Polsce z poza kraju, włamania z Polski do komputerów poza Polską, sygnały z innych krajów o próbach włamań z Polski, próby i udane przypadki włamań zgłaszane przez administratorów sieci w kraju.

Ilość i zagrożenie dla Internetu (nie tylko polskiego) jakie wynikają z tych statystyk stanowią poważny sygnał , że bez skoordynowanego działania w celu zapobiegania włamaniom i właściwej reakcji na pojawiające się zdarzenia naruszające bezpieczeństwo polski Internet będzie traktowany jako wygodne miejsce do działań sieciowych włamywaczy. Aby przeciwdziałać takiej sytuacji należy propagować ideę współpracy wszystkich administratorów sieci i osób odpowiedzialnych za ich bezpieczeństwo , zespołów reagujących na zdarzenia (w Polsce takim zespołem jest CERT NASK) a także przedstawicieli prawa - gdyż pewna część incydentów graniczy lub przekracza granicę poza którą sprawcy powinni być ścigani przez wymiar sprawiedliwości. Odrębnym problemem jest właściwe naświetlenie problematyki włamań w Internecie przez media - co w Polsce pozostawia wiele do życzenia.

Statystyka

Na podstawie danych zgromadzonych w czasie obsługi zgłoszonych do CERT NASK incydentów (obsługa polega na pomocy poszkodowanym lub narażonym na zagrożenia) opracowano podsumowanie typologiczne i statystyczne dotyczące charakteru incydentów, stosowanych przez intruzów technik oraz "obszaru rażenia" w podziale na domeny internetowe. Statystyka ta zostanie przedstawiona w dalszej części tekstu.

wiadomość dla B jego kluczem publicznym (i nawet sam nie może jej już odszyfrować!) i wysyła do B, który przy pomocy swojego klucza prywatnego odzyskuje wiadomość.

Możliwe jest również inne zastosowanie kluczy: A szyfruje swoim kluczem prywatnym wiadomość, a następnie wysyła ją do B, który co prawda nie może jej odczytać, ale może na podstawie klucza publicznego A stwierdzić, że to on ją zaszyfrował.

Jest to cenna właściwość w przypadku podpisów cyfrowych: tworzony jest wówczas najpierw skrót wiadomości (np. MD5), następnie szyfrowany jest on kluczem prywatnym nadawcy i dołączany do przesyłanej wiadomości. Odbiorca odszyfrowuje podpis kluczem publicznym nadawcy, a następnie porównuje go ze skrótem otrzymanej wiadomości, który sam zrobił. Jeśli te dwa skróty zgadzają się, odbiorca ma pewność co do dwóch rzeczy:

- wiadomość nie została po drodze przez nikogo zmieniona,
- nadawca jest tym, za kogo się podaje (jego klucz publiczny może zweryfikować urząd certyfikacyjny).

Dodatkowo, nadawca nie może wyprzeć się faktu nadania wiadomości oraz jej treści.

Ze względu na bardzo dużą intensywność obliczeniową operacji szyfrowania i deszyfrowania, algorytmy asymetryczne są bardzo wolne. Dlatego, jak wspomniano wyżej, stosuje się je w połączeniu z algorytmami symetrycznymi.

Najczęściej stosowanym algorytmem jest RSA - np. PGP stosuje klucze o długości 512 (uważany obecnie za niezbyt bezpieczny), oraz 1024 lub 1280 bitów. Wykorzystywany jest w większości omówionych rozwiązań (PEM, SSL, Cisco IOS). Innym konkurencyjnym algorytmem, zaproponowanym przez NIST (National Institute of Standards and Technology) jest DSA, według standardów FIPS zalecany do podpisów cyfrowych.

5. Współdziałanie omówionych technologii.

Poniżej zamieszczono przykład zastosowania przedstawionych technologii. Dzięki nim stworzono sieć korporacyjną charakteryzującą się następującymi cechami:

- bezpieczne połączenie z siecią Internet poprzez firewall,
- centralny serwer uwierzytelniania na potrzeby takich usług, jak telnet i ftp,
- urząd certyfikacyjny dla potrzeb bezpiecznej poczty w sieci korporacyjnej,
- wykorzystanie szyfrujących urządzeń sieciowych do stworzenia VPN po publicznych łączach.

Obydwa rozwiązania pozwalają na selektywne szyfrowanie pakietów na podstawie ich adresów źródła i przeznaczenia. Dzięki temu unika się niepotrzebnego nakładu środków na zabezpieczanie łączności, która bądź to może pozostać w postaci jawnej, bądź też przechodzi wyłącznie po sieciach wewnętrznych organizacji.

4. Przegląd stosowanych algorytmów kryptograficznych.

4.1 Jednokierunkowe funkcje skrótu

Są to funkcje opisujące takie przekształcenia matematyczne wejściowego ciągu bitów, że w ich wyniku powstaje określonej, stałej długości inny ciąg bitów jednoznacznie opisujący ciąg wejściowy, przy czym na podstawie skrótu niemożliwe[1] jest odtworzenie pierwotnej wiadomości. Jeśli istnieją dwie różne wiadomości, które dają taki sam wynik po zastosowaniu funkcji skrótu, mówimy, że nastąpiła kolizja. Oczywiście bezpieczna funkcja skrótu nie powinna mieć kolizji, albo powinna mieć ich bardzo mało.

Tego typu funkcje skrótu służą do otrzymania krótkiego „podsumowania" wiadomości. Funkcje te są tak dobrane, że nawet drobne zmiany w treści wiadomości powodują duże zmiany skrótu, co służy do sprawdzenia niezmienności oryginalnej treści.

Najczęściej stosowanym algorytmem jest MD5. Niedawno stwierdzono w nim istnienie kolizji, nadal jednak jest on bardzo dobrym i szybkim algorytmem, szeroko stosowanym przy np. szyfrowaniu haseł użytkowników, tworzeniu sum kontrolnych plików oraz cyfrowych podpisów wiadomości. Wykorzystywany jest praktycznie w większości z wymienionych rozwiązań, np. w PGP: najpierw tworzony jest skrót podpisywanej wiadomości, a potem szyfruje się skrót przy pomocy klucza RSA, co daje w wyniku stałą długość podpisu.

W standardzie FIPS zalecany jest algorytm SHA (Secure Hash Algorithm), który odznacza się większą długością skrótu niż MD5, co zapewnia większy poziom zabezpieczenia.

4.2 Algorytmy symetryczne (z kluczem tajnym)

Są to klasyczne szyfry, w których najistotniejszym elementem jest wspólny dla nadawcy i odbiorcy klucz. Na podstawie tego klucza wiadomość jest szyfrowana przez nadawcę i odszyfrowywana przez odbiorcę. W przeciwieństwie do jednokierunkowych funkcji skrótu, możliwe (i pożądane) jest odtworzenie oryginalnej wiadomości.

Najczęściej stosowanym algorytmem jest DES (Data Encryption Standard), w różnych odmianach: pojedynczy, potrójny, z różnymi sposobami przetwarzania ciągu bitów wejściowych. Stosowany jest np. w urządzeniach Cisco i KryptoLan, w protokole SSL i standardzie PEM. Innym często stosowanym algorytmem (nie obarczonym restrykcjami eksportowymi USA) jest IDEA - stosuje go np. PGP.

Zaleta algorytmów symetrycznych polega na szybkości - w porównaniu z algorytmami asymetrycznymi są one do 1000 razy szybsze. Poważną wadą natomiast jest konieczność bezpiecznej dystrybucji wspólnego klucza. Dlatego w praktyce stosuje się rozwiązania mieszane: do przekazania wspólnego klucza używa się algorytmu asymetrycznego, żeby w następnej fazie wymiany informacji przejść na szybkie szyfrowanie algorytmem symetrycznym.

[1] „niemożliwe" oznacza w tej części artykułu: „być może możliwe, ale niewykonalne w żadnym rozsądnym czasie przy pomocy wszelkich dostępnych środków"

firewalle pozwalają na uwierzytelnianie przy pomocy haseł jednokrotnych (np. przy użyciu tokenów SecurID).

Inną funkcją, często oferowaną przez firewalle, jest możliwość tzw. translacji adresów (NAT - Network Address Translation). Pozwala to na ukrycie struktury wewnętrznej sieci przed potencjalnymi napastnikami z zewnątrz. Dodatkową zaletą jest możliwość wykorzystania dowolnych adresów IP po stronie wewnętrznej, co znacznie ułatwia administrowanie wieloma połączonymi sieciami lokalnymi. Adresy wewnętrzne są następnie w sposób statyczny lub dynamiczny przekładane na oficjalnie przydzielone organizacji klasy IP.

Jednoczesne zapewnienie łączności oraz rozpoznanie i blokowanie prób nieuprawnionego dostępu do lub z sieci wewnętrznej nie jest łatwym zadaniem. Firewalle wykorzystują w tym celu poniższe techniki:

- *Filtrowanie pakietów (packet filtering firewall):* najprostszy sposób kontrolowania ruchu polegający na niezależnej analizie adresów poszczególnych pakietów. Na podstawie zapisanych reguł firewall odrzuca pojedyncze pakiety, nie wnikając w to, jaki jest ich kontekst. Ten typ firewalla jest bardzo szybki, ale też stanowi niezbyt dobre zabezpieczenie.

- *Proxy (application level firewall):* z zasady nie przepuszcza żadnych pakietów. Wszelkie transmisje muszą najpierw trafić do tzw. proxy (specjalnej aplikacji działającej na firewallu), które zazwyczaj zażąda od użytkownika potwierdzenia swojej tożsamości, i sprawdzi jego uprawnienia do danej operacji. Następnie, jeśli ten etap będzie pozytywny, proxy realizuje połączenia na zewnątrz i od tej chwili przekazuje w sposób przezroczysty dane pomiędzy użytkownikiem a zdalnym serwerem. Różnica w stosunku do poprzedniego typu polega na tym, że określenie pożądanej lub niepożądanej transmisji odbywa się na poziomie wyższych warstw protokołów. Ten typ firewalla jest bardzo bezpieczny, ale znacznie wolniejszy od pierwszego typu. Poza tym, nie wszystkie rodzaje protokołów dadzą się w ten sposób przekazywać (a więc część usług sieciowych jest niedostępna).

- *Analiza stanu połączeń (circuit level firewall):* stanowi kompromis pomiędzy poprzednimi dwoma rozwiązaniami. Firewall bada poszczególne pakiety, ale w szerszym kontekście, pamiętając stan logicznego połączenia, którego częścią są dane pakiety. To rozwiązanie zapewnia dużą przezroczystość dla użytkowników, oraz dobrą wydajność.

Jak już wspomniano, często uważa się firewall za uniwersalny środek na wszystkie bolączki związane z bezpieczeństwem transmisji danych w sieci. Podejście takie powoduje rozluźnienie zasad ochrony cennych danych, i w konsekwencji może doprowadzić do gorszych skutków, niż podłączenie sieci lokalnej bezpośrednio do Internetu.

Należy więc jeszcze raz podkreślić, że firewall powinien realizować określony program bezpieczeństwa organizacji.

- Firewall-1 (CheckPoint)

  Jest to rozbudowany produkt, oferujący m. in. takie możliwości, jak: mocne uwierzytelnianie, elastyczne tworzenie reguł opisujących dostęp poszczególnych użytkowników i maszyn do zasobów wewnętrznych i zewnętrznych, translacja adresów (NAT), opcjonalny moduł pozwalający na stworzenie sieci wirtualnych (VPN). Jest to firewall analizujący stan połączeń (circuit level). Zaletą takiego rozwiązania jest stosunkowo przezroczysty dostęp do sieci. Firewall ten działa jako aplikacja systemu Unix (np. SunOS), jednak moduł realizujący reguły dostępu działa na poziomie jądra

Bezpieczna poczta elektroniczna

Częstym wymaganiem jest zapewnienie bezpieczeństwa przesyłanych informacji w postaci poczty elektronicznej - podstawowej i najczęściej stosowanej usługi wymiany danych w sieciach teleinformatycznych. W niektórych przypadkach jest to nawet główne wymaganie organizacji posługujących się elektroniczną transmisją danych.

Obecnie stosowane są dwa główne rozwiązania, niestety niekompatybilne ze sobą.

- PGP (Pretty Good Privacy), autor: Phillip Zimmermann, USA

  Pakiet ten, ze względu na znakomite wykorzystanie kombinacji kilku silnych algorytmów kryptograficznych (klucze publiczne RSA, symetryczne szyfrowanie DES, IDEA), daje bardzo dobre zabezpieczenie zawartości dowolnych danych. Powszechna dostępność kodu źródłowego (za co zresztą autora spotkały znaczne nieprzyjemności ze strony rządu USA) spowodowała jego rozpowszechnienie. Obecnie najczęściej jest on stosowany w celu tworzenia cyfrowych podpisów, szyfrowania zawartości wiadomości i zabezpieczania ich przed podmianą.

  Dzięki kryptograficznej technice kluczy publicznych dowolna osoba może zabezpieczyć wysyłaną do odbiorcy informację, co znacznie ułatwia nawiązanie bezpiecznej wymiany wiadomości.

  Jedną z nielicznych wad tego konkretnego rozwiązania jest brak urzędu certyfikującego klucze publiczne, a co za tym idzie brak całkowitej pewności, że klucz publiczny należy rzeczywiście do danej osoby. Dlatego próbuje się to rozwiązywać przez wprowadzenie mechanizmu wzajemnego potwierdzania kluczy przez ufające sobie osoby.

  Wada ta jednak jest również zaletą - to dzięki niej PGP stał się de facto Internetowym standardem zabezpieczania poczty elektronicznej.

- PEM (Privacy Enhanced Mail)

  Wykorzystuje podpisy cyfrowe oraz certyfikaty autentyczności przesyłanych wiadomości, ujęte standardem X.509. Zaletą tego rozwiązania jest to, że pozwala na scentralizowane zarządzanie kluczami (certyfikatami) użytkowników. Jednak właśnie ta cecha spowodowała, że standard ten jak na razie nie jest zbytnio rozpowszechniony wśród użytkowników sieci Internet. Znakomicie natomiast nadaje się dla sieci korporacyjnych.

  Istnieje szereg dostępnych implementacji, między innymi PEM HEART, który zawiera również urząd certyfikacyjny (o czym poniżej) i jako taki stanowi kompletne rozwiązanie usługi bezpiecznej poczty elektronicznej w sieci korporacyjnej.

Usługi certyfikacji:

W sytuacji, gdy o tożsamości użytkownika (a co za tym idzie, dostępie do poufnych danych) decyduje jego elektroniczny podpis (lub klucz publiczny), pojawia się konieczność upewnienia, że klucz ten rzeczywiście należy do osoby, za którą użytkownik się podaje. Konieczne jest również zarządzanie kluczami grupy użytkowników tak, aby unieważniać skompromitowane klucze, wydawać nowe, niepowtarzalne, oraz na żądanie móc potwierdzić tożsamość użytkownika. Te same uwagi odnoszą się do serwerów sieciowych, do których użytkownicy wysyłają poufne dane.

Te wszystkie zadania spełniają tzw. urzędy certyfikacyjne. Urząd taki jest stroną, do której inni uczestnicy wymiany danych mają uzasadnione zaufanie, i która rozstrzyga wątpliwości co do

musi coś wiedzieć (PIN - Private Identification Number) i coś mieć (token), żeby móc dokonać autentyzacji w systemie. Całe hasło użytkownika (jednorazowe) składa się z kombinacji PIN-u i aktualnego kodu na tokenie. Procesu uwierzytelniania dokonuje centralny serwer, na którym znajduje się baza użytkowników i ich uprawnienia, dzięki czemu zarządzanie systemem jest proste. Wymiana informacji między stacją klienta a serwerem uwierzytelniania jest zaszyfrowana, co zabezpiecza przed przechwyceniem PIN-u. Raz użyty kod z tokenu nie może zostać powtórnie wykorzystany, co zabezpiecza przed atakami typu „packet replay".

Rozwiązanie to jest przetestowane, wdrożone i oferowane przez NASK.

- Lintel Security

  Rozwiązanie podobne do powyższego. Różnica polega na tym, że zamiast gotowego rozwiązania (które czasem trudno przystosować do istniejącego sprzętu) oferowany jest pakiet narzędzi programistycznych i sprzętowych pozwalający zbudować kompletny system uwierzytelniania i elastycznie dopasować go do własnych potrzeb (włącznie ze zmianą sposobu działania tokenów).

- Kerberos (Massachusets Institute of Technology, USA)

  System programowy wykorzystujący tzw. zaufaną trzecią stronę, którą jest centralny serwer uwierzytelniania. Autentyzacja dokonuje się w oparciu o standardowe, wielokrotnego użycia hasło znane użytkownikowi w postaci jawnej, a serwerowi w postaci jednokierunkowego skrótu. W przypadku zgodności haseł, oraz ustawionych odpowiednich uprawnień dla danego użytkownika, centralny serwer uwierzytelniania wydaje tzw. ticket (bilet) - najpierw TGT (ticket granting ticket), który potwierdza tożsamość użytkownika, a następnie na tej podstawie użytkownik zwraca się do konkretnego serwera o bilet pozwalający mu na korzystanie z określonych zasobów. Bilet posiada okres ważności, po którym konieczna jest powtórna autentyzacja użytkownika wobec systemu. Znaczniki czasowe dodatkowo utrudniają atak metodą „packet replay". Protokół Kerberos zapewnia również szyfrowanie transmisji na poziomie aplikacji.

  Wadą tego systemu jest konieczność dostosowywania strony klienckiej oprogramowania, co może się wiązać ze sporymi nakładami organizacyjnymi i finansowymi. Dodatkowo, istniejące produkty pochodzą zazwyczaj z USA, i są obwarowane restrykcjami eksportowymi (ITAR). Temu też należy przypisać małe rozpowszechnienie tego systemu w Europie (w przeciwieństwie do USA).

- TACACS i Radius - systemy zdalnej autentyzacji użytkowników terminali.

  Obydwa rozwiązania zapewniają scentralizowane zarządzanie różnymi metodami autentyzacji (m. in. normalne hasła, SecurID). Szczególnie cenne jest to w przypadku dostępu do urządzeń sieciowych (takich jak serwery, serwery komunikacyjne), ale również istnieje oprogramowanie klienckie pozwalające na zastosowanie tych systemów na innych maszynach.

  Zaletą tych systemów jest szyfrowanie dialogu uwierzytelniającego, natomiast brak jest zintegrowanych usług pozwalających na zabezpieczenie całej sesji użytkownika.

Poufność i niezaprzeczalność

Poufność oznacza, że dane przesyłane sieciami teleinformatycznymi zabezpieczone będą przed niepowołanym dostępem. Osiąga się to poprzez szyfrowanie danych, przy czym

- ogranizacja podłącza swoją sieć lokalną do Internetu przez firewall. Jest on bardzo dobrze zabezpieczony i gwarantuje odporność na wszelkie ataki, więc administratorzy poszczególnych maszyn mogą odetchnąć. Po kilku miesiącach jednak okazuje się, że nastąpiło włamanie poprzez modem, który jeden z użytkowników podłączył do swojej maszyny w sieci lokalnej.

Powyższe sytuacje, niestety, nie są tylko czarnym scenariuszem - wiele organizacji padło ich ofiarą. Najczęstszym jednak przypadkiem jest brak jakichkolwiek mechanizmów podwyższających bezpieczeństwo w warstwie technicznej, jak i organizacyjnej.

Z przytoczonych przykładów wynika jednak bardzo ważna zasada: **bezpieczeństwo sieci teleinformatycznych jest zagadnieniem systemowym, i wymaga od organizacji opracowania dokładnego i spójnego programu bezpieczeństwa**. Dzięki niemu unika się zagrożeń związanych z nieświadomością użytkowników, lub po prostu brakiem dyscypliny. Ważne jest, aby program ten był spójny, co wymaga umiejętnego przewidzenia potencjalnych zagrożeń związanych z różnymi sposobami wymiany danych, oraz skutków przechwycenia określonych informacji przez nieuprawnione osoby.

Jasno sformułowane zasady bezpieczeństwa pozwalają krytycznie ocenić istniejące rozwiązania dotyczące przechowywania i przekazywania istotnych danych, oraz właściwie podejść do projektowania przyszłych rozwiązań. Pozwalają one również na wyciąganie konsekwencji służbowych (lub nawet prawnych) w stosunku do tych pracowników, którzy ich nie przestrzegają.

Następna zasada, która wynika z przytoczonych przykładów, brzmi: **poszczególne elementy programu bezpieczeństwa muszą współpracować ze sobą**. Jakość zabezpieczeń danych jest taka, jak jakość najsłabszego ogniwa w programie bezpieczeństwa. Innymi słowy, jeśli szyfrujemy transmisje na wszystkich łączach, to powinniśmy również dopilnować, żeby pracownicy nie zapisywali sobie haseł na luźnych karteczkach.

Jeszcze raz wypada podkreślić, że konieczność opracowania kompleksowych zasad bezpieczeństwa jest często bagatelizowana, a konkretne rozwiązania techniczne traktuje się jako panaceum na wszelkie problemy związane z bezpieczną wymianą danych. Niestety, tak nie jest. Nawet najbardziej wyrafinowane technologie nie są w stanie zapewnić bezpieczeństwa, jeśli odpowiednie zasady nie zostaną jasno sformułowane i wprowadzone w życie.

3. Przegląd stosowanych technologii.

Obecnie stosowane technologie podwyższające bezpieczeństwo przesyłania danych można podzielić ze względu na funkcje, jakie spełniają, na następujące grupy:

Usługi sieciowe:

- uwierzytelnianie (autentyzacja) użytkownika: zapewnienie, że użytkownik jest tym, za kogo się podaje,
- autoryzacja użytkownika: przydzielenie określonych praw dostępu do informacji,
- niezmienność nadanej informacji: zapewnienie, że informacji nie będzie można zmienić bez wykrycia tego faktu,
- poufność przesłanej informacji: zapewnienie, że informacje będą dostępne tylko i wyłącznie dla określonych osób na określonych zasadach,
- niezaprzeczalność przesłania informacji: zapewnienie, że użytkownik nie będzie się mógł wyprzeć faktu nadania lub odebrania informacji,

informację i następnie wydzielić z niej tę poszukiwaną. Ponieważ informacja ma szybko malejącą w czasie wartość odpowiednie narzędzia są rzadkie i bardzo drogie.

- Największym zagrożeniem bezpieczeństwa jest zawsze człowiek, w tym pracownicy operatora sieci. W obsłudze tradycyjnych systemów udział ludzi jest duży, personel liczny. Przy obecnym rozchwianiu postaw osobowych, różnorodności opcji politycznych, bardzo mało prawdopodobne jest zapewnienie kadry, której można zaufać. Czyli ograniczanie ilości ludzi mających dostęp do systemu telekomunikacyjnego jest pierwszym wymogiem bezpieczeństwa, a to nowoczesne systemy zapewniają niejako z zasady.

- Wiedza na temat działania nowoczesnych systemów jest ograniczona, jej zdobycie nie łatwe, a elastyczność konfigurowania instalacji na tyle duża, że bez znajomości aktualnie pracującej struktury logicznej sieci dostęp do interesujących kanałów przesyłania nie łatwy. Do tego konfiguracja ta zmieniana z centrum zarządzania może być odpowiednio często modyfikowana. Wiedza na temat aktualnego logicznego układu sieci znana tylko nielicznemu gronu z pośród operatorów centrum zarządzania siecią.

- Wreszcie wszystko co wyżej napisano opiera się na doświadczeniach NASK, czyli jest wdrożone. Napewno nie w pełnej skali potrzeb, ale w stopniu zapewniającym nieporównywalne bezpieczeństwo sieci w porównaniu z bezpieczeństwem systemów tradycyjnych.

Warszawa maj 1997 r.

f) Odcięcie sieci od sieci światowej poprzez węzeł ochrony zabezpiecza przed lokalnymi przeciążeniami i gubieniem informacji - co jest typowym zjawiskiem na przykład w sieci pracującej według Internet Protocol.

3.6 Wadliwe interwencje legalnego i nielegalnego operatora

Przeciwdziałanie zakłóceniom wynikającym z błędnych interwencji operatorów musi być rozwiązane środkami odmiennymi od poprzednich. W referacie proponujemy:
a) Dobór rozwiązań minimalizujących konieczność interwencji operatorów oraz ograniczenie możliwości dokonywania interwencji szybkich, bezpośrednich prowadzących do przypadkowych błędów.
b) Wyraźny podział uprawnień operatorów tak, aby coraz poważniejsze interwencje były dostępne dla coraz węższego grona operatorów sieci.
c) Opracowanie scenariuszy postępowania w sytuacjach wymagających interwencji operatorów oraz stałe szkolenie i weryfikacja kwalifikacji.
d) System zatwierdzania zasadniczych scenariuszy działania operatorów, ciągła dokumentacja (log) dokonywanych interwencji oraz skutków tych interwencji, a także ciągła inwentaryzacja stanu sieci.
e) Maskowanie przed operatorem elementów działania sieci, w zakresie do jakiego nie ma uprawnień, w tym całego przebiegu informacji użytkownika.
f) Opracowanie i stopniowe wprowadzanie do działania systemów samouczących się, ostrzegających i utrudniających błędne operacje operatorskie.

4. Ochrona informacji użytkownika

Ochronę informacji użytkownika w sieci należy zapewnić w dwóch aspektach: ochrona informacji przed utratą w sieci oraz przed niewłaściwym jej wykorzystaniem.

Operator sieci telekomunikacyjnej chroni informacje jako powierzone mu mienie użytkownika. Ochrona ta jest bezwarunkowa. Operator nie zajmuje się jednak i nie powinien zajmować się kwalifikowaniem stopnia ochrony (tajnością itp.) informacji, jej wartościowaniem, metodami kryptografii, autentyzacji itp. Tego rodzaju działania należą całkowicie do użytkowników końcowych.

W sieci powinno się stosować kilka metod ochrony informacji.
a) Przesyłanie informacji powinno odbywać się wyłącznie pomiędzy portami określonymi przez użytkownika, informacja nie jest dostępna na żadnym innym porcie użytkowników.
b) System przesyłania informacji w sieci powinien być całkowicie oddzielony od systemów abonenckich i ich w żadnym zakresie nie wykorzystywać.
c) technologia przesyłania powinna zapewniać bardzo wysokie prawdopodobieństwo przesłania komunikatu oraz powiadamiać o niemożności, w wyniku wystąpienia niepokonywalnych trudności, przesłania komunikatu
d) Nie może być w sieci żadnego miejsca gromadzenia informacji użytkownika w sposób nieulotny. To znaczy w całym systemie przesyłania informacji nie może być miejsc, w których jest ona gromadzona w sposób trwały (na przykład do dalszego przesłania), umożliwiający jej późniejsze odczytanie.
e) Monitorowanie przesyłania musi być ograniczone co do zakresu jak i uprawnień operatorskich, a operatorzy monitorujący przesyłanie informacji muszą być osobiście odpowiedzialni za zachowanie w tajemnicy ewentualnie odczytanych jej fragmentów, oczywiście o ile użytkownik końcowy zaniedbał jej zamaskowania.

- fizyczne zakłócenie połączenia przez przerwanie kabla, zanik kanału cyfrowego i tym podobne czynniki uniemożliwiające transfer informacji,
- błędną pracę systemu transmisyjnego w warunkach wyjątkowych, nieprzewidzianych przez konstruktora systemu (w zakresie sprzętu, oprogramowania i konfiguracji systemu),
- przeciążenia sieci,
- wadliwego działania legalnego lub nielegalnego operatora oraz celowego zakłócania pracy sieci.

3.1 Uszkodzenia linii przesyłających

W referacie zaznaczono następujące środki przeciwdziałania tego rodzaju sytuacjom.
a) Wszystkie kierunki przesyłania powinny mieć alternatywne drogi przesyłania:
- pomiędzy węzłami sieci szkieletowej powinny istnieć co najmniej dwie dodatkowe drogi przesyłania, w sieci regionalnej conajmniej jedna, wykorzystywane automatycznie przez system komutacji lub system zarządzania,
- w każdej linii przesyłania powinien istnieć co najmniej zdublowany kanał przesyłania,
- urządzenia zestawiające połączenia powinny być zlokalizowane możliwie bezpośrednio w miejscu fizycznego zbiegania się linii fizycznych wykorzystywanych bezpośrednio lub niosących kanały cyfrowe.
b) Warunkiem wykorzystania w pracy sieci okablowania bezpośrednio lub jako podkładu zestawianych dla potrzeb sieci kanałów cyfrowych musi być jednoznaczna odpowiedzialność organizacji, będącej dysponentem tych kabli, za ich utrzymanie oraz reagowanie na zgłaszane przypadki zaniku możliwości transmisji. Powinny być opracowane i uregulowane umownie procedury zapewniające właściwe czasy reakcji oraz tryby zgłaszania awarii oraz podawania tymczasowych rozwiązań zastępczych.

3.2 Uszkodzenia wyposażenia sieciowego

W referacie zaznaczono następujące środki przeciwdziałania uszkodzeniom wyposażenia sieciowego:
a) Całe wyposażenie sieciowe powinno być zlokalizowane w odpowiednio wyposażonych pomieszczeniach zapewniających normatywne warunki pracy urządzeń sieci, zasilanie energetyczne przez urządzenia podtrzymujące zasilanie oraz zapewniające jego właściwą jakość, zasilanie urządzeń podtrzymujących bezpośrednio z miejsc głównego zasilania, wyposażonych możliwie w samoczynne włączanie zasilania rezerwowego.
b) W sieci powinny być instalowane wyłącznie urządzenia odpowiedniej klasy, bezobsługowe, zapewniające odpowiednio długie okresy pracy bez zawieszenia i bez uszkodzenia. W miejscach mających zasadnicze znaczenie dla pracy sieci urządzenia te powinny być dublowane oraz odpowiednio często wymieniane.
c) Instalowane w węzłowych punktach sieci urządzenia muszą mieć co najmniej zdublowany własny system zasilania oraz podstawowej logiki. Elementy przyłączeniowe muszą być instalowane w odpowiednim nadmiarze zapewniającym możliwość przełączenia bez konieczności napraw na miejscu.
d) Wszystkie urządzenia muszą mieć zdalny system dostępu umożliwiający dokonywanie interwencji operatorskich z centrum zarządzania siecią.
e) Centrum zarządzania siecią powinno być wyposażone w system monitorowania zakłóceń w sieci bez konieczności interwencji ze strony użytkownika sieci.
f) Wszyscy dostawcy sprzętu muszą zawrzeć umowę wieloletnią gwarantującą pracę sieci, dostarczanie koniecznych uaktualnień oprogramowania i sprzętu, naprawy uszkodzonych elementów oraz ciągłą linię wspomagania tzw. "hot line".

tej, jak i w wielu innych niemożliwe jest opracowanie uniwersalnych recept.
Aby zbudować bezpieczny system teleinformacyjny konieczne jest przede wszystkim metodyczne i konsekwentne inżynierskie działanie pamiętając o „prakseologicznej triadzie" - **chcieć, umieć, móc.**

Literatura

[1] Bogusław Kusina, Mirosław Machalski - Metodologia budowy dużych systemów telekomunikacyjnych - opracowanie własne na podstawie materiałów udostępnionych przez firmy TADIRAN oraz ALCATEL DEFENCE SYSTEMS;
[2] Bogusław Kusina - wybrane materiały z „Procedur Bezpieczeństwa Teleinformacyjnego" - opracowanie własne, Warszawa 1997;
[3] Marek Lipniowiecki - „Wybrane zagadnienia z zakresu administrowania bezpieczeństwem sieci teleinformatycznych" Warszawa 1996;
[4] Mirosław Suchenek - „Zakres Ochrony Informacji" Warszawa 1996;
[5] Przepisy Bezpieczeństwa UZE RS 100 - wydanie styczeń 1996;
[6] Władysław Aloksa - „Elektromagnetyczne aspekty walki informacyjnej" oraz „Wybrane problemy polityki ochrony informacji na przykładzie przepisów bezpieczeństwa Unii Zachodnioeuropejskiej" - materiały KNSŁ-96 Zegrze;
[7] wybrane przepisy prawa wraz z aktami wykonawczymi.

elementów wraz z konsekwentnie realizowaną polityką bezpieczeństwa teleinformacyjnego może dać pożądany efekt w postaci wymaganego poziomu bezpieczeństwa informacji.

W procesie kreowania polityki bezpieczeństwa teleinformacyjnego organizacji proponujemy zwrócenie szczególnej uwagi na:

a) aspekty prawne
- ustalenie z jakimi kategoriami informacji mamy do czynienia;
- ustalenie obowiązujących przepisów prawnych w zakresie ochrony informacji z jakimi mamy do czynienia;
- ustalenie odpowiedzialności prawnej, dyscyplinarnej i ekonomicznej za ewentualne ujawnienie informacji chronionych;
- ustalenie obowiązujących procedur organizacyjno-technicznych (homologacja, normalizacja, standaryzacja, certyfikacja, ocena, dopuszczenia, projektowanie, budownictwo);

b) świadomość zagrożeń i wyobraźnię
- zestawienie i analizę potencjalnych zagrożeń[9] (celowych i przypadkowych);
- analizę perspektyw i tendencji rozwojowych w kontekście charakteru i ilości przetwarzanych informacji, rozbudowy systemów teleinformacyjnych oraz wyobrażalnych (i niewyobrażalnych) zagrożeń;
- analizę własnych (kierowanej organizacji) możliwości opracowania i wdrożenia skutecznej polityki bezpieczeństwa teleinformacyjnego;
- poszukiwanie skutecznego wsparcia (jeśli negatywny wynik analizy z poprzedniego punktu);
- uświadomienie sobie i podwładnym skutków ekonomicznych, prawnych i dyscyplinarnych ewentualnego „omijania" procedur bezpieczeństwa zarówno na poziomie „taktycznym" jak i „strategicznym;
- uświadomienie sobie najsłabszych elementów systemu - skupienie uwagi właśnie na tych elementach;
- pamiętanie o fakcie, że każdy człowiek (nie tylko Polak !) stosuje się do wszelkich utrudnień (jakie wnoszą niewątpliwie systemy zabezpieczeń) tylko wtedy, kiedy musi;
- uświadomienie sobie faktu, że techniczne systemy zabezpieczeń „starzeją się" znacznie szybciej, niż techniki i technologie informatyczne;

c) zarządzanie ryzykiem
- analizę ryzyka w przypadku nie podjęcia koniecznych środków bezpieczeństwa;
- ustalenie dopuszczalnych odstępstw od przyjętych procedur;
- procedury postępowania w przypadku prawdopodobieństwa lub pewności utraty lub nieuprawnionej zmiany lub wprowadzenia informacji;
- procedury postępowania w przypadku prawdopodobieństwa lub pewności ujawnienia systemów zabezpieczeń;

d) aspekty ekonomiczne
- analizę możliwości ekonomicznych własnej organizacji - bezpieczeństwo jest bardzo kosztowne;

[9] jedno z istotniejszych zagrożeń - to zagrożenie budżetowe. dotyczy ono nie tylko instytucji finansowanych z budżetu Państwa - w każdej organizacji pojawiają się „grupy nacisku" wymuszające często irracjonalny z punktu widzenia bezpieczeństwa podział budżetu.

Przybliżenie wybranych pojęć i procedur z zakresu profesjonalnie organizowanego bezpieczeństwa teleinformacyjnego powinno - w zamiarze autora - ułatwić kreowanie skutecznej polityki w tej coraz to istotniejszej dziedzinie działalności każdej organizacji.

Spotykane definicje „Polityki Bezpieczeństwa Teleinformacyjnego" opisują ją następująco:

- jest to zestaw praw, reguł i zasad tworzenia, dystrybucji, użytkowania i przechowywania niejawnych informacji (definicja z dokumentów normatywnych Departamentu Obrony USA przekazana na konferencji AFCEA Rome Symposium and Exposition '94)
- to przeciwdziałanie zagrożeniom przypadkowej lub celowej utraty poufności, integralności lub dostępu do informacji (przepisy bezpieczeństwa UZE - RS100, dokument wydany w styczniu 1996 r.).

Głównym celem „Polityki Bezpieczeństwa Teleinformacyjnego" jest osiągnięcie wymaganego poziomu bezpieczeństwa informacji, poprzez:

- zabezpieczenie przetwarzanych, przesyłanych lub przechowywanych w urządzeniach lub systemach informacji przed ich nielegalnym ujawnieniem, modyfikacją lub zniszczeniem;
- ochrona przed przypadkową lub celową utrata poufności, integralności, dostępności lub wiarygodności informacji[7]

Bezpieczeństwo teleinformacyjne (INFOSEC - INFOrmation SECurity) definiowane jest jako zastosowanie zabezpieczeń systemu lub sieci EPD, w celu ochrony przed - lub zapobieżeniu nieupoważnionej eksploatacji, modyfikacji (włącznie ze zniszczeniem) lub odmowie dostępu, które mogą być dokonane przez stanowiące zagrożenia dla informacji: przechwycenie emisji ujawniającej, nieuprawniony dostęp elektroniczny lub zastosowanie innych środków rozpoznania technicznego[8]. Zastrzega się przy tym, że *środki takie dotyczą bezpieczeństwa informacji „w ogóle" i bezpieczeństwa łączności a także obejmują bezpieczeństwo procedur, składników fizycznych, personelu i dokumentów.*

Głównymi składowymi bezpieczeństwa teleinformacyjnego są:

- bezpieczeństwo łączności (COMSEC - COMmunication SECurity) oraz
- bezpieczeństwo komputerowe (COMPUSEC - COMPUter SECurity).

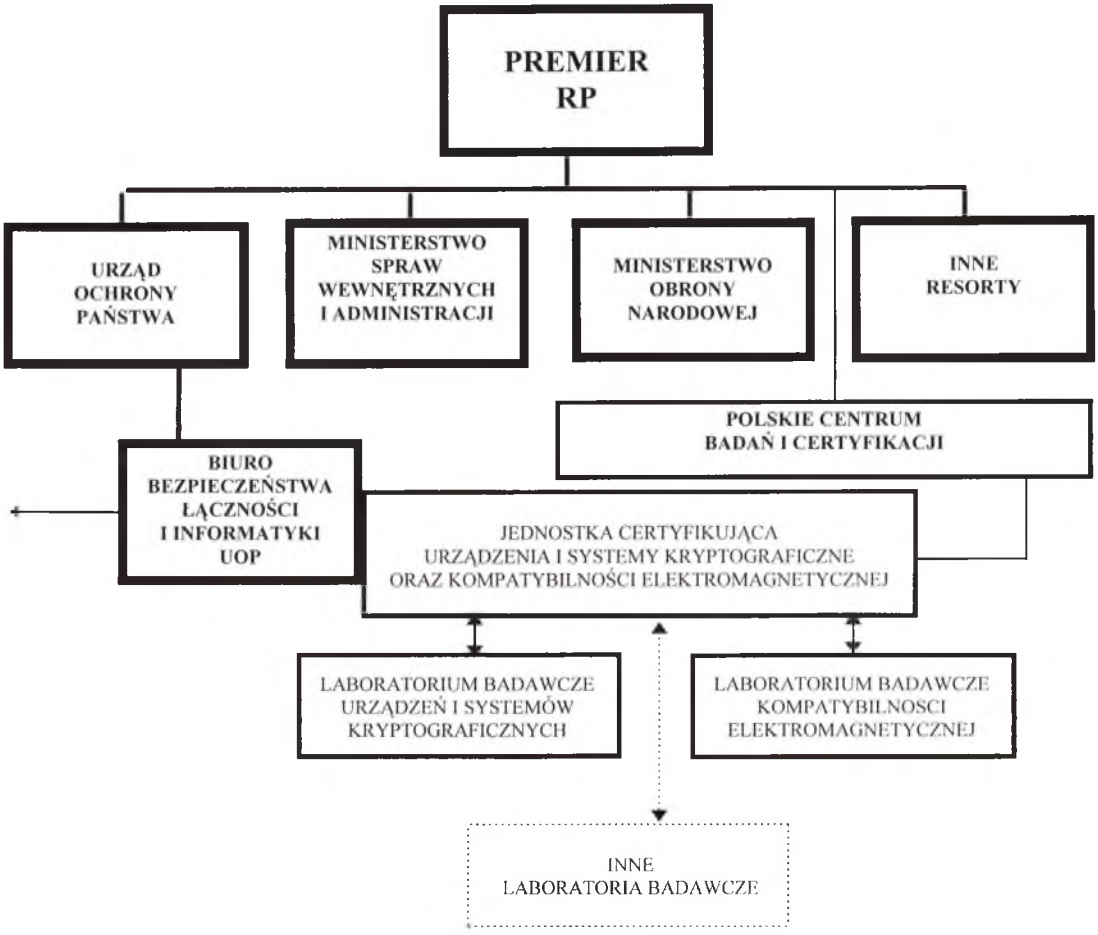
UZE definiuje bezpieczeństwo łączności jako zastosowanie w telekomunikacji środków bezpieczeństwa, w celu uniemożliwienia uzyskania przez nieupoważnione osoby użytecznych informacji poprzez wejście w posiadanie i zapoznawanie się z przekazywanymi wiadomościami, albo dla zapewnienia autentyczności takich wiadomości. Środki takie dotyczą bezpieczeństwa kodowania, transmitowania i emitowania, a także obejmują bezpieczeństwo procedur, składników fizycznych, personelu i dokumentów oraz zabezpieczenia komputerowe.

Natomiast bezpieczeństwo komputerowe zdefiniowano jako zastosowanie zabezpieczeń sprzętu, oprogramowania firmowego i oprogramowania użytkowego w systemie komputerowym, w celu

[7] Omawianiu podlega **tylko i wyłącznie** ta część bezpieczeństwa informacji, która ma ścisły i bezpośredni związek z elektronicznym przetwarzaniem danych (EPD) przechowywaniem i przesyłaniem informacji w postaci dźwięku (w tym głównie mowy), znaków pisma i obrazów (w tym grafiki, fotografii, sygnałów TV).

[8] § 85, część X przepisów bezpieczeństwa UZE

Biuro Bezpieczeństwa Łączności i Informatyki Urzędu Ochrony Państwa (BBŁII UOP) jest organem właściwym w dziedzinie bezpieczeństwa specjalnych systemów teleinformacyjnych Rzeczypospolitej w których przetwarzane, przechowywane i przesyłane są wiadomości klasyfikowane (stanowiące tajemnicę państwową i służbową).



Niezależnie od podstawowej działalności BBŁII UOP prowadzi:

- certyfikację urządzeń i systemów kryptograficznych dla ochrony informacji klasyfikowanych i nieklasyfikowanych;
- certyfikację urządzeń i systemów w zakresie kompatybilności elektromagnetycznej;
- konsultacje i doradztwo w zakresie ochrony informacji nieklasyfikowanych.

- Art. 22. 3. Minister Finansów może, w drodze zarządzenia, ze względu na ochronę tajemnicy państwowej, uregulować odrębnie tryb nadawania numerów identyfikacji podatkowej oraz warunki posługiwania się tymi numerami

- projekt ustawy o ochronie danych osobowych z dnia 1996-10-08 (rządowy i zbliżony do niego - poselski)

projekt rządowy	*projekt poselski*
- Art. 1. 2. Ustawę stosuje się do danych osobowych przechowywanych w systemach informatycznych, a także w formie kartotek, skorowidzów, ksiąg, wykazów i w innych podobnych zbiorach ewidencyjnych.	*- Art. 4. Ustawa określa zasady pozyskiwania, przetwarzania, udostępniania lub przekazywania danych osobowych w systemach informatycznych, a także w formie kartotek, skorowidzów, ksiąg, wykazów i innych zapisów imiennych.*
- Art. 29. Administrator zbioru jest obowiązany do podjęcia środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a przede wszystkim powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zaborem, uszkodzeniem lub zniszczeniem	*- Art. 1. Treść danych osobowych podlega szczególnej ochronie prawnej. Organy państwowe oraz osoby fizyczne i prawne administrujące danymi kierują się w ramach swojej ustawowej działalności zasadami:* - ... *- zabezpieczenia posiadanych danych przed zniszczeniem, sfałszowaniem lub dostępem podmiotów nieupoważnionych*
- Art. 30. Administrator zbioru prowadzonego w systemie informatycznym przed przystąpieniem do przetwarzania danych jest obowiązany uzyskać opinię podmiotu upoważnionego do dokonywania badań i wydawania opinii w sprawach doboru środków technicznych i organizacyjnych do przetwarzania danych osobowych ...	*- Art. 32. Prezes Rady Ministrów określi w drodze rozporządzenia niezbędne warunki techniczne i organizacyjne zabezpieczenia danych osobowych w zbiorach danych przetwarzanych automatycznie ...*

3. Rozwiązania instytucjonalne

Obowiązujące rozwiązania prawne w dziedzinie ochrony tajemnicy państwowej i służbowej w Rzeczypospolitej wskazują instytucje odpowiedzialne za jej ochronę i przeciwdziałanie ujawnianiu.

Rzeczpospolitą przepisy Unii Zachodnio-Europejskiej (UZE) oraz obowiązujące w Pakcie Północnoatlantyckim (NATO).
Kierunki te można zgrupować następująco:

- rozszerzenie grup klasyfikacyjnych

Dotychczas obowiązujące w RP	**Obowiązujące w UZE i NATO**	**Przewidywane do wprowadzenia w RP**
TAJNE SPECJALNEGO ZNACZENIA [Wymaga Szczególnej Ochrony]	FOCAL TOP SECRET	ŚCIŚLE TAJNE
TAJNE	SECRET	TAJNE
POUFNE	CONFIDENTIAL	POUFNE
-	RESTRICTED	ZASTRZEŻONE
JAWNE	UNCLASSIFIED[2]	NIEKLASYFIKOWANE

- dodatkowe klauzule.

Rozpatrywane jest - wzorem UZE i NATO - wprowadzenie dodatkowych oznakowań, wskazujących potrzebę ograniczenia dostępu i specjalnego postępowania niezależnie od klauzuli tajności (CRYPTO, STRICTLY LIMITED). Rozważana jest także możliwość i potrzeba wprowadzenia określania czasu ważności klauzuli tajności (chodzi tu głównie o informacje, których wartość po upływie krótkiego czasu jest niewielka - mogą po tym czasie mieć obniżona klauzulę).

- agregowanie danych.

Przyjmuje się, że dokument wynikowy otrzymuje z zasady najwyższą klauzulę, jaką posiada którakolwiek z informacji składowych. Zaleca się jednak analizowanie, czy połączenie poszczególnych elementów nie wymaga zastosowania wyższej klauzuli tajności.

- ustawowe powołanie organu odpowiedzialnego za organizację i kontrolę bezpieczeństwa teleinformacyjnego państwa.

Niezależnie od istniejących już struktur władz do spraw bezpieczeństwa

[2] należy podkreślić standardową w państwach UZE i NATO zasadę, według której **duży „pakiet" informacji nieklasyfikowanych jest klasyfikowany co najmniej jako RESTRICTED (zastrzeżone).**

Ustawa ta określa również (bezpośrednio lub w formie delegacji ustawowych):

- procedury ochrony tajemnicy państwowej i służbowej;
- tryb klasyfikowania wiadomości (Poufne, Tajne, Tajne Specjalnego Znaczenia);
- tryb uprawniania osób do zapoznania się z wiadomościami stanowiącymi tajemnicę państwową i służbowa;
- odpowiedzialność kierowników jednostek organizacyjnych za wdrażanie i stosowanie procedur ochrony tajemnicy;
- odpowiedzialność osób za naruszenie tajemnicy państwowej i służbowej;
- procedury nadzoru nad bezpieczeństwem tajemnicy państwowej i służbowej.

Syntetyzując powyższe przepisy prawa, można sprowadzić je do podstawowych zasad bezpieczeństwa informacyjnego:

- obowiązek przestrzegania tajemnicy państwowej i służbowej spoczywa na każdym, kto wszedł w jej posiadanie (bez względu na sposób jej uzyskania);
- podstawą formalną podejmowania działań ochronnych wobec wiadomości jest jej zaklasyfikowanie do kategorii niejawnej;
- podstawowe rodzaje wiadomości stanowiących tajemnicę państwowa i służbową klasyfikowane są „z urzędu" przez naczelne i centralne organy administracji państwowej w formie wykazów;
- za faktyczna klasyfikację wiadomości (nadanie jej odpowiedniej klauzuli tajności) odpowiada jej wytwórca;
- uprawnienia do zapoznania się z wiadomościami stanowiącymi tajemnicę państwową i służbową nadawane są w trybie administracyjnym i mają swój zakres - „... wyłącznie te ..., które wchodzą w zakres wykonywanych przez pracowników obowiązków";
- wiadomość stanowiąca tajemnicę państwową lub służbowa może mieć zróżnicowaną formę (mowa, pismo, obraz, rysunek, znak, dźwięk, być zawarta w urządzeniu, przyrządzie lub innym przedmiocie - art. 4 ustawy);
- ujawnienie tajemnicy państwowej i służbowej stanowi przestępstwo i zagrożone jest odpowiedzialnością karną (rozdział XXXIV Kodeksu Karnego art. 260 ÷ 264);
- wiadomości stanowiące tajemnicę państwową i służbową przesyłane mogą być wyłącznie środkami zapewniającymi ich ochronę.

Regulacje ustawy o ochronie tajemnicy państwowej i służbowej - mimo jej kilkunastoletniego już okresu obowiązywania - odnoszą się również do bezpieczeństwa informacji klasyfikowanych w systemach teleinformacyjnych. Często jednak pojawiają się wątpliwości interpretacyjne, czy zapis „przesyłanie" obejmuje wszystkie elementy łańcucha teleinformacyjnego. Wątpliwości te - moim zdaniem - mają charakter spekulacyjny (co Ustawodawca miał na myśli ?) i mogą pojawiać się wyłącznie w środowiskach nie związanych z Elektronicznym Przetwarzaniem Danych (EPD), gdyż każda operacja na danych powoduje ich przesyłanie.

2. 2. Akty prawne wykonawcze.

Istnieje szereg aktów prawnych - wydanych na podstawie ustawy o ochronie tajemnicy państwowej i służbowej (i innych ustaw) - regulujących różne aspekty bezpieczeństwa informacyjnego i teleinformacyjnego. Najistotniejsze z nich - dla problematyki bezpieczeństwa teleinformacyjnego - to:

• *NASK przystępuje do realizacji pierwszych usług teleinformatycznych w sieci telewizji kablowej.*

Rozwój polskiego Internetu, rozumianego jako zespół usług, nadal jest związany z wieloma dylematami, wśród których na pierwsze miejsce wysuwają się problemy organizacyjne i ekonomiczne oraz bezpieczeństwa. Tak było i w zeszłym roku, a ponieważ problemy te są i będą występowały zawsze, być może stopniowo polskie sieci telekomunikacyjne osiągają stan normalności?

Zgodnie z ugruntowaną tradycją „Miedzeszyn" jest okazją do szerokiej wymiany poglądów i doświadczeń we wszystkich kwestiach nurtujących środowiska operatorów i usługodawców w Polsce. Tym razem będzie mniej niż zwykle nowinek technicznych, być może dlatego, że coraz bardziej konkurencyjny rynek i nie najlepsze doświadczenia z przeszłości nie skłaniają do ujawniania tajemnic firmowych.