Naukowa i Akademicka Sieć Komputerowa - NASK

IX Konferencja NASK na temat sieci komputerowych

Miedzeszyn-99

Bezpieczne sieci telekomunikacyjne - nowe doświadczenia

Materiały Konferencji

Warszawa-Miedzeszyn 19-21 maja 1999 r.

Naukowa i Akademicka Sieć Komputerowa – NASK

IX Konferencja na temat sieci komputerowych

MIEDZESZYN-99

BEZPIECZNE SIECI TELEKOMUNIKACYJNE NOWE DOŚWIADCZENIA

Materiały konferencji

Warszawa-Miedzeszyn, 19-21 maja 1999 r.

Spis treści

Wstęp

Przygotowując kolejną, dziewiątą już edycję konferencji NASK na temat sieci komputerowych, uświadomiliśmy sobie, że jest to najstarsza w Polsce konferencja sieciowa, organizowana nieprzerwanie od 1991 roku. Od samego początku seminaria w Miedzeszynie służyły omówieniu aktualnych zagadnień wiążących się z wprowadzaniem na rynek nowych technologii i standardów w zakresie budowy i utrzymania sieci teleinformatycznych. Podobnie było z zagadnieniami natury formalno-prawnej czy organizacyjnej, bezpośrednio związanymi z tworzeniem systemów transmisji danych za pośrednictwem sieci komputerowych. I w tej dziedzinie Miedzeszyn stanowi od lat forum wymiany informacji i stwarza dogodne warunki dla przedyskutowania wielu palących kwestii związanych z intensywnym rozwojem Internetu i usług sieciowych w Polsce.

W programie tegorocznej imprezy staraliśmy się umieścić tematy istotne i ważne dla wszystkich zainteresowanych stron - zarówno dla osób odpowiedzialnych za rozwój sektora usług teleinformatycznych, jak i dla firm korzystających z tych usług. Tytuł konferencji: „Bezpieczne sieci telekomunikacyjne - nowe doświadczenia" wskazuje na kierunek, w jakim ewoluuje rozwój sieci, które służą przede wszystkim firmom i instytucjom o wysokich wymaganiach w dziedzinie bezpiecznej transmisji danych.

Podobnie jak w latach ubiegłych, zależało nam na wszechstronności tematyki naszej konferencji z wyraźnym jednak położeniem nacisku na bezpieczeństwo stanowiące obecnie najpoważniejszy problem dla wszystkich użytkowników korzystających z łączności sieciowej. Prezentacjom z tej właśnie dziedziny towarzyszy pakiet tematów związanych z kompleksową ochroną informacji w przedsiębiorstwie i omówieniem ustaw o ochronie informacji i ich konsekwencjach w praktyce operatorów i użytkowników sieci telekomunikacyjnych.

Z pewnością na uwagę zasługują też prezentacje odnośnie nowych usług i generalnie - rodzącej się „nowej generacji Internetu", a także prezentacje firmowe NASK i wszystkich zaproszonych do udziału w konferencji firm od lat współpracujących z NASK.

W tegorocznej edycji konferencji „Miedzeszyn" pragniemy zaznaczyć szczególnie takie tematy jak:

- *kompleks zagadnień związanych z bezpieczeństwem w sieciach komputerowych, ochroną informacji niejawnych, przeciwdziałaniem przestępczym zdarzeniom w sieci*
- *omówienie problemów organizacyjno-technicznych i prawnych związanych z budową sieci dla potrzeb państwa*
- *prezentacje systemów telekomunikacyjnych o podwyższonym bezpieczeństwie*
- *rozwój nowej generacji Internetu i zaawansowanych usług NASK*
- *budowa sieci korporacyjnych – rozwój łączności międzynarodowej*
- *„Voice over IP"*
- *Internet z gwarancją usług*
- *handel elektroniczny oraz perspektywy rozwoju usług finansowych w Internecie*

Rada Programowa składa gorące podziękowania wszystkim referentom i sponsorom za wkład w organizację kolejnej edycji konferencji NASK z cyklu „Miedzeszyn".

MEGATRENDY CYWILIZACJI INFORMACYJNEJ[1]

prof. dr hab. inż. Andrzej P. Wierzbicki

Instytut Łączności, Szachowa 1, 04-894 Warszawa

Poprzez *megatrendy* rozumiemy tu ważne tendencje rozwojowe, utrzymujące się przez dłuższy okres czasu. Poprzez *cywilizację informacyjną* rozumiemy tu okres rozwoju *społeczeństwa informacyjnego* lub - co niemal równoważne - społeczeństwa opartego na *gospodarce wiedzą.*

Istnieją przy tym przesłanki, by twierdzić, że okres cywilizacji informacyjnej będzie rozciągał się na wiele dziesiątków lat, być może - cały wiek XXI. Megatrendy, omawiane niżej, też mogą rozciągać się na dziesiątki lat. Dzieje się tak dlatego, że wiele zdobyczy współczesnej nauki i techniki nie jest wdrażane tak szybko, jak by to wynikało z możliwości nauki czy przyczyn czysto technicznych - a opóźnienia w ich wdrażaniu wynikają z różnych przyczyn społecznych i ekonomicznych. Przykładem takiego zjawiska jest rozwój telewizji cyfrowej, której podstawy teoretyczne powstały już niemal 40 lat temu - a masowe wdrożenie jeszcze jest przed nami. Gdyby decydowały tu względy czysto techniczne, okres rozpowszechniania telewizji cyfrowej mógłby być skrócony do około 20 lat; decydowały tu więc względy ekonomiczne i społeczne. Przykładów takich można przytoczyć wiele. Wszystkie one powodują, że możemy dziś przewidywać dość dokładnie, jakie to megatrendy określą przyszły rozwój cywilizacji informacyjnej; niepewność dotyczy natomiast skali, tempa pełnej realizacji i szczegółów technicznych różnorodnych trendów, których początki można obserwować już dzisiaj.

Wybór trendów, które uznamy za najbardziej istotne, zależy od ocen ich znaczenia ekonomicznego i społecznego, a w stosunku do trendów technicznych – ocen możliwości realizacji technicznej i uwarunkowań techniczno-ekonomicznych, wreszcie od oszacowania przewidywanego popytu rynkowego, gdyż to właśnie gotowość zakupu odpowiednich produktów czy usług przez rozmaitych konsumentów będzie decydowała o tym, które z obserwowanych dziś czy przewidywanych tendencji zamienią się w trwałe trendy.

Zacząć trzeba jednak od pewnych tendencji zasadniczych, obserwowanych już dzisiaj, które utrwalą się wraz z rozwojem społeczeństwa informacyjnego. Za decydujące o rozwoju cywilizacji informacyjnej można uznać dwa lub trzy megatrendy zasadnicze - z którymi wiąże się wiele trendów pochodnych bądź szczegółowych.

Megatrend zmiany zawodów

Pierwszy z tych megatrendów to ***społeczny megatrend kształtowania nowych zawodów,*** oznaczający w skrócie, że rozwój cywilizacji informacyjnej polega na zastępowaniu starych zawodów, wymagających dużego udziału pracy fizycznej i źle wyposażonych w narzędzia technik informacyjnych, zawodami nowymi, wymagającymi dużego udziału informacji i wiedzy oraz wykorzystującymi coraz w większym stopniu narzędzia technik informacyjnych. Można przy tym sformułować następujące tezy, wyjaśniające powolność

[1] Artykuł ten stanowi rozwinięcie tez referatu tegoż autora *Research for Information Society - Social Impacts and Technical Convergence* na konferencji międzynarodowej *Research for Information Society,* Warszawa-Miedzeszyn, październik 1998 r.

międzynarodowej tak, aby zapewnić własną ekspertyzę w tej szczególnie zaawansowanej i wymagającej dużych nakładów dziedzinie.

c) Obserwuje się już obecnie na świecie, w szczególności w krajach Unii Europejskiej, rozwój prac nad *usługami telematycznymi* - w różnorodnych dziedzinach zastosowań. Wśród wielu rodzajów takich usług, wymienimy tu tylko cztery związane z nimi - i wynikające także z zasadniczego megatrendu integracji technicznej - tendencje bardziej szczegółowe, ale mające też charakter megatrendów:

c1) Można przewidywać wzrost intensywności prac badawczych i zastosowań *telematyki operacyjnej* - przy czym słowo *operacyjny* rozumiane jest tu szeroko, obejmuje zarówno dosłowny sens medyczny (czyli operacje medyczne wykonywane zdalnie przez wysokiej klasy specjalistę), jak i sens laboratoryjny (czyli operacje nad eksperymentami laboratoryjnymi wykonywanymi zdalnie w najdroższych i najlepiej wyposażonych laboratoriach świata), jak wreszcie sens przemysłowy czy badań geologicznych (czyli operacje wykonywane przez zdalnie sterowane roboty).

c2). Obserwuje się już w Europie, w kilkudziesięciu miastach, początkowe prace nad upowszechnieniem *telematyki miejskiej* - znanej też pod hasłowymi nazwami *telepolis* lub *digital city,* oznaczającymi szerokie zastosowanie technik sieci komputerowej w celu usprawnienia miejskich systemów informacji, służb miejskich, systemów transportu oraz parkowania samochodów, a nawet wprowadzenia elementów demokracji elektronicznej (dyskusji aktualnych problemów miasta z użyciem sieci komputerowych). Są to wprawdzie prace jeszcze początkowe, ale wyznaczają one istotny trend: należy się spodziewać usprawnienia technicznego i upowszechnienia rozmaitych zastosowań telematyki miejskiej - i to w stosunkowo krótkim okresie najbliższego dziesięciolecia.

c3) Obserwuje się dziś na świecie zalążki prac nad *telematyką domową,* znaną też pod hasłowymi nazwami *inteligentnego domu* czy *mieszkania,* lub też *digital home,* oznaczającymi integrację różnorodnych domowych urządzeń elektrycznych i elektronicznych w jedną sieć, obejmującą nie tylko telefon, telewizję, magnetowid, komputer, lecz także nadzór nad ogrzewaniem, gotowaniem, zmywaniem, praniem, a także systemy zabezpieczenia domu czy mieszkania. Ten megatrend doczeka się powszechnej realizacji zapewne później, niż inne megatrendy opisane wyżej (może potrzeba jeszcze dwóch czy nawet kilku dziesięcioleci) ale jest dość nieuchronny - naturalne dążenie ludzkie do wygody zapewni duży popyt rynkowy na urządzenia i systemy inteligentnego mieszkania, skoro tylko rozwój techniczny doprowadzi do rozwiązań ekonomicznie akceptowalnych i szeroko dostępnych rynkowo.

c4) Wraz z rozwojem cywilizacji informacyjnej zmieniać się będzie nie tylko charakter sieci i usług telekomunikacyjnych, lecz także sieci i usług pocztowych. Na przykład, rozwój poczty elektronicznej w sieciach komputerowych może zmniejszyć intensywność stosowania listów, a zwłaszcza telegramów; natomiast rozwój handlu elektronicznego zwiększy zapotrzebowanie na przesyłki innego charakteru. Jednocześnie, zastosowanie technik informacyjnych do usprawnienia usług pocztowych będzie się wyrażać we wzroście znaczenia *telematyki pocztowej,* opierającej się na wykorzystaniu technik sieci komputerowych i komputerowego wspomagania decyzji dla usprawnienia działalności sieci pocztowej. Ten megatrend już jest obserwowany na świecie, ale doczeka się pełnej realizacji zapewne później, niż trend *telepolis,* ze względu na trudności szybkich zmian w dużych i tradycyjnych organizacjach pocztowych; dla przyspieszenia takich zmian, niezbędne jest zwiększenie intensywności kształcenia ustawicznego pracowników poczty. Natomiast znaczniejsze zmiany technologii dostarczania przesyłek (jak np. upowszechnienie poczty pneumatycznej) są jeszcze odległe o kilka dziesięcioleci, z uwagi na duże koszty niezbędnych inwestycji infrastrukturalnych.

retoryczne pytanie: *jeśli najwięksi gracze na rynku mogą dużo zyskać na niestabilności rynku, to rynek ten będzie stabilny czy niestabilny?* Pytanie to jest retoryczne, gdyż udzieliła już na nie odpowiedzi praktyka: światowy rynek spekulacji finansowych staje się coraz bardziej niestabilny, mówi się dziś poważnie o konieczności międzynarodowej regulacji tego rynku.

Nie przytaczam powyższego przykładu po to, aby uzasadniać powrót do interwencjonizmu państwowego w starym stylu - jest to raczej przykład zawodności powszechnie przyjętych sądów, słusznych przy tradycyjnych założeniach, które jednak nie muszą być spełnione wobec zupełnie nowych zjawisk, związanych z nową technologią informacyjną; jest to przykład megatrendu wyzwań intelektualnych, konieczności ciągłej rewizji utartych poglądów.

Konkurencja rynkowa jest niezbędna dla rozwoju społeczeństwa informacyjnego, nie da się tego społeczeństwa rozwijać w warunkach totalitaryzmu czy nadmiernego interwencjonizmu państwowego.[3] Ale trwałości mechanizmów rynkowych nie można uznawać za dogmat, trzeba tych mechanizmów bronić przed niebezpieczeństwami, które mogą wyniknąć ze spontanicznego rozwoju właśnie technologii informacyjnych. Jednym z takich niebezpieczeństw jest właśnie możliwość monopolizacji czy nawet destabilizacji rynków w wyniku zastosowań nowych technologii. Innym, chyba jeszcze poważniejszym, jest nadmierne bezrobocie związane ze zbyt liberalnym traktowaniem skutków pierwszego megatrendu zmiany zawodów - i to nie tylko z powodu możliwych konfliktów społecznych, które mogą sprzyjać rozwiązaniom populistyczno-totalitarnym, lecz także z powodu ograniczenia siły nabywczej znacznej części ludności, co może zagrozić nowoczesnej gospodarce rynkowej, opierającej się na masowym popycie - zagrozić deflacją i krachem giełdowym.

Przykłady powyższe tylko w niewielkim stopniu ilustrują megatrend wyzwań intelektualnych. Specjaliści mogą sami dodać tu wiele przykładów: zagrożeń dla demokracji, gdyby system totalitarny wykorzystał nowoczesne techniki informacyjne, czy zagrożeń praw osobistych człowieka, związanych np. z niedostateczną ochroną prywatności i bezpieczeństwa sieci komputerowych.

Zakończenie

Na tych rozmaitych, omawianych wyżej przykładach widzimy, że niektóre z dyskutowanych tu megatrendów będą realizowane szybciej, inne wolniej, niektóre bardziej powszechnie, inne mniej. Ale przykłady powyższe potwierdzają tezę wstępną, że już dziś możemy przewidywać z dużym stopniem pewności, jakie to megatrendy będą dominujące w rozwoju społeczeństwa czy cywilizacji informacyjnej, niepewne są tylko zakres i szybkość ich wdrażania oraz oczywiście szczegóły techniczne. Odnośnie megatrendów szczegółowych podaliśmy tu tylko przykłady, gdyż można wyciągnąć więcej wniosków z megatrendów zasadniczych i podać więcej przykładów szczegółowych. Natomiast megatrendy zasadnicze są dziś dość jasne: decydować o przyszłości będą *społeczny megatrend kształtowania nowych zawodów, techniczny megatrend zbieżności (convergence) czyli integracji,* wreszcie chyba najbardziej z nich niebezpieczny *megatrend wyzwań intelektualnych* - bowiem jeśli nie sprostamy tym wyzwaniom, jeśli będziemy uporczywie trzymać się utartego sposobu widzenia świata, to nie zapobiegniemy niebezpieczeństwom, wynikającym z rozwoju nowych technologii.

[3] Można uważać, że nadejście epoki cywilizacji informacyjnej było jednym z ważnych powodów upadku komunizmu. Inaczej mówiąc, ZSRR miał doskonałych informatyków, niezbędnych dla programów kosmicznych czy militarnych, o wspaniałych osiągnięciach naukowych czy pomysłach wynalazczych. Ale pomysły te nie przekładały się na intensywny rozwój technologii komputerowych i informacyjnych, bo brak było mechanizmu rynkowego, napędzającego taki rozwój. Obserwując rosnący dystans cywilizacyjny w stosunku do społeczeństw rynkowych, w dużym stopniu związany właśnie z rynkowym wykorzystaniem technik informacyjnych, ludzie w społeczeństwach "realnego socjalizmu" wyciągnęli odpowiednie wnioski.

❖ TR ISO/IEC 13335 Guidelines for the Management of IT Security

❖ Polska Norma PN-I-13335 Technika Informatyczna -Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych.

- ☞ Polityka bezpieczeństwa instytucji
- ☞ Polityka bezpieczeństwa systemów TI instytucji
- ☞ Polityka bezpieczeństwa systemu TI (konkretnego)
- ☞ Plan zabezpieczenia systemu TI

❖ Polityka bezpieczeństwa NATO

- ☞ NATO Security Policy - C-M(55)15(Final)
- ☞ Załączniki, wytyczne, poradniki, standardy, kryteria oceny, listy zalecanych produktów itd. *(unclassified, restricted, comfidential, secret, top secret)*
- ☞ Szczególne wymagania bezpieczeństwa
  - System-Specific Security Requirement Statement
  - System-specific Electronic Information Security Req.Stat.
  - System Interconnection Security Requirement Statement
  - Community Security Requirement Statement

❖ Zabezpieczenia (*administracyjne, fizyczne i techniczne środki i metody .....*)

❖ Wybór zabezpieczeń po przeprowadzeniu analizy ryzyka:

- ☞ oszacowaniu posiadanych aktywów (*zawierających informacje niejawne - dokumenty elektronicznie, bazy danych, podzespoły urządzeń, moduły programów, hasła, klucze kryptograficzne, dokumentacja)*
- ☞ identyfikacji możliwych zagrożeń
- ☞ oszacowaniu podatności już posiadanych zabezpieczeń na ataki
- ☞ dostosowanie zabezpieczeń do klauzuli chronionych informacji niejawnych *(np. konieczność stosowania ochrony elektromagnetycznej)*
- ☞ dostosowanie zabezpieczeń do ilości chronionych informacji niejawnych (agregacja) (*np.duża ilość informacji „zastrzeżonych" może być „poufna")*
- ☞ wybór środków zabezpieczeń na miarę możliwości finansowych (organizacyjne - techniczne)

Przepisy regulujące zasady ochrony systemów i sieci teleinformatycznych

❖ Ustawa z dn. 22.01.99 o ochronie informacji niejawnych Dz.U. 11 poz. 95 rozdział 10

❖ Rozporządzenie Prezesa RM z dn. 25.02.99 w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci TI

Ustawa o ochronie informacji niejawnych - rozdział 10 - zawartość

Art. 60 - Szczególna ochrona systemów TI w których jest wytwarzana, przechowywana, przetwarzana i przekazywana tajemnica państwowa

-- ust 2. Certyfikacja urządzeń i narzędzi kryptograficznych

Art. 61- Opracowanie szczególnych wymagań bezpieczeństwa systemu lub sieci

Art. 62 - Certyfikacja systemów (służby ochrony państwa)

Art. 63 - Nadzór nad systemami TI

Ustawa o ochronie informacji niejawnych - rozdział 10 – omówienie

- Systemy TI w których znajdują się IN nie można eksploatować bez zezwolenia (akredytacji) SOP
- Na każdym etapie życia systemu TI kierownik JO sporządza SWBS i przedstawia je SOP - art. 60, ust 3. oraz art. 61, ust 1.

- ochrona kryptograficzna (szyfrowanie i inne mechanizmy zapewniające poufność, integralność uwierzytelnienie) - §8 ust.1
- bezpieczeństwo transmisji (kontrola dostępu lub szyfrowanie przy podłączeniu do powszechnie dostępnej sieci) §11
- kontrola dostępu (uprawnienia, hasła i mechanizmy) §12

- Podstawowe wymagania:
  - przetwarzanie IN od „poufnych" w górę - tylko w strefach bezpieczeństwa - §6
  - przekazywanie tajemnicy państwowej w formie elektronicznej poza strefy bezpieczeństwa - wymaga ochrony kryptograficznej - §8 ust. 2
  - przemieszczanie urządzeń i nośników zawierających IN od „poufnych" w górę - pod warunkiem stosowania kryptograficznych lub innych środków ochrony - §8
  - algorytmy i środki ochrony algorytmów, kluczy, haseł musza być odpowiednie do klauzuli chronionych IN - §10 ust.1
  - podłączenie do powszechnie dostępnej sieci - dla tajemnicy państwowej możliwe w przypadku zastosowania ochrony kryptograficznej - (§ 11, ust.1), dla tajemnicy służbowej - właściwych mechanizmów kontroli dostępu (§ 11, ust. 2)
  - kierownik JO określa warunki przydzielania uprawnień (§ 12, ust. 1)
  - administrator systemu przydziela konta i hasła oraz zapewnia wykorzystanie mechanizmów kontroli dostępu (§ 12, ust. 2)
  - Jedna osoba nie może posiadać niekontrolowany dostęp do wszystkich zasobów systemu przetwarzającego tajemnice państwową (§ 13)
- *§14 do §19 - Wytyczne w zakresie sporządzania SWBS*
- SWBS należy opracowywać
  - po przeprowadzeniu analizy zagrożeń z uwzględnieniem warunków eksploatacji p (§ 14, ust.1)
  - na etapie projektowania, wdrażania, eksploatacji i modernizacji systemu (§ 14, ust. 2)
- Zawartość SWBS
  - charakterystyka systemu lub sieci TI
  - dane o budowie systemu lub sieci TI
  - środki ochrony zapewniające bezpieczeństwo IN
  - zadania administratora systemu i inspektora bezp.TI
- charakterystyka systemu TI - §17
  - klauzula tajności IN w systemie
  - uprawnienia użytkowników
- dane o budowie systemu TI - §18
  - lokalizacja
  - wykorzystywane urządzenia i oprogramowanie
  - połączenia wewnętrzne i zewnętrzne
  - konfiguracja
  - środowisko eksploatacji
- opis środków ochrony powinien uwzględniać (§19)
  - osoby odpowiedzialne za bezpieczeństwo systemu TI
  - procedury bezpiecznej eksploatacji
  - wymagania w zakresie szkoleń użytkowników i obsługi
- Kto jest odpowiedzialny za certyfikację urządzeń i oprogramowania kryptograficznego
  - Ustawa mówi o obowiązku używania tylko certyfikowanych urządzeń i narzędzi krypto do ochrony tajem. pań. -art. 60

KOMPLEKSOWA OCHRONA INFORMACJI W PRZEDSIĘBIORSTWIE. UTWORZENIE W POLSCE TRZECIEJ ZAUFANEJ STRONY TRANSAKCJI ELEKTRONICZNYCH

Jerzy Goraziński

Polska Wytwórnia Papierów Wartościowych S.A.

Wciąż rosnąca popularność Internetu, a tym samym zakresu wiedzy przeciętnego użytkownika o możliwości korzystania z domowego komputera jako terminala do realizowania transakcji elektronicznych i multimedialnego urządzenia, za pomocą którego może kontaktować się z innymi użytkownikami, stawia coraz wyższe wymagania w zakresie zapewnienia bezpieczeństwa transakcji i zachowania poufności kontaktów w sieciach teleinformatycznych.

Potrzeby „przeciętnego użytkownika" nie byłyby może tak istotne, gdyby nie fakt, że stał się on niezmiernie ważny jako końcowy klient dla instytucji, urzędów i banków. Rosnące wymagania klientów, którzy domagają się wprowadzenia łatwych i bezpiecznych form korzystania z sieci, stawiają wspomniane instytucje w coraz trudniejszej sytuacji. Wzrastających oczekiwań nie da się już zaspokoić zwiększając ilość personelu lub rozszerzając sieć placówek – konieczne są zmiany jakościowe i technologiczne, a nie jest to zadanie proste!

Technologia dzisiejszych sieci teleinformatycznych była pomyślana nie tyle jako rozwiązanie bezpiecznego przesyłania danych, co ich niezawodnego dostarczania. Na szczęście, od czasu powstania pierwszych sieci i protokołów, wiele się zmieniło. Użycie i rozwój kryptografii, wraz z ideą podpisu elektronicznego, stworzyły ważne narzędzia w toczącej się walce o utrzymanie prywatności i podniesienie bezpieczeństwa przekazywania informacji w sieciach.

Rozwiązania kryptograficzne, stosowane w obrocie kluczem publicznym, są doskonałym narzędziem służącym do zabezpieczania wszelkiego rodzaju danych i transakcji prowadzonych poprzez sieci teleinformatyczne. Stają się one szczególnie użyteczne w odniesieniu do systemów związanych z handlem elektronicznym. Dotychczas funkcjonujące w tym sektorze rozwiązania oceniane są jako wciąż niedoskonałe. Jednak wiele uczestniczących w transakcjach instytucji handlowych i finansowych coraz częściej łączy kilka dostępnych komercyjnie elementów ochrony, co czyni transakcje równie, a może nawet bardziej bezpiecznymi od realizowanych osobiście.

W Polsce, w dalszym ciągu zabezpieczenie dostępu do informacji ma charakter działań doraźnych, najczęściej pomyślanych jako źródło dodatkowego dochodu dla firm-pomysłodawców lub potrzeba samouspokojenia „szefów" zabezpieczanych instytucji. Nie jest to stała, systematycznie prowadzona i jednoznacznie prawnie i finansowo umocowana działalność, jaką powinien być program bezpieczeństwa informacyjnego w skali państwa i przedsiębiorstwa. Program taki mógłby zbierać i definiować zasady, elementy prawne, finansowe oraz metody i sposoby oceny ryzyka, a tym samym wartości informacji zawartych w systemach informacyjnych całego kraju. Należy pamiętać, że systemy te już funkcjonują w Polsce w formie rozproszonych ogniw, jakim są zasoby informacyjne działające w podmiotach wielkich i małych, państwowych i prywatnych. Systemy informacyjne już teraz zbierają, przetwarzają, a często przesyłają i magazynują informacje niezbędne do prawidłowego funkcjonowania i kierowania państwem. Jednak podstawowym problemem jest brak jasnych reguł ich działania, na przykład przesyłania i wymiany informacji, co powoduje, że te same dane, czasem w różnych wersjach są wielokrotnie magazynowane.

Na szczęście uwarunkowania zewnętrzne związane z przyjęciem Polski do NATO "wymusiły" uchwalenie 22 stycznia 1999r. ustawy o ochronie informacji niejawnych. Dotyczy ona jedynie wycinka wymiany informacji ale zawarte w niej regulacje i przepisy wykonawcze do ustawy umożliwiają jej odniesienie do wszystkich prac i działań związanych z ochroną i przesyłaniem informacji w sieciach.

również instytucjom o których mowa w ustawie, mieć przekonanie, że wymieniamy dokładnie te informacje, które chcemy wymieniać i tylko z tymi, z którymi chcieliśmy je wymienić.

Jest naturalne, że najwięcej uwagi i środków kierujemy na ochronę informacji przed zagrożeniami z zewnątrz. Przypomnijmy sobie jednak statystyki: ponad 85% naruszeń bezpieczeństwa systemów (szczególnie informatycznych) następuje od wewnątrz organizacji, a „nośnikiem" znacznej części „przecieków" są ludzie. Tu powołam się, na raport dotyczący bezpieczeństwa informacji, opracowany przez specjalistów pracujących na potrzeby Departamentu Obrony USA. Twierdzą oni, że aby dotrzeć do informacji z zewnątrz danej organizacji - szczególnie dużej i silnie zhierarchizowanej - najłatwiej manipulować ludźmi, a nie przełamywać jej zewnętrzne systemy zabezpieczeń.

Drugim podstawowym źródłem klasyfikowanych danych, są informacje oficjalnie ujawniane wskutek braku koordynacji wewnątrz samej instytucji lub dosłownie wyrzucane przez jej pracowników na śmietnik. Trzeba o tym pamiętać budując wszelkie programy bezpieczeństwa. Tak dochodzimy do kolejnego istotnego pytania – jak i jakie „programy bezpieczeństwa" budować? W tym zakresie, podobnie jak w tworzeniu norm prawnych, następują w Polsce wyraźne zmiany na lepsze. Zostały opracowane, lub są w przygotowaniu, polskie normy, które zapewne nie zakończą dyskusji: co, jak i czy tak właśnie należy chronić, ale przynajmniej wprowadzą początki „kodeksu drogowego" naszej polskiej infostrady.

Przepisy prawa, normy, polityki bezpieczeństwa - to tylko część zagadnień związanych z kompleksową ochrona systemów informacyjnych przedsiębiorstwa. Prawdziwe kłopoty zaczynają się, gdy te, zgodne z teorią i prawem założenia, zaczynamy wprowadzać w życie i musimy przygotować transmisję różnorodnie klasyfikowanych pod względem bezpieczeństwa danych, w bardzo zróżnicowanym środowisku sieci rozległych .

Kłopoty zaczynają się już na poziomie wyboru koncepcji. Pierwszym elementem, wymagającym decyzji ze strony każdej instytucji pragnącej uczestniczyć w bezpiecznym obrocie elektronicznym, jest określenie sposobu weryfikacji klienta, niezależnie czy jest to przysłowiowy „Kowalski", czy duża instytucja lub bank. W sieci klient musi być weryfikowany elektronicznie, a określenie sposobu takiej weryfikacji to kolejny poważny problem. Klient poza dynamicznie zmieniającym się w czasie hasłem, powinien posiadać podpis elektroniczny, a więc również certyfikat stwierdzający ważność jego kluczy szyfrujących. Musi być też Trzecia Zaufana Strona weryfikująca całość transakcji, określająca jej czas i niezaprzeczalność. Jednak najważniejsze jest wybranie zasad weryfikowania certyfikatu użytkownika. Do wyboru mamy dwie metody: można użyć danych, które krążą w sieci (jest to tzw. WEB certyfikat) albo stworzyć warunki do osobistego zgłoszenia się klienta dla dokonania weryfikacji (co wymaga utworzenia bazy i struktury certyfikatów). Pierwsza metoda jest powszechnie stosowana w transakcjach detalicznych o stosunkowo niskim poziomie ryzyka finansowego. Druga, uznawana za jednoznacznie identyfikującą klienta, znalazła zastosowanie w elektronicznych operacjach finansowych pomiędzy klientami instytucjonalnymi. Wymaga ona jednak istnienia hierarchicznej struktury certyfikacji i instytucji pełniącej rolę Trzeciej Zaufanej Strony w transakcjach elektronicznych. Tak zweryfikowane certyfikaty mogą być stosowane zarówno do przekazywania danych finansowych pomiędzy instytucjami, jak również potwierdzania transakcji dla dokumentów klasyfikowanych.

Kolejnym problemem do rozwiązania jest wybór produktu odpowiadającego potrzebom organizacji pragnącej obsługiwać klientów. Na rynku dostępna jest duża ilość produktów nazywanych przez producentów „serwerami certyfikatów" lub „kompleksowymi rozwiązaniami obrotu kluczem publicznym (PKI)". Są to jednak programy o niesłychanie zróżnicowanym poziomie wykonania i cen, realizujące bardzo różne funkcje. Duża różnorodność i brak ścisłych kryteriów wyboru są głównymi powodami trudności w określeniu odpowiedniego, realizującego założone cele, programu. Niezbyt pomocne są też standardy czy normy prawne, bo jedne i drugie są dopiero w trakcie tworzenia. Podobnie z rozwiązaniami już funkcjonującymi - nie tylko są strzeżone, ale też ściśle dopasowane do cudzych potrzeb i trudne do adaptacji.

PRZESTĘPCZE ZDARZENIA W SIECI

Krzysztof Jan Jakubski

Biuro Koordynacji Służby Kryminalnej
Komendy Głównej Policji

Obecny, lawinowy wręcz, wzrost możliwości w dziedzinie telekomunikacji sprawia, że do wspólnej sieci dołączane są nowe zbiory użytkowników, którzy nie są ściśle znani właścicielowi systemu i niekoniecznie są biorącymi udział w realizacji tych samych celów. Sieć komputerowa, jak i techniki łączności ułatwiają niewątpliwie wymianę informacji, lecz nie rozwiązują problemu kontrolowanego podziału informacji pomiędzy użytkownikami. Co więcej stają się miejscem działań, które zarówno z uwagi na swoje następstwa jak i charakter są działaniami niepożądanymi. Zagrożeniami systemów komputerowych są możliwości:

- ujawnienia przetwarzanej w systemie informacji,
- modyfikacji lub zniszczenie tej informacji,
- wymuszenia przerwy w pracy systemu,
- wykorzystaniu elementów systemu komputerowego do dokonania czynów zabronionych.

Dopóki działania te nie są zabronione przez prawo, nie można traktować ich jako przestępstwo. Jednakże prawo – choć ze swej natury konserwatywne – zaczyna coraz bardziej angażować się w problematykę nowych mediów. Obowiązujący od 1 września 1998 roku nowy kodeks karny zabrania dokonywania zamachów na bezpieczeństwo elektronicznie przetwarzanej informacji. Chronione są podstawowe atrybuty bezpieczeństwa systemów komputerowych: dostępność, poufność i integralność. Omówmy więc zapisy kodeksu karnego.

A. Przestępstwa przeciwko ochronie informacji

W rozdziale XXXIII k.k. znalazły się w normy umożliwiające pociągnięcie do odpowiedzialności karnej sprawców najbardziej klasycznych zamachów na bezpieczeństwo danych i systemów komputerowych, takich jak: *hacking* (art. 267 § 1), podsłuch komputerowy (art.267 § 2), naruszanie integralności komputerowego zapisu informacji (art. 268 § 2) oraz sabotaż komputerowy (art. 269 § 1 i 2).

Karalność nieuprawnionego wejścia do systemu komputerowego (hackingu)

> art. 267 § 1 k.k.
>
> Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie,
>
> podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Przepis ten jest w istocie zmienioną i uwspółcześnioną, na skutek użycia nowych określeń technicznych, wersją art. 172 k.k. z 1969 r., chroniącego tajemnicę korespondencji.

Przestępstwo może być popełnione w następujący sposób:

a/ otwarcie cudzego pisma, tj. naruszenie tajemnicy korespondencji,

b/ podłączenie się do przewodu służącego przekazywaniu informacji, np. do linii telefonicznej lub sieci

Indywidualnym przedmiotem ochrony przestępstwa z art. 267 § 2 k.k. jest **poufność** informacji. Omawiany przepis sankcjonuje wszelkie działania zmierzające do naruszenia prawa do wyłącznego dysponowania określonym rodzajem informacji. W odróżnieniu od przepisu § 1 art. 267 k.k., mamy tu do czynienia z przyjęciem bardziej zobiektywizowanego kryterium karalności, jakim jest zakładanie urządzeń technicznych lub posługiwanie się nimi w celu uzyskania zastrzeżonych rodzajów informacji. Karalne jest nie tylko zakładanie lub posługiwanie się w tym celu wspomnianymi urządzeniami, lecz także uzyskiwanie przy ich pomocy informacji przez osoby do tego nieuprawnione.

Poufność rozmów i innych form interpersonalnego porozumiewania się jest tylko jednym z elementów przedmiotu ochrony przestępstwa z art. 267 § 2 k.k. Przepis ten może być też podstawą sankcjonowania rozmaitych form ingerencji w życie prywatne i swobodne korzystanie z mieszkania, np. przez inwigilację przebywających w nim osób przy użyciu urządzeń optycznych, akustycznych, nokto - i termowizyjnych lub elektronicznych. Inwigilacja może polegać na przechwytywaniu informacji przesyłanych przy pomocy urządzeń telekomunikacyjnych albo na podsłuchu lub podglądzie elektronicznym bezpośrednim (ang. *bugging*), prowadzonym przy użyciu mikrofonów, kamer lub nadajników radiowych umieszczonych zarówno wewnątrz lokalu, jak i przy wykorzystaniu urządzeń znajdujących poza lokalem (np. mikrofonów kierunkowych, skanerów do przeszukiwania częstotliwości fal radiowych, satelitów)[5].

Istnieje duże ryzyko naruszenia poufności informacji przetwarzanej elektronicznie i przesyłanej sieciami komputerowymi. Wiąże się ono z możliwością podsłuchu transmisji teleinformatycznych wieloma metodami. Niestety koszty ujawniania takich zdarzeń są bardzo wysokie i na dzień dzisiejszy praktycznie nie ujawniane.

Karalność niszczenia danych lub programów komputerowych oraz sabotażu komputerowego

art.268

§ 1.

Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2.

Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca

podlega karze pozbawienia wolności do lat 3.

§ 3.

Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową,

podlega karze pozbawienia wolności do lat 5.

art. 269 § 1.

Kto, na komputerowym nośniku informacji, niszczy, uszkadza, usuwa lub zmienia zapis o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji lub funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej albo zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich informacji,

podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

art. 269 § 2.

Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji

[5] A. Adamski: "Przestępstwa komputerowe w nowym kodeksie karnym", Departament Kadr i Szkolenia Ministerstwa Sprawiedliwości 1998,

przekazywania informacji przewiduje druga część przepisu art. 269 § 1 k.k. Indywidualnym przedmiotem ochrony jest w tym przypadku dostępność informacji o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji lub funkcjonowania administracji publicznej. Czyn sprawcy może polegać zarówno na fizycznym, jak i logicznym zamachu na prawidłowe funkcjonowanie systemu służącego do gromadzenia lub przekazywania szczególnie chronionej informacji.

Sprawca zamachu na funkcjonowanie urządzeń służących do gromadzenia i transmisji danych może ponieść odpowiedzialność karną na podstawie art. 269 § 1 lub 2 k.k., o ile spełnione zostaną dwa warunki:

a) dojdzie do zakłóceń lub uniemożliwienia automatycznego gromadzenia lub przekazywania informacji chronionej przez te przepisy;
b) sprawcy będzie można postawić zarzut, że wywołanie tego rodzaju następstw przewidywał i co najmniej godził się na nie.

Przedmiotem wykonawczym sabotażu komputerowego może być zarówno wydzielona sieć teleinformatyczna, jak i publiczna sieć telekomunikacyjna, jeśli jest ona wykorzystywana do transmisji informacji chronionych przez art. 269 k.k. Świadomość tego stanu rzeczy przez sprawcę sabotażu komputerowego stanowi jednak niezbędny warunek pociągnięcia go do odpowiedzialności karnej na podstawie analizowanego przepisu.

Skutkową odmianę przestępstwa sabotażu komputerowego (art. 269 k.k.) przewiduje przepis art. 165 § 1 pkt. 4 k.k. Sabotaż komputerowy ścigany jest z urzędu.

Przestępstwa tego typu były już rejestrowane w Polsce.

Karalność szpiegostwa komputerowego

Art. 130. § 3.

Kto, w celu udzielenia obcemu wywiadowi wiadomości określonych w § 2, gromadzi je lub przechowuje, włącza się do sieci komputerowej w celu ich uzyskania albo zgłasza gotowość działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej,

podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

Warunkiem odpowiedzialności karnej na podstawie art. 130 § 2 k.k. jest „włączenie się do sieci komputerowej" w celu szpiegowskim, tj. w zamiarze bezpośrednim uzyskania informacji, których przekazanie obcemu wywiadowi może wyrządzić szkodę Rzeczypospolitej Polskiej. Działanie podjęte w innym celu nie wypełnia znamion ustawowych tego czynu zabronionego. Jeżeli sprawca włamuje się np. do sieci komputerowej Sztabu Generalnego WP po to, by „wypróbować" jakość jej zabezpieczeń, to w zależności od zastosowanej metody *hackingu* może on odpowiadać karnie wyłącznie na podstawie art. 267 § 1 lub 2 k.k.

Należy dodać, że z chwilą przyjęcia Polski do NATO nie tylko włamanie się do sieci komputerowej rodzimego MON-u, lecz także Pentagonu może być ścigane na podstawie prawa polskiego. Art. 138 k.k. nakazuje bowiem odpowiednie stosowanie przepisu art. 130 *„jeżeli czyn zabroniony popełniono na szkodę państwa sojuszniczego, a państwo to zapewnia wzajemność."*

B. Komputerowe przestępstwa przeciwko mieniu

Rozdział XXXV k.k. zatytułowany „Przestępstwa przeciwko mieniu" zawiera cztery podstawowe typy przestępstw związanych z elektronicznym przetwarzaniem informacji: nielegalne uzyskanie programu komputerowego (art. 278 § 2), pasersrwo programu komputerowego (art. 293 § 1), oszustwo komputerowe (art. 287) i oszustwo telekomunikacyjne (art. 285). *Novum* w polskim prawie karnym stanowią dwa ostatnie typy przestępstw. Natomiast art. 278 § 2 i 293 § 1 k.k. to swoista alternatywa dla

Art. 291.

§ 1. Kto rzecz uzyskaną za pomocą czynu zabronionego nabywa lub pomaga do jej zbycia albo tę rzecz przyjmuje lub pomaga do jej ukrycia,

podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. W wypadku mniejszej wagi, sprawca

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 292.

§ 1. Kto rzecz, o której na podstawie towarzyszących okoliczności powinien i może przypuszczać, że została uzyskana za pomocą czynu zabronionego, nabywa lub pomaga do jej zbycia albo tę rzecz przyjmuje lub pomaga do jej ukrycia,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. W wypadku znacznej wartości rzeczy, o której mowa w § 1, sprawca

podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Paserstwo umyślne

Karalność umyślnego paserstwa programu komputerowego przewiduje oprócz nowego kodeksu karnego (art. 293 k.k.) także art. 118 ust. 1 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. Nr 24, poz.83).[10]

Art. 118. 1. uoop

Kto w celu osiągnięcia korzyści majątkowej przedmiot będący nośnikiem utworu, artystycznego wykonania, fonogramu, wideogramu rozpowszechnianego lub zwielokrotnionego bez uprawnienia albo wbrew jego warunkom nabywa, pomaga w jego zbyciu, przyjmuje albo pomaga w jego ukryciu,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

W obu przypadkach istota czynu karalnego polega na nabyciu, pomocy do zbycia, przyjęciu lub pomocy w ukryciu nielegalnie uzyskanego programu komputerowego (jego pirackiej kopii). Istnieją też różnice w ujęciu tego przestępstwa przez każdą z wymienionych ustaw. Przepis art. 118 ust. 1 upapp ujmuje je węziej niż art. 293 w zw. z art. 291 k.k. Ogranicza bowiem karalność paserstwa programu komputerowego do sytuacji, w której sprawca tego przestępstwa działa w ściśle określonym celu, jakim jest osiągnięcie korzyści majątkowej. Ponadto przepis ten dotyczy wyłącznie przypadków paserstwa nośników programów komputerowych (np. dysków magnetycznych lub optycznych) nie zaś programu w postaci cyfrowej, w której paser może np. nabyć lub przyjąć program za pośrednictwem sieci komputerowej. Podobnych ograniczeń nie przewiduje art. 293 k.k. Jeżeli zatem sprawca działa „w celu osiągnięcia korzyści majątkowej" a przedmiotem wykonawczym przestępstwa jest nośnik

[10] Przepis ten został utrzymany w mocy przez § 2 pkt. 36 ustawy z dnia 6 czerwca 1997 r. przepisy wprowadzające kodeks karny (Dz. U. Nr 88, poz. 554).

Piractwo jest poważnym problemem w polskiej sieci. Ilość ofert oprogramowania pirackiego znajdująca się na listach dyskusyjnych jest tak duża, że coraz trudniej jest lokalizować sprawców tego przestępstwa. Odrębnym problemem jest także piractwo fonograficzne. Możliwości jakie dają nowe techniki kompresowania dźwięku oraz zwiększająca się ilość nagrywarek CD powodują, że coraz częściej spotykamy się z kopiowaniem płyt audio na te nośniki. Na wielu stronach WWW – nazywanych przez autorów jako testowe – znajdują się pokaźne ilości plików MP3 z pełnymi wersjami licznych przebojów muzycznych. Twórcy takich stron zabezpieczają się przed odpowiedzialnością zapisem, że pliki udostępniane są dla celów testowych i należy je skasować z pamięci komputera po upływie 24 godzin.

Odpowiedzialność za poniechanie zabezpieczeń

Aczkolwiek – o czym wspomniałem powyżej – kodeks karny nie zawiera przepisów karnych penalizujących brak zabezpieczeń systemu komputerowego, to jednak w niektórych wypadkach możliwe jest pociągnięcie do odpowiedzialności karnej osoby odpowiedzialnej za bezpieczeństwo tego systemu. Sytuacja taka może się zdarzyć w przypadku przechowywania w sieci komputerowej informacji chronionych na podstawie przepisów (informacji klasyfikowanych). Zwłaszcza w chwili obecnej, gdy UOIN i UODO oraz przepisy wykonawcze do tych ustaw wprowadzają prawny obowiązek zabezpieczenia takiej informacji. Art. 9 §2 kk inaczej ujmuje nieumyślność sprawcy niż kodeks karny z 1969 roku. Odmienność ta polega na odstąpieniu od wcześniejszego podziału tego czynu na lekkomyślność i niedbalstwo, a wprowadzeniu kryterium niezachowania ostrożności. Ustalenie tego, jaka ostrożność była w danych okolicznościach wymagana, zależeć będzie zawsze od warunków konkretnego zdarzenia i jej ustalenie należeć będzie do sądu. Co więcej ustawodawca w art. 18 §3 kk rozszerzył postać pomocnictwa do przestępstwa, wprowadzając zapis: „...odpowiada za pomocnictwo także ten, kto wbrew prawnemu, szczególnemu obowiązkowi niedopuszczenia do popełnienia czynu zabronionego swoim zaniechaniem ułatwia innej osobie jego popełnienie". Pomocnik ponosi odpowiedzialność karną niezależnie od odpowiedzialności głównego sprawcy i to nawet wtedy, gdy przestępstwo, w którym udzielił pomocy, w ogóle nie zostało popełnione.

Możliwości ścigania przestępstw w sieciach komputerowych

Zagadnieniu ścigania przestępstw komputerowych w nowym kodeksie postępowania karnego nie poświęcono żadnych unormowań szczególnych. Ustawodawca nie wziął pod uwagę specyfiki tej kategorii zdarzeń. Oznacza to, że w toku postępowania karnego mają zastosowanie ogólne zasady procesowe. W praktyce oznacza to, że prowadzenie postępowań karnych w sprawach o przestępstwa komputerowe jest stosunkowo trudne, kosztowne, długotrwałe i nie zawsze skuteczne.

Ponieważ większość czynów przestępczych skierowanych przeciwko informacji ścigana jest na wniosek pokrzywdzonego w praktyce brak takiego formalnego wniosku uniemożliwia działanie organów ścigania. Jednocześnie pokrzywdzony we wniosku takim zmuszony będzie dostarczyć organowi ścigania wszystkich dowodów popełnienia przestępstwa i dokonanie ich interpretacji. Trudno bowiem będzie oczekiwać od przyjmującego taki wniosek, by bez szczegółowego opisu zdarzenia na podstawie samodzielnej analizy materiałów (np. logów systemowych) organ ten był w stanie „powziąć uzasadnione podejrzenie popełnienia przestępstwa". Jednocześnie treść art. 307 § 2 kpk wyklucza możliwość przeprowadzenia dowodu z opinii biegłego po to, by wyjaśnić, czy zachodzą podstawy do wszczęcia postępowania karnego.

Kolejnym problemem jest zbytnie zbiurokratyzowanie polskiej procedury karnej co powoduje znaczne wydłużenie procesu decyzyjnego. W sytuacji „ulotnej natury" przestępstw komputerowych może to niejednokrotnie powodować utratę dowodów przestępstwa.

Zamiast zakończenia

Prawo nie dotrzymuje kroku technologii. Tempo jej rozwoju jest niekiedy porównywane do prędkości światła, co na tle tempa zmian ustawodawczych wydaje się ujęciem trafnym. Problematyka zabezpieczania systemów informatycznych staje się jednym z najważniejszych zagadnień dla coraz większego kręgu osób, co jest zresztą naturalne wobec ciągle zwiększającej się roli informacji w życiu

POTRZEBY I UWARUNKOWANIA BUDOWY SIECI DLA POTRZEB PAŃSTWA

mgr inż. Wiesław FILAR

Departament Rejestrów Państwowych,
Łączności i Informatyki MSWiA

1. Strategiczne założenia budowy systemów łączności dla potrzeb kierowania państwem.

Na przestrzeni ostatnich kilku lat technologie w dziedzinie telekomunikacji i systemów informacyjnych rozwijały się dynamicznie i przenikały wzajemnie. Wywarło to, i nadal wywiera w dużym stopniu wpływ na współczesne społeczeństwo. Dotyka to wszystkich aspektów współczesnego życia. Krajowe i międzynarodowe instytucje życia politycznego, gospodarczego, wojskowego, kulturalnego i naukowego, a nawet osoby fizyczne coraz bardziej uzależniają się od stałej dostępności usług opartych na tych technologiach. W efekcie łączy się to z zapotrzebowaniem na skuteczne, niezawodne i tanie systemy łączności oraz systemy informacyjne.

Uległa również zmianie organizacja telekomunikacji. W przeszłości za całość uregulowań dotyczących łączności, infrastrukturę i świadczenie usług odpowiedzialny był jeden resort rządowy - Ministerstwo Łączności. Na przestrzeni ostatnich kilku lat doszło do rozdziału funkcji regulacyjnych od świadczenia usług i budowy sieci.

Sprawy regulacyjne nadal leżą w kompetencji jednostki rządowej - Ministerstwa Łączności, natomiast budowa infrastruktury rozdzielona jest na "Operatorów". Można wyróżnić tu np.:

a) operatorów sieci - odpowiedzialnych za infrastrukturę;
b) usługodawców - odpowiedzialnych za świadczenia usług w ramach infrastruktury.

W tej sytuacji zadaniem i obowiązkiem rządu będzie tworzenie odpowiednich mechanizmów ekonomicznych, prawnych i administracyjnych gwarantujących powszechny dostęp do informacji, zapewnienie uczciwej konkurencji, umożliwienie tworzenia nowych rozwiązań techniczno - organizacyjnych oraz pełne wykorzystanie istniejących i przyszłościowych technologii.

Ustawa z dnia 4 września 1997 roku o działach administracji rządowej tworzy klimat do organizowania wirtualnych sieci teleinformatycznych z profesjonalnym oprogramowaniem zapewniającym efektywne spożytkowanie informacji na rzecz danego działu administracji rządowej.

Przygotowywana do wdrożenia ustawa - "Prawo telekomunikacyjne" - zachęci różnych przedsiębiorców do rozbudowy usług i sieci teleinformatycznych, a działy administracji rządowej - do tworzenia bezpiecznych styków wzajemnego informowania się.

Sprzyjający klimat dla bezpieczeństwa teleinformatycznego w układach wewnętrznych państwa i zewnętrznej komunikacji informacyjnej - zapewnia ustawa z dnia 22 stycznia 1999 roku "O ochronie informacji niejawnych".

Ustawa o ochronie informacji niejawnych formułuje wyraźnie nowe jakościowo prawa, zadania i obowiązki dla administracji rządowej, przedsiębiorców, jednostek naukowych i

W realizacji zadań w dziedzinie bezpieczeństwa państwa, w tym zadań obronnych, uczestniczą w stosownym zakresie, organy władzy, organy administracji rządowej i samorządowej, podmioty gospodarcze, jednostki organizacyjne, organizacje społeczne, a także obywatele.

Wszystkie te ogniwa powinny być powiązane informacyjnie, mieć precyzyjnie określone zadania w zakresie bezpieczeństwa i być właściwie przygotowane do ich realizacji na wypadek zagrożeń czasu pokoju i wojny.

Kierowanie reagowaniem na sytuacje kryzysowe oraz obroną państwa jest procesem skomplikowanym, przenikającym wszystkie strefy działalności państwa zarówno w okresie pokoju, kryzysu i wojny. Wymaga ono efektywnego systemu kierowania, który powinien stanowić integralną część systemu kierowania państwem.

System taki obejmuje wzajemnie powiązane informacyjnie organy kierowania, techniczne środki kierowania oraz stanowiska kierowania. Jego rola polega na sprzężeniu wszystkich sił i państwa w jednolitą, sprawnie funkcjonującą całość umożliwiającą realizację zadań w dziedzinie bezpieczeństwa narodowego.

Podstawowymi ogniwami systemu kierowania państwem są:

- naczelne organy władzy i administracji państwowej;
- centralne organy administracji rządowej;
- terenowe organy administracji rządowej;
- organy samorządu terytorialnego.

W sytuacjach zagrożeń kryzysowych uruchamia się system kierowania reagowaniem kryzysowym. W tym celu tworzy się na poszczególnych szczeblach kierowania państwem "Zespoły" lub "Sztaby Kryzysowe".

Organem właściwym do tworzenia procedur postępowania oraz koordynowania działalności administracji państwowej i służb publicznych w danej sytuacji kryzysowej będzie resort (instytucja) wiodący wyznaczany każdorazowo przez nadrzędne ośrodki decyzyjne np. Rady Ministrów, BBN ...., na podstawie zbioru danych o kryzysie.

Nadrzędny ośrodek decyzyjny zachowałby prawo akceptacji wszelkich podejmowanych działań. Przy tym należy przyjąć, że generalnie dla kryzysów

o charakterze polityczno - militarnym będzie to MON, a dla kryzysów niemilitarnych (cywilnych) MSWiA.

Dla potrzeb kierowania reagowaniem kryzysowym (w wypadku o charakterze niemilitarnym) przewiduje się dwuszczeblowy system kierowania:

- pierwszy poziom stanowi Rada Ministrów oraz Urząd Zarządzania Kryzysowego i Obrony Ludności;
- drugi powinien stanowić Wojewoda, który jako terenowy organ administracji rządowej podejmuje stosowne decyzje dotyczące likwidacji zagrożenia kryzysowego w skali województwa.

Dla tych organów przygotowuje się odpowiednio powiązane informacyjnie stanowiska kierowania zdolne do funkcjonowania w każdych warunkach, w okresie pokoju, kryzysu i wojny i wydziela się odpowiednie siły i środki.

Na czas zagrożenia bezpieczeństwa państwa, kryzysu i wojny w zależności od sytuacji i potrzeb, pokojowy system kierowania państwem rozwija się w wojenny system kierowania państwem (stopniowo - selektywnie) na poszczególnych szczeblach kierowania lub w wybranych elementach i ogniwach albo też całościowo, z takim wyliczeniem aby mógł on zapewnić nieprzerwane kierowanie państwem i jego obroną.

Do dowodzenia wojskami wydziela się autonomiczny system dowodzenia, którego ogniwami są:

transmisyjne linie światłowodowe. Przewiduje się stosowanie cyfrowych linii radiowych jako awaryjnych linii łączności;

- współpraca z krajową siecią teletransmisyjną powinna być realizowana przez trakty cyfrowe o przepływnościach 2048 kbit/s i większych w zależności od potrzeb;
- podstawowym stykiem współpracy węzłów z siecią teletransmisyjną, dla wszystkich szybkości, powinien być znormalizowany przez styk G.703/704;
- sieć teletransmisyjna powinna charakteryzować się elastycznością umożliwiającą w razie potrzeby szybkie udostępnienie nowych traktów lub zwiększenie przepustowości traktów już zestawionych.

2.3. Sieć komutacyjna.

- w systemie powinna być zapewniona elastyczność budowy nowych węzłów oraz ich ewentualnej rozbudowy, węzły komutacyjne powinny mieć budowę modularną;
- powinna być zapewniona możliwość komutacji kanałów, pakietów i komórek;
- system numeracji w systemie komutacyjnym powinien być jednolity
- i gwarantować abonentom wejście do systemu w dowolnym jego punkcie
- z zachowaniem przyznanego priorytetu;
- system numeracji powinien umożliwiać nadawanie numerów abonentom
- z możliwością określenia usługi oraz poziomu priorytetu zestawianego połączenia;
- system numeracji powinien zapewnić możliwość wyjścia do innych, współpracujących sieci;
- system powinien umożliwiać wymianę informacji sygnalizacyjnych związanych
- z zarządzaniem i utrzymaniem;
- powinna być możliwość wymiany sygnalizacji związanej z tworzeniem optymalnych tras połączeń;
- w węzłach powinna być zapewniona możliwość programowania co najmniej trzech dróg kolejnego wyboru dla każdego kierunku ruchu wychodzącego;
- ze względów niezawodnościowych moduły funkcjonalne centralne i grupowe poszczególnych elementów systemu powinny być dublowane. Moduł rezerwowy powinien pracować w trybie " gorącej rezerwy" i w przypadku awarii modułu głównego samoczynnie podjąć jego funkcje.

2.4. Bezpieczeństwo systemu łączności.

- system powinien zapewnić, w zależności od szczebla kierowania, przekazywanie informacji niejawnych, w tym również o najwyższej klauzuli tajności obowiązującej w państwie - "ściśle tajne";
- zagadnienia bezpieczeństwa w systemie powinny być rozważane
- w następujących aspektach :
  - bezpieczeństwa fizycznego,
  - bezpieczeństwa transmisji,
  - kryptograficznej ochrony informacji,
  - bezpieczeństwa emisji,
  - stosowania odpowiednich kryteriów i zasad doboru personelu,
  - ochrony kontrwywiadowczej.
- urządzenia stacyjne powinny być instalowane w oddzielnych pomieszczeniach przeznaczonych specjalnie dla planowanego systemu;
- pomieszczenia chronione powinny mieć zabezpieczenia przeciwwłamaniowe wraz z sygnalizacją alarmową;

- fonia:
  - połączenie telefoniczne;
  - przekazywanie informacji fonicznych na bazie " usługi zapamiętaj i przekaż" (poczta foniczna);
  - telefoniczne wyszukiwanie informacji w bazach danych;
  - telekonferencje.
- dane:
  - komunikacja międzykomputerowa;
  - połączenia teleakcyjne (telealarmy, telenadzór, telemetria);
  - wyszukiwanie informacji w bazach danych;
  - poczta elektroniczna.
- tekst:
  - przekazywanie tekstu za pomocą terminali wideotekstowych;
  - poczta elektroniczna;
  - telegraf.
- obraz:
  - przekazywanie obrazu za pomocą terminali telefaksowych;
  - połączenia wideofoniczne;
  - połączenia wideokonferencyjne;
  - wyszukiwanie informacji obrazowych;
  - systemy nadzoru;
  - komunikacja między terminalami graficznymi.

- niezależnie od przedstawionego wyżej podziału użytkownicy powinni, odpowiednio do przyznanych uprawnień, mieć dostęp do usług dodanych.

2.7. Podsystem dostępu radiowego.

- - system powinien posiadać podsystem radiodostępu. Może to być zapewnione poprzez:
  - własny podsystem radiodostępu;
  - wykorzystanie innych systemów radiodostępu funkcjonujących w państwie.
- podsystem radiodostępu powinien zapewnić:
  - utajnioną łączność telefoniczną, teleksową oraz transmisję danych na całym odcinku łącza od abonenta do abonenta;
  - pewną łączność abonentom znajdującym się w ruchu lub na postoju;
  - realizację połączeń wyłącznie abonentom upoważnionym.

2.8. Odtwarzanie naruszonego systemu łączności.

- struktura systemu oraz przyjęte rozwiązania organizacyjne i technologiczne powinny gwarantować ciągłość jego działania w każdych warunkach;
- w wytypowanych węzłach łączności powinny być zmagazynowane mobilne zestawy sprzętu transmisyjnego i komutacyjnego przeznaczone do odtwarzania uszkodzonych lub zniszczonych elementów systemu.

2.9. Współpraca z innymi sieciami telekomunikacyjnymi.

- system powinien umożliwiać stałą lub okresową współpracę z innymi sieciami funkcjonującymi w systemie telekomunikacyjnym państwa.

PROBLEMY PRAWNE I ORGANIZACYJNO-TECHNICZNE WYSTĘPUJĄCE PRZY BUDOWIE BEZPIECZNYCH SYSTEMÓW TELEINFORMACYJNYCH

inż. Włodzimierz Zaleszczyk

SERWIS PRO-TELEKOM

Wszystkie budowy, w tym również budowa systemów teleinformacyjnych, realizowane winny być w zgodzie z regulacjami prawa budowlanego oraz zgodnie z kanonami sztuki inżynierskiej.

Pozostawać w zgodzie z wymogami prawa budowlanego, to znaczy przestrzegać regulacji wynikającej z ustawy Prawa Budowlane z dnia 7 lipca 1994r. oraz przepisów wykonawczych związanych bezpośrednio i pośrednio z tą ustawą.
Spis ważniejszych aktów załączony jest do niniejszego opracowania. Warto wiedzieć, że Ustawa Prawo Budowlane w sposób jednoznaczny określa uczestników procesu budowlanego.

Są nimi:

- inwestor
- inspektor nadzoru inwestorskiego
- projektant
- kierownik budowy

Każda ze stron tego procesu ma określone prawa i obowiązki.

Do obowiązków inwestora należy:

- zorganizowanie procesu budowlanego budowy przez zapewnienie opracowania projektów oraz wykonanie i odbiór robót budowlanych przez osoby o odpowiednich kwalifikacjach zawodowych.
- ustanowienie w miarę potrzeb lub w związku z decyzją administracyjną – inspektora nadzoru inwestorskiego.

Do obowiązków projektanta należy:

- opracowanie projektu budowlanego w sposób zgodny z ustaleniami określonymi w decyzji o warunkach zabudowy i zagospodarowania terenu, wymogami ustawy, przepisami i obowiązującymi Polskimi Normami oraz kanonami wiedzy technicznej.
- uzyskanie wymaganych opinii, uzgodnień i sprawdzeń rozwiązań projektowanych w zakresie wynikającym z przepisów.
- wyjaśnienie wątpliwości dotyczących projektu i zawartych w nim rozwiązań ,
- sprawowanie nadzoru autorskiego na żądanie inwestora lub właściwego organu
- w zakresie:
  1. sprawdzenie w toku wykonywanych robót budowlanych zgodności realizacji z projektem,
  2. uzgodnienia możliwości wprowadzenia rozwiązań zmiennych w stosunku do przewidzianych w projekcie, zgłaszanych przez kierownika budowy lub inspektora nadzoru inwestorskiego.

- sprawdzenie jakości wykonywanych robót wybudowanych obiektów, a w szczególności zapobieganie zastosowania wyrobów wadliwych i niedopuszczonych do obrotu i stosowania w budownictwie łączności
- sprawdzenie i odbiór robót ulegających zakryciu lub zanikających, uczestniczenie w próbach i odbiorach technicznych instalacji, urządzeń technicznych oraz całych systemów i obiektów,
- potwierdzenie faktycznie wykonanych robót oraz usunięcie wad, a także na żądanie inwestora kontrolowanie rozliczeń budowy,

Jednocześnie inspektor nadzoru inwestorskiego ma prawo:

- wydawać kierownikowi budowy lub kierownikowi robót polecenia potwierdzonego wpisem do dziennika budowy dotyczące:
  1. usunięcia nieprawidłowości lub zagrożeń,
  2. wykonywania prób lub badań, także wymagających odkrycia robót lub elementów zakrytych oraz przedstawienia ekspertyz dotyczących prowadzonych robót,
  3. sprawdzania dowodów dopuszczania do obrotu i stosowania w budownictwie łączności.
- żądać od kierownika budowy lub kierownika robót dokonania poprawek bądź ponownego wykonania wadliwie wykonanych robót, a także wstrzymanie dalszych robót w przypadku gdy ich kontynuacja może spowodować zagrożenie lub niedopuszczalną niezgodność z projektem.

Uważam, że :

- -zapoznanie się z przytoczonymi wyżej obowiązkami i usprawnieniami stron procesu inwestycyjnego jest rzeczą nieodzowną przed przystąpieniem do jego programowania i realizacji.

Programowanie, albo jak kto woli przygotowanie procesu budowlanego leży w interesie ekonomicznym, każdego inwestora niezależnie od tego, czy jest on firmą prywatną czy też instytucją budżetową.

Stwierdzenie to nabiera jeszcze większej wagi, kiedy planujemy budowę tak zwanych systemów bezpiecznych. Planowanie rozpoczynamy od jednoznacznego określenia tego co chcemy wybudować. W przypadku systemów teleinformacyjnych elementem tego planowania jest przygotowanie programu funkcjonalno-użytkowego, który jest opisem tego czego inwestor oczekuje od planowanego do wybudowania systemu.

Program ten jest jednocześnie płaszczyzną porozumienia pomiędzy inwestorem, a projektantem.

Ważnym elementem tych oczekiwań będzie określenie:

- przeznaczenie systemu,
- ustalenie rygorów jego funkcjonowania,
- określenie warunków i parametrów styku z innymi systemami,
- ustalenie kryteriów bezpieczeństwa jakim podlegać ma za równo sam system teleinformacyjny jak i przesłane lub gromadzone za jego pomocą informacje.

Sprawy bezpieczeństwa systemów i sieci teleinformatycznych są przedmiotem regulacji ustawowej w rozdziale 10 ustawy z dnia 22 stycznia 1999r. o ochronie informacji niejawnych.

- środowisko eksploatacji,
- system nadzoru i utrzymania technicznego,
- charakterystyka systemu dotycząca klauzuli tajności i kategorii uprawnień użytkowników systemu,
- przewidywane środki ochrony i procedury bezpieczeństwa związane z ochroną
- wskazanie osób odpowiedzialnych za bezpieczeństwo.

Szczegółowe wymagania bezpieczeństwa systemu podlegają zatwierdzeniu zgodnie z Art. 61 pkt. 2 Ustawy z dnia 22 stycznia 1999r. o ochronie informacji niejawnych. Zatwierdzenia tego dokonują służby ochrony państwa w terminie 30 dni od daty ich dostarczenia /przekazania/.

Dopiero po uzyskaniu wymogów możliwe jest rozpoczęcie procedury projektowania zarówno systemu jak i jego infrastruktury technicznej, w tym stosowanych systemów ochrony.

Należy zwrócić uwagę, że zatwierdzenie to może mieć istotny wpływ na dobór dostawców i stosowanych rozwiązań. Może również mieć zasadnicze znaczenie dla kosztów jakie inwestor będzie musiał ponieść przy budowie bezpiecznego systemu teleinformacyjnego.

Do osiągnięcia właściwego poziomu bezpieczeństwa we wszystkich jego aspektach, o których mowa w rozporządzeniu Prezesa Rady Ministrów z dnia 25 lutego 1999r. przyczyniać się będą takie elementy infrastruktury towarzyszącej jak:

- systemy klimatyzacji,
- systemy kontroli i rejestracji dostępu,
- systemy sygnalizacji p.poż.,
- systemy antywłamaniowe,
- systemy telewizji dozorowanej,
- systemy dystrybucji sieci strukturalnej,
- systemy ochrony elektromagnetycznej,

Rolą projektanta jest uzyskanie właściwego poziomu bezpieczeństwa przy użyciu tych systemów z uwzględnieniem optymalizacji kosztów. Jak powszechnie wiadomo podwyższenie bezpieczeństwa wpływa w sposób znaczący na poziom ponoszonych kosztów.

Informacje powyższe na podstawie obowiązujących aktów prawnych wyselekcjonował i zestawił na zlecenie Naukowej i Akademickiej Sieci Komputerowej inż. Włodzimierz Zaleszczyk, SERWIS PRO-TELKOM

ANALIZA MOŻLIWOŚCI BUDOWY SIECI ŁĄCZNOŚCI DLA POTRZEB PAŃSTWA

Andrzej Zienkiewicz

1. Wprowadzenie

Referat zawiera poglądy niezależnego eksperta oparte na wykształceniu i wieloletnim doświadczeniu w budowie, uruchamianiu i eksploatacji przedsięwzięć rozwojowych, w tym telekomunikacyjnych. Referat nie nawiązuje i nie analizuje poglądy instytucji i osób zainteresowanych w realizacji omawianego tematu. Celem referatu jest globalna analiza problemu, którego realizacja w zależności od konkretnych uwarunkowań odbiegać będzie od modelu optymalnego.

2. Przedmiot analizy

Przedmiotem przedsięwzięcia jest budowa i utrzymanie systemu telekomunikacyjnego dla Państwa spełniającego wymogi bezpieczeństwa w zakresie łączności cywilnej. Zarówno system jak i pomieszczenia, w których zlokalizowane są jego węzły musi spełniać wymagania wysokiej niezawodności jak i bezpieczeństwa informacji w nim przesyłanych. System łączności ma wspomagać niezbywalne funkcje władzy i administracji Państwa, które nie mogą być wykonywane sprawnie przez inne instytucje i organizacje w państwie. Funkcje te są związane najogólniej z utrzymaniem i zapewnieniem porządku i bezpieczeństwa dla ogółu obywateli w Polsce. Zakres odpowiedzialności poszczególnych organów Państwa jest opisany szczegółowo w odpowiednich aktach prawnych.
Przedsięwzięcie obejmuje swoim zasięgiem cały kraj. Realizowany w ramach przedsięwzięcia system telekomunikacyjny z założenia wykorzystuje w połączeniach szkieletowych trakty cyfrowe wynajmowane u różnych operatorów telekomunikacyjnych, zapewniając jednocześnie podwyższony standard bezpieczeństwa sieci w rozumieniu jej niezawodności jak i ochrony przed nieuprawnionym dostępem do przesyłanych informacji. Wysoka niezawodność budowanej sieci wynika ze stosowania automatycznie przełączalnych dróg obejściowych w razie awarii połączenia i związanego z tym specjalnego systemu nadzoru. Ochrona informacji polega na tym, że wprowadzana jest ona do systemu telekomunikacyjnego i wyprowadzana z niego w specjalnie przystosowanych obiektach telekomunikacyjnych, mieszczących całość urządzeń przetwarzających i przesyłających informacje, przed i po szyfrowaniu. Połączenia abonenckie systemu są w zasadzie własne głównego użytkownika lub użytkowników.
Tak duże przedsięwzięcie nie może być uruchamiane jednorazowo, wobec tego faza budowy i utrzymania systemu będą przez pewien czas nakładać się wzajemnie.
Przedsięwzięcie telekomunikacyjne musi zapewnić warunki dla utrzymania systemu telekomunikacyjnego w ruchu. Powodów jest kilka:

- znacznie łatwiej jest przekonać decydentów co do konieczności jednorazowych nakładów inwestycyjnych niż do zapewnienia warunków ekonomicznych funkcjonowania systemu, zwłaszcza, że koszty utrzymania są w dłuższej perspektywie czasu znacząco większe niż jednorazowe koszty budowy,
- nowoczesny system telekomunikacyjny, przy wielkich zaletach funkcjonalnych i ekonomicznych, wymaga stałego unowocześniania (up grade), w przeciwieństwie do systemów tradycyjnych jest znacznie bardziej podatny za tak zwane zużycie moralne,

- Przechwytywanie informacji z takiej sieci jest ekonomicznie najłatwiejsze, ponieważ brak "zaszumienia" informacjami nieistotnymi dla przechwytującego ułatwia zgromadzenie interesujących zbiorów,
- Budowa sieci wydzielonej od podstaw wymaga wielkich środków inwestycyjnych i pokonania ogromnych trudności związanych z uzyskaniem prawa do określonych tras prowadzenia infrastruktury.

Jedynie rozsądnym i stosowanym na świecie rozwiązaniem jest skorzystanie z infrastruktury transmisyjnej działających w Polsce operatorów.

Analiza wykonalności wskazuje na wiele możliwości uzyskania połączeń pomiędzy węzłami sieci. Przyjmuje się jako podstawowe założenie, że w każdym przypadku przekaz informacji wychodzący poza obręb własnych węzłów sieci jest traktowany jako przekaz przez obce terytorium i wobec tego jest odpowiednio chroniony przed niepowołanym dostępem. W tej sytuacji o wyborze wariantu powinna decydować niezawodność i ekonomiczność rozwiązania. Wobec tego przeanalizujemy kolejno różne możliwości.

- Wszystkie potrzebne kanały cyfrowe można wynająć na normalnych warunkach od TP S.A. Zaletą takiego rozwiązania jest mała kłopotliwość oraz elastyczność modyfikacji w fazie projektu i eksploatacji. Wadami są stosunkowo wysoki koszt oraz ograniczona do normalnych warunków niezawodność połączeń.
- Podobnie można wynająć kanały cyfrowe od TELENERGO. Ceny kanałów cyfrowych mogą być w tym przypadku mniejsze. Wadami są: ograniczona dostępność kanałów, brak dojścia do końcowych lokalizacji oraz obserwowana niska niezawodność połączeń, szczególnie w czasie podnoszenia z awarii.
- Również PKP posiada kanały cyfrowe do wynajęcia. Ceny są w tym przypadku pośrednie pomiędzy TP S.A. i TELENERGO. Natomiast jakość usługi niska.
- Należy wspomnieć o akademickiej sieci POL34. Brak jednak operatora oraz ogólnych zasad wykorzystania tej sieci poza środowiskiem akademickim nie pozwala na rozważanie tej sieci jako podkładu transmisyjnego w ramach przedsięwzięcia.
- Możliwe jest wykorzystanie dla systemu łączności Państwa systemu telekomunikacyjnego MSWiA, a dokładniej z systemu Policji. System ten w części rozległej nosi nazwę POLWAN w części lokalnej WARMAN (Zakryty). Omówimy te systemy osobno.
  - POLWAN jest systemem nowym w ciągłej rozbudowie, posiada dobry system przełączania awaryjnego połączeń, dobrą integrację głosu i danych oraz adaptacji różnego rodzaju środków łączności do systemu podstawowego. Również koszt korzystania z POLWANu może być niski, ograniczony wyłącznie do ponoszonych rzeczywiście kosztów. Wadą systemu jest jego ewolucja, w wyniku zmian organizacyjnych w resorcie, w kierunku systemy wewnętrznego Policji. Wynika z tego ograniczona przepustowość połączeń, z zasady 2 Mbps. Dołączenie do tego systemu sieci łączności Państwa bez zasadniczej rozbudowy przepustowości oraz uregulowania statusu prawnego tego systemu może być trudne lub niemożliwe.
  - WARMAN jest lokalną sieci w Warszawie wspólnie użytkowaną przez NASK i MSWiA w ramach porozumienia. Zaletą tego systemu jest duża przepływność połączeń do 155 Mbps. Również koszt korzystania z tego systemu jest niski, podobnie jak w przypadku sieci POLWAN. Wadą jest stosunkowo zaawansowany wiek wyposażenia, niemodyfikowanego od 1994 roku. Wykorzystanie tych urządzeń w sieci byłoby możliwe po zmodyfikowaniu (up grade). Niejasny jest przyszłościowy status tej sieci wobec ponawianych przez jednostkę nadzorującą NASK postulat wycofania z sieci urządzeń obsługujących środowisko naukowe i akademickie, a tym samym podważenie statusu ekonomicznego tej sieci. W opisanej sytuacji nie można założyć, że sieć ta może być wykorzystana przez przedsięwzięcie bez rozwiązania wyżej opisanych problemów.

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".
Koniecznie trzeba również przewidzieć błędną pracę 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.
Trzeba również przewidzieć 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

lokalnego operatora dyspozycyjnego dopuszczonego do realizacji pewnego zakresu prac zlecanych przez poziom centralny.
Poziom nadrzędny obejmuje sterowanie i nadzorowanie działania poszczególnych funkcji systemu telekomunikacyjnego jak: komutacja, tranzyt, system teleinformatyczny, podsieć telekomunikacyjne, zasilanie, systemy zabezpieczeń, klimatyzacja, bezpieczeństwo systemu i obiektów.
Poziom centralny obejmuje sterowanie i nadzorowanie działaniem poziomu nadrzędnego poprzez monitorowanie działania poszczególnych systemów oraz generowanie wynikających z tego alarmów.
Przy wyżej opisanym podziale zakresu zadań dla poszczególnych służb przedstawiałyby się następująco:

- Obsługa dyżurna będzie się zajmowała bieżącą obsługą połączeń oraz wspomagała abonentów węzła bez prawa dokonywania jakichkolwiek zmian konfiguracyjnych w urządzeniach węzła oraz zestawionych połączeniach. Do obowiązków obsługi dyżurnej należeć będzie stała obserwacja urządzeń oraz w przypadku zaobserwowania nieprawidłowości w działaniu przywoływaniu operatorów dyspozycyjnych.
- Operatorzy dyspozycyjni będą się zajmować konfigurowaniem i zmianami konfiguracji w urządzeniach węzła mieszczących się w zakresie obsługi lokalnej i nie mających wpływu na działanie innych węzłów sieci. W przypadku trudności lub obserwowanych awarii będą się kontaktować z odpowiednimi służbami utrzymania sieci, z którymi będą ściśle współpracować w usuwaniu nieprawidłowości nie wymagających przyjazdu serwisu na miejsce.
- Operatorzy poziomu nadrzędnego będą nadzorowali pracę poszczególnych systemów wchodzących w skład i zabezpieczających pracę sieci oraz będą podejmować działania mieszczące się w zakresie zarządzania siecią bez prawa dokonywania zmian w konfiguracji pracującego systemu, co należy do obowiązków zespołów utrzymania sieci. W razie trudności w zarządzaniu siecią będą kontaktować się z odpowiednimi służbami utrzymania sieci.
- Operatorzy poziomu centralnego nadzorują działanie systemów sieci jako całości, generują odpowiednie alarmy oraz stale dokonują kontroli systemów zabezpieczenia sieci. Do ich obowiązków należeć będzie sporządzanie okresowych audytów poszczególnych systemów oraz całości sieci pod kątem niezawodności i bezpieczeństwa w świetle pojawiających się nowych zagrożeń oraz możliwości.

Następnym problemem jest utrzymanie sieci telekomunikacyjnej łącznie z obiektami, na których sieć pracuje bez omawiania problemów eksploatacji oraz pochodzenia środków koniecznych dla sprawnego działania.
Sieć telekomunikacyjna, a w szczególności sieć nowoczesna, w dużej części skonfigurowana na poziomie oprogramowania "soft", jest systemem zmieniającym się w czasie, w wielu elementach stosunkowo krótkim.
Utrzymanie sieci telekomunikacyjnej rozpatrzymy w trzech warstwach:

- Utrzymanie sieci rozumiane jako jej ciągła rozbudowa w zakresie tworzenia nowych węzłów, nowych tras połączeń międzywęzłowych, przyłączania nowych abonentów oraz modyfikacja związana ze zmianą oprogramowania telekomunikacyjnego lub wymianami sprzętu na nowszy.
- Rekonfiguracja oprogramowania i wyposażenia sieci związana z jej optymalizacją działania wynikającą ze zmieniających się potrzeb, modyfikacją systemu ochrony sieci lub klasy traktów cyfrowych.
- Przeciwdziałanie awariom wyposażenia, oprogramowania oraz traktów cyfrowych.

Zespół zajmujący się rozbudową sieci przygotowuje oraz przeprowadza prace mające na celu rozbudowę sieci oraz jej przebudowę związaną ze zmianami funkcji jak i technologii.

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 .
Należy również omówić ochronę 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.
Jak z powyższego omówienia 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.
Porównanie wymagań dla sieci dla potrzeb Państwa przedstawionych w 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 kiedyś napisał Mirosław Machalski w referacie przed dwoma laty, 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 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

Chociaż w tak trudnej dziedzinie chętnych na branie odpowiedzialności za łączność może brakować.
Wreszcie można powołać Operatora w postaci agencji, jednostki budżetowej lub podobnej, która otrzyma środki w celu zapewnienia użytkownikom odpowiednich usług rzeczowych. Zaletą takiego rozwiązania jest prostota finansowania. Jednak poza tym jest to rozwiązanie ryzykowne, prowadzące do niepowodzeń i częstych nadużyć. Skierowanie środków do realizatora powoduje, że de facto prowadzi on politykę udostępniania łączności sam się z niej bieżąco rozliczając. W praktyce pojawia się natychmiast coś w rodzaju "gospodarki deficytu". Użytkownicy uważają, że są niewłaściwie obsługiwani, Operator uważa, że nie otrzymał wystarczających środków. Do tego dysponowanie środkami, nawet jeśli nie powoduje nadużyć to co najmniej stwarza rozliczne podejrzenia, że tak się dzieje. Reprezentowanie użytkowników nie ma żadnego umocowania prawnego, a rozliczanie normalnie w postaci sprawozdań z wykorzystania środków bardzo słabe.
W każdej formie organizacyjnej należy dążyć do stworzenia formy reprezentacji użytkowników. W postaci Rady Użytkowników w systemie budżetowym lub agencyjnym, gdzie rola rady z natury jest doradcza, a decyzje podejmują odpowiednio prawnie umocowane władze lub Rady Nadzorczej w systemie spółki, gdzie rada ma prawnie umocowaną władzę nad zarządem spółki.
Niezależnie od formy organizacyjnej bazą kadrową i organizacyjną Operatora mogą i chyba powinny być zespoły dawnego Biura Łączności Komendy Głównej Policji oraz NASK, które od wielu lat realizują podobnego rodzaju przedsięwzięcia. Wiele tych zespołów jest zaangażowanych, chyba nieodwracalnie w innych pracach w różnych organizacjach jednak podstawowa kadra stanowiąca zalążek kadr Operatora mogłąby być w przedsięwzięcie zaangażowana.

6. Metody finansowania

Sieć telekomunikacyjna na potrzeby Państwa może być finansowana dwojako. Poprzez skierowanie środków budżetowych wprost do Operatora, który ma zapewnić łączność dla wszystkich zainteresowanych, lub poprzez skierowanie środków do użytkowników, którzy zapłacą operatorowi za postawione do dyspozycji środki. Pierwsza metoda pozornie wygodna jest mało skuteczna. Problem jest dokładnie znany i nie będę go omawiał przyjmując, że konieczne jest przyjęcie wariantu drugiego pozwalającego na uzgodnienie warunków łączności pomiędzy operatorem i użytkownikiem i rozliczenie wzajemne stron.
W rozdziale rozważono przypadek, gdyby budowana sieć jest wykorzystywana przez więcej niż jednego użytkownika. System rozliczeń za wykorzystanie sieci mógłby przedstawiać się tak jak to w dalszym ciągu jest opisane.
Sieć telekomunikacyjna budowana i uruchamiana w ramach przedsięwzięcia jest przeznaczona dla zamkniętego grona użytkowników. W sieci tej nie będą świadczone usługi publiczne. Przy takim założeniu zbędne jest posiadania koncesji na świadczenie usług w tej sieci jak i zezwolenie telekomunikacyjne na jej budowę.
Dla zamkniętego grona użytkowników nie określa się cen za usługi świadczone w sieci. Ponieważ użytkownikami tej sieci są różne organizacje wobec tego powinny one uczestniczyć w kosztach jej utrzymania. Ze swej natury sieć musi mieć operatora, który jest odpowiedzialny za jej działanie i odpowiednie modyfikacje. Operator, żeby utrzymać sieć musi posiadać środki, które powinien otrzymać od użytkowników sieci.
Proponujemy, aby podstawą wpłat na rzecz operatora sieci był w ciągu czterech kwartałów planowany koszt utrzymania sieci. Natomiast w czwartym kwartale powinno nastąpić skorygowanie kosztu. Być może ze względu na specyfiką użytkowników, w

trudności z uzyskaniem wystarczających środków. Po realizacji środki zostają zamrożone, a ich odtworzenie wymaga gromadzenia odpisów amortyzacyjnych co w niektórych systemach jest trudne lub odzyskiwane środki nie są przeznaczane na odtworzenie zrealizowanych obiektów. Po drugie finansowanie ze środków własnych powoduje, że finansujący staje się właścicielem obiektu, na którym ciążą wszelkie obowiązki związane z jego utrzymaniem, co często zmusza właściciela do zajmowania się sprawami dalekimi od jego profesji, chyba że jego głównym przedmiotem działania jest operowanie siecią telekomunikacyjną.

Finansowanie poprzez kredyt pozwala ominąć trudności zgromadzenia odpowiednich środków własnych . Jednak konieczność spłaty kredytu zmusza do podniesienia kosztów działania sieci (skrócona amortyzacja) tak, aby starczyło na spłatę kredytu oraz na zgromadzenie środków na jej odtwarzanie zanim do konieczności takiego odtworzenia dojdzie. Inne wady i zalety korzystania z kredytu są podobne jak przy finansowaniu ze środków własnych.

Finansowanie przez najem pozwala uniknąć wad wynikających z konieczności pełnienia funkcji właściciela i w dużej części konserwatora systemu oraz nie wymaga posiadania własnych środków finansowych na wybudowanie sieci. Wadą tego rozwiązania jest stałe powiązanie z wynajmującym sprzęt dostawcą. Sumaryczny koszt korzystania z wyposażenia jest zbliżony, ponieważ z jednej strony wynajmujący odnosi dodatkowe korzyści z wynajmu, z drugiej jednak jego koszty ze względu na fachowość i skalę działania są mniejsze.

W przypadku omawianego przedsięwzięcia najlepszy wydaje się wariant mieszany, gdzie wszelkie adaptacje związane z obiektami powinny być finansowane ze środków własnych, natomiast wyposażenie mogłoby być wynajmowane.

7. Wnioski

Studium wykazuje możliwość zbudowania sieci dla potrzeb Państwa nawet w jednym rzucie przy wykorzystaniu przedstawionych wyżej możliwości. Nie wydaje się potrzebnym udowadnianie, że system oddany w całości jest bardziej ekonomiczny. Podstawowy koszt musi być poniesiony na wstępie na budową jądra systemu, natomiast koszty jego zakończeń są mniejsze. Efekty natomiast związane są z wykorzystaniem zakończeń systemu, dla których jądro jest koniecznym, ale nieużytecznym bezpośredni zapleczem.

Mało jest jednak prawdopodobnym porozumienie zainteresowanych budową wspólnego systemu łączności. Raczej należy się spodziewać walki o pozycję głównego realizatora. Walka ta jest łatwa ponieważ odbywa się w oderwaniu od trudności związanych z budową i utrzymaniem systemu, a nakierowana jest na potencjalne, polityczne korzyści związanego z jego posiadaniem.

W takiej sytuacji prawdopodobnie głównym realizatorem będzie ten, kto pierwszy taki system uruchomi i to przy pomocy sił własnych, bez wchodzenia w nieuniknioną kolizję z "konkurentami" przy zdobywaniu środków budżetowych.

Warszawa maj 1999 r.

- klucz publiczny, który jest ogólnie dostępny
- klucz prywatny, który jest znany tylko właścicielowi klucza

Klucz publiczny powinien być dostępny w sieci, zaś klucz prywatny musi być przechowywany w sposób bezpieczny, uniemożliwiający jego przejęcie przez osoby niepowołane.

Klucz prywatny nadawcy może być użyty do wygenerowania podpisu cyfrowego, pozwalającego na identyfikację nadawcy wiadomości (usługa niezaprzeczalności nadawcy), jak również integralności przesyłanych danych.

Certyfikacja Kluczy Publicznych

Klucze publiczne, przetrzymywane z prawami tylko do czytania w bezpiecznym miejscu, zapewniają tylko podstawowe formy ochrony przed modyfikacją lub podmianą tych kluczy. Niemniej jednak istnieje możliwość podszycia się pod właściciela danego klucza i oszukania osoby, z którą prowadzona jest korespondencja. Taka możliwość w praktyce wymusza stosowanie mechanizmu, który by potwierdzał autentyczność używanego klucza i prawo do korzystania z niego. Takim mechanizmem jest proces certyfikacji klucza.

Certyfikat jest dokumentem cyfrowym, który przypisuje klucz publiczny do osoby, aplikacji lub serwisu. Zaufany Urząd Certyfikacji (Certificate Authority – CA) tworzy certyfikat i podpisuje go cyfrowo, używając prywatnego klucza Urzędu Certyfikacji. Urząd Certyfikacji jest więc podstawowym, centralnym składnikiem PKI.

Składniki i Funkcje PKI

PKI składa się z trzech zasadniczych części:

- Urzędu Certyfikacji (CA), jednostki wydającej certyfikaty, uznanej jako Zaufana Trzecia Strona (Trusted Third Party), składającej się zazwyczaj z jednego lub kilku serwerów.
- „Składnicy" dla kluczy, certyfikatów i List Certyfikatów Unieważnionych (Certificate Revocation Lists – CRLs), bazującej zazwyczaj na protokole LDAP (Light-wight Directory Access Protocol.
- Funkcję zarządzania, typowo obsługiwaną poprzez konsolę zarządzania

Jeżeli PKI umożliwia automatyczną funkcję odzyskiwania klucza (*key recovery)*, również tego typu serwis może być udostępniony.

Dodatkowo może zostać uruchomiony Urząd Rejestracji (Registration Authority – RA), jednostka dedykowana do rejestracji użytkownika występującego o wydanie certyfikatu. Rejestracja użytkownika jest procesem zbierania informacji o użytkowniku i ich weryfikacji, co jest konieczne dla podjęcia decyzji o wydaniu certyfikatu. RA może być jednostką wydzieloną lub wchodzącą w skład Urzędu Certyfikacji (CA).

Należy pamiętać, że zarówno CA, jak i RA mogą być zaimplementowane na różne sposoby, zarówno jeśli chodzi o rozwiązania sprzętowe jak i programistyczne. W szczególności CA może być zaimplementowane na jednym lub więcej serwerze, określanym jako Serwer Certyfikacji lub odpowiednio Serwer Rejestracji.

Zaufanie
Każdy użytkownik klucza publicznego musi posiadać klucz publiczny od CA, który jest w pełni zaufaną stroną. Organizacje mogą dla własnych wewnętrznych celów utrzymywał własny Urząd Certyfikacji, jednak przy kontaktach wykraczających pza granice oddziaływania danego Urzędu konieczne jest korzystanie z hierarchicznego układu Urzędów Certyfikacji.

Ścieżka Procesu Certyfikacji
Najbardziej znaną architekturą opisującą ścieżkę procesu certyfikacji jest ta wykorzystywana w Infrastrukturze Klucza Publicznego takich organizacji jak np. VeriSign i wygląda następująco:

1. *Jednostka Centralna* na szczycie hierarchii.
2. Jednostka Centralna certyfikuje *podstawowe władze certyfikacji (primary certifikation authorities – PCAs)*, które wydają, zawieszają i odwołują certyfikaty dla wszystkich Urzędów Certyfikacji w hierarchii.
3. PCAs certyfikują CAs. PCAs mogą także certyfikować się wzajemnie (cross-certyfikation)
4. CAs autoryzują podległe CAs , które należą do serwisu PKI firmy lub klienta.
5. Na najniższym poziomie hierarchii znajdują się *lokalne władze rejestracyjne (local registration authorities – LRAs)*, które mogą przyjąć zapytanie o certyfikat w imieniu certyfikującej Jednostki Centralnej, PCA, lub CA, które wydają certyfikat.

Jeśli użytkownik nie ufa urzędowi, który podpisał certyfikat, może odpytać wyższy w hierarchii CA, któremu ufa.

Cross-certyfikacja
Określony CA może wydać certyfikat drugiemu CA, który pozwala na wydanie przez drugi CA certyfikatu, który będzie rozpoznawany przez pierwszy CA. Cross-certyfikacja nie wymaga angażowania ZaufanejTrzeciej Strony.

Oznaczanie czasu

Oprócz potwierdzania ważności i autentyczności transakcji sieciowej, również ważnym może okazać się ustalenie dokładnego czasu transakcji. Na przykład transakcja, aby być ważną, musi być dokonana przed upływem oznaczonego czasu. Potwierdzeniem tego może być połączenie podpisu cyfrowego z oznaczeniem czasu. Może to być dokonane poprzez dołączenie do struktury PKI serwisu oznaczania czasu.

Zarządzanie okresem ważności certyfikatu

PKI spełnia pewne funkcje, takie jak wydawanie certyfikatu i publikowanie list z certyfikatami unieważnionymi (CRL). W odróżnieniu od tego funkcje związane z okresem ważności certyfikatu, takie jak uaktualnianie, archiwizacja i tworzenie kopii zapasowych są spełniane w sposób sformalizowany. Każdy użytkownik posiada zazwyczaj jedną parę kluczy dla każdej aplikacji, klucze te wymagają kontroli i zarządzania z punktu widzenia okresu ich ważności.

BEZPIECZNA STRUKTURA INFORMATYCZNA W PRZEDSIĘBIORSTWIE W OPARCIU O SYSTEMY OTP (ONE-TIME-PASSWORD) I SSO (SINGLE-SIGN-ON)

Mirosław Maj, Krzysztof Silicki

Wprowadzenie

Postępujący wzrost wymagań w stosunku do bezpieczeństwa transakcji elektronicznych dokonywanych w sieciach otwartych (tzw. e-commerce) jak również w ramach firmowej sieci lokalnej czy korporacyjnej (np. dostęp do sieciowych aplikacji bazodanowych) stymuluje rozwój takich technologii jak PKI (infrastruktura klucza publicznego), które w prosty i bezpieczny sposób realizują bezpieczeństwo transakcji rozumiane jako zapewnienie usług uwierzytelniania, poufności, niezaprzeczalności i podpisu cyfrowego przy pomocy aplikacji wykorzystujących kryptografię.

Korzyści i możliwości wynikające ze stosowania techniki kluczy publicznych będącej podstawą PKI są tak duże z punktu widzenia ochrony danych, że należy sobie zadać pytanie jakie warunki muszą zaistnieć aby stosowanie aplikacji wykorzystujących infrastrukturę klucza publicznego było pozbawione zagrożeń dla bezpieczeństwa.

Jednym z podstawowych warunków bezpieczeństwa użytkowania PKI jest zapewnienie ochrony dostępu do kluczy prywatnych użytkowników biorących udział w transakcjach elektronicznych. W tym znaczeniu dużej wagi nabiera na przykład zastosowanie różnych form kart inteligentnych (ang. smartcard) sprzęgniętych z aplikacjami sterującymi dostępem do komputerów, sieci lokalnych, systemów bazodanowych w przedsiębiorstwie, które mogą zostać zastosowane dla realizacji bezpiecznego SSO (single-sign-on) w ramach danej sieci. Maksymalne bezpieczeństwo struktury informatycznej w przedsiębiorstwie uzyskuje się natomiast poprzez zaimplementowanie – wspólnie z technologiami wymienionymi powyżej - idei bezpiecznych, jednorazowych haseł dostępu do zasobów w oparciu o systemy typu OTP (one-time-password).

W niniejszym referacie zostanie zaprezentowany przykład realizacji bezpiecznej struktury informatycznej w przedsiębiorstwie w oparciu o nowoczesne, przyszłościowe rozwiązania.

Karty inteligentne

W systemach klucza publicznego każdy użytkownik posiada parę kluczy kryptograficznych zwanych kluczem publicznym i kluczem prywatnym. Dodatkowo użytkownik legitymuje się cyfrowym certyfikatem potwierdzającym związek osoby z kluczami. Wszystko to są to ciągi bitów, które powinny być przechowywane w określony sposób, tak aby zapewnić ich dostępność w czasie przeprowadzania bezpiecznej transakcji (np. szyfrowanego dostępu do firmowej aplikacji SAP). Klucze i certyfikaty mogą być przechowywane w różny sposób: na dysku komputera lokalnego, na dyskietce, na dysku serwera bądź na karcie inteligentnej. W przypadku klucza prywatnego użytkownika kluczową sprawa dla bezpieczeństwa jest właściwa ochrona dostępu do klucza , tak aby zapewnić, że nikt inny oprócz właściciela klucza nie jest w stanie nim się posłużyć. Klucze są więc chronione poprzez hasło lub PIN. W przypadku kluczy składowanych na dyskach lokalnych

Systemy SSO

Idea SSO (ang. single-sign-on) polega na tym aby w sposób bezpieczny zidentyfikować i zweryfikować użytkownika w pojedynczym procesie komunikacji z systemem w czasie pierwszego logowania do systemu w danej sesji a następnie automatycznie zezwolić na dostęp tego użytkownika do zasobów zdefiniowanych w centralnej bazie. W ten sposób użytkownik w zakresie posiadanych praw dostępu (zdefiniowanych przez np. administratora bezpieczeństwa) po pozytywnym uwierzytelnieniu w czasie zalogowania do sieci uzyskuje w danej sesji dostęp do określonych komputerów, aplikacji, baz danych itp.

Oczywistym faktem jest, że w takim scenariuszu krytyczne jest dobranie takich mechanizmów bezpieczeństwa, które zapewnią, że uwierzytelnianie i autoryzacja – mimo, ze dokonywana „w imieniu" użytkownika będą odporne na rozmaite zagrożenia (np. podszywanie się, przechwytywanie sesji). Jest to możliwe tylko i wyłącznie przy zastosowaniu nowoczesnych i mocnych mechanizmów kryptograficznych i struktury PKI.

Niezawodność i bezpieczeństwo

W systemach SSO kluczową sprawą jest zapewnienie mocnego uwierzytelnienia na etapie dostępu do uprawnień. Hasło, które jest kluczem do wielu systemów i/lub aplikacji nie może być statyczne a sesja użytkownika z serwerem powinna być szyfrowana algorytmem o odpowiedniej mocy kryptograficznej. Centralny serwer uwierzytelniający jest w systemach SSO czułym miejscem: może stanowić obiekt ataków a także nie było by dobrze gdyby stał się pojedynczym punktem awarii (ang. single point of failure). Serwery SSO muszą zapewniać redundancję.

Przykładowy system bezpiecznego dostępu do zasobów w ramach przedsiębiorstwa

Założywszy, że użytkownik jest wyposażony w kartę inteligentną rzeczywistą lub wirtualną, na której posiada swoje klucze i certyfikaty możemy zaproponować bezpieczne rozwiązanie komunikacji użytkownika z zasobami, do których dostęp musi być chroniony. Rozwiązanie zostanie omówione na przykładzie systemu Keon firmy Security Dynamics. Keon składa się z kilku elementów:

- *Oprogramowanie na stację roboczą (Keon Desktop)*

Oprogramowanie stacji użytkownika pozwala na bezpieczną komunikację i selektywne szyfrowanie zawartości dysków lokalnych. Zapewnia transparentne szyfrowanie sesji przy dostępie do serwerów i aplikacji, zabezpieczenie przed nieuprawnionym wykorzystaniem certyfikatów i kluczy prywatnych, wykorzystanie podpisu cyfrowego w celu uwierzytelnienia komunikujących się procesów. Podstawową funkcją jest zapewnienie dostępu do komputerów i aplikacji w rozproszonym, heterogenicznym środowisku teleinformatycznym przedsiębiorstwa czy organizacji.

RAPORT CERT NASK W ZAKRESIE BEZPIECZEŃSTWA SIECI W 1998 R.

Krzysztof Silicki, Mirosław Maj

CERT NASK

CERT NASK został powołany do życia z uwagi na gwałtowny wzrost społecznego naczenia Internetu oraz ogólniej transmisji w sieciach komputerowych, szczególnie w kontekście ponadgranicznej wymiany danych (naukowych, ekonomicznych, komercyjnych, innych) oraz związany z tym nieuchronnie proces zagrożenia bezpieczeństwa pracy z siecią komputerową.

Działania CERT NASK, mające charakter służby na rzecz podnoszenia poziomu świadomości i realnego bezpieczeństwa pracy użytkowników sieci są prowadzone w wielu krajach poprzez zespoły reagujące na zdarzenia naruszające bezpieczeństwo sieci (ang: IRT - Incident Response Team).

Do zadań tego zespołu należy:

- rejestrowanie zdarzeń naruszających oraz bezpośrednio zagrażających bezpieczeństwu sieci NASK, sieci abonentów NASK oraz sieci innych operatorów na teranie Polski,
- natychmiastowe podejmowanie czynności takich jak: diagnozowanie, analizowanie, znoszenie lub pomoc w znoszeniu skutków zdarzeń naruszających lub bezpośrednio zagrażających bezpieczeństwu sieci NASK i sieci abonentów NASK oraz czynności zapobiegających powstawaniu tych zdarzeń w przyszłości,
- alarmowanie użytkowników sieci o wystąpieniu bezpośrednich dla nich zagrożeń,
- współpraca z zespołami o podobnym charakterze działającymi samodzielnie lub będącymi częścią innych podmiotów prawnych (krajowych i zagranicznymi, w tym współpraca w ramach FIRST) oraz osobami odpowiedzialnymi za bezpieczeństwo sieci w poszczególnych instytucjach dołączonych do sieci,
- prowadzenie działalności informacyjno-zapobiegawczej mającej na celu podniesienie świadomości i troski użytkowników o właściwy stan bezpieczeństwa sieci

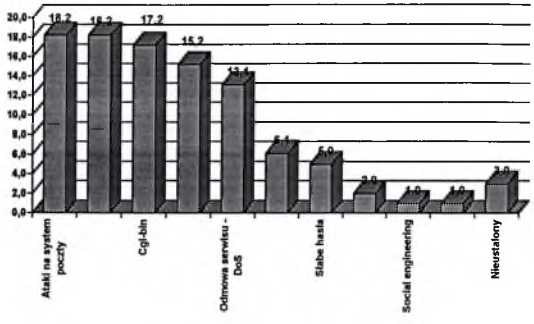
Raport CERT NASK 1998

Podobnie jak w roku 1997, również w roku 1998 odnotowaliśmy poważny wzrost liczby zarejestrowanych incydentów naruszających bezpieczeństwo.

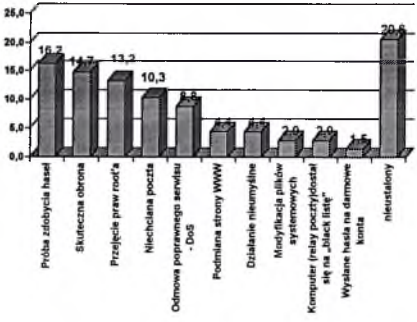
Rozkład czasowy
Ataki te odnotowywane były w przeciągu całego roku z nasileniem na takie miesiące jak marzec i październik, szczególne nasilenie tego procesu w październiku może być spowodowane aktywnością środowiska akademickiego, z którego jak wskazuje statystyka wywodzi się najwięcej ataków.

Typ ataku
Wśród ataków prym wodzą te, które jako cel obrały sobie system poczty elektronicznej. Poważna część z tych ataków związana jest z popularnością, i dużą ilością dziur w oprogramowaniu *sendmail*. Poważnym problemem okazało się też skanowanie sieci, czy też

Wykres nr1. Procentowy rozkład typów ataków, 1998.



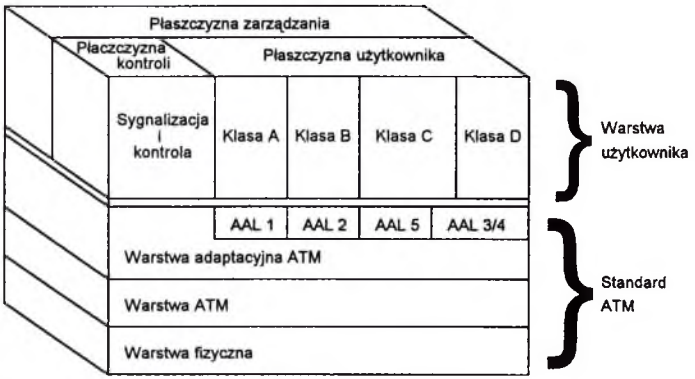
Wykres nr 2. Procentowy rozkład efektów ataków, 1998.



Typ ataku	Ataki na system poczty	skanowanie	Cgi-bin	Spam	Odmowa serwisu - DoS	DNS	Słabe hasła	Rozpowszechnia nie nielegalnych i obraźliwych treści	Social engineering	NFS	Nieustalony	
	18,2	18,2	17,2	15,2	13,1	6,1	5,0	2,0	1,0	1,0	3,0	
Efekt	Próba zdobycia haseł	Skuteczna obrona	Przejęcie praw root'a	Niechciana poczta	Odmowa poprawnego serwisu - DoS	Podmiana strony WWW	Działanie nieumyślne	Modyfikacja plików systemowych	Komputer (relay poczty)dostał się na „black listę"	Wysłane hasła na darmowe konta	nieustalony	
	16,2	14,7	13,2	10,3	8,8	4,4	4,4	2,9	2,9	1,5	20,6	
Źródło	Uczelnia, instytut, szkoła	TPNET	Konto u provider'a	Użytkownik zagraniczny	Darmowe konta	Niezwiązany (no: socila engineering)	Konto w firmie	Nieustalone				
	29,4	25,6	11,8	7,3	6,1	3,6	2,4	20,7				
Miesiąc	Styczeń	Luty	Marzec	Kwiecień	Maj	Czerwiec	Lipiec	Sierpień	Wrzesień	Październik	Listopad	Grudzień
	2,4	4,7	14,1	9,4	5,9	8,2	9,4	9,4	10,6	18,8	4,7	2,4
Źródło zgłoszenia	Użytkownik krajowy	Użytkownik zagraniczny	IRT	Policja								
	48,8	27,9	22,1	1,2								

Tabela nr 1. Procentowy rozkład zarejestrowanych incydentów, CERT NASK 1998.

ITU i ETSI. Wykorzystanie protokołu IP w sieciach ATM jest zdefiniowane w dokumentach RFC IETF. Przy omawianiu aspektów bezpieczeństwa w niniejszym artykule posługujemy się modelem odniesienia, który uwzględnia trzy płaszczyzny odpowiadające zakresowi działania użytkownika, kontroli (sygnalizacji) i zarządzaniu siecią.



Rys. A. Model odniesienia dla ATM

3. Bezpieczeństwo sieci ATM w normach i zaleceniach

Ciała normatywne zaangażowane w prace standaryzacyjne dotyczące ATM rozpoczęły prace w zakresie bezpieczeństwa stosunkowo niedawno. W serii zaleceń ITU-T znajdziemy rekomendacje dla sieci transmisji danych i otwartych systemów telekomunikacyjnych (np. X.800 - X.835) oraz kilka zaleceń poruszających problem wybranych elementów bezpieczeństwa w sieci ATM wydanych w serii I (I.251, I.255, I.259). W serii M znajdziemy zalecenia mające charakter edukacyjny. Prace ITU-T generalnie nie mają charakteru systematycznie opracowanych zestawów zaleceń dla sieci ATM.

W październiku 1995 w ATM Forum został powołany zespół roboczy, którego celem było „zidentyfikowanie problemów bezpieczeństwa wynikających ze stosowanych rozwiązań technicznych oraz określenie metod badawczych tej problematyki". Opracowania tej grupy są opóźnione i nie wszystkie zostały przyjęte przez ATM Forum. Planowane na lipiec 1998 zatwierdzenie dokumentu „ATM Security Specification Version 1.0" [k] nie zostało dokonane, to samo dotyczy „UNI Signaling 4.0 Security Addendum" [j]. Z serii dotyczącej bezpieczeństwa w sieci ATM został zatwierdzony „ATM Security Framework 1.0" [b]. Jest to podstawowe i w chwili pisania artykułu jedyne zalecenie dotyczące wyłącznie bezpieczeństwa w sieciach ATM.

4. Prace prowadzone w ATM Forum

W zaleceniu **„ATM Security Framework 1.0"** zatwierdzonym przez ATM Forum w lutym 1998 roku, zawarte są ustalenia dotyczące podstawowych wymagań stawianych usługom bezpieczeństwa w sieci ATM. Nie są uwzględniane specyficzne aspekty bezpieczeństwa użytkowników ATM i takich zastosowań, jak sieci bezprzewodowe ATM, łączność szerokopasmowa o ograniczonym zasięgu, zarządzanie siecią ATM. Dokument ten będzie dalej rozwijany. Zawiera stabilne definicje dotyczące podstawowych elementów bezpieczeństwa, zagrożeń, wymagań funkcjonalnych i usług bezpieczeństwa, oraz częściową

Wymagania funkcjonalne w zakresie bezpieczeństwa, które powinny być w całości lub w części spełnione przez otwartą sieć ATM zawierają się w „dziesięciu przykazaniach":

1. **Weryfikacja tożsamości**
   (AF SEC-1) - Sieć ATM powinna zawierać mechanizmy pozwalające ustalić i sprawdzić tożsamości wszystkich podmiotów.
2. **Kontrola dostępu i upoważnienie**
   (AF SEC-2) - Sieć ATM powinna zawierać mechanizmy zapobiegania nieupoważnionemu dostępowi do informacji i zasobów.
3. **Ochrona poufności**
   (AF SEC-3) - Sieć ATM powinna zawierać mechanizmy pozwalające zachować poufność przechowywanych i przesyłanych danych.
4. **Ochrona integralności danych**
   (AF SEC-4) - Sieć ATM powinna zawierać mechanizmy zapewnienia integralności przechowywanych i przesyłanych danych.
5. **Bezwzględna odpowiedzialność**
   (AF SEC-5) - Sieć ATM powinna zawierać mechanizmy uniemożliwiające podmiotom uniknięcia odpowiedzialności za swoje działania, jak również za efekty tych działań.
6. **Rejestracja zdarzeń**
   (AF-SEC-6) - Sieć ATM powinna zawierać mechanizmy pozyskiwania zgromadzonych w Elementach Sieci informacji związanych z bezpieczeństwem z możliwością odszukania w tej informacji osób lub podmiotów.
7. **Raportowanie o alarmach**
   (AF SEC-7) - Sieć ATM powinna zawierać mechanizmy generacji alarmów powiadamiających o pewnych regularnych i wybranych zdarzeniach związanych z bezpieczeństwem.
8. **Audyt**
   (AF SEC-8) - Sieć ATM powinna zawierać mechanizmy do analizy i eksploatacji zarejestrowanych danych o zdarzeniach związanych z bezpieczeństwem żeby sprawdzić je pod kątem naruszenia bezpieczeństwa systemu i sieci.
9. **Przywracanie bezpieczeństwa, zarządzanie bezpieczeństwem**
   (AF SEC-9) - Sieć ATM powinna zawierać mechanizmy służące przywróceniu bezpieczeństwa po jego udanym i zamierzonym naruszeniu
10. **Zarządzanie bezpieczeństwem**
    (AF SEC-10) - Sieć ATM powinna zawierać mechanizmy kierowania usługami w zakresie bezpieczeństwa.

W tabeli (tabela b) przedstawiono przegląd zasadniczych wymagań funkcjonalnych w zakresie bezpieczeństwa zapobiegających podstawowym zagrożeniom. „Tak" w tabeli oznacza, że specyficzne zagrożenie (np. „maskarada") prowadzi do określonego wymagania funkcjonalnego w zakresie bezpieczeństwa (np. „weryfikacja tożsamości"). Należy zwrócić uwagę, że pojedyncze zagrożenie może wymagać więcej niż jednego zabezpieczenia.
„Przywracanie bezpieczeństwa/Zarządzanie bezpieczeństwem" to wymaganie warunkowe rozumiane następująco: tak długo, jak długo pojawia się „tak" w pozostałych kolumnach w odpowiednim rzędzie, „Przywracanie bezpieczeństwa/Zarządzanie bezpieczeństwem" jest wstępnym warunkiem gwarantującym wszystkie pozostałe.
W tabeli (tabela c) przedstawiono odwzorowanie wymagań w zakresie bezpieczeństwa na usługi bezpieczeństwa, które gwarantuje wypełnienie tych wymagań. Dla każdego z wymagań bezpieczeństwa wskazano podstawowe usługi bezpieczeństwa.

Specyficzne dla poszczególnych płaszczyzn usługi w zakresie bezpieczeństwa wymagają usług wspierających. Wymienione są następujące usługi wspierające:

- protokoły wymiany komunikatów bezpieczeństwa i podstawowych negocjacji,
- przesyłanie komunikatów dotyczących bezpieczeństwa w płaszczyźnie kontrolnej,
- przesyłanie komunikatów dotyczących bezpieczeństwa w płaszczyźnie użytkownika,
- wymiana kluczy,
- aktualizacja klucza sesji,
- certyfikacja.

„ATM Security Specification, wersja 1.0" będzie dokumentem (nie jest oficjalnie zatwierdzony) obejmującym szczegółowe zalecenia dotyczące sposobu wdrożenia usług bezpieczeństwa w sieci ATM w płaszczyźnie użytkownika i kontroli oraz funkcji wspomagających. Nie są definiowane usługi dotyczące płaszczyzny zarządzania. Jednakże funkcje, które są zdefiniowane dla połączeń w płaszczyźnie użytkownika są zalecane do użytku w płaszczyźnie zarządzania. Zasięg tej specyfikacji jest ograniczony do ochrony sieci ATM, tzn. że mechanizmy muszą być wdrożone w warstwie ATM lub w warstwach adaptacyjnych ATM (AAL).

W specyfikacji tej zgodnie z definicjami i modelem zaprezentowanym w ATM Security Framework sprecyzowano zakres działania usług bezpieczeństwa.:

- **Usługi bezpieczeństwa w płaszczyźnie użytkownika**

Usługi te są określone dla połączeń od końca do końca, dla każdego połączenia wirtualnego (zarówno dla wirtualnego łącza VCI i ścieżki VPI). Funkcje te nie dotyczą łącza fizycznego. Zakres definicji obejmuje połączenia typu SVC, punkt-punkt i punkt - wiele punktów.

- **Uwierzytelnienie (AUTH)**

Usługa uwierzytelniania obejmuje kontrolę tożsamości strony wywołującej i wywoływanej w momencie nawiązywania połączenia. Uwierzytelnienie może być jedno lub dwustronne oraz powinno się opierać się na kluczach jednokrotnych i podpisach cyfrowych.

- **Poufność (CONF)**

Jest realizowana poprzez szyfrowanie danych w czasie transmisji. Szyfrowanie dotyczy wszystkich lub wybranych komórek ATM w części użytkowej komórki (ang. payload) i opiera się na algorytmach kryptograficznych wykorzystujących klucze symetryczne, które są uzgadniane w momencie nawiązywania połączenia. Szyfrowanie dotyczy warstwy ATM. Niektóre z komórek (komórki OAM i RM) mimo iż stanowią część szyfrowanego łącza VC użytkownika są przepuszczane bez szyfrowania i transmitowane w postaci jawnej.

- **Integralność (INTEG)**

Usługa integralności jest dostępna jedynie dla wirtualnych łączy (VCI) nie jest implementowana w ścieżkach wirtualnych (VPI). Usługa ta opiera się na sumie kryptograficznej (funkcja haszująca lub sygnatura cyfrowa) dołączanej w warstwie adaptacyjnej ATM AAL3/4 lub AAL5 w „części wspólnej" jednostki danych. Dostępne są dwie funkcje zapewniające integralność danych z zabezpieczeniem przed powtórką/zmianą kolejności i bez takiego zabezpieczenia. Funkcje zapewnienia integralności są ulokowane w warstwie adaptacyjnej (AAL).

- **Kontrola dostępu (ACC)**

Jest realizowana podczas zestawiania połączenia. Decyzja kontroli dostępu - jeżeli jest to konieczne - może być podjęta w każdym urządzeniu ATM leżącym w ścieżce połączenia. Tylko jeden algorytm oparty o mechanizm kontroli dostępu na

Certyfikacja ATM opiera się na zaleceniu X.509v1 kiedy wymiana certyfikatów jest realizowana w kanale sygnalizacji. Dla realizacji wymiany certyfikatów wewnątrz pasma wykorzystuje się zalecenia X.509v1, X509v2, i X509v3. Podczas wymiany certyfikatów kluczy publicznych używa się protokołu bezpiecznej wymiany danych

Innym dokumentem ATM Forum jest **„UNI Signaling 4.0 Security Addendum"** będący w fazie przygotowania. Zawiera procedury sygnalizacji niezbędne do realizacji usług bezpieczeństwa. Podstawą wymiany sygnalizacji jest decyzja zdefiniowanego w specyfikacji agenta bezpieczeństwa, który po przetworzeniu informacji dotyczących bezpieczeństwa przyjmuje lub odrzuca wywołanie. Agent bezpieczeństwa jest funkcjonalnie ulokowany w płaszczyźnie kontroli. W cytowanym dokumencie nie definiuje się wewnętrznych funkcji agenta. Istotne zmiany w specyfikacji sygnalizacji UNI 4.0 są związane z nowymi Elementami Informacyjnymi (SSIE) i obsługą protokołów trójstronnej wymiany w czasie zestawiania połączenia. zasadniczo wszystkie zmiany w procedurach sygnalizacyjnych związane są z wprowadzeniem agenta bezpieczeństwa i dodatkowego komunikatu CONNECT ACKNOWLEDGE i związanego z tym przetwarzania.

5. Bezpieczeństwo w sieci ATM i protokół IP

Podstawowe problemy związane z bezpieczeństwem sieci ATM wynikają z przenoszenia protokołów sieci pakietowych a w szczególności protokołu IP. Jeżeli protokół IP jest przenoszony przez kanał typu PVC poziom bezpieczeństwa jest zbliżony do sytuacji w której wykorzystujemy łącza dzierżawione. Jeżeli wykorzystujemy usługi obejmujące jakąkolwiek sygnalizację ATM pojawiają się dodatkowe elementy mające wpływ na bezpieczeństwo sieci. Wiele standardów IETF zaleca używanie rozszerzonych możliwości sygnalizacji w celu poprawnego odwzorowania usług IP w sieć ATM [n],[o]. W dokumentach IETF można znaleźć dokumenty zawierające analizę problematyki bezpieczeństwa [p], [q].
Przykładem protokołów, które są dedykowane dla sieci ATM są CLIP [m] (ang. Classical IP over ATM), MARS [n] (ang. Multicast Addres Resolution Servers) i NHRP [o] (ang. Next Hop Routing Protocol).
Powyższe protokoły wykorzystując sygnalizację UNI 3.0/3.1 realizują:

- podstawowe połączenia IP w obrębie tej samej podsieci IP (CLIP),
- wewnątrzsieciowe połączenia rozsiewcze (MARS),
- połączenia pomiędzy hostami i ruterami w różnych podsieciach IP (NHRP).

Wszystkie problemy bezpieczeństwa występujące w tych technikach mają swoje źródło w dwóch podstawowych słabościach ochrony sieci ATM:

- braku mechanizmu uwierzytelniania hosta,
- braku kontroli dostępu.

We wszystkich przypadkach istnieje możliwość wstawienia przez host fałszywego adresu w polu „Calling Address Information Element" w komunikatach zestawiania połączenia (ang. SETUP). Stanowi to poważny problem ponieważ możliwe jest wykorzystanie fałszywego adresu IP i względnie proste oszukanie systemów kontroli dostępu, które opierają się na adresach IP. ATMARP serwer jest całkowicie nieodporny na „zatrucie bazy danych" (ang. database poisoning) przez intruza. Pozwala to na skanowanie obszaru adresowego obsługiwanej sieci. Możliwe jest również stosując tę samą technikę aktywowanie fałszywego ATMARP serwera.
W protokole MARS istnieje możliwość dołączenia się do dowolnej grupy i odbieranie jej całego ruchu. Wystarczy zdobyć adres NSAP serwera MARS. Przy niewielkiej znajomości topologii wybranej sieci możliwe jest przeprowadzenie wielu różnych ataków na serwery i klientów systemu.

duże i wymaga zastosowania odpowiednich mechanizmów bezpieczeństwa. Oprócz tych dobrze znanych zagrożeń, sieć ATM wprowadza nowe protokoły, których bezpieczeństwo nie jest jeszcze w pełni znane. Możliwe są ataki oparte o protokoły ILMI i P-NNI

Kolejnym istotnym wnioskiem jest to, że przełączniki ATM są bardzo ważnym elementem bezpieczeństwa sieci. ATM oferuje „wspólną kontrolę" zasobów sieci. Ta cecha jest podstawą dla mechanizmów kontroli dostępu w przełącznikach ATM. Przykładem zabezpieczenia sieci jest ustawienie filtrów adresów ATM dla kontroli dostępu. Do pełnego zabezpieczenia sieci muszą być użyte filtry adresów ATM w kombinacji z zaporą sieciową (ang. firewall).Wymaga to konfiguracji trzech podsieci (wewnętrznej, zewnętrznej i tzw. „strefy zdemilitaryzowanej") zamiast dwóch (wewnętrznej i zewnętrznej).

Przełączniki odpowiednio (statycznie) skonfigurowane mogą być użyte do ochrony przed niektórymi atakami typu blokowanie usługi. Jest to konieczne w przypadku, gdy protokoły oparte na ATM, takie jak P-NNI i ILMI, nie oferują wiarygodnego mechanizmu autoryzacji.

Wiele problemów bezpieczeństwa ma swoje źródło w konfiguracjach „Plug and Play". Producenci starają się, aby ich przełączniki były wyposażone w narzędzia automatycznej konfiguracji (takie jak ILMI), które pozwalają na łatwe skonfigurowanie sieci. Ale bezpieczeństwo sieci wymaga dokładnej i przemyślanej konfiguracji przełączników, protokołów oraz urządzeń (np. firewall), mających wpływ na dostęp do sieci.

Ciała normatywne zaangażowane w prace standaryzacyjne dotyczące ATM rozpoczęły prace w zakresie bezpieczeństwa od niedawna. Z tego powodu nie istnieją spójne zalecenia obejmujące wszystkie aspekty bezpieczeństwa w sieciach ATM. Prace normalizacyjne są obecnie zaawansowane w wybranych aspektach problematyki bezpieczeństwa. Nie ma powszechnie dostępnych materiałów przedstawiających poziom wdrożenia zaleceń bezpieczeństwa w produkowanych urządzeniach sieciowych.

W oczekiwaniu na wdrożenia funkcji bezpieczeństwa w urządzeniach sieciowych już dzisiaj możemy chronić nasze sieci używając konsekwentnie systemu list dostępu ATM, które pozwolą zdefiniować użytkowników na zasadzie „swój - obcy". W starszych przełącznikach jedyną metodą może być obsługa ruchu w trybie połączeń statycznych z wyłączeniem sygnalizacji. Odpowiadając na pytanie zawarte w tytule - sieci ATM nie są bezpieczne jeżeli administratorzy systemów nie zdają sobie sprawy z potencjalnych zagrożeń. Obecnie bezpieczeństwo sieci ATM zależy przede wszystkim od umiejętności administratorów wykorzystujących elementy bezpieczeństwa implementowane w poszczególnych urządzeniach. Wydaje się, że należałoby przeprowadzić badania eksperymentalne, które pozwoliłyby ocenić bezpieczeństwo sieci ATM budowanych w Polsce. Jako kryterium porównania różnych rozwiązań sprzętowych i programowych należałoby przyjąć zalecenia ATM Forum.

7. Literatura

[A]. D.J. Bem, W.E. Grzebyk, J.M. Janukiewicz; „Analiza zagrożeń i wymaganych środków ochrony dla transmisji w sieciach ATM i Frame Relay" wersja 1.0, Praca wykonana przez NASK na zlecenie Komitetu Badań Naukowych, grudzień 1998

[B]. ATM Forum 1998: Approved ATM Forum Specifications: „ATM Security Framework Version 1.0"; February, 1998

[C]. C. Benecke, U. Ellermann ;"Securing Classical IP over ATM Networks"; 7th USENIX Security Symposium, January 26-29, 1998, San Antonio, Texas,USA.

PROBLEMY „VOICE OVER IP"

Roman Adamiec

NASK

Ostatnie lata przyniosły ze sobą burzliwy rozwój różnych sposobów transmisji informacji. Jedną z dziedzin, która podlega takiemu rozwojowi jest VoIP - *Voice over IP.* Sama idea oraz technika znane są od lat - nowością jest masowość jej stosowania.

Technika VoIP jest próbą pogodzenia ze sobą dwóch zupełnie różnych "światów" - transmisji z wykorzystaniem protokołu TCP/IP jako warstwy podkładowej oraz transmisji głosu w warstwie użytkowej. Wyzwanie jest spore, ponieważ klasyczna telefonia oraz fizjologia człowieka wyznacza standardy, których niespełnienie jest po stronie użytkownika odbierane jednoznacznie jako usługa o znacznie gorszej jakości w stosunku do klasycznej telefonii.

Trudność polega na tym, że pomimo podobieństwa po stronie użytkownika do klasycznej telefonii (w obydwu przypadkach użytkownik końcowy korzysta z normalnego aparatu telefonicznego), VoIP jest zupełnie inną usługą. W przypadku klasycznej telefonii wybranie numeru innego abonenta i odebranie przez niego rozmowy powoduje zestawienie kanału pomiędzy nimi - poprzez wszystkich operatorów pośrednich w sposób niewidoczny dla użytkownika końcowego. Usługa polega tu na komutacji takich kanałów pomiędzy wieloma użytkownikami końcowymi. W wypadku VoIP nie ma żadnego kanału pomiędzy użytkownikami końcowymi - jest tylko sieć transmisji danych oparta na protokole TCP/IP np. Internet. Usługa polega więc na zamianie głosu na pakiety IP i ich transmisji do określonego punktu.

Tutaj właśnie zaczyna się pewna trudność: jakość odbieranego głosu wymaga spełnienia ściśle określonych parametrów technicznych. Wymaga, aby kolejne pakiety, niosące w sobie zakodowany głos, przychodziły w jednostajnym rytmie (izochronizm) z jak najmniejszym opóźnieniem. Niespełnienie tego wymagania powoduje natychmiastową utratę jakości połączenie - z utratą słyszalności włącznie. Trudność polega na tym, że protokół TCP/IP a w szczególności Internet nie był budowany z myślą o gwarancji pasma i izochronizmu. Skutkiem tego trzeba stosować bardzo wyrafinowane techniki, aby ją zapewnić.

Problem nie jest trudny do rozwiązania na małą skalę. Jednakże ostatnio doświadczamy wkraczania techniki VoIP w fazę masowego użytkowania i to niesie ze sobą określone konsekwencje, związane z niedostosowaniem sieci IP - rozumianej jako klasyczna sieć transmisji danych - do masowego przesyłania głosu. Chęć oferowania tej usługi na większą skalę pociąga za sobą konieczność posiadania przez operatora sieci podkładowej IP umożliwiającej zapewnienie dużej wydajności przesyłania pakietów informacji niosących głos. Łączą się z tym następujące zagadnienia:

1. zdolność do gwarantowania/rezerwacji pasma użytkowego - VoIP wymaga dedykowania każdej parze abonentów prowadzących rozmowę określonego pasma. W przypadku transmisji głosu poprzez TCP/IP niespełnienie tego wymogu powoduje natychmiastowe pogorszenie jakości.
2. zapewnienie minimalnego opóźnienia sieci IP - chęć oferowania VoIP na skalę masową narzuca spore rygory projektowe w stosunku do sieci podkładowej.
3. zdolność sieci do transmisji dużych ilości małych pakietów - przesyłanie głosu wiąże się z nadawaniem przez urządzenia końcowe tzw. "krótkich" pakietów. Odbiega to od

SATELITARNE SYSTEMY KOMUNIKACJI OSOBISTEJ

Daniel Józef Bem

Naukowa i Akademicka Sieć Komputerowa
Zakład Telekomunikacji
50-327 Wrocław, ul. Janiszewskiego 7/9, tel./faks: (71) 321 95 29

Streszczenie. Przedstawiono rolę satelitarnych systemów komunikacji osobistej w ogólnej koncepcji systemów komunikacji osobistej. Omówiono wymagania stawiane satelitarnym systemom komunikacji osobistej. Krotko scharakteryzowano cztery systemy: *Irydium*, *Globalstar*, *Teledesic* i *SkyBridge*.

1. Wprowadzenie

Współczesna telekomunikacja ma za zadanie zapewnić możliwość porozumiewania się ludzi i maszyn (komputerów) w każdych warunkach, tzn. bez względu na miejsce, w którym się znajdują (ląd, morze, powietrze, kosmos) i bez względu na to czy są w stanie spoczynku, czy też w ruchu. Komunikacja z abonentami ruchomymi jest możliwa tylko drogą radiową.

Abonenci ruchomi mają obecnie do dyspozycji wiele systemów radiokomunikacji ruchowej, oferujących różnego typu usługi. Wszystkie one stanowią rozszerzenie stacjonarnej sieci telekomunikacyjnej. Podstawową wadą tych systemów jest brak wzajemnej kompatybilności. Użytkownik korzystający z usług oferowanych przez systemy przywoławcze, komórkowe, czy bezprzewodowe musi mieć odpowiedni dla każdego z tych systemów terminal. Dodatkowo działanie tych systemów jest ograniczone do jednego kraju lub kilku krajów. Dopiero wprowadzenie w Europie systemu GSM doprowadziło do możliwości korzystania z systemu telefonii komórkowej na całym kontynencie, nie istnieje natomiast taki system o zasięgu światowym, choć GSM ma szansę stać się systemem globalnym[1)].

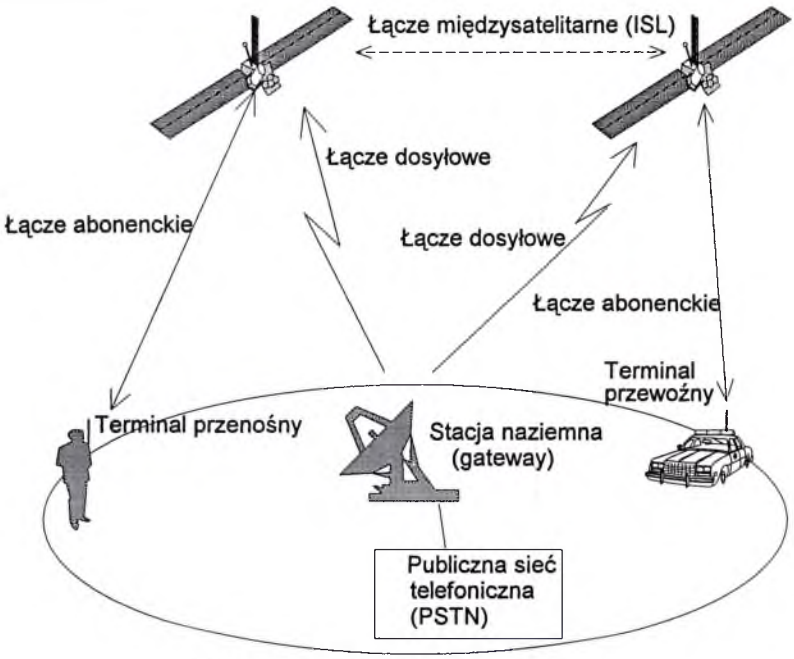
Wprowadzane obecnie do eksploatacji systemy telekomunikacyjne zmieniają swój charakter. Rozpoczyna się bardzo ważny proces personalizacji usług, co oznacza, że ostatnim elementem systemu nie będzie jak dotychczas urządzenie końcowe ze swoim własnym numerem, ale abonent z przypisanym mu na stałe numerem identyfikacyjnym, z którego będzie korzystał niezależnie od typu urządzenia jakiego będzie używał. Ze względu na coraz większą ruchliwość abonentów wszystkie usługi telekomunikacyjne muszą być dostarczane do różnych miejsc, w których znajduje się abonent. Powoduje to rozbudowę sieci radiotelefonii ruchowej i bezprzewodowej oraz systemów przywoławczych, a ponadto prowadzi do konieczności stworzenia połączeń międzysystemowych i integracji systemów.

Prowadzi się prace zmierzające do stworzenia systemu komunikacji osobistej. System taki ma zapewnić łączność z abonentem znajdującym się w dowolnym miejscu, stosując do tego celu różne sieci i różnego rodzaje terminale. Systemy komunikacji osobistej charakteryzują się następującymi właściwościami:

- mobilnością (oferowane usługi są niezależne od położenia abonenta i terminala);
- lokalizacją abonenta;
- dopasowaniem do abonenta (parametry usług są definiowane przez abonenta);
- dużą pojemnością i łatwym dostępem;

[1)] Początkowo akronim GSM oznaczał Groupe Spéciale Mobile - zespół roboczy powołany w roku 1982 do opracowania wspólnego dla całej Europy standardu telefonii komórkowej. W latach 90. akronimowi GSM nadano nowe znaczenie: Global System for Mobile communications (globalny system telekomunikacji ruchowej).

stałe stacje naziemne, które realizują typowe zadania związane z zarządzaniem siecią, takie jak: kierowanie ruchem, zarządzanie zestawianiem połączeń, monitorowanie sieci, wykrywanie błędów oraz inicjacja procedur awaryjnych. Oprócz tego - najczęściej jako oddzielne - instaluje się stacje naziemne, których zadaniem jest dokonywanie pomiarów telemetrycznych, śledzenie satelitów oraz zarządzanie konstelacją (korekcja parametrów orbit).



Rys. 1. Satelitarny system komunikacji ruchowej

3. Typy orbit

Orbity systemów S-PCN muszą być tak dobrane, aby można było uzyskać:

- akceptowalne opóźnienie,
- maksymalnie duży obszar działania systemu,
- możliwie duże kąty elewacji,
- możliwie małe tłumienie na trasie Ziemia - satelita.

Ze względu na wysokość orbit wyróżnia się trzy typy systemów:

- wysokość orbity 500 - 2000 km - systemy z satelitami na niskich orbitach (LEO - ang. *Low Earth Orbit*);
- wysokość orbity 8000 - 12000 km - systemy z satelitami na średnich orbitach (MEO - ang. *Medium Earth Orbit*, ICO - ang. *Intermediate Circular Orbit*);
- wysokość orbity około 36000 km - systemy z satelitami na orbicie geostacjonarnej (GSO - ang. *GeoStationary Orbit*).

MEO-p - (ang. *Medium Earth Orbit - polar*) - średnie orbity biegunowe. Kąt inklinacji $i = 90^{\circ}$. Mogą być zarówno kołowe, jak i eliptyczne. Łączność o zasięgu światowym.

MEO-i - (ang. *Medium Earth Orbit - inclined*) - średnie orbity nachylone. Kąt inklinacji $i \in (0, 90^{0})$. Mogą być kołowe lub eliptyczne.

HEO - (ang. *Highly Elliptical Orbit*) - wydłużone orbity eliptyczne (duży mimośród). Orbity tego typu są bardzo użyteczne dla systemów regionalnych. Umożliwiają one osiąganie dużych kątów elewacji (gdy satelita znajduje się na średnich i wysokich częściach orbity), co jest bardzo istotne w terenach górzystych i zurbanizowanych. Zaletą tych orbit jest niewielka liczba satelitów potrzebna do zapewnienia ciągłej łączności na planowanym obszarze, zwykle 2-10. Dla tego typu orbit zaleca się kąt inklinacji $i = 63{,}4^{0}$, co wiąże się z brakiem rotacji linii apsyd ($d\omega/dt = 0$).

ICO - (ang. *Intermediate Circular Orbit*) - średnie orbity kołowe. Są to właściwie kołowe orbity MEO.

GEO - (ang. *Geostationary Orbit*) - orbita geostacjonarna. Satelita geostacjonarny umożliwia zapewnienie łączności na całej powierzchni Ziemi z wyjątkiem rejonów podbiegunowych. Zaletą tej orbity jest to, że do zapewnienia łączności o zasięgu globalnym wystarczają trzy satelity. Wadą - jest duża wysokość orbity powodująca opóźnienie sygnałów i konieczność zwiększenia mocy zarówno terminala użytkownika, jak i nadajnika na satelicie.

4. Opóźnienie i tłumienie sygnału

Jednym z bardzo ważnych czynników jakie należy brać pod uwagę przy analizowaniu systemów satelitarnych jest opóźnienie sygnału. W systemach satelitarnych stanowiących elementy stacjonarnej publicznej sieci telekomunikacyjnej, opóźnienie to objawia się w postaci bardzo dokuczliwego echa i nakładania się głosu rozmówców. Abonenci odczuwają efekty wywołane opóźnieniem jako pogorszenie jakości usługi.

Wysokość nad powierzchnią Ziemi satelity geostacjonarnego wynosi 35786 km, więc opóźnienie wynikające z propagacji fali na tej drodze

$$t_o = \frac{L}{c} = \frac{35786 \text{ km}}{300000 \ \frac{\text{km}}{\text{s}}} = 0{,}119 \text{ s} \approx 120 \ ms,$$

przy czym:
L - odległość Ziemia - satelita (35786 km),
c - prędkość światła w próżni (300000 km/s).

Sygnał retransmitowany przez satelitę dwukrotnie pokonuje drogę Ziemia - satelita. Wypadkowe opóźnienie wynosi zatem 2 × 120 ms = 240 ms. W rzeczywistości jest ono jeszcze większe, gdyż dolicza się do niego czas potrzebny na przetwarzanie transmitowanych sygnałów (np. w wokoderze) zarówno w segmencie naziemnym, jak i kosmicznym.

W systemach S-PCN stosuje się na ogół satelity umieszczone na orbitach o mniejszej wysokości niż orbita geostacjonarna. Jednym z powodów stosowania tego typu orbit jest konieczność zmniejszenia opóźnienia związanego z czasem propagacji sygnałów do wartości, która jest akceptowana przez użytkownika oraz zmniejszenia tłumienia sygnału na trasie Ziemia - satelita. Na przykład czas propagacji na trasie Ziemia - satelita na średniej orbicie (H = 10354 km) wynosi

Télécommunications) w Europie, prowadziły prace zmierzające do lepszego uregulowania zasad przydziału częstotliwości dla systemów S-PCN.

Nowego przydziału częstotliwości dla systemów S-PCN dokonano w roku 1995 podczas konferencji WARC-95. Przede wszystkim przydzielono częstotliwości w pasmie Ka dla systemów S-PCN i łączy dosyłowych. Zakresy częstotliwości przyznane systemom S-PCN zestawiono w tabeli 2.

Zmodyfikowano rezolucję 46 przygotowaną przez WARC-92. Stwierdzono, że w dalszym ciągu nie opracowano metod koordynacji zarówno w odniesieniu do interferencji wzajemnych między systemami stosującymi satelity na orbitach niegeostacjonarnych (ang. *non-GSO*), jak i w odniesieniu do interferencji między systemami non-GSO i systemami geostacjonarnymi.

W przypadku zakłócania systemów naziemnych przez systemy non-GSO określono dwa rodzaje sygnałów stosowanych w procesie koordynacji. Dla analogowych systemów naziemnych poziom zakłóceń od satelitów systemów S-PCN określa się na podstawie gęstości strumienia mocy na powierzchni ziemi (PFD - *ang. Power Flux Density*). W przypadku cyfrowych systemów naziemnych w procesie koordynacji bierze się pod uwagę obniżenie jakości łącza cyfrowego (FDP - ang. *Fractional Degradation in Performance*).

Tabela 2

Przydział częstotliwości dla systemów S-PCN dokonany podczas konferencji WARC-95

Pasmo	Zakres częstotliwości [GHz]	Typ łącza	Uwagi
S	1,99 - 2,01	abonenckie - w górę[1)]	dotyczy systemu ICO
	1,98 - 1,99	abonenckie - w górę[2)]	
	2,01 - 2,025	abonenckie - w górę	
	2,17 - 2,2	abonenckie - w dół[3)]	
	2,16 - 2,17	abonenckie - w dół	
C	5,091 - 5,25	dosyłowe - w górę	dotyczy systemu Globalstar
C	6,7 - 7,075	dosyłowe - w dół	dotyczy systemu ICO
Ku	15,4 - 15,45	dosyłowe - w dół	
Ku	15,45 - 15,65	dosyłowe - w obu kierunkach	
Ku	15,65 - 15,7	dosyłowe - w dół	
Ka	19,3 - 19,6	dosyłowe - w obu kierunkach	dotyczy systemu Iridium
Ka	29,1 - 29,4	dosyłowe - w górę	dotyczy systemu Odyssey
Ka	18,9 - 19,3	abonenckie - w dół	dotyczy systemu Teledesic
Ka	28,7 - 29,1	abonenckie - w górę	

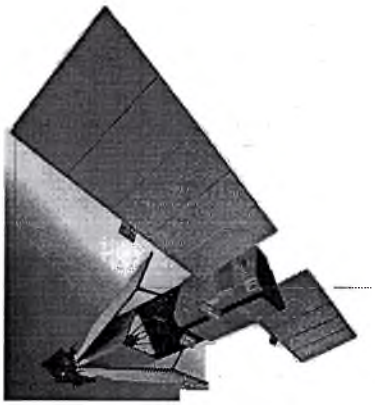
1) Globalnie dostępne od 1 stycznia 2000 r.

2) W regionie 1 i 3 dostępne od 2000 r., w regionie 2 dostępne od 2005 r. (niedostępne w USA i Kanadzie - w tym zakresie częstotliwości przewidziano prace systemów komunikacji osobistej naziemnej (PCS).

3) Dostępne w regionie 2 od 2005 r. (od 2000 r. dostępne w USA i Kanadzie).

6. Kierunki rozwoju

Pierwszy satelitarny system komunikacji osobistej typu duże LEO, znany pod nazwą **Irydium**, uruchomiono w listopadzie 1998 r. 26 czerwca 1990 roku podczas czterech równoczesnych konferencji prasowych w Londynie, Melbern, Nowym Jorku i Pekinie przedstawiono rewolucyjny projekt satelitarnego systemu komunikacji osobistej. Człon kosmiczny systemu



Rys. 2. Satelita komunikacyjny systemu Irydium

Każdy satelita jest wyposażony w cztery anteny do komunikacji z czterema sąsiednimi satelitami: północnym i południowym na tej samej orbicie oraz wschodnim i zachodnim na sąsiednich orbitach, a także w 48-wiązkową antenę do komunikacji z Ziemią. Łączna liczba wiązek w systemie wynosi 66×48=3168. Z tej liczby wiązek aktywnych przez cały czas jest 2150, niektóre wiązki są bowiem wyłączane nad biegunami Ziemi, gdzie wiązki się nakładają. Każda wiązka obsługuje na powierzchni Ziemi obszar (komórkę) o średnicy około 600 km. Całkowity obszar obsługiwany przez jednego satelitę ma średnicę ponad 3000 km. Jego powierzchnia wynosi około 8 milionów km^2, co stanowi 1,5% powierzchni Ziemi ($5{,}1 \cdot 10^8$ km^2). Komórki przemieszczają się wzdłuż powierzchni Ziemi z prędkością 6,65 km/s (24 tys. km/h). Przy takiej prędkości nawet bardzo szybko jadący samochód można uważać za stacjonarny.

System Irydium opiera się na architekturze systemu GSM, połączeniach międzysatelitarnych (*ISL* - ang. *Inter-Satellite Links*) i zorientowanemu geograficznie dostępowi. Połączenia ISL są cechą charakterystyczną systemu Irydium, w większości planowanych podobnych systemów nie przewi-duje się połączeń międzysatelitarnych. Połączenia między siecią Irydium i publiczną siecią telekomunikacyjną dokonuje się za pomocą naziemnych adapterów międzysieciowych (ang. *Gateways*). Jest ich dwanaście, rozproszonych po całym świecie.

Świadczenie usług dla użytkowników odbywa się w zakresie częstotliwości od 1616 MHz do 1626,5 MHz (pasmo L). Na połączenia międzysatelitarne zarezerwowano częstotliwości od 23,18 GHz do 23,38 GHz (pasmo K). Łączność między naziemnymi adapterami międzysieciowymi i satelitami odbywa się w zakresie częstotliwości od 29,1 GHz do 29,3 GHz (pasmo K), a między satelitami i naziemnymi adapterami międzysieciowymi - w zakresie częstotliwości od 19,4 GHz do 19,6 GHz (pasmo K).

System oferuje następujące usługi:

- transmisja głosu z szybkością 2,4 kb/s;
- transmisja danych z szybkością 2,4 kb/s;
- transmisja faksów grupy III;
- przywoływanie (alfanumeryczne).

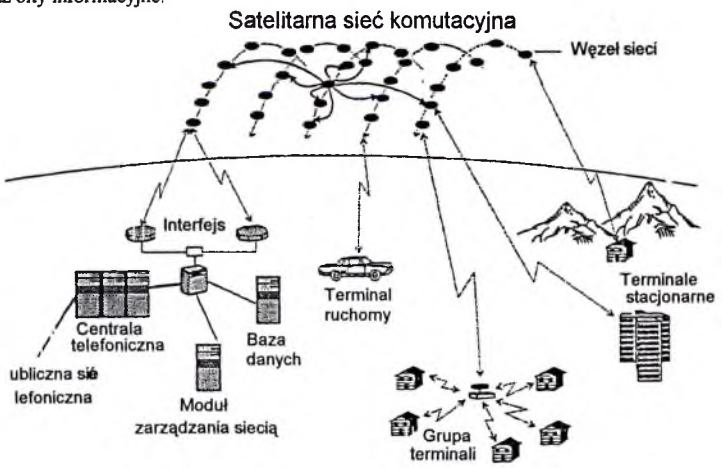
lokalizacja położenia	
Zasięg	70^0 S - 70^0 N
Termin uruchomienia	1999

Architektura sieciowa Globalstara jest oparta na znanej koncepcji stosowanej w systemie GSM. W adapterach międzysieciowych będą ulokowane i obsługiwane bazy danych dotyczące położenia abonentów (rejestr macierzysty, rejestr gości). Do zadań adaptera międzysieciowego będzie należało również uzyskanie połączenia z siecią publiczną. Jeden adapter ma obsługiwać obszar w przybliżeniu 1,3 milionów km^2. Podstawowe parametry systemu podano w tabeli 3.

W realizację inwestycji są zaangażowane 33 kraje, w tym 14 krajów z Europy, 8 z Azji, 5 z Afryki i 6 z obu Ameryk. Globalstar ma rozpocząć pracę w 1999 roku. Zakłada się że w roku 2002 system będzie obsługiwał 2,7 miliona abonentów, a w roku 2012 -16 milionów abonentów. Koszt lokalnego połączenia szacuje się na 0,35 - 0,53 USD za minutę.

Teledesic jest jedną z ciekawszych propozycji satelitarnych systemów komunikacji osobistej. Charakterystycznymi cechami systemu są: duża pojemność, którą określa się na 20 milionów abonentów; stacjonarne komórki, adaptacyjne marszrutowanie, zakres częstotliwości 20/30 GHz.
Początkowo (rok 1990) zakładano, że człon kosmiczny systemu będzie się składać z 840 satelitów aktywnych i 84 satelitów zapasowych umieszczonych równomiernie na 21 orbitach o wysokości około 700 km i kącie inklinacji 98,16^0. W roku 1998 zmieniono konstelację satelitów. Obecnie składa się ona z 288 satelitów aktywnych rozmieszczonych równomiernie na 12 orbitach o wysokości 1350 km.

Na rysunku 5 przedstawiono poglądowo architekturę systemu Teledesic . Stosuje się tu szybką komutację pakietów, podobną do ATM. Każdy rodzaj komunikacji jest traktowany jako strumień pakietów o ustalonej długości. Pakiet zawiera nagłówek z adresem, bity kontrolne oraz bity informacyjne.



Rys. 5. Architektura satelitarnego systemu komunikacji osobistej Teledesic

rozmowy kanał, niezależnie od tego przez ile satelitów będzie w tym czasie obsługiwany. Małe, stacjonarne komórki umożliwiają ograniczenie obszaru obsługiwanego do granic państwa, co jest niemożliwe przy dużych komórkach lub komórkach, które poruszają się z satelitą. Baza danych komórki zawarta w każdym satelicie, określa rodzaj usług, które powinny być udostępnione na aktualnie obsługiwanym obszarze.
Zastosowanie naziemnych stacjonarnych komórek bazuje na dokładnej znajomości pozycji satelity i jego orientacji oraz precyzyjnym sterowaniu wiązką. Do realizacji takiej koncepcji konieczne jest automatyczne określanie pozycji satelity na orbicie, zastosowanie aktywnych układów antenowych, wykorzystanie metod zwielokrotnienia dostępu, szybkie przełączanie pakietów i adaptacyjne marszrutowanie.

SkyBridge jest europejskim satelitarnym systemem multimedialnym opracowanym przez firmę Alcatel. Można go traktować jako szerokopasmowy system dostępowy umożliwiający dołączenie do stacjonarnych sieci szerokopasmowych abonentów zlokalizowanych w różnych miejscach na Ziemi, nie mających dotychczas dostępu do tego typu sieci. System będzie świadczył następujące usługi:

- dostęp do Internetu (szybkie łącza)
- dostęp do baz danych i lokalnych sieci komputerowych,
- obsługa poczty elektronicznej,
- transfer plików,
- połączenia sieci lokalnych z sieciami rozległymi,
- wysokiej jakości wideotelefonia i wideokonferencje,
- telemedycyna,
- nauka na odległość,
- rozrywka (telewizja na żądanie, gry),
- połączenia pomiędzy stacjami bazowymi sieci telefonii komórkowej,
- dołączanie do sieci stacjonarnej systemów radiowego dostępu abonenckiego.

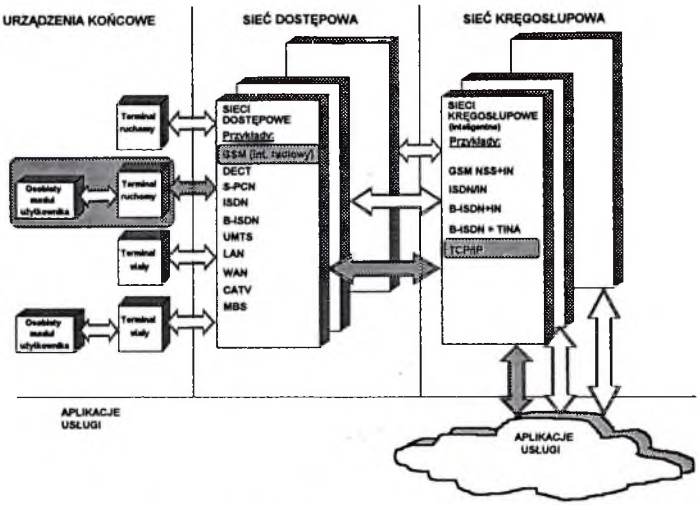
Człon kosmiczny systemu SkyBridge składa się z 64 satelitów umieszczonych na orbitach o wysokości 1457 km. Konstelacja satelitów jest podzielona na dwie symetryczne podkonstelacje, po 32 satelity w każdej. Satelity w podkonstelacjach są umieszczone na ośmiu orbitach, po cztery satelity na każdej orbicie. Kąt inklinacji orbit wynosi 55^0, co umożliwia obsłużenie obszarów od 68^0 S do 68^0 N. System nie obsługuje obszarów podbiegunowych. Orbity podkonstelacji są przesunięte względem siebie tak, że satelity, po jednym z każdej podkonstelacji, tworzą parę poruszającą się współbieżnie. Umożliwia to uzyskanie większej przepływności. Uruchomienie systemu jest możliwe po umieszczeniu na orbitach satelitów tylko jednej podkonstelacji. Zwiększenie liczby satelitów poprawia właściwości transmisyjne systemu.

Na satelitach przewidziano zainstalowanie wielowiązkowych anten aktywnych. Każda wiązka będzie obsługiwać obszar o promieniu 350 km. Satelita jest w stanie wygenerować jednocześnie do 45 wiązek. Umożliwia to obsłużenie przez jednego satelitę obszaru o promieniu około 2500 km. W systemie SkyBridge przewiduje się stosowanie częstotliwości z pasma Ku (11/14 GHz) zarówno w łączach dosyłowych (adapter międzysieciowy - satelita), jak i w łączach komunikacyjnych (terminal użytkownika - satelita).

Przewiduje się stosowanie trzech rodzajów terminali abonenckich: osobistych dla indywidualnych użytkowników, terminali instytucjonalnych dla biur lub budynków wielorodzinnych (tab. 4) oraz terminali o największej przepływności, stanowiącej węzły sieci teletransmisyjnej.

Tabela 4

18. Prasad R., Jansen M.G., Kegel A., *Capacity Analysis of a Cellular Direct Sequence Code Division Multiple Access System with Imperfect Power Control*, IEICE Trans. Comm., Vol. E 76-B, August 1993, pp. 894-905.
19. Prasad R., *CDMA for Wireless Personal Communications*, Artech House, Bostson , London, 1996.
20. Rouffet D., *Globalstar: a Transparent System*, Alcatel, Electrical Communication, 1st Quater 1993, pp. 84-90.
21. *The Global Handheld Phone Forum*, Proceedings of The Inmarsat International Conference and Exhibition on Mobile Satellite Communications, 12-14 October, Paris, 1993.
22. QUALCOMM, *An Overview of the Application of Code Division Multiple Access (CDMA) to Digital Cellular Systems and Personal Cellular Networks*, Document No. EX60-10010, May 21, 1992.
23. Speltz L.J., *Personal Communications Satellite Systems*, 44th Congress of the International Astronautical Federation, Graz, October 16-22, 1993.
24. Speltz L.J. *Personal Communications Satellite Systems*, 18th Annual Pacific Telecommunications Conference, Honolulu, 14 - 18 January, 1996, pp. 100 - 104.
25. Taylor J.T., *PCS in the U.S. and Europe*, IEEE Communication Magazine, June 1992.
26. Vojcic B., Pickholtz R., *Total Capacity in a Shared CDMA LEOS Environment*, IEEE J. Select. Areas Comm., Vol.13, February 1995.
27. Werner M., Jahn A., *Analysis of System Parameters for LEO/ICO-Satellite Communication Network*, IEEE J. Select. Areas Comm., Vol.13. February 1995.
28. Wiedeman R.A., *The Role of Globalstar in Future Public Land Mobile Telefone Systems (FPLMTS)*, Loral Qualcomm Satellite Services, 1993.
29. Wimmer K.A., Barclay J., *Global Development of PCS*, Communication Magazine, June 1992.
30. Wood L., *Big LEO*, http://www.ee.surrey.ac.uk/Personal/L.Wood/constellations, last updated June 1998.



Rys. 1. Architektura ruchowej sieci multimedialnej

3. Ograniczenia technik komórkowych

Techniki komórkowe stosowane w chwili obecnej na świecie, w tym GSM, nie umożliwiają pracy z efektywnością podobną do efektywności uzyskiwanej w przypadku transmisji poprzez modem dołączony do stacjonarnej sieci telefonicznej. Uzyskiwane szybkości transmisji danych użytkownika często nie przekraczają 1200 b/s. Obecny stan braku kompatybilności pomiędzy interfejsem radiowym systemu GSM a protokołem TCP/IP wynika z zupełnie niezależnego rozwoju telefonii komórkowej GSM oraz sieci komputerowych.

Opracowane dla sieci komputerowych sposoby transmisji danych od samego początku brały pod uwagę jedynie stosowanie łączy o stałej, dostatecznie dużej przepływności i małej stopie błędu. Dlatego też trudno się dziwić, że nie są one efektywne w przypadku łączy radiowych charakteryzujących się małą i zmieniającą się w czasie przepływnością. Ze względu na zjawiska propagacyjne, uzyskanie odpowiednio niskiej stopy błędu w łączach radiowych wymaga zastosowania dużo bardziej złożonych technik kodowania protekcyjnego niż w łączach przewodowych. Dlatego też kanał radiowy systemu GSM nie jest kanałem przezroczystym. Dane na wejściu telefonu komórkowego muszą być odpowiednio przygotowane i są poddawane wielokrotnemu przetwarzaniu.

Kolejnym problemem rzadko spotykanym w łączach stacjonarnych, a występującym w łączu radiowy GSM, jest możliwość utraty połączenia. Jeśli utrata połączenia występuje podczas rozmowy telefonicznej, to w konsekwencji należy jedynie ponownie wybrać numer abonenta i nawiązać zerwane połączenia. Przerwanie łącza w przypadku transmisji danych prowadzi zwykle do zawieszenia działania komputera i utraty danych.
Podsumowując można stwierdzić, że podstawowymi czynnikami ograniczającymi możliwość stosowania interfejsu radiowego GSM jako dostępu do Internetu są:

- szybkość transmisji danych ograniczona do 9600, 4800 lub 1200 b/s,

Protokoł TCP nie umożliwia również nadzoru nad transmisją strumienia danych, trudno zatem realizować usługi interakcyjne z pracującym w tle procesem, np. kopiowania dużego zbioru. Dodatkowo sytuację komplikują różne implementacje protokołu TCP związane z doborem właściwych wartości okna natłoku oraz okna czasowego (*timeout*), po którym następuje retransmisja.

W protokole TCP zastosowano następujące mechanizmy samokontroli.

Algorytm wolnego startu, który polega na rozpoczęciu transmisji danych z małą szybkością. Jeśli transmisja danych odbywa się bez problemów, to szybkość nadawania jest zwiększana, aż dojdzie do zakładanej szybkości maksymalnej lub wcześniej wystąpią znaczne błędy transmisji. Algorytm ten jest stosowany również do rozładowywania natłoku. Przekroczenie dozwolonego czasu opóźnienia przez potwierdzenia jest traktowane przez TCP jako objaw natłoku w sieci. Jest to zazwyczaj prawdą, jeśli do transmisji stosuje się łącza stacjonarne. Jeśli jednak dane są transmitowane poprzez łącze radiowe, w którym zastosowano kodowanie protekcyjne i transmisję z potwierdzeniem w celu zmniejszenia stopy błędu, to duże i zmienne w czasie opóźnienia są zjawiskiem normalnym.

Znaczniki czasu i opóźnienia związane z kolejkowaniem. W protokole TCP nadzór nad szczególnie dużymi opóźnieniami, które mogą być spowodowane utratą pakietów realizowany jest przy użyciu znaczników retransmisji RTO. Wielkość RTO jest w sposób ciągły dostosowywana do zmierzonego czasu upływającego od momentu wysłania danych do uzyskania potwierdzenia RTT (*Round Trip Time*). W przypadku wystąpienia opóźnień przekraczających RTT protokół TCP rozpoczyna automatyczną retransmisję niepotwierdzonych pakietów. Retransmisja ta jest w większości przypadków niepotrzebna i powoduje znaczne obciążenia łącza.

6. Architektura klient - mediator - serwer

Architekturę rozległej sieci WWW pokazano na rysunku 2. Aplikacje i zawartość strony są prezentowane w standardowym formacie i przeglądane (*browsed*) przez aplikacje, tzw. przeglądarki WWW. Przeglądarki te są aplikacjami sieciowymi, tzn. wysyłają zapytanie o określony obiekt danych do serwera sieciowego, który odpowiada wysyłając do aplikacji zakodowane przy użyciu standardowego formatu dane. Standardy opisujące sieć WWW określają niezbędne mechanizmy służące do budowy podstawowego środowiska aplikacji. Środowisko to umożliwia łatwe dotarcie do dużej liczby niezależnych aplikacji i usług przez dużą liczbę użytkowników. Protokoły stosowane w sieci WWW definiują trzy klasy serwerów:

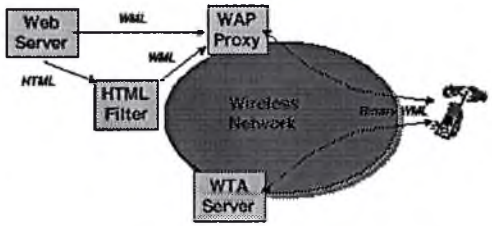
- serwer źródłowy (*origin server*), na którym znajdują się dane zasoby (zawartość strony) lub są one tworzone;

zainstalowana w terminalu ruchomym koordynuje współprace z interfejsem użytkownika i pełni analogiczną rolę jak przeglądarka w sieci WWW.

Protokoł WAP definiuje zbiór standardowych elementów, umożliwiających komunikacje pomiędzy ruchomym terminalem a serwerami sieciowymi. Elementami tymi są:

- standardowy model nazewnictwa - stosuje się nazewnictwo WWW URL w celu określenia zawartości WAP na serwerze źródłowym; standardowe WWW URL stosuje się do określenia lokalnych zasobów urządzenia, np. funkcji sterujących wywołaniem,
- typy zawartości - wszystkim zawartościom WAP przypisano typy zgodne z typami przypisanymi przez WWW,
- standardowe formaty zawartości - formaty te opracowano w oparciu o formaty WWW i obejmują one m.in.: sposób prezentacji, informacje kalendarzowe, obrazy i skrypty językowe,
- standardowe protokoły komunikacyjne - obejmujące m.in. przesyłanie zapytań pomiędzy przeglądarką terminala ruchomego a sieciowym serwerem WWW.

Przykład sieci WAP przedstawiono na rysunku 4.



Rys. 4. Przykładowa sieć WAP

Na tym rysunku klient WAP komunikuje się z dwoma serwerami bezprzewodowej sieci. Serwer WAP proxy tłumaczy zapytanie w formacie WAP na zapytanie w formacie WWW. Umożliwia w ten sposób przesłanie klientowi WAP zapytania do serwera WWW. Serwer proxy dodatkowo przekodowuje odpowiedź od serwera WWW do formatu zrozumiałego przez przeglądarkę klienta (*compact binary format*).

Jeśli serwer WWW wysyła odpowiedzi w formacie WAP (np. przy użyciu języka WML), to serwer proxy może uzyskać odpowiedź bezpośrednio z tego serwera WWW. W przeciwnym przypadku, jeśli serwer WWW przesyła odpowiedzi na przykład w formacie HTML, to potrzebny jest filtr do przetłumaczenia zawartości WWW do postaci zawartości WAP. Przykładowo filtr HTML tłumaczy HTML na WML.

Serwer WTA (*Wireless Telephony Application*) jest przykładem serwera źródłowego lub gatewaya, który odpowiada bezpośrednio na zapytania z przeglądarki WAP klienta. Serwer WTA zapewnia dostęp do usług oferowanych przez infrastrukturę sieciową operatora bezprzewodowej sieci telefonicznej.
WAP zabezpiecza również infrastrukturę poprzez bezpieczną realizację wymiany danych pomiędzy klientem WAP i serwerem. Jeśli przeglądarka i serwer źródłowy wymagają zabezpieczenia transmisji na całej drodze (*end - to - end*), to muszą się komunikować stosując protokół WAP.

• wspólne udogodnienia do wymuszania transmisji danych z określonym poziomem ufności,

• negocjacyjne właściwości protokołu.

Protokoły z rodziny WSP są zoptymalizowane z myślą o zastosowaniu w radiowych systemach wąskopasmowych z relatywnie długim opóźnieniem. Protokół WSP/B jest przygotowany do połączenia poprzez serwer proxy klienta WSP/B ze standardowym serwerem HTTP.

Bezprzewodowy protokół warstwy transmisyjnej WTP (*Wireless Transaction Protocol*) pracuje na szczycie usług datagramowych i stanowi prosty, zorientowany transakcyjnie protokół, który można zastosować w skromnych pod względem możliwości (*„thin"*) terminalach abonenckich. WTP pracuje skutecznie w bezprzewodowych sieciach datagramowych, zabezpieczonych i niezabezpieczonych. Ma on następujące właściwości:

• obsługuje trzy klasy usług transportowych:
  - przekazanie zapytania bez zabezpieczenia (*unreliable*),
  - przekazanie zapytania z zabezpieczeniem (*reliable*) - w niezawodny sposób,
  - przekazanie zapytania z zabezpieczeniem i potwierdzeniem,

• opcjonalnie umożliwia zabezpieczenie transmisji pomiędzy użytkownikami poprzez potwierdzanie przez użytkownika każdej odebranej wiadomości,

• opcjonalnie umożliwia realizację potwierdzenia poza stosowanym pasmem łącza, łączenie (grupowanie) i opóźnianie potwierdzeń w celu zmniejszenia liczby wysyłanych wiadomości,

•możliwość transmisji asynchronicznych.

Bezprzewodowy protokół zabezpieczający warstwę transmisyjną WTLS (*Wireless Transport Layer Security*) jest protokołem zabezpieczającym opracowanym na podstawie protokołu TLS (*Transport Layer Security*) stanowiącego standard. Protokół ten został zoptymalizowany pod względem zastosowań w wąskopasmowych kanałach radiowych. Ma on następujące właściwości:

• zapewnia integralność danych - zawiera mechanizmy pozwalające wykryć wszelkie zmiany w postaci danych przesłanych pomiędzy terminalem i serwerem aplikacji,

• zapewnia prywatność (poufność) danych - zawiera mechanizmy uniemożliwiające zrozumienie danych przesyłanych pomiędzy terminalem i serwerem aplikacji przez urządzenia pośredniczące, które mogą podsłuchiwać strumień danych,

• zapewnia uwierzytelnienie - zawiera mechanizmy sprawdzające autentyczność terminala i serwera aplikacji,

• ma możliwość odmowy zabezpieczenia transmisji - zawiera mechanizmy wykrywające i uniemożliwiające niepotrzebne powtarzanie transmisji tych samych wiadomości lub wiadomości, które zostały negatywnie zweryfikowane, zabezpiecza to wyższe warstwy protokołów przed atakami.

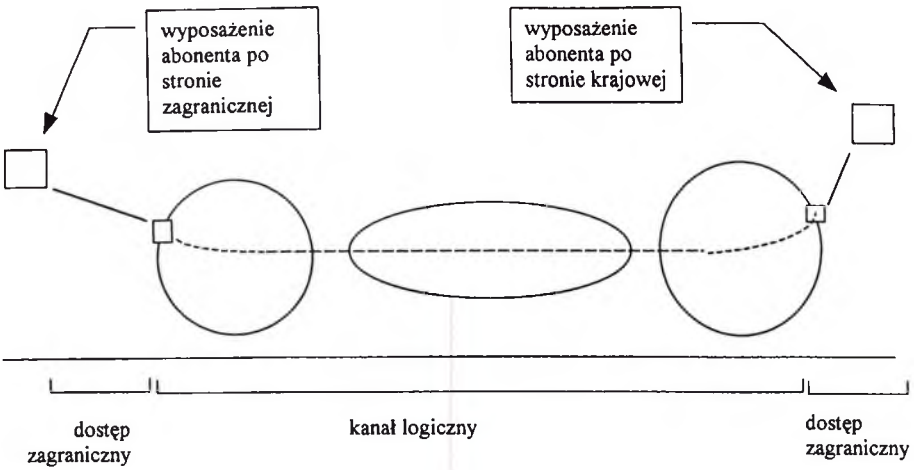
Protokół WTLS może być również stosowany do zabezpieczenia transmisji pomiędzy terminalami, np. do uwierzytelniania wymiany dokumentów elektronicznych. Aplikacje mogą w sposób selektywny uaktywniać działanie WTLS w zależności od wymaganego poziomu bezpieczeństwa i charakterystyki stosowanej sieci. Jeśli na przykład sieć jest wyposażona w działające w niższych warstwach mechanizmy zabezpieczające, to WTLS może być wyłączone.

metody kompresji, współpraca z aplikacjami multimedialnymi stosującymi większe szybkości transmisji (np. GPRS), wprowadzenie wskaźników QoS (jakości świadczonych usług) itd.

Obecnie na rynku pojawiły się już pierwsze telefony zgodne ze standardem GSM z implementacją protokołu WAP. Są to telefony Alcatela (One Touch POKET), Nokii (7110) i Samsunga (SGH-800). Wyświetlacze w nowych telefonach zostały znacznie powiększone i zwiększono ich rozdzielczość. Są wyposażone one w mikroprzeglądarki WML Firmy opracowały już i wprowadziły na rynek serwery proxy kompatybilne ze standardem WAP. Pojawiły się również pierwsze firmy świadczące specjalistyczne usługi. Od października firma Webraska uruchomiła system nawigacji po Paryżu o nazwie TeleAtlas. System dostarcza do terminali WAP informacji o warunkach na drogach, możliwych połączeniach pomiędzy zadanymi punktami miasta, mapki wybranych fragmentów miasta. Być może, że obserwujemy więc narodziny nowego rynku usług dla telefonii bezprzewodowej.

Literatura

1. Piotr Dybiec, *WAP - Wireless Application Protocol*, Telecom Forum, nr 1, 1999.
2. Piotr Dybiec, *Pierwsze telefony WAP*, Telecom Forum, nr 4, 1999.
3. *WAP Architecture, Wireless Application Protocol Architecture Specification*, WAP Forum, ver. 30, kwiecień 1998.
4. *WAP over GSM USSD, Specification*, WAP Forum, wer. z 30 kwietnia 1998.
5. *Wireless Datagram Protocol Specification*, WAP Forum, wer. z 30 kwietnia 1998.
6. *Wireles Telephony Application Interface Specification*, WAP Forum, wer. z 30 kwietnia 1998.
7. *Wireles Telephony Application Interface Specification, GSM Specific Addendum*, WAP Forum, wer. z 30 kwietnia 1998.
8. Daniel J. Bem, Ryszard J. Zieliński,: *GSM jako dostęp do Internetu*, Materiały konferencyjne z POLMAN'98, Poznań, 1998 (str. 107 - 117).
9. Daniel J. Bem, Ryszard J. Zieliński,: *Internet przez GSM*, Networld, nr 7/1998 (str. 69 - 76).
10. Alanko T., Kari H.H., Markku K., Kojo M., Laamanen H., Liljeberg M., Rastikainen K.: *Communication Services for Mobile Office in Wireless WAN Environments, Technology - Interactive Multimedia*, Global Communication Interactive '97, str. 219 - 223.
11. *Global Multimedia Mobility (GMM), A Standardization Framework*, ETSI PAC EG5 Report, 1996.
12. Parker T., *TCP/IP*, Helion, Gliwice, 1997.



Schemat logiczny rozwiązania VPN

Międzynarodowa usługa VPN (schemat powyżej) składa się z wielu elementów wymagających od operatora silnego przygotowania organizacyjno-formalnego. Jest to związane głownie faktem, że znaczna część rozwiązania jest oferowana poza granicami sieci operatora a od zgodności tej części z siecią operatora zależy jakość całego rozwiązania. Dodatkowo, w wypadku wybrania takiej opcji przez abonenta, po obydwu stronach kanału logicznego stawiane są urządzenia stanowiące wyposażenie abonenta. Muszą one nie tylko dobrze współpracować z siecią do której są podłączone, ale również ze wszystkimi innymi urządzeniami stanowiącymi wyposażenie abonenta. Zagadnienie jest tym bardziej skomplikowane, że sieć VPN konfigurowana dla abonenta może mieć swoje zakończenia w wielu krajach, a tym samym wymaga współpracy wielu operatorów. Wymaga to szczególnie starannego określenia spójnego sposobu konfigurowania swoich sieci przez partnerów, co z kolei pociąga za sobą konieczność posiadania przez operatora znacznego doświadczenia i dużej fachowości kadry, a przede wszystkim umów międzyoperatorskich gwarantujący wysoki poziom współpracy przy realizacji tego typu połączeń.

Rys. 1

Poniżej przedstawione zostały bardziej szczegółowe informacje dotyczące każdego z wymienionych typów usług.

1. Prywatne sieci ATM.

Sieci takie łącząc dwie lub więcej lokalizacji jednego lub kilku właścicieli pozwalają na bezpośrednią łączność urządzeń pracujących w technologii ATM. W ten sposób można budować sieci o dużej skalowalności oraz łatwej i szybkiej rekonfiguracji. Sieć korporacyjna tego typu może wyróżniać się bardzo dużą przepustowością oraz daje możliwość realizowania wszystkich usług opartych na ATM'ie. Przy zastosowaniu VP switching'u sieć szkieletowa jest praktycznie przezroczysta dla dołączonych sieci użytkownika. Dzięki odpowiedniej konfiguracji możliwe jest nawet bezpośrednie wymienianie sygnalizacji oraz własnych protokołów pomiędzy urządzeniami użytkownika. Na każdym porcie służącym do podłączenia użytkownika może być zakończone wiele kanałów zarówno VC jak i VP.

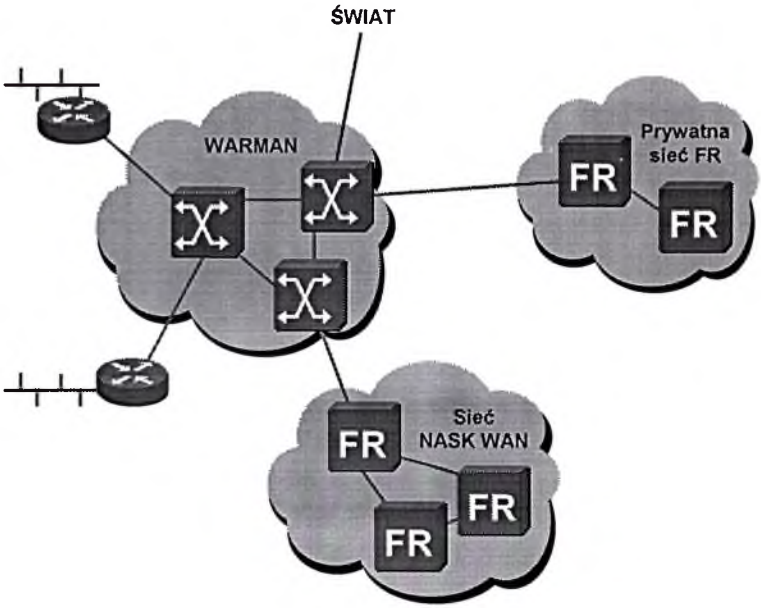
możliwości WARMAN'a:

- realizacja VC i VP switching'u,
- policing: ograniczenia SCR i PCR,
- typy ruchu: CBR, VBR,
- podłączanie stacji roboczych/serwerów, routerów i switch'y,
- realizacja kanałów o zasięgu międzynarodowym,
- proponowany typ podłączenia: STM-1 (155 Mb/s) na światłowodzie jednomodowym ze złączem FC/PC (możliwe są także rozwiązania niestandardowe na światłowodzie wielomodowym ze stykiem SC lub linii E3).

kanałów PVC na każdym z portów oraz nadania im dowolnych numerów DLCI (unikalność wymagana jest jedynie na porcie). Dzięki zgodności protokołu z używanym w krajowej sieci NASK oraz współpracy z operatorami zagranicznymi możliwe jest włączenie do sieci korporacyjnej Frame Relay kanałów o zasięgu ogólnopolskim oraz międzynarodowym.

możliwości WARMAN'a:

- realizacja LMI: ANSI T.617 ANNEX D, LMI,
- przepustowość portów Frame Relay do 2Mb/s,
- styk fizyczny: V.36 (RS-449) DTE, V.35
- realizacja kanałów o zasięgu ogólnopolskim i międzynarodowym.



Rys. 4

3. Kanały cyfrowe.

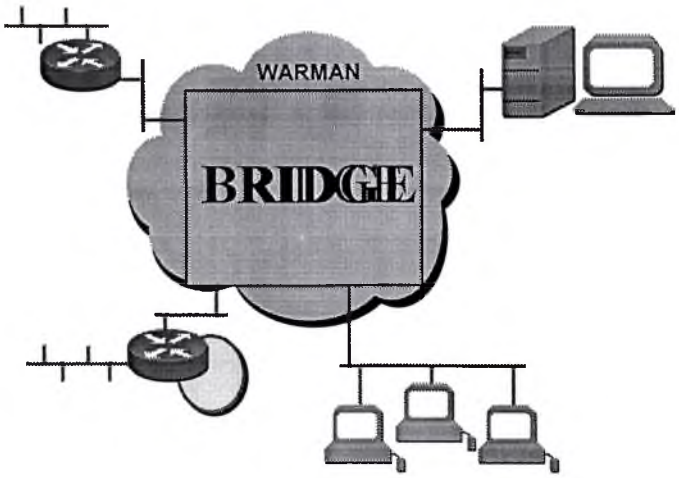
Na bazie sieci WARMAN możliwe jest zrealizowanie kanałów cyfrowych o przepustowości 2 Mb/s i 34 Mb/s (E1 i E3). Z punktu widzenia ATM'u kanały te pracują z całkowicie gwarantowanym pasmem. Mogą być one wykorzystane do łączenia urządzeń przystosowanych do współpracy ze standardowymi dzierżawionymi traktami cyfrowymi.

Obecnie możliwe są jedynie połączenia typu punkt-punkt (co oznacza, że do każdego z portów może być dołączony tylko jeden kanał), jednakże w najbliższym czasie możliwe będzie

pozwalający na bezpośrednią i przezroczystą komunikację nawet pomiędzy nietypowymi protokołami warstw wyższych.

możliwości WARMAN'a:

- styk fizyczny: AUI (daje możliwość łatwego przejścia na dowolny inny standard, jako dostęp proponujemy wykorzystanie UTP lub światłowodów),
- łączenie stacji roboczych/serwerów, LAN'ów i routerów.



Rys. 7

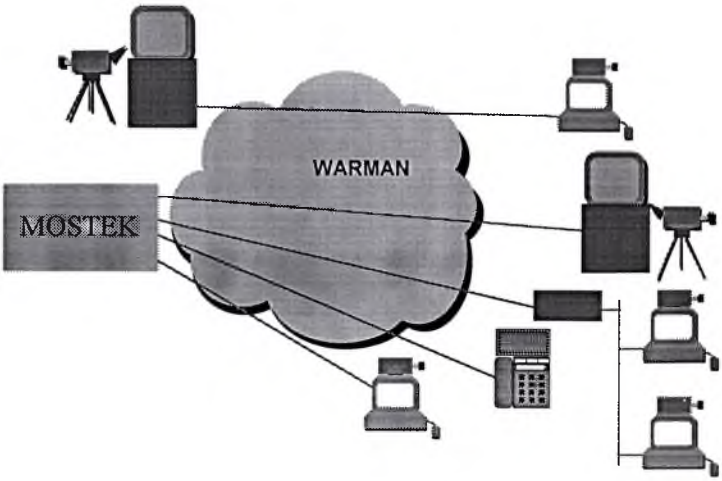
II. Usługi dodatkowe.

1. Wideokonferencje.

Wideokonferencje polegają na przesyłaniu dźwięku i obrazu o dopuszczalnej jakości z możliwym do przyjęcia stabilnym opóźnieniem. Jako opcja występuje możliwość wspólnej pracy nad dokumentami przy pomocy programów typu edytor tekstów, arkusz kalkulacyjny lub program do obróbki grafiki.

W zależności od pasma jakie możemy przeznaczyć na transmisję oraz sprzętu, którym dysponujemy otrzymamy odpowiednią jakość obrazu i wielkość opóźnienia.

Opóźnienie transmisji podczas wideokonferencji z obustronnym aktywnym udziałem uczestników jest bardzo istotne ze względu na komfort rozmówców. Zbyt duże opóźnienie powoduje efekt „zadumania się" rozmówcy i może powodować nawet podświadomą irytację w oczekiwaniu na odpowiedź. W przypadku wykorzystania techniki wideokonferencyjnej do nauczania na odległość lub innych pokazów, w których odzew słuchaczy, na przykład w postaci pytań, jest raczej sporadyczny opóźnienie nie jest tak istotne.



Rys. 8

2. Przesył głosu.

Kolejnym tematem dotyczącym przesyłu sygnałów analogowych jest transmisja głosu. Nie jest to zadanie tak spektakularne jak wideokonferencje, jednakże ze względu na niezbędność rozmów telefonicznych w naszym życiu temat ten może być bardziej popularny.

Tradycyjny przesył rozmowy telefonicznej drogą cyfrową zajmował pasmo 64 kb/s. W chwili obecnej rozwój metod kompresji głosu pozwala na ograniczenie pasma do 16 kb/s, a w przypadkach zmniejszonych wymagań na jakość fonii nawet do 8 kb/s. Przepustowości te pozwalają na transmisję głosu razem z danymi bez konieczności rozbudowy łącz pomiędzy routerami.

Posiadając sieć korporacyjną routerów przeznaczonych do transmisji danych możliwe jest dodanie usług polegających na przesyle wewnętrznych rozmów telefonicznych. Możemy tego dokonać podłączając do routera w każdej z lokalizacji od kilku analogowych linii telefonicznych (z aparatami telefonicznymi lub przyłączonych do lokalnej centralki) aż do centrali podłączonej przy pomocy traktu E1.

W zależności od sposobu realizacji sieci korporacyjnej łączącej routery transmisja głosu może odbywać się bezpośrednio po kanałach Frame Relay lub z wykorzystaniem enkapsulacji w IP. Wykorzystanie do transmisji IP daje większą elastyczność co do protokołów pracujących na łączach korporacyjnych. W przypadku sieci Frame Relay pominięcie dodatkowej enkapsulacji pozwala na lepsze wykorzystanie pasma łącz.

Zasięg takiej usługi może być rozszerzony i może obejmować lokalizacje podłączone do sieci krajowej NASK.

- przepustowość do 2 Mb/s, (możliwe są niestandardowe łącza o większej przepustowości),
- protokoły PPP, HDLC ,FR,
- proponowane sposoby obsadzenia linii dostępowych: modemy analogowe, modemy światłowodowe, xDSL, linie cyfrowe + konwertery.

c) ethernet

- proponowane media dla linii dostępowych: UTP, światłowód.

d) ATM

Dostęp do routerów poprzez kanały ATM typu VC.

- proponowane styki: STM-1 (155 Mb/s) na światłowodzie jednomodowym ze złączem FC/PC (możliwe są także rozwiązania niestandardowe na światłowodzie wielomodowym ze stykiem SC lub linii E3)

Przyczyny problemów.

Internet historycznie jest środowiskiem dla systemów wymieniających informację komputerową nie wymagających małych opóźnień, czy dostępnego stabilnie pasma. Z tego powodu jako zasadę projektową przyjmuje się tzw. „overbookowanie' łącz. Polega ono na wykorzystywaniu w szkielecie sieci łącz o niższej przepustowości niż teoretycznie możliwy na nich ruch. Taka zasada powoduje powstawanie korków i opóźnień w godzinach szczytu, które dla zwykłych aplikacji takich jak WWW czy email nie mają większego znaczenia. Dla aplikacji z wymaganiem izochroniczności taka sytuacja jest niedopuszczalna.

Następną barierą rozwoju aplikacji multimedialnych są duże i zmienne opóźnienia w sieci. Wynikają one z prób łagodzenia skutków korków przez zwiększanie buforów w routerach oraz stosowania łącz satelitarnych, wprowadzających „na początek" opóźnienia rzędu 400 ms, co z punktu widzenia omawianych aplikacji jest wartością zbyt dużą. Opóźnienia wynikają także z samej konstrukcji protokołu IP, w którym ramka ma zmienną długość i pakiet zostaje opóźniany ze względu na zajętość łącza przez transmisję pakietu o dużej długości. Wielkość opóźnienia dla wymagających aplikacji jest sprawą podstawową i dlatego stanowi obecnie największą barierę z punktu widzenia dostępnych w Internecie nowych usług.

Zaletą, ale i niestety wadą Internetu jest jego „publiczność". Transmisja przez taka siec nie jest praktycznie chroniona przed celowym i ukierunkowanym podsłuchem. Stawia to dodatkowe wymagania przed systemami np. „telefonu" internetowego. Programy musza odpowiednio szyfrować transmisję, co dodatkowo zwiększa i tak już krytyczne opóźnienia.

Jako ostatni przytoczę typowy problem okresu wprowadzania nowych usług: wielość standardów. Prawie każdy producent używa swojego systemu transmisji, proponowane są nowe protokoły i usługi, a wreszcie budowane całe sieci niekompatybilne pomiędzy sobą. Dopiero przyjęcie ogólnoświatowych unormowań pozwoli na pełne wykorzystanie nowych usług.

Wiele alternatyw, czyli próby rozwiązania problemów.

Najprostszym sposobem rozwiązania przedstawionych wyżej problemów jest zbudowanie w oparciu o warstwę 2 wydzielonej sieci Intranet. Połączenia w technologii ATM lub Frame Relay zapewniają spełnienie praktycznie wszystkich wymagań stawianych Internetowi z gwarancją usług. Rozwiązanie takie powoduje powstanie pytania: po co przesyłać np. głos przez IP? Dysponując wydzieloną sieci Frame Relay lub ATM można te usługi zorganizować w oparciu właśnie o warstwę drugą. Inna wadą jest zamkniętość rozwiązania. Ogranicza ona gwarancję usług jedynie do sieci korporacyjnej.

Innym prostym, choć drogim rozwiązaniem jest zastosowanie dużych, nadmiarowych łącz. Takie rozwiązanie dedykowane jest głównie dla dostawców i dużych użytkowników Internetu. przy dużym ruchu, gdzie selekcjonowanie pakietów przez routery nie jest możliwe. Zapewnia ono rozwiązanie większości opisanych wyżej problemów.

Dla końcowego użytkownika Internetu najlepsze jest rozwiązanie z rezerwacją pasma na żądanie. Użytkownik pracuje normalnie na obciążonych łączach, a jedynie pakiety wymagających aplikacji poruszają się przez specjalnie dla nich wydzielony na łączach kanał. Istnieje kilka sposobów takiego wydzielenia. Podstawowy wiąże się z zastosowaniem priorytetów ramek. W pakiecie IP można ich ustawić 7, co pozwala na zdefiniowanie kilku poziomów usług. Innym rozwiązaniem jest zastosowanie protokołów informujących routery o konieczności zestawienia kanału o odpowiedniej przepustowości dla transmisji między

TRANSMISJA DANYCH W TELEWIZJI KABLOWEJ ASTER CITY

Jan Zalewski

Aster City Cable Sp z o.o.
ul. Domaniewska 41, 02-672 Warszawa
tel: 606-00-51 fax: 606-00-50, e-mail: j.zalewski@astercity.net

Rozwój sieci telewizyjnej Aster City do celów transmisji danych

Telewizja kablowa Aster City powstała w 1995 r z połączenia kilku niezależnych operatorów działających na terenie Warszawy przy współpracy amerykańskiej sieci telewizyjnej Bresnan. Liczba abonentów Aster City zwiększyła się od około 50 tys. w 1995 r. do 250 tys. w 1998 r. – Aster City obejmuje swoim zasięgiem większą część Warszawy i dociera do prawie miliona odbiorców. Równolegle z powiększaniem zasięgu trwała przebudowa infrastruktury sieci. W 1995 r większa część sieci miała strukturę typową dla telewizji kablowych. Sieci takie mają topologię drzewa i zbudowane są z użyciem kabli koncentrycznych. Od centrum transmisji do końcowego odbiorcy sygnał przechodzi przez kaskady wzmacniaczy. Transmisja w takiej sieci ma charakter jednostronny – od centrum do klientów. Uruchomienie transmisji dwukierunkowej, aczkolwiek nie niemożliwe, związane jest z bardzo dużymi nakładami i trudnościami technicznymi. W ostatnich latach sieć Aster City została przebudowana tak aby umożliwiać świadczenie usług telekomunikacyjnych.

Struktura sieci ACC

Przez centralne części Warszawy przeprowadzono pierścień swiatłowodowy będący podstawową sieci transmisyjnej. Pierścień ten ma węzły w centrum transmisji oraz kilku tzw. hubach optycznych na terenie miasta. Długość swiatłowodów zainstalowanych w sieci Aster City wynosi około 1600 km. Transmisja danych i sygnału telewizyjnego odbywa się z centrum transmisji do węzłów, z kąd po światłowodach rozchodzi się do poszczególnych osiedli. W docelowej konfiguracji jedna wiązka światłowodowa przypadać ma na około 500 abonentów, obecnie obsługuje około 1000 – 2000 abonentów. Na terenie osiedla sygnał ze światłowodu konwertowany jest na sygnał elektryczny i rozprowadzany do budynków przez sieć zbudowaną na kablach metalowych. Dzięki takiej strukturze sieci ograniczona jest liczba wzmacniaczy sygnału (znajdują się one tylko na końcowym odcinku sieci i jest ich nie więcej niż trzy), tym samym uruchomienie transmisji dwukierunkowej jest znacznie prostsze.

Transmisja danych w sieci telewizji

Aby umożliwić transmisję danych w sieci należy uruchomić tzw. kanał zwrotny. W tym celu należy wyposażyć wzmacniacze pomiędzy budynkiem a najbliższym węzłem światłowodowym w tzw. wkładkę kanału zwrotnego. Sygnał zwrotny transmitowany jest w jednym z pasm o szerokości 2 MHz leżących w zakresie częstotliwości 5 – 60 MHz. Od węzła do huba optycznego sygnał przesyłany jest po wydzielonych włóknach światłowodowych. W hubie sygnał z kanału zwrotnego dekodowany jest do postaci pakietów ethernetowych i trafia do urządzeń aktywnych. Z kolei dane przeznaczone dla odbiorców, a pochodzące z urządzeń aktywnych, są kodowane do postaci sygnału telewizyjnego i transmitowane łącznie z programami telewizyjnymi. Zwykle na transmisję w kierunku w dół

stworzenia logicznie rozłącznych sieci transmisji pracujących na tej samej sieci fizycznej. Jednakże podejście takie oznacza konieczność zmniejszenie liczby dostępnych kanałów telewizyjnych. Podejście, które zastosowano w Aster City wykorzystuje istniejący pierścień swiatłowodowy do połączenia modemów centralnych pracujących w węzłach optycznych. Dzięki wykorzystaniu pierścienia do transmisji danych możliwe jest zapewnienie pracy sieci nawet przy przerwaniu pojedynczych połączeń. Dane w obrębie pierścienia transmitowane będą z szybkością 155 Mbit/s z wykorzystaniem technologii ATM.

Usługi ISP

Oprócz stosunkowo dużego ruchu wewnątrz sieci (pomiędzy abonentami) bardzo duży jest również ruch do i z internetu. Wynika to z dużej przepustowości modemów kablowych. W celu odciążenia łącz prowadzących poza naszą sieć zdecydowaliśmy się na zainstalowanie dużego serwera proxy w centrum transmisji. W centralnym węźle, oprócz serwera proxy, znajdują się również inne serwery internetowe świadczące standardowe usługi (typu www, e-mail, ftp itd.). Serwery te dołączone są do internetu przez łącza pochodzące od różnych dostawców, zarazem odgradzają one sieć Aster City od świata zewnętrznego. Umożliwia to nam świadczenie dostępu do usług z pełną prędkością pomiędzy końcówkami znajdującymi się w obrębie sieci telewizyjnej. Planujemy uruchomienie dodatkowych serwisów typu usługi informacyjne, multimedialne itp. wykorzystujących specyficzne własności sieci telewizyjnej.

W ramach usługi podstawowej Aster City oferuje obecnie swoim klientom do pięciu kont pocztowych, stronę WWW i do 30 MB miejsca na dysku. Opłata za te usługi jest zryczałtowana i nie zależy od czasu podłączenia ani od ilości przesłanych danych. W miarę rozwoju sieci oraz po wprowadzeniu rozwiązań zawierających w sobie QoS Aster City planuje oferowanie bardziej zróżnicowanych usług.

Internet w Aster City – stan obecny

Obecnie w sieci Aster City z internetu korzysta około 1000 odbiorców, do końca roku planowane jest znaczne powiększenie tej liczby. Dzięki dużej przepustowości sieci abonenci mogą transferować pliki z dużą szybkością – np. do szeregu miejsc w kraju możliwe jest uzyskanie przesyłu na poziomie 80 – 90 k bajtów/s, co jest kilkadziesiąt razy więcej niż można uzyskać z połączeń telefonicznych, mimo tego, iż obecnie naszym głównym wyjściem do internetu jest dwu-Mbitowe łącze Polpak-T oraz jedno-Mbitowe łącze satelitarne do USA. W niedługim czasie zamierzamy, ze względu na duże obciążenie istniejących łącz zastąpienie ich łączami ATM do poszczególnych sieci (NASK i innych).

Dobrym przykładem ilustrującym przepustowość sieci są dane dotyczące wykorzystania serwera proxy: w skali miesiąca serwer proxy obsługuje ruch rzędu 300 GB (przy 1000 odbiorcach), przy czym, ze względu na to, iż Aster City nie wprowadziło dotąd limitu na maksymalny ruch, pojedynczy użytkownicy w skali miesiąca dokonują transferów rzędu setek mega - do gigabajtów.

Sieć kablowa Aster City dzięki nowoczesnej konstrukcji jest dobrze przystosowana do świadczenia na szeroką skalę usług transmisji danych o dużej przepustowości.

przez klienta. W ten sposób klient staje się tzw. „front office", co eliminuje konieczność zatrudniania rzeszy pracowników obsługi. Z „back office" pozostaje jedynie serwer.

W ten sposób radykalnie zmniejszają się koszty funkcjonowania instytucji. Oszczędności, które wynikają z tego procesu są częściowo przekazywane klientom w postaci braku opłat za prowadzenie konta oraz innych podstawowych czynności bankowych, a także poprzez korzystniejsze oprocentowanie depozytów i kredytów. Bank internetowy staje się bardziej konkurencyjny od tradycyjnych banków.

- Transakcje wiązane, ze względu na fakt posiadania licznej bazy danych klientów możliwe jest oferowanie usług bankowych, ubezpieczeniowych i inwestycyjnych. Wystarczy odpowiednio zaprezentować na stronach WWW banku powyższe rozwiązania, żeby zwrócić uwagę potencjalnych klientów. Zakładając, że klienci są zadowoleni z usług bankowych oraz mają zaufanie do danej instytucji, można zachęcić ich do skorzystania z kolejnej usługi. Łatwiej jest sprzedać produkty finansowe aktualnym klientom, niż szukać nowych.

- Brak uregulowań prawnych, ponieważ aż do końca 1998 roku nie istniały ogólnoeuropejskie normy dotyczące działalności gospodarczej w Internecie.

Komisja Europejska określiła już minimalne ramy prawne tej działalności. Kraje członkowskie oraz kandydaci do Unii Europejskiej powinni w najbliższym czasie umieścić w swoim prawodawstwie następujące zagadnienia:

- Usług społeczeństwa informacyjnego, czyli usług dokonywanych odpłatnie, na odległość, poprzez wykorzystanie elektronicznych środków przekazu, związane z odpowiedzią na zapytanie klienta,

- Miejsca zawarcia transakcji internetowej jako faktyczną siedzibę sprzedającego. Wiąże się z tym w sposób automatyczny wybór prawodawstwa danego kraju w umowie z klientami.

- Ważność zawierania kontraktów on-line w sposób samoistny, czyli nie wymagający potwierdzenia w formie pisemnej poza Internetem,

- Podpis elektroniczny jako metoda identyfikacji uczestników transakcji gospodarczych,

- Przejrzystość i prawdziwość reklamy, która nie może wprowadzać w błąd,

- Ograniczona odpowiedzialność pośredników biernych, czyli podmiotów użyczających sklepom internetowym miejsca na serwerze,

- Zastosowanie istniejących przepisów prawa, zamiast tworzenia nowych reguł specjalnie dla transakcji internetowych.

Bazując na cechach usług internetowych, można zdefiniować role, którą spełnia Internet w procesie dystrybucji usług finansowych:

- Informacyjna, czyli dostęp do danych,

Najstarszym bankiem na świecie działającym wyłącznie w Internecie jest Security First Network Bank, który rozpoczął działalność w 1995 roku. W Polsce pierwszą instytucją finansową, która zdecydowała się na taki krok był Powszechny Bank Gospodarczy z Łodzi, obecnie część Grupy Pekao SA. Poprzez Oddział Elektroniczny można korzystać z rachunku bieżącego oraz ROR. Dostępne są przelewy krajowe, zakładanie lokat oraz historia rachunku. Zdecydowany nacisk położono na zapewnienie wysokiego poziomu bezpieczeństwa oraz dużej przepustowości transakcyjnej.

Za granicą istnieje już sporo banków internetowych, między innymi: Bank24 (w Grupie Deutsche Bank), Credit Suisse First Boston, Union Bank of Switzerland, First Direct (Grupa HSBC), Union Bank of California oraz wiele innych. Ostatnio dołączyły do tego grona banki hiszpańskie i portugalskie. Należy się spodziewać, ze za kilka lat łatwiej będzie wymienić banki, które nie prowadzą obsługi transakcyjnej poprzez Internet niż na odwrót.

Fakt założenia i korzystania z rachunku bankowego jest dopiero pierwszym elementem wykorzystywania usług finansowych. Banki z powodzeniem oferują tzw. transakcje wiązane.

Rynek kredytowy

Usługi na rynku kredytowym są prowadzone głównie z myślą o osobach fizycznych. Za pośrednictwem banku internetowego można otrzymać pożyczki i kredyty konsumpcyjne. Najszybsze z banków są w stanie podjąć decyzję prawie natychmiast od momentu przesłania wniosku drogą elektroniczną. Należą do nich Beneficial National Bank w przypadku kredytów oraz Bank of Montreal z Kanady w przyznawaniu kredytów hipotecznych.

Ponadto liczne instytucje finansowe i niefinansowe oferują karty płatnicze Visa lub Mastercard. Między innymi jest to biuro maklerskie E*Trade oraz wyszukiwarki internetowe, np. Yahoo.

Zdaniem autora, ze względu na istniejącą bazę danych klientów banku, jest to perspektywiczne pole oferowania detalicznych usług bankowych. W Polsce powstaje Biuro Informacji Kredytowej, które do końca roku 2000, będzie centralną hurtownią danych o kondycji finansowej osób fizycznych. Umożliwi to świadczenie podobnych usług w kraju.

Pochodne instrumenty finansowe

Niektóre biura maklerskie w USA, np. DLJ Direct umożliwiają dostęp do rynku instrumentów pochodnych. Są to kontrakty opcyjne oraz tzw. opcje pokryte. Jednak ze względu na niską wiedzę potencjalnych klientów nie należy spodziewać się szybkiego rozwoju usług detalicznych w tym segmencie rynku.

Rynek ubezpieczeniowy

Istnieją już trzy rodzaje instytucji oferujących ubezpieczenia. Są to ubezpieczyciele majątkowi, na życie oraz specjalistyczne wyszukiwarki ofert. Pierwszym polskim podmiotem sprzedającym ochronę ubezpieczeniową jest Hestia Insurance z Sopotu. Ubezpieczenia na życie są dostępne w Wielkiej Brytanii oraz USA, gdzie można również odszukać wyszukiwarkę ubezpieczeń, określić warunki brzegowe niezbędnej ochrony, a następnie pozwolić na znalezienie najlepiej dopasowanych ofert do wymagań klienta spośród kilku tysięcy istniejących na rynku.

PROGRAM „INTERNET" FUNDACJI IM. STEFANA BATOREGO

Marek Tuszyński, Wojciech Bogusz

Fundacja im. Stefana Batorego
e-mail: internet@batory.org.pl http://www.batory.org.pl/internet/
tel.: (0-22) 48 80 55 fax: (0-22) 849 30 41

Priorytety

Celem działania Programu jest promowanie Internetu w środowiskach, które nie biorą udziału w przemianach zachodzących w sposobach komunikacji zbiorowej. Internet traktujemy nie tylko jako narzędzie, ale jako nowy środek do osiągnięcia nowych celów: powszechnej demokracji, zamazania pojęcia "prowincji", ograniczenia władzy opartej na posiadaniu informacji, nowoczesnej edukacji, promowania nowoczesnej medycyny, powszechnego dostępu do informacji prawnej, powszechnego dostępu do wiedzy na poziomie gminy i powiatu, działań organizacji pozarządowych, wyrównywania szans niepełnosprawnych do edukacji i pracy, wykorzystania sieci Internet do celów zawodowych w środowiskach medycznych w Polsce.

Historia

Program Internet został powołany przez Zarząd Fundacji Batorego w październiku 1995 roku.

Internet dla Szkół i Edukacja

- W 1995 roku po przeprowadzeniu ankiet w szkołach i wysłaniu listów do operatorów Internetu, postanowiliśmy wspierać projekt "Internet dla Szkół". W chwili obecnej IdS (http://www.ids.pl/) dostarcza Internet dla ponad 1 200 szkół ponad podstawowych w Polsce, w czasie realizacji projektu przeszkolono ponad 6 000 uczniów i nauczycieli, udostępniono liczne zasoby edukacyjne, stworzono listy dyskusyjne.
- Internet dla Szkół koordynuje w Polsce projekty międzynarodowe takie jak
  - I*EARN – projekt działający na zasadzie forum dyskusyjnego (poprzez USENET News) uczniów i nauczycieli z całego świata. W jego ramach wydawanych jest kilka periodyków (papierowych i wirtualnych), organizowane są konferencje oraz liczne warsztaty. Główny nacisk tego projektu skoncentrowany jest na zagadnieniach humanistycznych.
  - ThinkQuest - jest to konkurs dla uczniów w wieku 12-19 lat, w ramach którego tworzone są edukacyjne strony WWW. Finał konkursu organizowany jest w USA, a suma nagród przekracza milion USD. Co roku w konkursie bierze udział kilkanaście tysięcy projektów przygotowanych przez uczniów z ponad 60 krajów,
  - Web for Schools – projekt koordynujący i uaktywniający współpracę nauczycieli z Europy w wielu dziedzinach (wspólne projekty, periodyk, zasoby internetowe);
- Przeprowadziliśmy trzy konkursy "edukacja przez Internet" w wyniku których zrealizowano 50 projektów dydaktycznych w sieci Internet,
- Współfinansowaliśmy letnie i zimowe warsztaty z Internetem (wspólnie z IdS, TP S.A., Sun Microsystems, Optimusem i Microsoftem) w ramach których przeszkolono ponad 450 uczniów i nauczycieli,
- We współpracy z IdS i Ministerstwem Edukacji Narodowej dofinansowaliśmy szkolenia dla 1 000 nauczycieli przeprowadzone w Polsko Japońskiej Wyższej Szkole Technik Komputerowych w Warszawie,

- Na początku 1998 roku otworzyliśmy serwer, który daje możliwość bezpłatnego uzyskania kont pocztowych, uzyskania miejsca na strony WWW oraz pomocy w konfiguracji oprogramowania i sprzętu komputerowego dla instytucji i osób zajmujących się organizacjami pozarządowymi (adres: http://free.ngo.pl/, obecnie znajduje się tam ok. 700 instytucji), medycyną (http://free.med.pl/) i kulturą (http://free.art.pl/).

Konkurs: „Nie jestem Sam" - Internet dla Niepełnosprawnych

- W 1997 roku przyznaliśmy grant na pilotażowy projekt Fundacji Matematyków i Informatyków Niesprawnych Ruchowo. Przyznana dotacja została wykorzystana na unowocześnienie pracowni komputerowej i przeprowadzenie podstawowych i zaawansowanych szkoleń dotyczących wykorzystania Internetu oraz tworzenia jego zasobów, stworzenie pierwszego w Polsce serwera gromadzącego informacje ważne dla niepełnosprawnych (http://www.idn.org.pl/ , obecnie na serwerze znajduje się również ponad 300 kont osób niepełnosprawnych)

- W wyniku tych doświadczeń w 1998 roku ogłosiliśmy konkurs "Nie jestem sam" w ramach którego poszukujemy przede wszystkim następujących rozwiązań:
  - Serwisy internetowe dla niepełnosprawnych,
  - Szkolenia osób niepełnosprawnych w posługiwaniu się Internetem,
  - Internet formą pracy (np. tzw. telepraca),
  - Działania integrujące niepełnosprawnych ze "sprawną" częścią społeczeństwa, których podstawową formą będzie Internet.

  W konkursie „Nie jestem sam" można otrzymać dofinansowanie na:
  - opracowanie materiałów w wersji HTML
  - konwersję danych
  - podłączenie do Internetu
  - szkolenie w posługiwaniu się Internetem
  - oprogramowanie sieciowe i unowocześnienie sprzętu

  Chcielibyśmy, aby projekty przez nas finansowane przyczyniły się do przełamania społecznego stereotypu osoby niepełnosprawnej - często postrzeganej jako nieefektywna i niezdolna, by sprostać oczekiwaniom społecznym.

Konkurs: „Pomysł"

- W 1998 roku ogłosiliśmy otwarty konkurs „Pomysł", którego celem jest dotowanie projektów, które mogą być przez nas wykorzystane w przyszłości jako rozwiązania łączące w sobie cele wybranych programów Fundacji z techniką ich realizacji jaką jest Internet

  Projekty mają dotyczyć następujących dziedzin:
  - Wsparcie i promocja działań organizacji pozarządowych oraz ich współpracy z samorządem lokalnym,
  - Przystąpienie Polski do Unii Europejskiej,
  - Promocja wiedzy i działań z zakresu prawa i praw obywatelskich,
  - Integracja, edukacja i Telepraca osób niepełnosprawnych,
  - Zastosowanie Internetu w medycynie
  - Promocja i wspieranie działań na rzecz kultury, edukacji i mediów lokalnych.

SYSTEMY INFORMATYCZNE O TRÓJWARSTWOWEJ ARCHITEKTURZE SIECIOWEJ

Jerzy Brzeziński, Tomasz Koszlajda, Jan Wiktorowicz

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

1. Wstęp

W strukturze logicznej systemów informatycznych można wyodrębnić kilka uniwersalnych warstw programowych: moduł zarządzania danymi, moduły przetwarzania danych i interfejs systemu ze światem zewnętrznym. Logiczna architektura systemów informatycznych określa wzajemne relacje między tymi modułami i ich lokalizację. Różnice w architekturze poszczególnych systemów informatycznych są wynikiem specyfiki poszczególnych systemów i zmieniających się możliwości technologicznych. Wybór określonej architektury systemu informatycznego ma istotny wpływ na koszt budowy i utrzymania systemu (w krańcowych wypadkach na jego realizowalność) oraz na wydajność pracy systemu.

W historii rozwoju informatyki można wyróżnić pewne dominujące trendy stosowanych architektur systemów informatycznych. W latach sześćdziesiątych i siedemdziesiątych dominującym typem architektury była architektura scentralizowana. Systemy informatyczne były konstruowane na pojedynczych dużych komputerach, do których dla umożliwienia równoległej pracy wielu użytkowników jest przyłączonych wiele terminali. W architekturze scentralizowanej wszystkie warstwy systemu są zlokalizowane na pojedynczym komputerze.

W latach osiemdziesiątych w związku z upowszechnieniem sieci komputerowych i komputerów osobistych dominującym rozwiązaniem stała się architektura rozproszona. Rozproszeniu mogą podlegać: przetwarzane dane i moduły zarządzania danymi (mówimy wówczas o rozproszonych bazach danych) lub aplikacje przetwarzające dane (jest to tzw. architektura typu klient-serwer). Rozproszone systemy informatyczne są instalowane na wielu komputerach połączonych lokalną lub rozległa siecią komputerową. Poszczególne komputery pełnią w systemie jedną z dwóch ról: serwera danych lub stacji przetwarzania i wizualizacji danych, czyli tak zwanego *klienta*. Zaletami systemów rozproszonych jest ich większa skalowalność, większa dostępność danych, większa odporność na awarie i krótsze czasy dostępu do danych. Bardziej dyskusyjną zaletą, bo zależną od zmieniającej się sytuacji rynkowej, jest niższy koszt budowy tych systemów, będący wynikiem zastąpienia drogiego komputera centralnego – tańszymi komputerami pełniącymi funkcje serwerów systemu rozproszonego. Wadami architektury rozproszonej są większa złożoność takich systemów i bardziej skomplikowane zarządzanie nimi. W systemach rozproszonych znacznie trudniej jest nadzorować pielęgnację i rozwój replikowanych elementów systemu.

W połowie lat dziewięćdziesiątych alternatywą dla dotychczas stosowanych architektur stała się trójwarstwowa architektura sieciowa (ang. Network Computing Architecture - NCA). W porównaniu z systemami rozproszonymi wprowadzono w niej trzeci specjalizowany typ węzłów systemu - serwery aplikacji. Przesłanką do stosowania architektury NCA jest obniżenie kosztów systemu, ułatwienie administrowaniem systemami z wieloma klientami oraz zwiększenie efektywności przetwarzania danych. Pozamerytoryczną przesłanką poszukiwania nowej architektury systemów informatycznych jest walka konkurencyjna firm informatycznych ORACLE i SUN z dominacją firmy MICROSOFT. Jej celem jest ułatwienie eksploatacji produktów tych firm poza platformą WINDOWS.

Obniżenie kosztów systemów o architekturze NCA jest wynikiem ograniczenia funkcjonalności stacji klienckich do roli interfejsu systemu. Dzięki temu rolę klientów mogą pełnić tańsze

3. Standard komunikacji obiektowej - CORBA

CORBA (*ang. Common Object Request Broker Architecture*) jest standardem architektury komunikacji między obiektami, niezależnej od platformy sprzętowej, systemu operacyjnego, fizycznej lokalizacji obiektów i języka programowania, w którym dane obiekty zostały zaimplementowane. Standard ten zakłada, że współpraca między obiektami odbywa się zgodnie z modelem klient-serwer, co odzwierciedla mechanizm komunikacji przyjęty w obiektowych językach programowania: obiekt-klient wysyła komunikat do obiektu-serwera, a obiekt-serwer wykonuje odpowiednią metodę. W architekturze CORBA klienci i dostawcy usług są reprezentowani przez zbiory obiektów. Komunikują się one ze sobą przez magistralę programową Object Request Broker - ORB, która zapewnia wysłanie komunikatów do obiektów usługodawców, a następnie zwrotne przesłanie wyników do klientów.

Ze względu na oferowane usługi można wydzielić trzy grupy obiektów: obiekty realizujące usługi uznane za podstawowe (*ang. Object Services*), obiekty udostępniające funkcje służące budowie aplikacji (*ang. Common Facilities*), oraz na obiekty specyficzne dla konkretnej aplikacji (*ang. Application Objects*).

Do usług podstawowych należą między innymi:

- **Concurrency Control Service** – obejmuje usługi związane z zarządzaniem współbieżnością przetwarzania,
- **Persistence Service** - zapewnia jednolity interfejs służący składowaniu obiektów na różnych rodzajach systemów baz danych i systemów plików,
- **Naming Service** - umożliwia obiektom znajdowanie innych obiektów poprzez nazwę. Wspomaga również dołączanie obiektów do istniejących katalogów lub kontekstów nazw - włącznie z X.500, DCE, NIS+, NDS i LDAP,
- **Security Service** - wspiera identyfikację, kontrolę dostępu oraz poufność; zarządza również przekazywaniem uprawnień pomiędzy obiektami,
- **Query Service** - zapytania dotyczące obiektów w standardach SQL3 oraz Object Query Language,
- **Trader Service** - umożliwia obiektom upublicznianie swoich usług na zasadzie "Żółtych stron",
- **Event Service** - pozwala obiektom na odbieranie specyficznych informacji. Obiekt chcący pozyskiwać takowe rejestruje się w ES,
- **Time Service** - zapewnia synchronizację czasu w środowisku rozproszonym oraz umożliwia definiowanie i zarządzanie zdarzeniami związanymi z upływem czasu,
- **Transaction Service** - obsługuje algorytm 2PC zarówno dla transakcji płaskich jak i zagnieżdżonych.

Wśród usług pomocniczych przy budowie aplikacji wyróżniono następujące grupy:

- zarządzanie prezentacją informacji użytkownikowi (np. pomoc kontekstowa)
- zarządzanie informacją (np. wymiana i konwersja danych)
- zarządzanie obiektami i zadaniami (np. zarządzanie przepływem danych)

Magistrala ORB z trzema wyróżnionymi grupami usług, tworzy OMA (Object Management Architecture) [4,5]. Model architektury OMA został pokazany na rysunku 1.

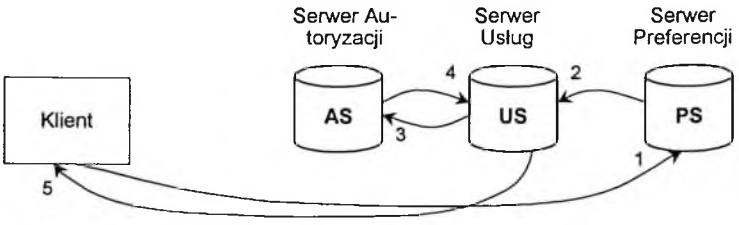
- API Repozytorium Interfejsów (ang. Interface Repository API) pozwala na pozyskiwanie i modyfikację opisu wszystkich zarejestrowanych interfejsów obiektów, metod jakie udostępniają oraz parametrów jakich żądają.
- Łącznik (ang. Object Adapter) znajduje się w warstwie usług komunikacyjnych rdzenia ORB i przyjmuje wołania na rzecz obiektów serwera. Oferuje on mechanizmy tworzenia obiektów serwera, przekazywania parametrów i nadawania obiektom identyfikatorów. Łącznik rejestruje również obiekty obsługiwane przez siebie i ich metody w Repozytorium Implementacji (ang. Implementation Repository).
- Repozytorium Implementacji (ang. Implementation Repository) zawiera informacje o klasach udostępnianych przez serwer, wystąpieniach obiektów i ich identyfikatorach.
- Interfejs ORB (ang. ORB Interface) składa się z kilku API do obsługi usług lokalnych, jak np.: zamiana referencji obiektu w łańcuch znaków i na odwrót. Jest on funkcjonalnie identyczny po stronie klienta i serwera.

4. Projekt prototypowego systemu o architekturze NCA

W projekcie skoncentrowano się głównie nad problemem scentralizowanego administrowania klientami w systemie rozproszonym. W architekturze prototypu oprócz klientów wyróżniono trzy podstawowe warstwy programowe: serwera usług, serwera autoryzacji i serwera preferencji.

- Serwer Usług - US, którego przeznaczeniem jest udostępniane usług dla stacji klienckich. W zrealizowanym prototypie serwer usług oferuje usługi związane z obsługą systemu plików. W ogólności system rozproszony może obejmować wiele wyspecjalizowanych serwerów usług.
- Serwer Autoryzacji - AS , jest odpowiedzialny za zarządzanie autoryzacją dostępu klientów do określonych usług. Serwer ten został wyodrębniony w celu scentralizowania zarządzania prawami dostępu wielu klientów do wielu serwerów usług.
- Serwer Preferencji - PS, jest odpowiedzialny za nadzorowanie preferencji poszczególnych klientów. Preferencje obejmują wskazanie domyślnych serwerów i usług dla poszczególnych klientów. Preferencje klienta mogą dotyczyć również korzystania z lokalnych zasobów stacji klienckich. W wyniku zastosowania serwera preferencji uzyskuje się pełną transparentność odwoływania się klientów do zdalnych zasobów systemu rozproszonego. Dla ułatwienia pracy administratora przyjmuje się, że w systemie występuje dokładnie jeden taki serwer.

Ogólna architektura prototypu systemu została przedstawiona na rysunku 2.



Rys. 2 - Architektura prototypu

współpracują ze sobą poprzez magistralę ORB. Plik IDL definiujący usługi przedstawiono poniżej.

```
module FinalServer
{
        const long ArrayBound = 100;
        typedef string sarray[ArrayBound];

        exception RIOException{};

        interface RemoteInputStream
        {
                attribute string path;
                void init();
                long available();
                long read() raises (RIOException);
                void close() raises (RIOException);
        };

        interface RemoteOutputStream
        {
                attribute string path;
                void init();
                void flush() raises (RIOException);
                void write(in long b) raises (RIOException);
                void close() raises (RIOException);
        };

        interface RemoteFile
        {
                attribute string separator;
                attribute char separatorChar;
                attribute string pathSeparator;
                attribute char pathSeparatorChar;
                void init(in string path, in string RAname);
                string getName();
                string getPath();
                string getAbsolutePath();
                string getCanonicalPath() raises (RIOException);
                string getParent();
                boolean exists();
                boolean canWrite();
                boolean canRead();
                void setWrite();
                void setRead();
                boolean isFile();
                boolean isDirectory();
                boolean isAbsolute();
                long lastModified();
                long length();
                boolean mkdir();
                boolean renameTo(in string dest);
                boolean mkdirs();
                sarray list();
                boolean delete();
                long hashCode();
                string toString();
        };

        interface RemoteFactory
        {
                RemoteInputStream createRIS();
                RemoteOutputStream createROS();
                RemoteFile createRF();
        };
};
```

Klasy `RemoteFile`, `RemoteInputStream` i `RemoteOutputStream` zapewniają dostęp do plików po stronie serwera. Brak możliwości definiowania metod polimorficznych w CORBIE wymusił stworzenie klas "opakowań" (ang. wrapper classes) po stronie klienta odpowiadających metodom wielopostaciowym.

Aby umożliwić przekazywanie wyjątków generowanych przez klasy po stronie serwera zdefiniowano wyjątek CORBY RIOException. Wyjątki generowane przez język JAVA po stronie

```
//RemoteFileInputStream
public int read() throws java.io.IOException;
[...]
public int read(byte b[]) throws java.io.IOException;
[...]
public int read(byte b[], int off, int len) throws java.io.IOException;
[...]

//RemoteFileOutputStream
public void write(int b) throws java.io.IOException;
[...]
public void write(byte b[]) throws java.io.IOException
[...]
public void write(byte b[], int off, int len) throws java.io.IOException;
```

W swym rdzeniu metody te korzystają z metod `read()` i `write()` zdefiniowanych po stronie serwera. Zastosowany mechanizm został wybrany ze wzlędu na swą prostotę i naturalność, a także na niewielkie możliwości definiowania w IDLu tablic o nieznanej długości, nie jest on jednakże mechanizmem najefektywniejszym. Rozważmy sytuację zapisu tablicy znaków. Wówczas dla każdego znaku wołana jest metoda `write()`, co wiąże się z tworzeniem żądania i przesyłania go poprzez ORB do serwera. Generalnie dla tablicy n-elementowej mamy *n* przesłań. Implementując jako funkcję podstawową (po stronie serwera) `write(byte[], int , int)` uzyskujemy większą efektywność implementacji, gdyż zapisanie n-elementowej tablicy wymaga pojedynczego przesłania. Co prawda przesłanie pojedynczego elementu wymaga skonstruowania tablicy, lecz jest to operacja lokalna w stosunku do klienta i jako taka wykonywana jest stosunkowo szybko.

5.2. Serwer Preferencji i Autoryzacji (PAS)

Serwer ten jest serwerem pomocniczym i podrzędnym w stosunku do FS. Przechowuje on prawa dostępu oraz preferencje użytkowników. Zrealizowany jest na bazie List Kontroli Dostępu (ang. ACL - Access Control List). ACL jest strukturą danych wykorzystywaną do kontroli użycia szeroko rozumianych zasobów. Składa się ona z wpisów (ang. ACL entries), zawierających zbiór praw skojarzonych z określonym zleceniodawcą (ang. principal). Zleceniodawca może reprezentować zarówno pojedynczego użytkownika jak i całą ich grupę. Wpis na listę może być pozytywny (zezwalający) lub negatywny (zabraniający). Wpis pozytywny umożliwia zleceniodawcy dostęp do zasobu, zaś wpis negatywny uzyskanie takowego uniemożliwia.

Zarządzanie wpisami zrealizowane w JDK opiera się na następujących zasadach:

- każdy zleceniodawca może posiadać co najwyżej jeden wpis pozytywny i co najwyżej jeden wpis negatywny. Wielokrotne wpisy dla jednego zleceniodawcy są zabronione. Każdy wpis specyfikuje zbiór uprawnień (wpis pozytywny) lub zakazów (wpis negatywny);
- jeśli nie ma wpisu dla konkretnego zleceniodawcy, zakłada się że posiada on pusty zbiór uprawnień;
- jeśli dla zleceniodawcy istnieje wpis zarówno pozytywny jak i negatywny dotyczący tej samej operacji zakłada się że operacja nie jest ani dozwolona ani zakazana;
- wpisy indywidualne zawsze przewyższają wpisy dotyczące grup.

W zrealizowanym systemie przyjęto ziarnistość kontroli dostępu na poziomie użytkownika, czyli nadane prawa dotyczą wszystkich plików w systemie. Rozwiązanie to zostało przyjęte ze względu na możliwość realizacji FS na różnych systemach, które będą oferowały różny poziom kontroli dostępu (praktycznie brak kontroli w systemach MICROSOFT, model użytkowników i grup w systemach UNIX czy też ACL w systemach VMS). Wobec tego faktu niższy poziom gradacji (pliki), zmuszałby potencjalnego administratora systemu do tworzenia

nie bezpośrednio w metodach dostępu do plików. Na metodach dynamicznych mogłoby być oparte rozpoznawanie otoczenia przez serwer usług, i komunikowanie się z innymi specjalizowanymi serwerami systemu. Umożliwiłoby to automatyczne tworzenie zbioru sfederowanych serwerów świadczących sobie nawzajem określone usługi.

7. Literatura

1. Robert Orfali, Dan Harkey „Client/Server Programming with JAVA and CORBA. 2nd edition", John Wiley & Sons, Inc. 1998
2. „The Common Object Request Broker:Architecture and Specification. Revision 2.2", OMG February 1998
3. „CORBAservices: Common Object Services Specification", OMG November 1997
4. „OMA Guide", September 1997, OMG
5. „A Discussion of the Object Management Architecture", January 1997, OMG
6. „ORBACUS for C++ and JAVA. Version 3.0", Object-Oriented Concepts Inc. 1998
7. Bruce Eckel „Thinking in Java", Prentice-Hall Inc. 1998
8. Gamma, Helm, Johnson, Vlissides „Design Patterns", Addison-Wesley 1995

zakres. Obecnie pretenduje do roli globalnej internetowej usługi katalogowej. Jednak szczegółowe specyfikacje LDAP-a są ciągle przedmiotem prac grup roboczych, także replikacja — przedmiot dyskusji w niniejszym artykule, jest w fazie standaryzacji.

Zasoby usługi katalogowej są lokalizowane w specjalnej bazie danych, nazywanej książką informacyjno-adresową lub w skrócie katalogiem. Zakres informacji umieszczanej w takiej bazie jest bardzo różnorodny. Mogą to być mniej lub bardziej rozbudowane informacje o jednostkach organizacyjnych i osobach w nich zatrudnionych (adresy, telefony, faxy, e-maile, tytuły naukowe, stanowiska itp.), a także opisy zasobów sieciowych: urządzeń, aplikacji, struktury domenowej. Podstawową jednostką informacyjną bazy jest **encja** (ang. *entry*), nazywana zamiennie **wpisem**. Utrzymuje ona informację na temat konkretnego egzemplarza obiektu. Obiekty o podobnej charakterystyce są identyfikowane przez wspólną **klasę obiektów** (ang. *object class*). Każdy wpis w bazie X.500 należy do co najmniej jednej klasy obiektów. Jednostką informacji w ramach encji jest **atrybut** (ang. *attribute*). Składa się on z **typu atrybutu** (ang. *attribute type*) oraz jednej lub więcej **wartości atrybutu** (ang. *attribute values*).

Istotną specyfiką usługi X.500 jest hierarchiczna struktura zasobów oraz identyfikowanie obiektów za pomocą **nazwy wyróżnionej** (ang. *distinguished name*, DN), powstającej poprzez dołączenie do nazwy encji macierzystej (nadrzędnej) **relatywnej nazwy wyróżnionej** (ang. *relative distinguished name*, RDN). Zapytania nadchodzące do systemu obsługującego zasoby katalogowe podają **domniemaną nazwę** obiektu (ang. *purported name*), która ma właściwą dla X.500 składnię (sekwencja RDN-ów), chociaż nie musi być nazwą obiektu istniejącego w zasobach. Procedura nazywana **analizą nazwy** (ang. *name resolution*) sprawdza, czy obiekt o zadanej nazwie istnieje. Z logicznego punktu widzenia jest to sekwencyjne dopasowanie kolejnych RDN-ów nazwy wyróżnionej do poszczególnych gałęzi drzewa X.500. Proces analizy nazwy obiektu może mieć, z powodu dystrybucji zasobów, istotny wpływ na efektywność, ponieważ zdarza się, że aby dotrzeć do wskazanego obiektu trzeba wykonać wiele operacji.

Wybór właściwej usługi katalogowej nie jest rzeczą prostą (zob. artykuł [4]). Istnieje kilka produktów ubiegających się o miano globalnej usługi katalogowej. Chociaż podstawą do rozwoju oprogramowania usługi katalogowej stał się standard X.500, często jest on implementowany w ograniczonym zakresie. Prowadzi to do istotnych utrudnień, nieraz nawet uniemożliwia współpracę systemów, używających różnego oprogramowania. Jest to szczególnie istotna sprawa, jeżeli stosowana jest replikacja. Sam standard, zawierający dobrą definicję infrastruktury lokalizacji obiektów w sieci komputerowej, nie jest wystarczający. W celu powszechnej adaptacji prezentowanych rozwiązań konieczna jest dobra dostępność oprogramowania. Omówienie tych problemów można znaleźć w pracy [2].

2. Rozproszony charakter zasobów katalogowych

Ilość danych, które potencjalnie mogą być umieszczone w zasobach katalogowych jest ogromna. Standard X.500 definiuje podstawowe klasy obiektów oraz atrybuty, ale mogą one zostać rozbudowane, w celu dopasowywania schematu bazy do lokalnych potrzeb rodzaju i zakresu gromadzonych danych — istotnie podnosi to możliwości zastosowania prezentowanego systemu do obsługi różnych dziedzin życia. Ze swojej natury usługa X.500 jest globalną, rozproszoną bazą danych zasobów sieciowych, swego rodzaju książką informacyjno-adresową. Utrzymywanie scentralizowanej bazy danych tego typu nie dawałoby dobrych rezultatów. Baza musiałaby być bardzo duża, co zmniejszałoby efektywność pracy, poza tym awaria uniemożliwiałaby całkowicie korzystanie z usługi. Drugim argumentem przeciw takiemu podejściu jest uciążliwość zarządzania danymi. Zasadnicze przyczyny dystrybucji zasobów X.500 są typowe, wspólne dla większości systemów rozproszonych:

- **Względy organizacyjne i ekonomiczne**
  Poszczególne bazy danych, tworzące jeden system globalny są rozdzielone pomiędzy instytucje, które nimi zarządzają. Bardzo często sama natura aplikacji bazodanowych decyduje o ich rozproszonym charakterze. W przypadku lokalnie utrzymywanej bazy jej struktura może zostać rozbudowana stosownie do potrzeb i obsługiwanego środowiska.
- **Połączenie istniejących baz danych**
  Lokalne bazy danych mogą istnieć początkowo niezależnie. Potrzeba korzystania z nich za pomocą jednego rodzaju interfejsu użytkowego wymusza utworzenie globalnej aplikacji, której komponentami są systemy lokalne.

- poprawa efektywności realizacji zleceń pobrania danych z zasobów — kopie danych mogą zostać umieszczone bliżej rzeczywistych użytkowników i są używane mniej intensywnie,
- niezawodność — jeżeli jedna kopia danych jest czasowo niedostępna, można w jej miejsce użyć innej.

Nie sposób jednak zyskać nie tracąc czegoś w zamian. Kosztem replikacji jest wzrost złożoności systemu oraz konieczność przechowywania i zarządzania replikami, a nie jest to zagadnienie trywialne. Teoria replikacji jest bardzo rozbudowana. Wiążą się z nią takie problemy jak: transakcyjne przetwarzanie, kontrola współbieżności i niepodzielności, synchronizacja dostępu, spójność zasobów. Na ogół specyfika albo rola systemu narzuca wyraźne żądania odnośnie spójności danych. Niektóre systemy, przede wszystkim te, które pracują w trybie rzeczywistym, wymagają, by były zachowane reguły przetwarzania zadań, gwarantujące synchronizację i właściwe uporządkowanie realizowanych operacji. Opierają się one na pojęciu **transakcji**, jednostki grupującej akcje niezbędne do wykonania zadania, wymagające atomowej obsługi. Przetwarzanie transakcji jest kluczowym pojęciem wielu systemów rozproszonych. Rozwój tej teorii przyczynił się do powstania koncepcji rozproszonych obliczeń i zasobów danych, a także systemów tolerujących uszkodzenia. Każda wykonywana transakcja musi spełniać cztery własności, nazywane w skrócie ACID. Musi ją charakteryzować atomowość (ang. *atomicity*), czyli jest realizowana w całości lub odrzucana, spójność (ang. *consistency*), tj. ma powodować przejście bazy danych z jednego stanu spójnego do drugiego, odseparowanie (ang. *isolation*), czyli jest niezależna od innych zachodzących w systemie działań oraz trwałość (*durability*), co oznacza, że dokonana przez transakcję aktualizacja zasobów nie ulegnie skasowaniu albo wycofaniu.

Jeżeli system musi spełnić ostro postawione wymagania odnośnie spójności, to znacznie komplikuje się obsługa replikacji. Każdej modyfikacji zasobów musi towarzyszyć powielenie nowej informacji do wszystkich replik. Oznacza to, że aktualizacja replikowanych danych musi być transakcją operującą na wszystkich replikach. Jednocześnie replikacja nie może wprowadzać żadnej dwuznaczności z punktu widzenia użytkownika, aspekty użytkowe muszą ukrywać stosowanie replikacji.

Szczegółowa prezentacja typowych technik replikacji zawarta jest w pracy [6].

Oto kilka przykładów technik replikacji, które są stosowane, gdy istotna jest silna spójność zasobów. Najbardziej rygorystyczny, a jednocześnie najprostszy protokół replikacji — metoda **„czytaj jedną kopię, zapisuj do wszystkich kopii"** (ang. *Read one write all*, ROWA) wymaga, by każda operacja zapisu oznaczała, poza modyfikacją oryginalnego elementu danych, aktualizacje wszystkich replik, w których element jest umieszczony. Takie rozwiązanie sprawdza się tylko, gdy przeważają zlecenia odczytu. Daje wówczas dużą niezawodność, dane są dostępne dopóki działa poprawnie co najmniej jeden węzeł posiadający replikę. Wadą takiego podejścia jest konieczność blokowania wszystkich zleceń zapisu, jeśli chociaż jedna z replik nie jest dostępna. Modyfikacją protokołu ROWA jest metoda **„czytaj jedną kopię, zapisuj do wszystkich dostępnych"** (ang. *Read one write all available*, ROWA-A), nazywana algorytmem dostępnych kopii, w której aktualizacje są dokonywane we wszystkich czynnych replikach.

Istnieje sporo rozwiązań stosujących strategię zajmowania większościowego zasobów przed wykonaniem zapisu albo odczytu. Dla potrzeb replikacji wprowadzane jest często pojęcie kopii **podstawowej** (ang. *primary copy*) albo **wyróżnionej** (ang. *distinguished copy*). Według tej teorii, jedna z replik jest traktowana w sposób szczególny. Z nią wiążą się żądania zajęcia elementu danych albo jego zwolnienia. Istnieją metody wykorzystujące ogólne założenia tej strategii, ale różniące się sposobem wyboru kopii wyróżnionych. Można tu wymienić m.in. odmianę protokołu ROWA, korzystającą z kopii podstawowej (ang. *Primary Copy* ROWA). Jedna z replik jest wskazywana jako podstawowa, pozostałe są kopiami **zapasowymi** (ang. *backup*). Operacja zapisu jest wykonywana na kopii podstawowej oraz wszystkich funkcjonujących kopiach zapasowych, natomiast operacja odczytu dotyczy kopii podstawowej. W podejściu tym kopie zapasowe służą do awaryjnego zastąpienia repliki podstawowej. Inna technika jest nazywana po prostu metodą **kopii podstawowej** (ang. *primary copy*). Zasoby są dzielone na jednostki zwane fragmentami, które mogą być replikowane pomiędzy różne węzły. Lokalizacja replik jest znana, dodatkowo wszystkie węzły są uporządkowane w znany sposób. Każdy węzeł przechowuje listę odwołań do swoich partnerów, przechowujących repliki i może ją wykorzystać listę dla określenia, która z kopii jest podstawowa. Kopią podstawową jest ta, która występuje na liście najniżej w określonym uporządkowaniu. Operacja zapisu jest zawsze przekazywana do kopii podstawowej, a potem zmiany wartości elementów są kolejno propagowane do wszystkich replik. Operacja odczytu może, w zależności od decyzji, dotyczyć kopii podstawowej albo jest realizowana w

główny i tylko on może modyfikować kopię podstawową obiektu (ang. *primary copy*). Wszystkie pozostałe repliki mogą być wykorzystywane wyłącznie do operacji odczytu danych i dlatego są nazywane kopiami wtórnymi (ang. *secondary copy*). Będzie o tych metodach mowa w części 4.

Tradycyjny model replikacji, spełniający zasady przetwarzania transakcji w systemie rozproszonym, często nazywany jest **gorliwą propagacją zmian danych** (ang. *eager propagation*). Wymaga się w nim, by transakcja zapisująca nowe dane od razu aktualizowała wszystkie repliki tego elementu, czyli mamy do czynienia z synchroniczną aktualizacją wszystkich replik danego elementu danych w ramach jednej atomowej transakcji. Najnowsze technologie preferują **powolną propagację zmian danych** pomiędzy replikami (ang. *lazy propagation*). Każdy węzeł ma prawo modyfikować lokalne dane. Aktualizacja replik jest dokonywana asynchronicznie, po zatwierdzeniu transakcji zapisu w węźle źródłowym, potem następuje propagacja kopii. Istotną zaletą jest poprawa czasu odpowiedzi systemu. Podejście to stwarza jednak możliwość zatwierdzenia dwóch transakcji aktualizacji , które wprowadzają kolizję. W efekcie konieczne jest zastosowanie transakcji kompensującej, która musi ustalić ostateczny wynik takiej modyfikacji. Z tym zagadnieniem związane są **procedury uzgadniania** (ang. *reconsilation procedures*).

4. Replikacja w usługach katalogowych

Bieżąca część artykułu stanowi przegląd metod replikacji, które są stosowane w usłudze katalogowej opartej na X.500 oraz LDAP na tle technik zaprezentowanych powyżej.

Zajmijmy się najpierw edycją standardu **X.500'88**. Niestety, nie zawierała ona definicji techniki replikacji, ani odpowiednich do potrzeb replikacji rozszerzeń metod realizacji operacji rozproszonych. Już na początku lat 1990 powstało zaimplementowane na podstawie rekomendacji X.500'88 bardzo popularne w środowisku akademicko-naukowym oprogramowanie QUIPU, będące integralną częścią pakietu ISODE. W oparciu o QUIPU został uruchomiony projekt o nazwie PARADISE, który miał służyć przetestowaniu funkcjonowania serwisu X.500 oraz stanowił podłoże do licznych eksperymentów. W konsekwencji prace te przyczyniły się do intensywnego rozwoju kolejnych wersji standardu. Eksploatacja pakietu QUIPU pokazała wiele niedostatków międzynarodowych rekomendacji. W szczególności problemy dotyczyły braku ustaleń dotyczących techniki replikacji zasobów. Mimo że usługa X.500 działała wówczas eksperymentalnie, pojawiła się potrzeba stosowania replikacji. Przykładowo, serwer funkcjonujący w jednostce organizacyjnej dla zwiększenia efektywności powinien mieć kopie danych poziomu kraju albo świata — istnienie tych danych znacznie przyspiesza fazę analizy nazwy encji dostarczonej w zapytaniu. W listopadzie 1991 roku ukazały się dokumenty Internetowe z serii Request for Comments, nr 1275 i 1276, autorstwa S. Hardcastle-Kille z University College London ([11], [12]). Zawierają one zalecenia, dotyczące niezdefiniowanych w standardzie metod realizacji operacji rozproszonych oraz obsługi replikacji. Prezentowane w RFC rozwiązania oparte były na testach efektywności implementacji QUIPU. Autor zastrzegał, że zalecenia te powstały z powodu konieczności wprowadzenia doraźnych rozwiązań, podkreślał wewnętrzny oraz przejściowy charakter proponowanych technik. Fakt, że metody replikacji oraz związane z tym rozszerzenia obsługi operacji rozproszonych nie zostały zestandaryzowane od razu miał znaczny wpływ na trudności współpracy serwisów X.500 zaimplementowanych przez różnych producentów. Stanowiło to również ograniczenie w popularyzacji tej usługi.

Rzeczywiście, propozycja replikacji zawarta w RFC1276 jest modelem bardzo uproszczonym. Zakłada, że w systemie jest możliwe występowanie czasowych niespójności. Takie podejście wynika przede wszystkim z funkcji usługi katalogowej. Zasoby gromadzone w bazach X.500 są przede wszystkim odczytywane i przeszukane. Modyfikacje są znacznie rzadsze. Porównanie z rozważaniami na temat technik replikacji wskazuje, że jest to typowy system o obniżonej, czy wręcz słabej spójności danych.

Mechanizm replikacji stosuje rozszerzony model zasobów X.500, w którym przewiduje się umieszczanie wielowartościowych odesłań, wskazujących serwer zawierający dane podstawowe (ang. *master*) oraz serwery utrzymujące podrzędne kopie danych (ang. *slave*). Aktualizacja dotyczy zawsze danych podstawowych. Zlecenia odczytu mogą korzystać z kopii podrzędnych.

Model danych, rekomendowany w RFC 1276 wprowadza dla potrzeb protokołu replikacji pewne ograniczenia. Określa się mianowicie jednostkę replikacji jako kompletny zbiór encji bezpośrednio podporządkowanych bieżącej encji. Jest to **blok danych encji** (ang. *Entry Data Block*, EDB). EDB

strategią, są propagowane do kopii wtórnych. Serwer główny (ang. *master DSA*) jest **dostawcą** danych (ang. *supplier DSA*), serwer utrzymujący replikę — **konsumentem** (*consumer DSA*). Informacja podlegająca odzwierciedlaniu to poddrzewo, odpowiadające określonemu kontekstowi nazewnictwa, którym zarządza serwer-dostawca. Można również, poprzez zawarcie specjalnych uzgodnień, zażądać odzwierciedlania wybranych encji z poddrzewa, a nawet w ramach wybranych encji kopiować wskazane atrybuty.

W celu realizacji odzwierciedlania zawierane jest **porozumienie** (ang. *shadowing agreement*) między serwerem-dostawcą a serwerem-konsumentem, które ustala jednostkę replikacji, tryb aktualizacji, nazwę i adres głównego DSA oraz zezwala lub nie na zawieranie porozumień wtórnego odzwierciedlania.

Jednostka replikacji (ang. *unit of replication*), zwana również **obszarem replikacji** (ang. *replicated area*) musi mieścić się w kontekście nazewnictwa, którym zarządza serwer. Jeżeli obszar replikacji kończy się powyżej najniższego poziomu globalnego drzewa danych, to towarzyszy mu zestaw odsyłaczy informacyjnych, po jednym dla każdej encji umieszczonej bezpośrednio poniżej replikowanego obszaru. Odsyłacze takie wskazują serwer, który posiada bliższą informację na temat encji, której dotyczy, niekoniecznie zawiera pełny jej opis. Ta zawężona informacja odnośnie wskazań serwerów przechowujących konteksty nazewnictwa wprowadza pewne opóźnienia w trakcie obsługi zlecenia związane z koniecznością wielokrotnego nawigowania wzdłuż drzewa danych w celu dotarcia do miejsca docelowego. Dla poprawy efektywności rekomendacje dopuszczają stosowanie tzw. **rozbudowanej informacji na temat kontekstu** (ang. *extended knowledge*) poprzez duplikowanie w obszarze replikacji odsyłaczy do encji podporządkowanych w stosunku do danego kontekstu nazewnictwa.

Odzwierciedlanie danych z podstawowego serwera do wskazanego DSA zwane jest **odzwierciedlaniem zasadniczym** (ang. *primary shadowing*). Alternatywna metoda polega na wykorzystaniu kopii danych rezydującej na serwerze, który otrzymał replikę z podstawowego DSA. Serwer ten, jeśli porozumienie z podstawowym DSA na to zezwala, może zawrzeć uzgodnienie z innymi serwerami i przekazywać im wtórną kopię danych, w ten sposób realizowane jest **odzwierciedlanie wtórne** (ang. *secondary shadowing*). Zaletą takiego rozwiązania jest ograniczenie liczby serwerów, do których główny serwer DSA musi przekazać aktualizacją danych, dzięki czemu zostaje rozłożone obciążenie poszczególnych węzłów. Poza tym taka metoda może być bardzo korzystna w konkretnych sytuacjach połączeń między serwerami, np. gdy część serwerów znajduje się w szybkiej sieci LAN, a pozostałe w wolniejszej sieci rozległej. Wadą techniki wtórnego odzwierciedlania jest oddalenie konsumenta od głównego DSA, jest to szczególnie niekorzystne w przypadku konieczności łańcuchowania operacji typu aktualizacja, które muszą zostać wykonane przy użyciu kopii głównej.

Tryb aktualizacji reguluje zasady propagowania zmian. Służy do podania kiedy i w jakich odstępach czasowych ma nastąpić przesłanie nowej repliki oraz kto inicjuje wymianę danych. Do wyboru są trzy możliwości:

1. Inicjuje dostawca po aktualizacji danych podlegających replikacji.
2. Okresowa aktualizacja inicjowana jest przez dostawcę.
3. Okresowa aktualizacja inicjowana jest przez konsumenta.

W przypadku okresowej aktualizacji można wyspecyfikować termin pierwszego transferu, jeśli nie zostanie on podany zakłada się, że transmisja informacji nastąpi zaraz po uaktywnieniu porozumienia dotyczącego odzwierciedlania. Wszystkie dopuszczalne tryby mają charakter asynchroniczny, typowy dla opisanej wcześniej replikacji powolnej, propagacja następuje według ustalonych reguł, po zatwierdzeniu operacji zapisu w węźle utrzymującym kopie główną.

Po pomyślnym zakończeniu fazy uzgodnień między serwerami może nastąpić właściwe przesyłanie danych, które odbywa się zgodnie z **protokołem odzwierciedlania informacji** (ang. *Directory Information Shadowing Protocol*). Jest on zorientowany połączeniowo, podobnie jak DAP (*Directory Access Protocol*) i DSP (*Directory Service Protocol*). Przed właściwą wymianą informacji realizowana jest operacja nawiązania połączenia, która może wiązać się z uwierzytelnieniem stron (jeśli wymagają tego uzgodnienia odzwierciedlania). Protokół DISP zezwala na realizacje replikacji według ustalonego trybu aktualizacji — definiuje dwie możliwości dotyczące strony inicjującej transfer repliki: chęć wysłania kopii zgłasza konsumentowi serwer-dostawca lub serwer-konsument zwraca się do dostawcy repliki ze zleceniem przekazania kopii danych. Operacja aktualizacji repliki może być **pełna** (ang. *total*) lub **przyrostowa** (ang. *incremental*).

nictwa tylko jedna może być repliką podstawową (dopuszcza się również brak repliki podstawowej).

2. Modyfikowalna (ang. *updateable*) – replika przyjmująca wszystkie operacje aktualizacji zasobów, ale nie będąca repliką podstawową, kontekst nazewnictwa może nie posiadać tego typu repliki lub dostarczać dowolną ich ilość.
3. Tylko do odczytu (ang. *read-only*) – akceptująca tylko polecenia nie modyfikujące danych.

Dodatkowo z punktu widzenia zakresu encji, biorących udział w procesie replikacji wyróżnia się repliki:

1. Rzadkie (ang. *sparse*) – zawierające wybrane encje z obszaru replikacji (mogą dotyczyć tylko replik modyfikowalnych lub tylko do odczytu).
2. Fragmentaryczne (ang. *fractional*) – gromadzące wybrane atrybuty w ramach encji (muszą zawsze być tylko do odczytu).
3. Częściowe (ang. *partial*) – będące połączeniem metody 1. i 2, repliki częściowe będące fragmentarycznymi (muszą być tylko do odczytu).

W skrajnym przypadku, jeżeli tylko jedna z kopii głównych jest modyfikowalna, replikacja *multi-master* może stać się *single-master*.

Wprowadzenie replikacji, korzystającej z wielu kopii głównych i dopuszczającej aktualizację danych w dowolnej z tych kopii jest istotną zmianą w technologii replikacji zasobów katalogowych. Standaryzacją replikacji *multi-master*, równolegle do prac w ramach LDAP-a, zajmują się grupy robocze X.500. Przygotowywany jest nowy protokół replikacji — *Directory Multi-Master Replication Protocol*, DMRP, który ma zastąpić przedstawiony wcześniej protokół DISP. Technika *multi-master* daje nowe możliwości, ale jednocześnie stawia nowe wymagania. Obsługa replikacji staje się bardziej skomplikowana. Przegląd technik replikacji udowodnił, że im więcej chcemy otrzymać dzięki replikacji, tym trudniejsza implementacja. Strategia *multi-master* korzysta z osłabionego modelu spójności, dopuszcza się czasowe niezgodności w obrębie replik, przy założeniu, że docelowo repliki muszą być identyczne. Ponieważ aktualizacje danych są propagowane między replikami asynchronicznie, mogą wystąpić konflikty aktualizacji, będące efektem zatwierdzenia sprzecznych modyfikacji danych (np. aktualizacja encji, którą właśnie usunięto w innej kopii danych). Ratunkiem w takiej sytuacji jest realizacja wspominanych wcześniej procedur uzgadniania. Zakres działań, które mają wykonywać te procedury jest bardzo rozbudowany, muszą one uwzględniać różnorodne aspekty, przykładowe rozwiązania są zaprezentowane w dokumencie [16]

5. Podsumowanie

Dokonana w niniejszym artykule prezentacja wskazała główne tendencje widoczne w dziedzinach replikacji oraz obsługi zasobów katalogowych. Przegląd podstawowych technik pokazał, że w systemach rozproszonych stosujących replikację warto dopasować formę replikacji do wymagań systemu. Wprowadzenie ostrych wymagań odnośnie spójności zasobów jest bardzo kosztowne i mimo, że wiodącym założeniem replikacji jest poprawa efektywności, może dać efekt odwrotny. Natura zasobów katalogowych nie wymusza wprowadzania silnej spójności. Techniki replikacji powinny być tu jednocześnie skuteczne i proste. Skuteczność oznacza ostateczne doprowadzenie replik do stanu spójności, mimo przejściowego wystąpienia niezgodności danych. Metody replikacji implementowane eksperymentalnie w pierwszych produktach opartych na standardzie X.500 były bardzo proste, wręcz prymitywne. Podstawową ich rolą było ułatwienie wyszukiwania obiektów w rozproszonej, hierarchicznej bazie katalogowej, ograniczenie liczby operacji potrzebnych do odczytania obiektu. Technika wcielona wraz ze standardem X.500'93 jest dużo bardziej zaawansowana, dopuszcza różnorodne konfiguracje, ale główna idee replikacji pozostaje taka sama — dysponujemy jedną kopią główną i opcjonalnie wieloma kopiami wtórnymi — replikami, zlecenia aktualizacji muszą być realizowane w węźle dysponującym kopią główną, kopie wtórne wspomagają operacje odczytu, wyszukiwania oraz analizy nazwy obiektu. Dopiero będąca obecnie w fazie standaryzacji technologia *multi-master* wprowadzi możliwość operowania na kilku kopiach danych. Kierunek działań w zakresie replikacji w usługach katalogowych świadczy o tym, że rozwiązania minimalistyczne nigdy nie są dobre w profesjonalnych systemach. Wymagania użytkowników systemów rozproszonych są różnorodne i muszą zostać udostępnione technologie bardziej zaawansowane. Usługa katalogowa może być stosowana również w systemach, które narzucają potrzebę zagwarantowania wysokiej spójności zasobów. Są przykłady

EUROPEJSKA USŁUGA KATALOGOWA PARADISE-NAMEFLOW: PERSPEKTYWY I ZASTOSOWANIA

Maja Górecka **Tomasz Wolniewicz**

Maja.Gorecka@cc.uni.torun.pl *twoln@hpc.uni.torun.pl*

Uniwersytet Mikołaja Kopernika w Toruniu
Naukowa Akademicka Sieć Komputerowa NASK
Zakład Rozproszonych Systemów Informacyjnych

Podstawowym celem niniejszego opracowania jest podsumowanie działania światowej usługi katalogowej, ze szczególnym uwzględnieniem udziału Polski, przedstawienie nowych wyzwań i perspektyw na przyszłość. Nie opisujemy tutaj szczegółów związanych z określeniem usługi katalogowej, nazewnictwem obiektów itp. Te informacje można znaleźć we wprowadzeniu pracy [3].

1. Projekt PARADISE

W roku 1988 CCITT zdefiniowało standard X.500 [1]. Określenie rozproszonej usługi katalogowej nie było oparte o wcześniejsze, testowe implementacje, a zatem pozostawiało wątpliwości co do bezbłędności rozwiązań i stwarzało konieczność przeprowadzenia szeroko zakrojonego testu praktycznego. Trzeba podkreślić, że były to zaledwie początki Internetu, w połączeniach sieciowych dominował standard X.25, w poczcie elektronicznej — X.400. Usługa katalogowa, realizowana w protokołach OSI wydawała się bardzo naturalna i niezbędna. W University College Computer Centre w Londynie opracowano oprogramowanie QUIPU implementujące standard X.500, uzyskano dofinansowanie COSINE i w roku 1990 uruchomiono projekt o nazwie PARADISE.
Celem PARADISE było zainstalowanie rozproszonej usługi katalogowej w środowiskach akademickich i sprawdzenie mechanizmów współpracy serwerów oraz poprawności definicji protokołów X.500.
Zainteresowanie uczestnictwem było znaczne i projekt objął swoim zasięgiem niemal cały świat (do prac włączyły się North American Directory Forum i jego odpowiednik w Australii).
Polska przystąpiła do PARADISE w 1992 roku, po uruchomieniu pierwszego serwera na UMK w Toruniu.
Finansowanie projektu PARADISE przez COSINE zakończyło się w roku 1994 i koordynację usługi katalogowej przejęło DANTE pod nazwą NameFlow-Paradise. DANTE wprowadziło system odpłatności dla krajów uczestniczących w projekcie, pozostawiając jednak nadal szansę udziału bezpłatnego, bez prawa do uczestniczenia w pewnych spotkaniach koordynacyjnych oraz wpływania na losy projektu.

2. Oprogramowanie dla X.500

Podstawowym oprogramowaniem wykorzystywanym dotąd w projekcie PARADISE jest QUIPU, które powstało na bazie pakietu ISODE i stało się jego częścią. Do wersji 8.0 oprogramowanie było dystrybuowane bezpłatnie i rozwijane w ULCC. W roku 1993 zawiązało się ISODE Consortium, którego celem był dalsza praca nad pakietem ISODE, z wykorzystaniem jego potencjału komercyjnego. Z uwagi na duży wkład środowiska akademickiego w dotychczasowy rozwój pakietu ISODE, podtrzymano dystrybucję źródeł oprogramowania na zasadzie bezpłatnych licencji dla jednostek o charakterze naukowym. Taka sytuacja trwała do 1996, kiedy to wprowadzono konieczność wnoszenia opłat subskrypcyjnych. Oprogramowanie nadal rozpowszechniane jest w postaci źródłowej.
QUIPU stało się punktem wyjścia dla całej gamy produktów X.500 rozwijanych komercyjnie. Takie oprogramowanie oferują m.in. firmy Nexor, ISOCOR.

pośredniczące – odsyłające do innych serwerów). Ilości zapytań, czy połączeń nie należy mylić z ilością operacji wykonanych przez serwer (takich operacji w czasie jednego połączenia może być bardzo wiele). Serwer krajowy wykonuje w ciągu godziny średnio ponad 1100 operacji przeszukania, a ponad 2100 operacji w ogóle.

Raport z 99-05-06 15:00

Instytucja	DSA	OK	Ilość danych	Ostatnie próby
Politechnika Gdańska	Anaconda	Tak	6190	10/10
Poznan Poznań	Cayman	Tak	6095	9/10
UAM w Poznaniu	Condor	Tak	5453	10/10
Uniwersytet Szczeciński	Gibbon	Tak	3013	10/10
ATR Bydgoszcz	Hawk	Tak	1554	10/10
Politechnika Zielonogorska	Iguana	Tak	1299	10/10
UMK Toruń	Jaguar	Tak	4174	10/10
Politechnika Łódzka	Lodz	Tak	3857	10/10
ICM Warszawa	Piranha	Tak	9249	10/10
Cyfronet Kraków	Puma	Tak	17384	9/10
Akademia Ekonomiczna we Wrocławiu	Racoon	Nie	1453	9/10
Politechnika Wrocławska	Vampire Bat	Nie	8368	9/10
Toruń - Serwer krajowy	Ocelot	poza testem	15554	
Razem wszystkich danych w polskim X.500			83643	
Procent dostępnych danych			88.3%	

Znacznym wyzwaniem było dostosowanie bazy X.500 do języka polskiego z jednoczesnym przestrzeganiem ogólnych reguł nazewnictwa w ramach światowego projektu. Projekt i implementacja były dalece nietrywialne i są unikalnym rozwiązaniem w całym projekcie PARDISE ([4],[5],[6])
Innym, opracowanym w NASK, projektem było przystosowanie bazy X.500 do obsługi certyfikatów PGP [7].

5. Inne standardy usług katalogowych

Active Directory
Jest to globalna usługa katalogowa wprowadzana przez Microsoft razem z Windows 2000. Globalność oznacza, że ma ona zastąpić wszystkie usługi typu katalogowego, stosowane do wszelkich obiektów i typów informacji, wspomagając zarówno komunikację jak i zarządzanie zasobami. Zgodnie z informacjami Microsoft [8], Active Directory jest oparte o serwer LDAP i z tego powodu będzie całkowicie kompatybilne z produktami LDAP, dodatkowo baza ma udostępniać swoją pełną funkcjonalność za pomocą tego właśnie protokołu. Active Directory będzie zawierało interfejs programisty (ADSI) o bardzo dużych możliwościach (stosowany zarówno w typowych językach C, C++, Java, jak i skryptach). Niezależnie Active Directory będzie również wspierało dotychczasowe, typowe API dla LDAP. Dzięki oparciu schematu bazy o standard LDAP, możliwe jest proste rozbudowywanie go poprzez dodawanie nowych klas obiektów (jest to wspólna cecha wszystkich systemów X.500 i LDAP).
Active Directory nie obsługuje protokołów X.500.
Active Directory ma być w pełni zintegrowane z systemem operacyjnym Windows 2000, w szczególności ma przekładać ograniczenia dostępu stosowane w usłudze katalogowej na prawa dostępu używane wewnątrz systemu operacyjnego, tak aby całkowicie integrować lokalne zasoby ze zdalnymi.

w serwery wielu producentów, rodzi wiele trudności i PARADISE jest znakomitym polem do testów. Poważną trudnością jest jednak stosunkowo drogie oprogramowanie.
DANTE wyraża zdecydowaną chęć kontynuowania serwisu. Planowane są nowe zastosowania (np. wsparcie infrastruktury PGP), nie ma jednak jeszcze skonkretyzowanych planów działania, co biorąc pod uwagę problem roku 2000 (patrz p. 8), wydaje się stosunkowo niepokojące. Planowane jest przestawienie serwisu na LDAPv3, ale z drugiej strony konieczne jest zapewnienie współpracy z serwerami działającymi w oparciu o stare oprogramowanie ISODE 8.0.

7. Nowe wyzwania przed usługami katalogowymi

Jak już wspomnieliśmy, bez usług katalogowych nie sposób wprowadzić globalnego systemu bezpiecznej komunikacji. Standard bezpieczeństwa X.509 jest elementem X.500 i chociażby z tego powodu usługa katalogowa wykorzystująca nazewnictwo zgodne z X.500 jest naturalną bazą do przechowywania certyfikatów. Większość pakietów certyfikujących jest ściśle związana z produktem wspierającym X.500 (lub przynajmniej jego nazewnictwo).
Usługa katalogowa jest również naturalnym miejscem przechowywania certyfikatów PGP. W ramach prac NASK opracowaliśmy projekt takiego wykorzystania bazy X.500 oraz przygotowaliśmy zestaw narzędzi umożliwiających automatyczny dostęp do bazy [7]. Najnowsze implementacje PGP wprost wspierają protokół LDAP do pobierania kluczy, konieczne jest jednak odpowiednie przygotowanie samej usługi katalogowej. Zasadniczą trudnością związaną z obsługą PGP jest fakt, że podpisy elektroniczne na zawierają informacji o właścicielu klucza, a jedynie o jego odcisku. Kiedy użytkownik otrzymuje podpisany plik, a nie ma w swoim zbiorze klucza tego, który odpowiada podpisowi, nie jest w stanie dowiedzieć się od kogo on pochodzi. Stwarza to konieczność globalnego przeszukiwania bazy wszystkich kluczy ze względu na odcisk (niewykonalne z powodu globalnego rozproszenia), albo tworzenia ogromnych indeksów. Trwają obecnie prace nad wykorzystaniem do takiego celu struktury projektu NameFlow-PARADISE.
Przy opisie usług Active Directory, NDS i FNS zauważyliśmy, że poza czysto informacyjną, mają one przede wszystkim rolę przy zarządzaniu. Jest to powrót idei stosowania usług katalogowych w sposób zgodny z ich pierwotnym przeznaczeniem. Innym podobnym przykładem może być zastosowanie serwera LDAP do obsługi systemu zarządzającego metakomputerem o nazwie Globus.
Usługa katalogowa typu X.500 tym się różni od sytemu DNS, że udostępnia możliwość wyszukiwania informacji. Zakres wyszukiwania nie zależy do sposobu rozproszenia danych. Trudności związane z przeszukaniem znacznych obszarów danych (pomimo równoległego wykonywania się) powodują jednak, że typowe zastosowanie X.500 to tzw. White Pages, czyli proste przeglądanie kolejnych poziomów, ew. przeszukanie w stosunkowo wąskim zakresie (pojedynczej instytucji). Wielu użytkowników jest jednak zainteresowanych usługą Yellow Pages, czyli wyszukiwaniu ze względu na kategorie. Skuteczna realizacja takich wyszukań wymaga wstępnego indeksowania. W ramach PARADISE prowadzono kilka projektów indeksowania zasobów, ale nie przyjęło się żadne z proponowanych rozwiązań. Podstawowym problemem jest konieczność modyfikacji oprogramowania klienckiego. Uruchomienie usługi indeksującej jest jednym z zamiarów DANTE.
Dostrzegając ten problem Microsoft wbudował w Active Directory współpracę z serwisem indeksującym o nazwie Global Catalog.

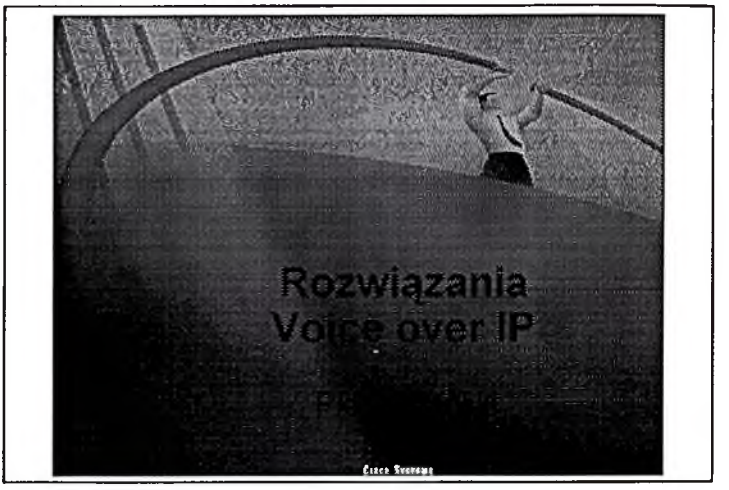
8. Problem roku 2000

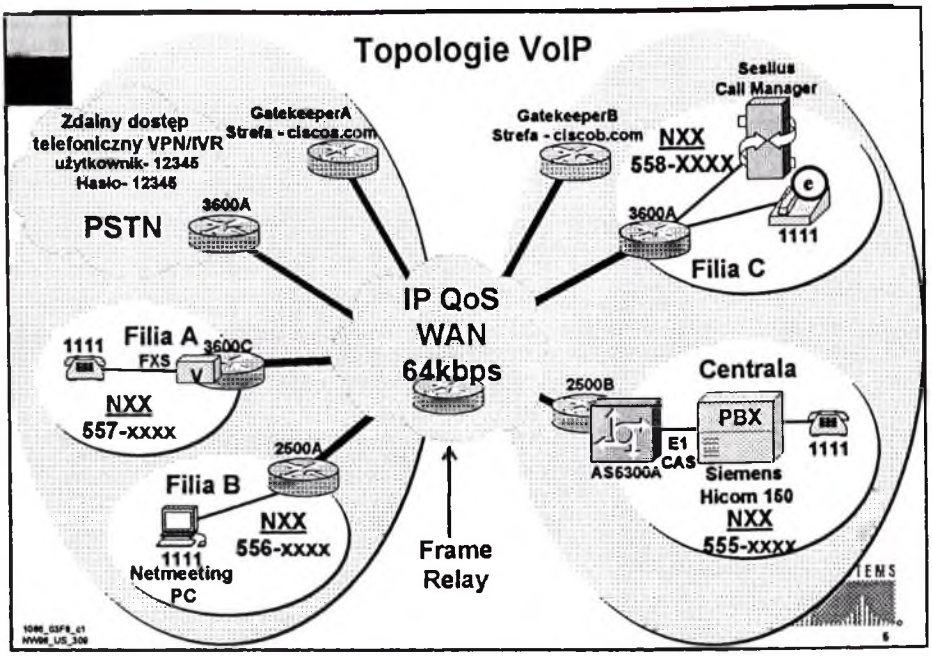
Wiadomo, że dostępne bezpłatnie wersji QUIPU nie są odporne na problem roku 2000. Daty występują w znacznikach replik i w znacznikach ostatniej modyfikacji. Autorzy oprogramowania oceniają, całkowite poprawienie kodu wymagałoby ok. 3 miesięcy pracy programisty. W Polsce tylko UMK wykorzystuje najnowsze oprogramowanie X.500, wszystkie inne środowiska stosują serwery, które nie są "bezpieczne". Do końca października 1999 przeprowadzone zostaną próby w ramach polskiego projektu X.500, które pozwolą określić rozmiar problemu. W tym czasie powinno być również więcej informacji na temat możliwości wykorzystania innych produktów usługi katalogowej. Na podstawie

ROZWIĄZANIA „VOICE OVER IP" CISCO SYSTEMS

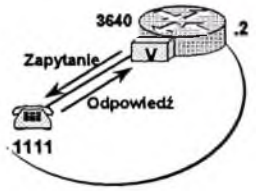
Piotr Orlański

CISCO Systems





Autentykacja użytkownika



Podstawowa aplikacja autentykująca dla sieci VoIP

Zapytanie: "Proszę podać numer użytkownika"
Odpowiedź: "12345"
Zapytanie: 'Proszę podać hasło"
Odpowiedź: "12345"
Zapytanie: "Proszę wprowadzić numer telefonu"
Odpowiedź: "(22) 6722713"

Wymagane pasmo

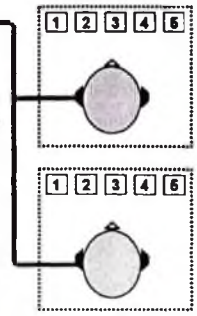
Dla pojedynczego kanału głosowego

Kodowanie/ kompresja	pasmo
G.711 PCM	64 kbps (DS0)
G.726 ADPCM	16, 24, 32, 40 kbps
G.727 E-ADPCM	16, 24, 32, 40 kbps
G.729 CS-ACELP	8 kbps
G.728 LD-CELP	16 kbps
G.723.1 CELP	6.3/5.3 kbps

CISCO SYSTEMS

Pomiar jakości

"Nowadays, a chicken leg is a rare dish."



Ocena	Jakość	Poziom zniekształceń
5	Doskonała	Niesłyszalny
4	Dobra	Ledwo słyszalny, nie przeszkadza
3	Przeciętna	Słyszalny, nie przeszkadza
2	Słaba	Przeszkadza, pozwala rozumieć
1	Zła	Bardzo przeszkadza, uniemożliwia rozmowę

MOS-f4.0 = jakość operatorska

CISCO SYSTEMS

Wpływ traconych pakietów na jakość transmisji (Mean Opinion Scores)

Utracone kolejne pakiety	1	2	3	4	5
M.O.S.:	4.2	3.2	2.4	2.1	1.7

"G.729 Error Recovery for Internet Telephony",
Jonathan Rosenberg, Lucent Technology and Columbia University
V.O.N. Conference 9/97

Cisco Systems

13

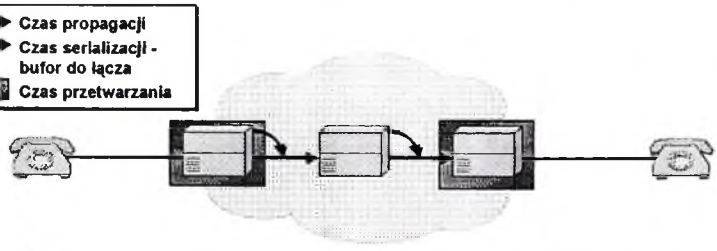
Echo

- Echo staje się problemem wraz z czasem powrotu i siłą

Cisco Systems

14

Opóźnienie - składniki stałe



- Propagacja—Sześć mikrosekund na kilometr
- Serializacja
- Przetwarzanie
  - Kodowanie/kompresja/dekompresja/dekodowanie
  - Konwersja pakietowa

Cisco Systems

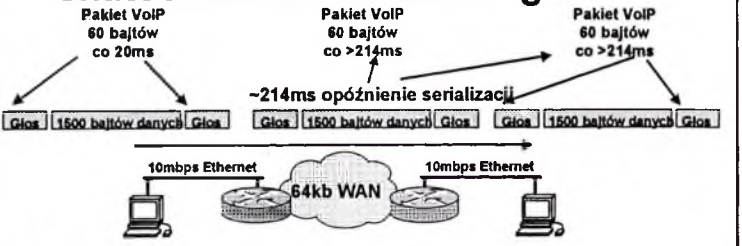
Tablica czasu serializacji

Rozmiar ramki

Prędkość łącza							
			128	256	512	1024	1500
56kbps	143us	9ms	18ms	36ms	72ms	144ms	214ms
64kbps	125us	8ms	16ms	32ms	64ms	128ms	187ms
128kbps	62.5us	4ms	8ms	16ms	32ms	64ms	93ms
256kbps	31us	2ms	4ms	8ms	16ms	32ms	46ms
512kbps	15.5us	1ms	2ms	4ms	8ms	16ms	23ms
768kbps	10us	640us	1.28ms	2.56ms	5.12ms	10.24ms	15ms
1536kbs	5us	320us	640us	1.28ms	2.56ms	5.12ms	7.5ms

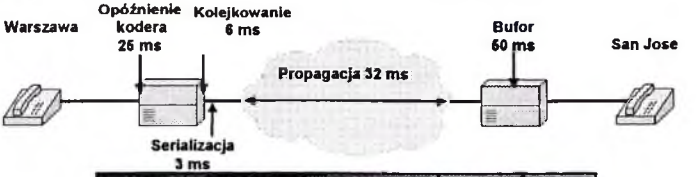
Cisco Systems

Wielkość pakietu danych może skutecznie zniekształcać głos



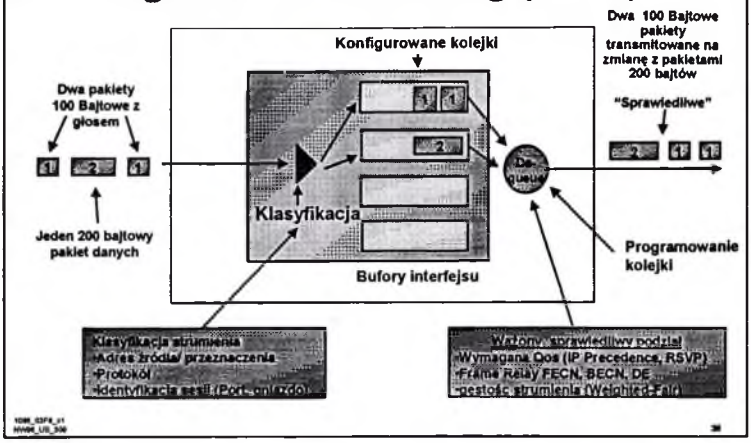
- Duże pakiety danych mogą blokować bufor wprowadzając zniekształcenia w transmisji głosu
- Jitter i sposób buforowania pozwala częściowo wyrównać opóźnienie i jego zmiany

Obliczenie budżetu opóxnień



	Fixed Delay	Variable Delay
Kolejkowanie 64 kbps		6 msec
Propagacja	32 msec	
Bufor	60 msec	
Razem	110 msec	

Weighted Fair Queuing (WFQ)



IP Precedence

- **Ustaw wyższe IP Precedence dla VoIP**
  - Rezultat = Dedykowana kolejka WFQ dla VoIP
  - Konfiguracja: Węzeł brzegowy, proxy, lub statycznie
- **Może dać lepsze rezultaty niż RSVP**
- **Brak trwałej alokacji pasma**

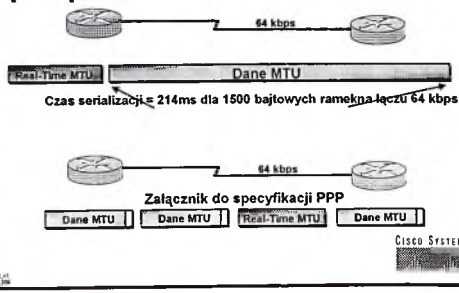
CISCO SYSTEMS

Weighted Random Early Detection (W-RED)

- Zapobieganie natłokowi
- Reakcja protokołu transportowego na utratę pakietu
- Synchronizacja

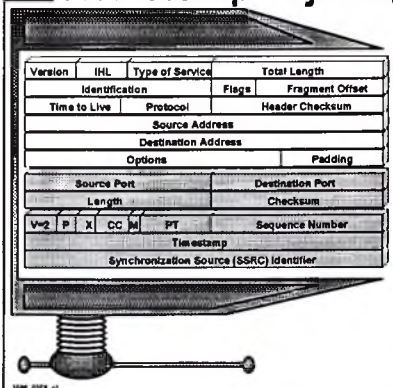
Cisco Systems

Multilink PPP z fragmentacją i przeplotem



Cisco Systems

RTP Kompresja nagłówka



Overhead

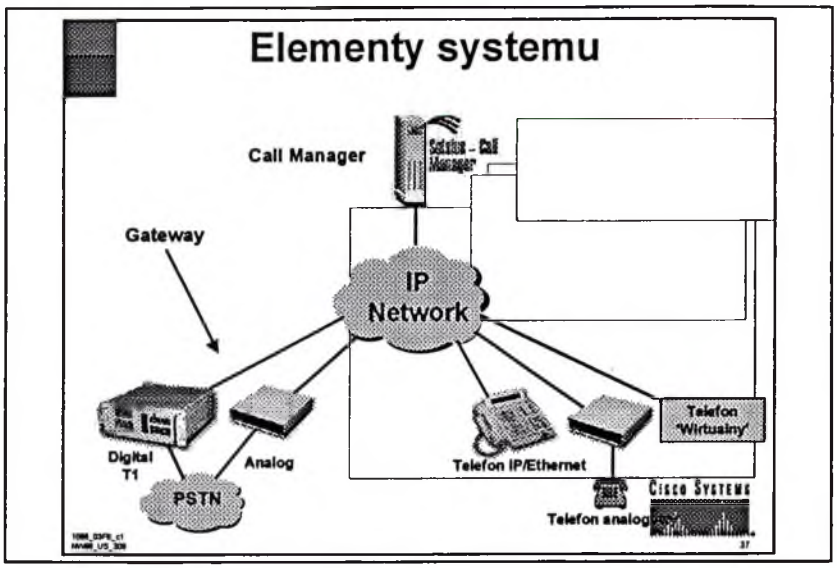
- 20ms@8kb/s oznacza 20 bajtów "danych"
- Nagłówek IP = 20; UDP = 8; RTP = 12
  - 2X więcej od zawartości!!!!!!!!!
- Kompresja nagłówka z 40 do 2-4 bajtów
- CRTP—Compressed Real-time protocol

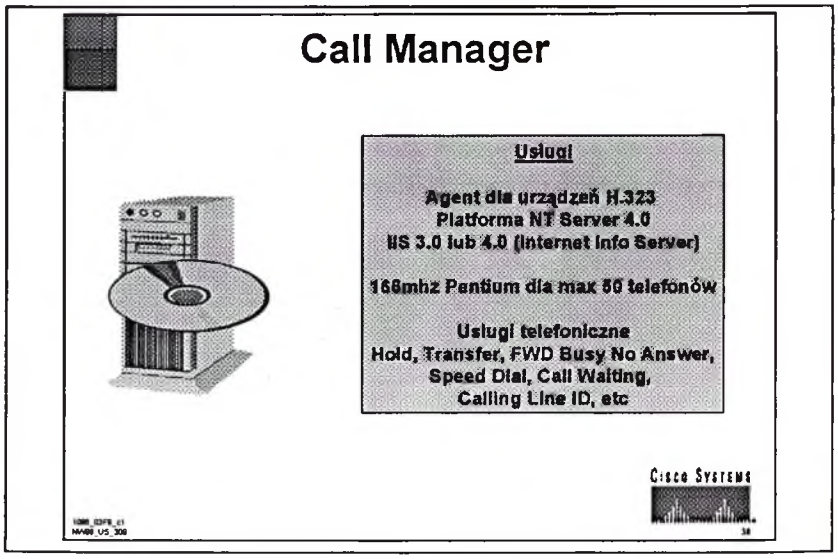
CISCO SYSTEMS

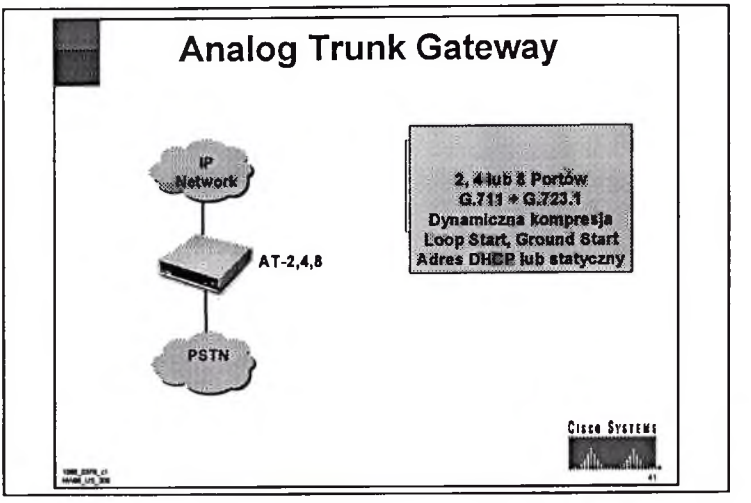
Kiedy i co ?

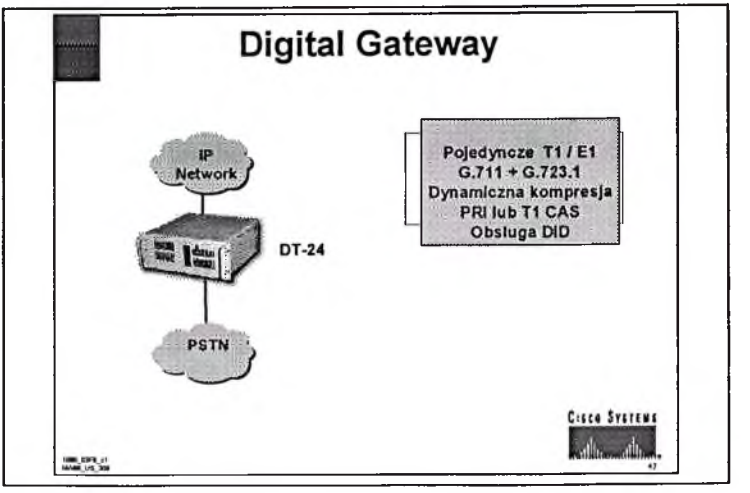
- IP precedence
  - Telefonia sieciowa
  - Telekonferencje
- RSVP
  - Videokonferencje
- Oba
  - Aplikacje interaktywne
  - Aplikacje tranzakcyjne
  - SNA w TCP/IP

CISCO SYSTEMS


Elementy systemu
Call Manager
Gateway
IP
Network
Digital
T1
Analog
PSTN
Telefon IP/Ethernet
Telefon
'Wirtualny'
Telefon analog
Cisco Systems


Call Manager
Usługi
Agent dla urządzeń H.323
Platforma NT Server 4.0
IIS 3.0 lub 4.0 (Internet Info Server)
166mhz Pentium dla max 50 telefonów
Usługi telefoniczne
Hold, Transfer, FWD Busy No Answer,
Speed Dial, Call Waiting,
Calling Line ID, etc
Cisco Systems





TAJEMNICA PAŃSTWOWA I SŁUŻBOWA
OCHRONA TAJEMNICY PRZEDSIĘBIORSTWA
/ZESTAW TEMATÓW/

1. Akty prawne z zakresu ochrony tajemnicy państwowej i służbowej.
2. Zasady ochrony informacji stanowiących tajemnicę państwową i służbową.
3. Ochrona tajemnicy przedsiębiorstwa.
4. Zasady ochrony informacji stanowiących tajemnicę przedsiębiorstwa.
5. Koncepcja ochrony tajemnicy przedsiębiorstwa /projekt/.
6. Formy i metody pracy wywiadu gospodarczego i wynikające z niej zagrożenia.
7. Zasady ochrony informacji przed szpiegostwem gospodarczym.

USTAWA Z DNIA 22 STYCZNIA 1999 ROKU O OCHRONIE INFORMACJI NIEJAWNYCH

OKREŚLA W SZCZEGÓLNOŚCI ZASADY:

1. Organizowania ochrony informacji niejawnych.
2. Klasyfikowania informacji niejawnych.
3. Udostępniania informacji niejawnych.
4. Postępowania sprawdzającego, w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy.
5. Szkolenia w zakresie ochrony informacji niejawnych.
6. Ewidencjonowania, przechowywania, przetwarzania i udostępniania danych uzyskiwanych w związku z prowadzonymi postępowaniami o ustalenie rękojmi zachowania tajemnicy, w zakresie określonym w ankiecie bezpieczeństwa osobowego oraz w ankiecie bezpieczeństwa przemysłowego.
7. Organizacji kontroli przestrzegania zasad ochrony informacji niejawnych.
8. Ochrony informacji niejawnych w systemach i sieciach teleinformatycznych.
9. Stosowania środków fizycznej ochrony informacji niejawnych.

USTAWĘ STOSUJE SIĘ MIĘDZY INNYMI WOBEC:

Przedsiębiorców, jednostek naukowych lub badawczo – rozwojowych ubiegających się o zawarcie lub wykonujących umowy związane z dostępem do informacji niejawnych, dotyczące realizacji zadań opłacanych w całości lub w części ze środków publicznych, w rozumieniu przepisów ustawy z dnia 10 czerwca 1994 roku „O zamówieniach publicznych" /D.Z. U. z 1998r. Nr 119, poz. 773/.

5. ROZPORZĄDZENIE PREZESA RADY MINISTRÓW

z dnia 25 lutego 1999 r.

w sprawie szczegółowego trybu prowadzenia przez służby ochrony państwa kontroli w zakresie ochrony informacji niejawnych stanowiących tajemnicę państwową.

6. ROZPORZĄDZENIE PREZESA RADY MINISTRÓW

z dnia 25 lutego 1999 r.

w sprawie sposobu i trybu udostępniania danych z ewidencji.

Rozporządzenie określa sposób i tryb udostępniania danych z ewidencji osób, które uzyskały poświadczenie bezpieczeństwa, a także dane osób, z którymi łączy się dostęp do informacji niejawnych.

7. ROZPORZĄDZENIE PREZESA RADY MINISTRÓW

z dnia 25 lutego 1999 r.

w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych.

8. ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia 23 lutego 1999 r.

w sprawie wzoru poświadczenia bezpieczeństwa oraz wzoru odmowy wydania poświadczenia bezpieczeństwa.

9. ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia 23 lutego 1999 r.

w sprawie wzoru zaświadczenia stwierdzającego odbycie przeszkolenia w zakresie ochrony informacji niejawnych.

KLAUZULE TAJNOŚCI

TAJEMNICA PAŃSTWOWA

Informacje **ŚCIŚLE TAJNE** – w przypadku gdy ich nieuprawnione ujawnienie mogłoby spowodować istotne zagrożenie dla niepodległości, nienaruszalności terytorium albo polityki zagranicznej lub stosunków międzynarodowych Rzeczpospolitej Polskiej albo zagrażać nieodwracalnymi lub wielkimi stratami dla interesów obronności, bezpieczeństwa państwa i obywateli lub innych istotnych interesów państwa, albo narazić je na szkodę w wielkich rozmiarach.

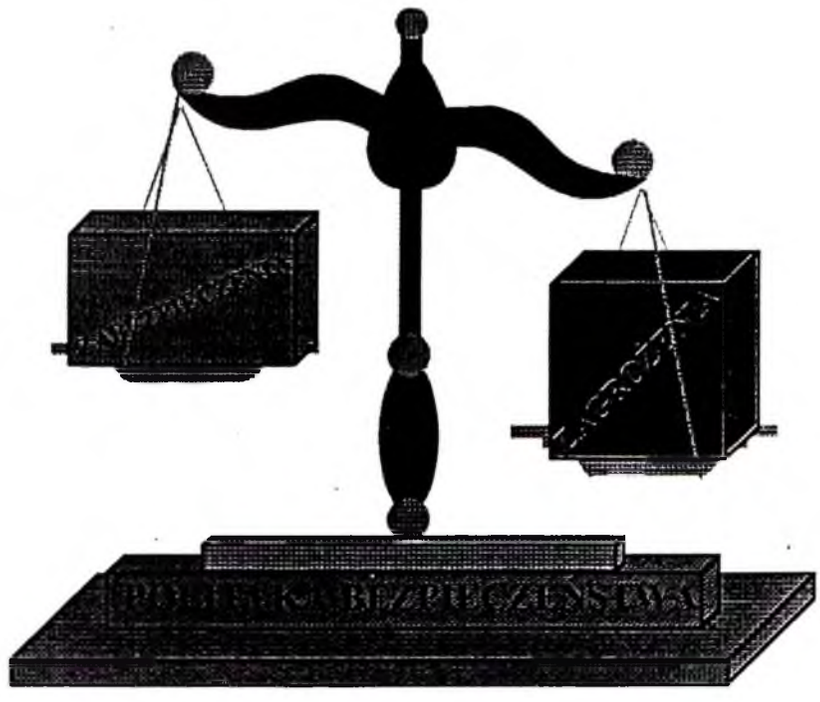
Informacje **TAJNE** – w przypadku, gdy ich nieuprawnione ujawnienie mogłoby spowodować zagrożenie dla międzynarodowej pozycji państwa, interesów obronności, bezpieczeństwa państwa i obywateli, innych istotnych interesów państwa albo narazić je na znaczną szkodę.

TAJEMNICA SŁUŻBOWA

Informacje **POUFNE** – w przypadku, gdy ich nieuprawnione ujawnienie powodowałoby szkodę dla interesów państwa, interesu publicznego lub prawnie chronionego interesu obywateli.

Informacje **ZASTRZEŻONE** – w przypadku, gdy ich nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej.

POLITYKA BEZPIECZEŃSTWA FIRMY



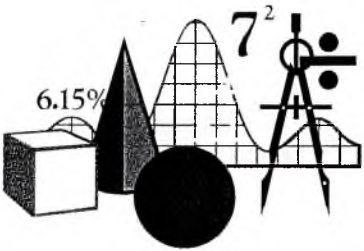
Światowa Organizacja Handlu. World Trade Organisation /WTO/. ustanowiona porozumieniem podpisanym w Marakeszu w 1994 roku. Dotyczy ona wielu aspektów handlu międzynarodowego. Porozumienie rozszerzone zostało o handlowe aspekty praw wolności intelektualnej w formie załącznika /TRIPS/. Porozumienie to zawiera normy dotyczące dostępności, zakresu oraz korzystania z praw wolności intelektualnej, także ochrony tych praw odnoszących się do:

- **praw autorskich i pokrewnych, w tym ochrony programów komputerowych i zbioru danych;**
- **znaków towarowych;**
- **oznaczeń geograficznych, którymi są oznaczenia identyfikujące towar;**
- **wzorów przemysłowych;**
- **topografii /wzorów masek/ układów scalonych;**
- **ochrony informacji nieujawnionej. A będą to takie informacje, które:**

1. *są poufne wówczas gdy jako całość lub w szczególnym zestawie ich elementów nie są ogólnie znane lub łatwo dostępne dla osób, które normalnie nie zajmują się tym rodzajem informacji;*
2. *mają określoną wartość handlową, dlatego że są poufne, a podane zostały przez osobę pod której legalną kontrolą informacje te pozostają.*

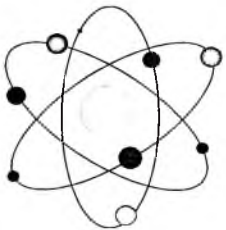
Osoby fizyczne i prawne będące zgodnie z prawem w posiadaniu lub pod ich kontrolą pozostają informacje poufne, winny **skutecznie zabezpieczać te informacje, aby nie zostały ujawnione,** nabyte lub użyte bez ich zgody przez innych w sposób sprzeczny z uczciwymi praktykami handlowymi. Ochronie jako informacja **nieujawniona** podlegają także dane przedstawione rządowi lub agencjom rządowym.

Polska ratyfikowała Porozumienie WTO dnia 30.05.1995 roku. Porozumienie TRIPS opublikowano w Polsce 19.06.1996 roku. Całość przepisów porozumienia TRIPS będzie w Polsce obowiązywała od 01.01.2000 roku. Polska nie jest członkiem Europejskiej Organizacji Patentowej, ale podpisanie Układu Europejskiego 16.12.1991 roku o stowarzyszeniu Polski z Unią Europejską zobowiązało nasz kraj m.in. **„do doskonalenia ochrony praw własności intelektualnej w tym i przemysłowej, aby do końca piątego roku od wejścia w układ osiągnąć poziom podobny do tego istniejącego we Wspólnocie, również w zakresie porównywalnych środków dochodzenia tych praw."**



Główne ośrodki naukowo - dydaktyczne w Polsce zajmujące się problematyką nieuczciwej konkurencji oraz ochroną i zabezpieczaniem tajemnicy przedsiębiorstwa.

1. Międzyuczelniany Instytut Wynalazczości i Ochrony Własności Intelektualnej Uniwersytetu Jagiellońskiego - **KRAKÓW**;
2. Uniwersytet Łódzki - Wydział Prawa Gospodarczego Publicznego i Prawa Finansowego - **ŁÓDŹ**;
3. Instytut Prawa Karnego Uniwersytetu Marii Curie - Skłodowskiej w **LUBLINIE**.
4.
5.
6.



DYSCYPLINARNA. „Za nieprzestrzeganie przez pracownika ustalonego porządku i regulaminu pracy, pracownik może być ukarany – art. 108 §1 KP."

- naganą;
- upomnieniem.

„W przypadku ciężkiego naruszenia przez pracownika podstawowych obowiązków pracowniczych lub popełnienie przez pracownika oczywistego lub stwierdzonego prawomocnym wyrokiem przestępstwa – art. 52 §1 KP."

- rozwiązać umowę o pracę **bez wypowiedzenia z winy pracownika**.

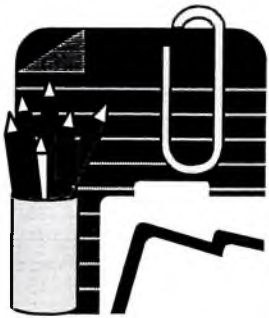
MATERIALNA.

- żądanie naprawienia szkody;
- żądanie odszkodowania;
- żądanie zaniechania działalności konkurencyjnej /ust. o z n k/.

KARNA.

- Kodeks Karny /XXXIII art. 265 – 269/;
- Ustawa o ochronie danych osobowych /roz 8 – art. 49 – 54/;
- Ustawa o zwalczaniu nieuczciwej konkurencji /art. 23/;
- Prawo Prasowe /art. 43/.

ALGORYTM POSTĘPOWANIA W ZAKRESIE KSZTAŁTOWANIA POLITYKI ZABEZPIECZENIA I OCHRONY WIADOMOŚCI STANOWIĄCYCH TAJEMNICĘ PRZEDSIĘBIORSTWA



Polityka ochrony informacji powinna być kształtowana przez kierownictwo przedsiębiorstwa.

W okresie restrukturyzacji i przekształceń własnościowych firmy problematyka ochrony tajemnicy powinna polegać na:

- zdefiniowaniu „majątku informacyjnego firmy" oraz opracowaniu i wdrożeniu **wykazu rodzaju wiadomości stanowiących tajemnicę przedsiębiorstwa**, to jest określeniu najistotniejszych obszarów /wiadomości/, których ujawnienie mogłoby zaszkodzić interesom firmy;
- powołaniu stanowiska menadżera do spraw bezpieczeństwa, który zająłby się kompleksową ochroną całego biznesu, od ochrony fizycznej obiektów firmy, zabezpieczeniu danych w systemach teleinformatycznych /komputerowych/ aż po kontrwywiad firmowy /organizację wywiadowni gospodarczej/;
- opracowaniu struktury organizacyjno - funkcjonalnej biura /zespołu/ odpowiedzialnego za zabezpieczenie i ochronę tajemnicy przedsiębiorstwa i bezpieczeństwa firmy;
- dostosowaniu do obowiązującego prawa i przepisów polityki ochrony tajemnicy przedsiębiorstwa i bezpieczeństwa firmy;
- ustaleniu zasad zarządzania, nadzoru, szkolenia, kontroli w zakresie ochrony informacji stanowiących tajemnicę przedsiębiorstwa;
- zdefiniowaniu i zaplanowaniu reakcji na naruszanie zasad bezpieczeństwa w tym zasad zabezpieczenia i ochrony tajemnicy przedsiębiorstwa.

RAPORT HANDLOWY O FIRMIE

☐ CO ZAWIERA STANDARDOWY RAPORT O FIRMIE?

- dane identyfikujące firmę /teleadresowe, rejestrowe/;
- historię firmy;
- skład zarządu;
- strukturę kapitałową;
- zakres działalności;
- zatrudnienie;
- dane finansowe /obroty, bilans/;
- nieruchomości;
- bank;
- oddziały / filie;
- dane dodatkowe;
- doświadczenia płatnicze;
- **ocenę wiarygodności handlowej;**

☐ CZYM JEST RAPORT HANDLOWY O FIRMIE?

Raport handlowy o firmie w sposób czytelny i zwięzły przekazuje obraz stosunków ekonomiczno – prawnych firmy. W warunkach niepewności towarzyszącej decyzjom gospodarczym jest niezbędnym narzędziem oceny sytuacji Twojego partnera handlowego. Sprawdzenie wiarygodności handlowej firmy jest powszechnie praktykowane w obrocie gospodarczym na całym świecie.

☐ KORZYŚCI PŁYNĄCE Z RAPORTU HANDLOWEGO O FIRMIE:

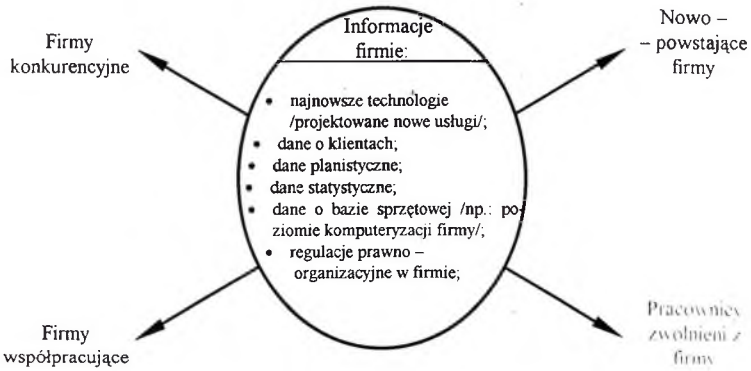
- ograniczenie ryzyka przy nawiązywaniu kontaktów handlowych i rozpoczynaniu współpracy z nowym partnerem;
- sprawdzenie wiarygodności kredytowej firmy i jej standingu finansowego na każdym etapie transakcji;
- wyeliminowanie niepewności przy podpisywaniu kontraktu;
- zapewnienie obiektywnego źródła wiedzy o kontrahencie;

Polityka bezpieczeństwa

BEZPIECZEŃSTWO JAKO CZYNNIK KONKURENCYJNOŚCI FIRMY

Bezpieczeństwo kreuje:	Brak bezpieczeństwa to:
* satysfakcje klientów; * pozytywny image firmy; * rzetelne, mocne podstawy na przyszłość, dynamiczny rozwój firmy; * silną pozycję firmy na rynku i stabilność zatrudnienia;	* niezadowolenie klientów; * naruszenie wizerunku firmy * finansowe straty firmy, w tym powodowane przez klientów; * narastające problemy walki konkurencyjnej na rynku; * redukcje stanowisk pracy;

KTO POSZUKUJE I KORZYSTA Z INFORMACJI O FIRMIE?



BEZPIECZEŃSTWO WYSTĘPUJE W WIELU RÓŻNORODNYCH FORMACH

SECURITY POLICY

- **ZBIÓR PRZYJĘTYCH ZASAD OKREŚLAJĄCYCH STANOWISKO FIRMY WOBEC PROBLEMU BEZPIECZEŃSTWA**
- **POLITYKA OKREŚLAJĄCA ZAKRES AKCEPTOWALNYCH ZACHOWAŃ ORAZ KONSEKWENCJI W PRZYPADKU ICH NARUSZENIA**

KANCELARIE TAJNE

1. Jednostka organizacyjne, w której są wytwarzane, przetwarzane, przekazywane lub przechowywane dokumenty zawierające informacje niejawne oznaczone klauzulą „poufne", lub stanowiące tajemnicę państwową ma obowiązek zorganizowania kancelarii tajnej.
2. Kancelaria tajna stanowi wyodrębnioną komórkę organizacyjną podległą bezpośrednio pełnomocnikowi ochrony, odpowiedzialną za właściwe rejestrowanie, przechowywanie, obieg i wydawanie takich dokumentów uprawnionym osobom. Kancelaria tajna powinna być zorganizowana w wyodrębnionym pomieszczeniu zabezpieczonym zgodnie z przepisami o środkach ochrony fizycznej informacji niejawnych i być obsługiwana przez pracowników pionu ochrony.

BEZPIECZEŃSTWO SYSTEMÓW I SIECI TELEINFORMATYCZNYCH

I. Szczególna ochrona przed nieuprawnionym dostępem do informacji niejawnych, a także przed możliwością przypadkowego lub świadomego narażenia bezpieczeństwa.
II. Certyfikowanie urządzeń i narzędzi kryptograficznych przez służby ochrony państwa.
III. Wymagania bezpieczeństwa systemu i sieci teleinformatycznych:
    1. etap projektowania;
    2. etap wdrażania;
    3. etap funkcjonowania.

KIEROWNIK JEDNOSTKI ORGANIZACYJNEJ WYZNACZA:

1. osobę lub zespół osób odpowiedzialnych za funkcjonowanie systemu lub sieci teleinformatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci teleinformatycznych, zwanych „administratorem systemu";
2. pracownika pionu ochrony odpowiedzialnego za bieżącą kontrolę zgodności funkcjonowania sieci albo systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa, o których mowa w art. 61 ust. 2 i 3.

10. ROZPORZĄDZENIE MINISTRÓW SPRAW WEWNĘTRZNYCH I ADMINISTRACJI ORAZ OBRONY NARODOWEJ

z dnia 26 lutego 1999r.

w sprawie sposobów oznaczania materiałów, w tym klauzulami tajności, oraz sposobu umieszczania klauzul na tych materiałach.

11. ROZPORZĄDZENIE MINISTRÓW SPRAW WEWNĘTRZNYCH I ADMINISTRACJI ORAZ OBRONY NARODOWEJ

z dnia 26 lutego 1999 r.

w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów.

1. ROZPORZĄDZENIE RADY MINISTRÓW
z dnia 9 lutego 1999 r.

w sprawie stanowisk i rodzajów prac zleconych w organach administracji rządowej, których wykonywanie może łączyć się z dostępem do informacji niejawnych stanowiących tajemnicę państwową.

Wykaz stanowisk w organach administracji rządowej, których zajmowanie może łączyć się z dostępem do informacji niejawnych stanowiących tajemnicę państwową.

Rodzaje prac zleconych w organach administracji rządowej, których wykonywanie może łączyć się z dostępem do informacji niejawnych stanowiących tajemnicę państwową.

2. ROZPORZĄDZENIE RADY MINISTRÓW
z dnia 9 lutego 1999 r.

w sprawie organizacji kancelarii tajnych.

Rozporządzenie określa wymagania w zakresie:

- *organizacji kancelarii tajnych,*
- *stosowania środków ochrony fizycznej,*
- *trybu obiegu informacji niejawnych,*
- *wzoru zapoznania się z dokumentem,*
- *obowiązki kierownika kancelarii tajnej /w szczególności/*

3. ROZPORZĄDZENIE PREZESA RADY MINISTRÓW
z dnia 25 lutego 1999 r.

w sprawie szczegółowego trybu funkcjonowania Komitetu Ochrony Informacji Niejawnych, zasad udziału w jego posiedzeniach oraz zakresu czynności sekretarza Komitetu.

4. ROZPORZĄDZENIE PREZESA RADY MINISTRÓW
z dnia 25 lutego 1999 r.

w sprawie szczegółowego zakresu, warunków i trybu współdziałania organów, służb i innych państwowych jednostek organizacyjnych ze służbami ochrony państwa w toku prowadzonych postępowań sprawdzających.

UMOWA
MIĘDZY STRONAMI TRAKTATU
PÓŁNOCNOATLANTYCKIEGO

- o ochronie informacji – Bruksela - 06.03. 1997 roku;
- o przekazywaniu informacji technicznych dla celów obronnych – Bruksela – 19.10.1970 rok;
- o wzajemnej ochronie tajemnicy wynalazków dotyczących obronności, w przypadku których zostały złożone wnioski o udzielenie patentów – Paryż – 1970 rok.

NATO – ORGANIZACJA TRAKTATU PÓŁNOCNOATLANTYCKIEGO

Procedury sprawdzające mają na celu ustalenie, czy dana osoba może, z uwagi na jej lojalność i zaufanie, jakim się cieszy, mieć dostęp do informacji niejawnych bez powodowania niedopuszczalnego zagrożenia dla bezpieczeństwa.

Informacja niejawna NATO jest określona w następujący sposób:

1. **Informacja oznacza wiedzę, która może być przekazana w jakiejkolwiek formie;**
2. **Informacja niejawna oznacza informację lub materiał, który został tak oznaczony, wymagający ochrony przed nieupoważnionym dostępem;**
3. **Wyraz „materiał" obejmuje dokumenty, jak też dowolną część urządzenia, wyposażenia lub broni wyprodukowanych lub będących w trakcie produkcji;**
4. **Wyraz „dokument" oznacza dowolną zarejestrowaną informację, niezależnie od jej fizycznej postaci lub cech charakterystycznych, w tym, bez ograniczeń, tekst pisany lub drukowany, dane w postać kart i taśm, mapy, wykresy, fotografie, obrazy, rysunki, ryciny, szkice, notatki i materiały robocze, kalki węglowe i taśmy atramentowe lub kopie wykonane dowolnymi środkami i metodami oraz nagrania dźwiękowe, magnetyczne, elektroniczne, optyczne lub video w dowolnej postaci, jak również przenośny sprzęt elektroniczny z wbudowaną na stałe lub wymienną pamięcią.**

TAJEMNICA PAŃSTWOWA I SŁUŻBOWA OCHRONA TAJEMNICY PRZEDSIĘBIORSTWA

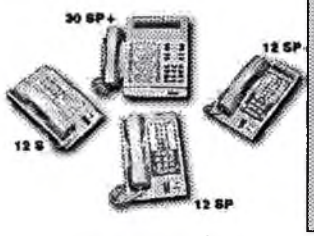
Szkolenie przeznaczone jest przede wszystkim dla Kierowniczej Kadry instytucji, przedsiębiorstw i firm prywatnych. **Dla wszystkich,** którym w pracy zawodowej niezbędna jest znajomość przepisów **o ochronie tajemnicy.**

Przekazane treści w czasie wykładu i dyskusji mają na celu:

1. zapoznać uczestników szkolenia z podstawowymi przepisami o ochronie tajemnicy;
2. wyrobić umiejętność właściwej interpretacji i posługiwania się przepisami o ochronie tajemnicy;
3. rozbudzić odpowiedzialność za przestrzeganie przepisów o ochronie tajemnicy.

Szkolenie daje możliwość wymiany poglądów i **poszukiwania praktycznych rozwiązań** w zakresie ochrony tajemnicy, szczególnie dla pracowników mających styczność z problematyką współpracy z zagranicą, zajmujących się obsługą delegacji zagranicznych, zawieraniem umów z kontrahentami oraz udostępnianiem informacji handlowych firmy.

Electronic Phones



4 typy urządzeń
+ "VirtualPhone"

G.711, G.723.1, G.728
Dynamiczna kompresja
H.323
H.323 RAS
Adresowanie IP - DHCP lub statyczne
IP Precedence
2 Portowy 10Base-T Hub
Zewnętrzny zasilacz 48VDC

Cisco Systems

Analog Gateway

Telefon analogowy

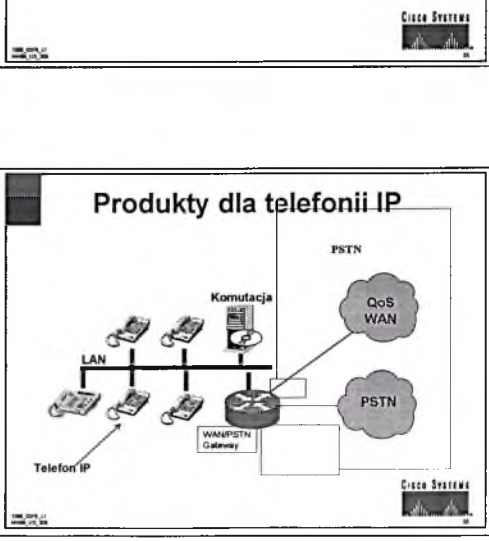
2, 4 lub 8 Portów
G.711 + G.723.1
Dynamiczna kompresja

Adres DHCP lub statyczny

Cisco Systems

Wymagana wersja IOS

- WFQ - 11.0
- IP Precedence - 11.0
- RSVP - 11.2
- MLPPP - 11.3
- Generic Traffic Shaping - 11.2



Uwaga: MLPPP nie jest obsługiwany na Frame Relay

Rekomendacje dotyczące fragmentacji w sieci Frame Relay

- FRF.12 (Luty 99)
- Redukcja IP MTU (Metoda zastępcza)
  - Uwaga - Jitter od innych protokołów,
  - Uwaga - IP "do not fragment" będą gubione
- MTU Interfejsu (zwykle nieskuteczne)

CISCO SYSTEMS

PPP Tablica fragmentacji pakietu

Odstęp między pakietami RT

Prędkość łącza	10ms	20ms	30ms	40ms	50ms	100ms	200ms
56kbps	70 Bytes	140 Bytes	210 Bytes	280 Bytes	350 Bytes	700 Bytes	1400 Bytes
64kbps	80 Bytes	160 Bytes	240 Bytes	320 Bytes	400 Bytes	800 Bytes	1600 Bytes
128kbps	160 Bytes	320 Bytes	480 Bytes	640 Bytes	800 Bytes	1600 Bytes	3200 Bytes
256kbps	320 Bytes	640 Bytes	960 Bytes	1280 Bytes	1600 Bytes	3200 Bytes	6400 Bytes
512kbps	640 Bytes	1280 Bytes	1920 Bytes	2560 Bytes	3200 Bytes	6400 Bytes	12800 Bytes
768kbps	1000 Bytes	2000 Bytes	3000 Bytes	4000 Bytes	5000 Bytes	10000 Bytes	20000 Bytes
1536kbs	2000 Bytes	4000 Bytes	6000 Bytes	8000 Bytes	10000 Bytes	20000 Bytes	40000 Bytes

X—Fragmentacja jest zbędna

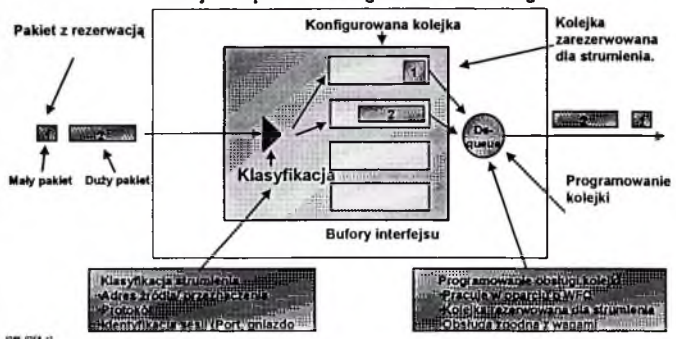
RSVP: Resource Reservation Protocol

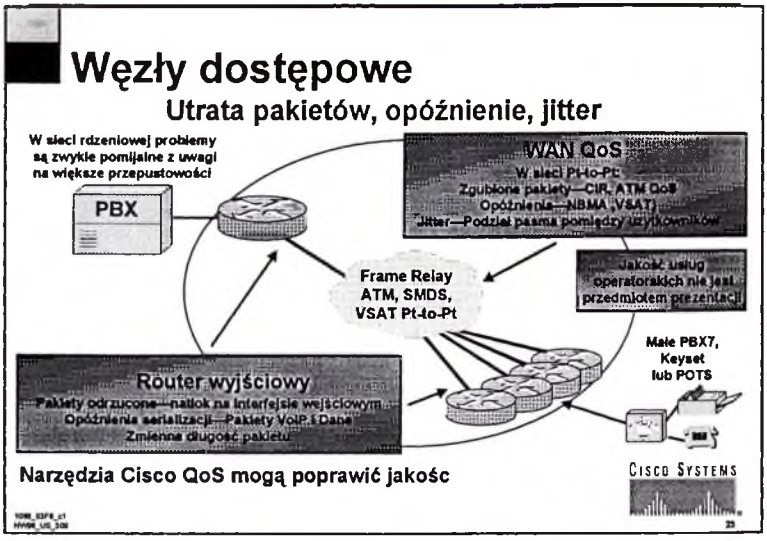
- Protokół sygnalizacji IETF
  - Rezerwacja pasma i opóźnienia
- Dynamiczna " lista dostępowa" w sieci WAN
  - ustawia strategię kolejkowania
- Strumień może być definiowany przez stacje końcową lub statycznie przez router

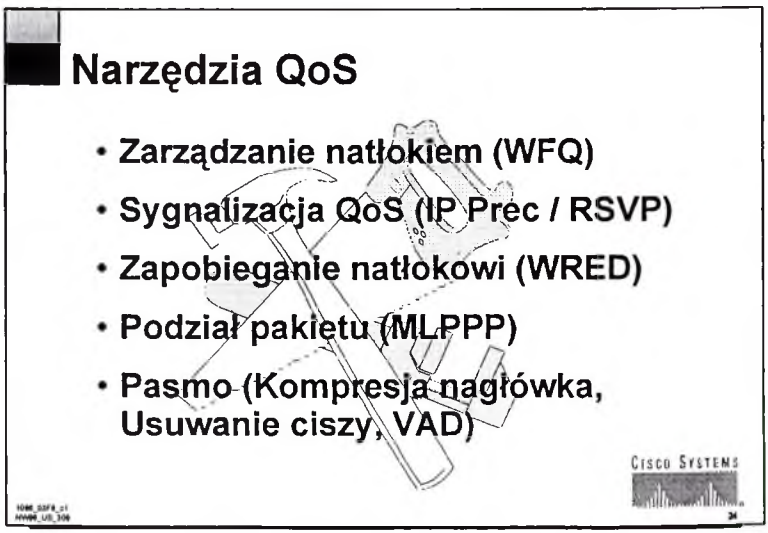
CISCO SYSTEMS

Resource Reservation Protocol (RSVP)

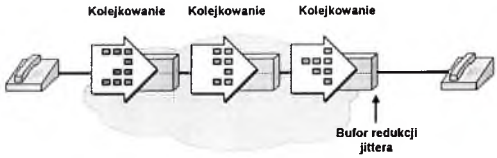
Pracuje w oparciu o Weighted Fair Queuing




Węzły dostępowe
Utrata pakietów, opóźnienie, jitter
W sieci rdzeniowej problemy są zwykle pomijalne z uwagi na większe przepustowości
PBX
WAN QoS
W sieci Pt-to-Pt:
Zgubione pakiety—CIR, ATM QoS
Opóźnienia—NBMA, VSAT
Jitter—Podział pasma pomiędzy użytkowników
Frame Relay
ATM, SMDS,
VSAT Pt-to-Pt
Jakość usług operatorskich nie jest przedmiotem prezentacji
Małe PBX7, Keyset lub POTS
Router wyjściowy
Pakiety odrzucone—natłok na interfejsie wejściowym
Opóźnienia serializacji—Pakiety VoIP i Dane
Zmienna długość pakietu
Narzędzia Cisco QoS mogą poprawić jakość
Cisco Systems


Narzędzia QoS
• Zarządzanie natłokiem (WFQ)
• Sygnalizacja QoS (IP Prec / RSVP)
• Zapobieganie natłokowi (WRED)
• Podział pakietu (MLPPP)
• Pasmo (Kompresja nagłówka, Usuwanie ciszy, VAD)
Cisco Systems

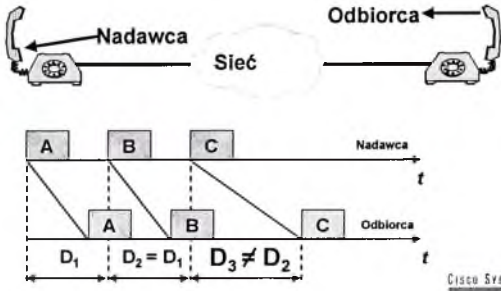
Opóźnienie - składniki zmienne



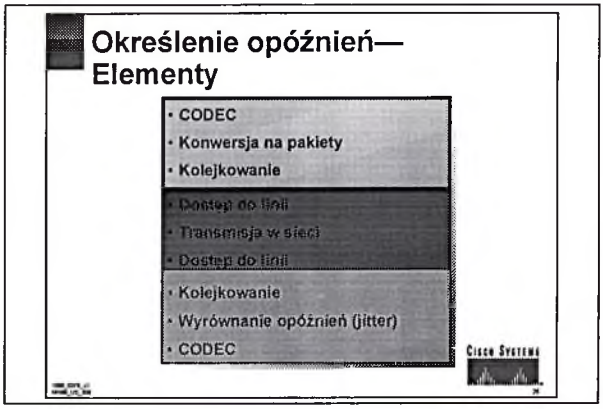
- Opóźnienie kolejkowania
- Buforowanie redukujące jitter
- Zmienna długośc pakietu

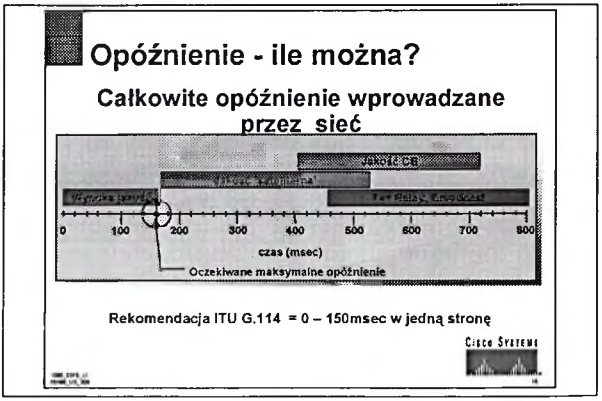
CISCO SYSTEMS

Zmiana opóźnienia—"Jitter"



CISCO SYSTEMS

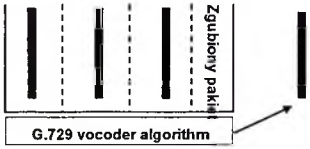




Transmisja głosu - wymagania

- Jakość subiektywna
  MOS
- Opóźnienie i zmiana opóźnienia
- Usuwanie echa
- Szum tła
- Usuwanie 'ciszy'
- Specyfika językowa

VoIP (G.729) toleruje sporadyczną utratę pakietu

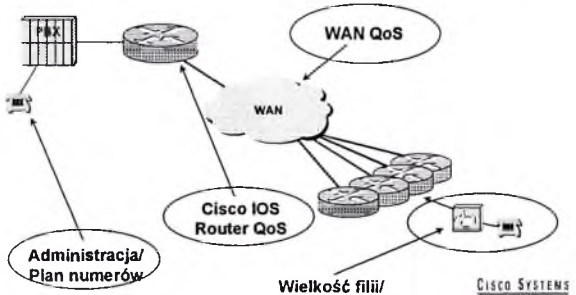


- Przyjazna retransmisja jest całkowicie nieprzydatna w świecie telefonii. Późno jest tak samo dobre jak wcale
- Złożone algorytmy uzupełniające interpolują zgubiony pakiet

Cisco Systems

Zagadnienia projektowania sieci Voice over "X"

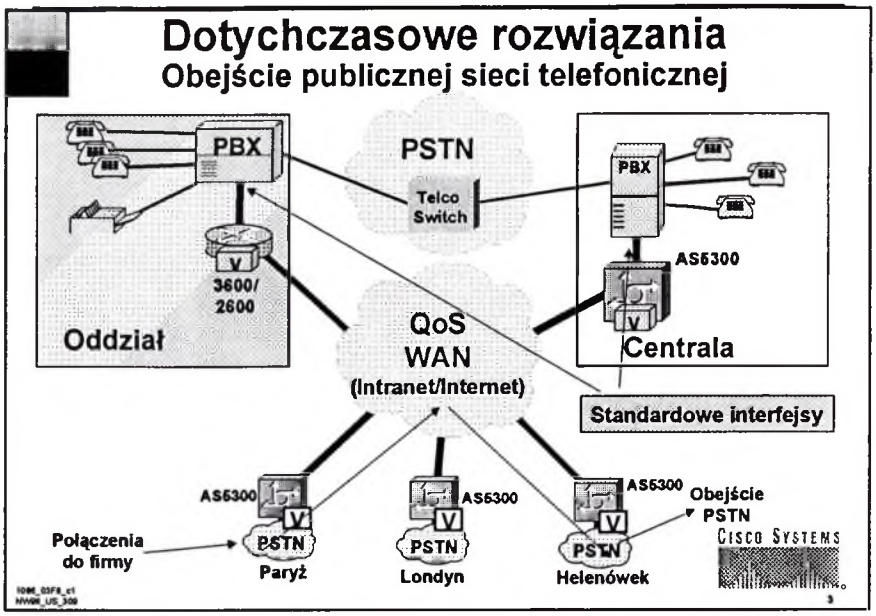
(VoIP, VoFR, VoATM)

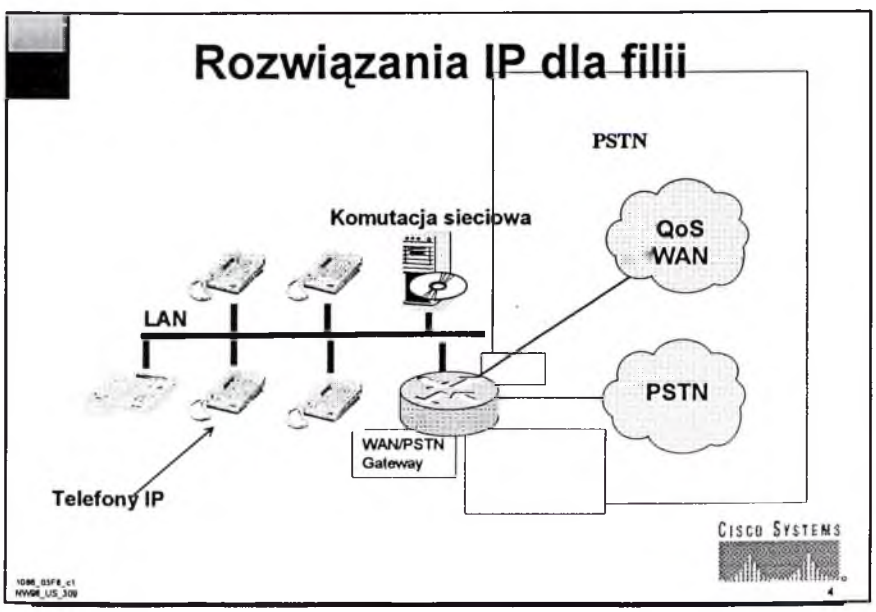


RTP/RTCP—RFC 1889/1890

- End-to-end network transport function
  - Identyfikacja strumienia danych
  - Numeracja sekwencji
  - Znacznik czasu
  - Monitoring
- RTCP (Real-Time Control Protocol) udostępnia informacje dotyczące jakości dystrybucji
- RTP nie realizuje rezerwacji zasobów i gwarancji jakości usługi

Cisco Systems


Dotychczasowe rozwiązania
Obejście publicznej sieci telefonicznej
PBX
PSTN
Telco Switch
PBX
AS5300
3600/ 2600
Oddział
QoS WAN
(Intranet/Internet)
Centrala
Standardowe interfejsy
AS5300
AS5300
AS5300
Obejście PSTN
Połączenia do firmy
PSTN
PSTN
PSTN
Paryż
Londyn
Helenówek
Cisco Systems


Rozwiązania IP dla filii
PSTN
Komutacja sieciowa
QoS WAN
LAN
PSTN
WAN/PSTN Gateway
Telefony IP
Cisco Systems

wstępnej oceny uważamy, że problem roku 2000 nie jest specjalnie poważny. Pomimo, że daty wykorzystuje się jako znaczniki tablic przy replikacji, to decyzje o replikacji podejmowane są nie na podstawie porównania liczb, a napisów i istotna jest tylko ich różnica. Serwery mogą zachować się niestabilnie w momencie zmiany daty, z tego powodu będziemy sugerowali zatrzymanie ich przed północą i ponowny start w roku 2000. Z uwagi na to, że usługa nie jest absolutnie krytyczna, takie postępowanie jest całkowicie uzasadnione.

Bibliografia

[1] Data Communication Networks: *Directory*, Recommendations X500-X.521, CCITT, Fascile VIII.8 of Blue Book

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

[3] M. Górecka, *Replikacja w usługach katalogowych X.500 i LDAP a podstawowe techniki replikacji w systemach rozproszonych*, materiały konferencyjne Miedzeszyn'99

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

[5] M. Górecka, T. Wolniewicz, *Use of national languages in X.500 Directory*, listopad 1996, materiały konferencyjne Bled, Słowenia, konferencja robocza n.t. standardu Unicode.

[6] M. Górecka, T. Wolniewicz, *Nazewnictwo obiektów w rozproszonej międzynarodowej bazie X.500*, maj 1997, materiały konferencyjne Miedzeszyn'97.

[7] M. Górecka, T. Wolniewicz, *System bezpiecznej wymiany informacji w polskiej sieci Internet wykorzystujący adresowo-informacyjną bazę X.500*, maj 1998, materiały konferencyjne Miedzeszyn'98.

[8] Microsoft, http://www.microsoft.com/windows/server/Technical/directory/

NDS (Novell Directory Services)
Novell wprowadził usługę katalogową w celu zarządzania zasobami swojej sieci. Pomimo, że model informacyjny i nazewnictwo jest wzorowane na X.500, protokoły służące do porozumiewania się serwerów są specyficzne dla tej konkretnej usługi. Najnowsza wersja NDS stawia sobie zadania identyczne jak Active Directory, posiada niewątpliwą przewagę w postaci wieloletnich doświadczeń i znacznej bazy użytkowników. Wadą NDS jest stosowanie nietypowych protokołów. NDS posiada obecnie narzędzia do uruchomiania dostępu poprzez LDAP, ale wymaga to wewnętrznej bramy protokołowej.

FNS (Federated Naming Service)
Ta usługa katalogowa promowana przez Sun Microsystems rozszerza funkcjonalność systemu NIS+. Jak NDS służy w pierwszej kolejności do zarządzania zasobami komputerowymi. Posiada możliwość porozumiewania się z usługą X.500 i LDAP. Stosowane nazewnictwo obiektów daje się odwzorować na notację zgodną z X.500, ale w zapisie odbiega od niej. Sun Microsystems dostarcza niezależnie serwer X.500/LDAP.

Podstawowym niebezpieczeństwem stojącym przez usługami katalogowymi jest utrzymanie jednorodności protokołów wymiany informacji. Niestety w sytuacji kiedy jeden produkt ma szanse odgrywać dominującą rolę na rynku, pojawia się tendencja do wprowadzania rozszerzeń, które w konsekwencji prowadzą do niekompatybilności. Takie działanie może być albo powodowane chęcią zwiększenia funkcjonalności, gdy standard nie jest dostatecznie obszerny, albo dążenia do osłabienia pozycji konkurencji.

6. Perspektywy projektu NameFlow-Paradise

Usługa katalogowa PARADISE jest dostępna od niemal 10 lat, pomimo tego nie osiągnęła takiej popularności jak DNS, e-mail, czy WWW. Powodów jest kilka:

1. usługa katalogowa w założeniu miała pozostawać w tle, dopiero projekt PARADISE utworzył z niej pierwszoplanową usługę informacyjną,
2. usługa katalogowa nie była dotąd niezbędna do funkcjonowania systemów komputerowych (tak jak to jest w przypadku DNS), a zatem trud jej utrzymywania mógł być postrzegany jako mało opłacalny,
3. utrzymanie usługi katalogowej jest pracochłonne, chyba że jest ona podstawową bazą danych instytucji lub jest dobrze z taką bazą połączona,
4. udostępnianie informacji o osobach musi podlegać ograniczeniom związanym z ustawami o ochronie danych osobowych,
5. konfiguracje systemów X.500 i LDAP jest nadal stosunkowo skomplikowana.

Spośród wymienionych powodów tylko ostatni – trudności w konfiguracji – jest związany z oprogramowaniem, pozostałe mają charakter organizacyjny. Pomimo tego można odnieść wrażenie, że konkurencja na rynku standardów jest motywowana przeświadczeniem, że nowy standard może zapobiec dotychczasowym trudnościom. Naszym zdaniem jest to przekonanie całkowicie błędne.
Rozrost Internetu i mnogości usług wymusza powstanie systemów katalogowania i ten fakt powoduje, że wśród producentów oprogramowania trwa obecnie bardzo ostra walka. Zmiany standardów są częścią walki konkurencyjnej również na tym polu. Usługi katalogowe są niezbędnym zapleczem systemów bezpieczeństwa opartych o klucze publiczne. To wszystko sprawia, że w najbliższym czasie należy się spodziewać prawdziwej eksplozji zainteresowania. Umieszczenie serwisu katalogowego w każdym serwerze Windows 2000 niewątpliwie zachęci do eksperymentowania.
Projekt PARADISE był typowym testowym projektem badawczym, pomimo, że usługa nie jest już nowa, doświadczenie pokazuje, że połączenie tak skomplikowanego systemu, jak X.500, wyposażonego

Niezależne implementacje mają ICL, AT&T/Lucent Technologies, SUN Microsystems i wiele innych. W projekcie PARDISE pracowały serwery francuskie oparte na oprogramowaniu stworzonym w INRIA, trudności przy współpracy z serwerami QUIPU wskazały na pewne niezgodności implementacji QUIPU ze standardem X.500 '88.
Obecnie nie ma darmowych implementacji X.500, z wyjątkiem przestarzałego QUIPU/ISODE 8.0.

3. Historia standardu usługi katalogowej

Jak już wspomnieliśmy pierwsza wersja X.500 została opublikowana w 1998 r. [1]. Następną była wersja X.500 '93 [2] (faktycznie opublikowana w 1995). Standard został znacznie rozszerzony (objętościowo ponad dwukrotnie), pojawiły się m. in. mechanizmy replikacji oraz ochrony danych. Wprowadzono też znaczne rozszerzenia sposobu zarządzania (dokładniejsze informacje można znaleźć w pracy [3]). Standard w wersji '97 poprawia poprzednią wersję, głównie wprowadzając kontekst atrybutu (co pozwala na przykład stosować różne wersje językowe tego samego atrybutu). W tej chwili trwają prace nad standardem X.500-2000.
We wczesnym okresie rozwoju systemów X.500 okazało się, że mocno rozbudowany protokół dostępu (DAP) stwarza problemy twórcom interfejsów użytkownika. Z tego powodu zdefiniowano "odchudzoną" wersję (LDAP). Autorem najszerzej używanej implementacji był Tim Howes z Uniwersytu Michigan (obecnie w Netscape).
Założeniem LDAP było uruchomienie bramy protokołowej, która rozmawiała z X.500 za pomocą DAP, a z klientem poprzez LDAP. W ten sposób LDAP nie musiał w ogóle obsługiwać operacji rozproszonych – brama była pojedynczym punktem styku z usługą katalogową i większość obsługi brała na siebie. Implementacja z Michigan dostarczała bramę, bibliotekę LDAP i kilku prostych klientów LDAP. Klient obsługujący usługę gopher bardzo spopularyzował X.500 w Internecie. Prawdziwy przełom spowodowało jednak dopiero pojawienie się klientów pośredniczących pomiędzy LDAP i HTTP.
W czasie eksperymentów z implementacjami LDAP stworzono slapd, stanowiący pojedynczy serwer bez możliwości pracy rozproszonej. Stał się on punktem wyjściowym do zmiany podejścia — zamiast skomplikowanego serwera i złożonego protokołu transakcji pomiędzy serwerami, większość obciążenia nałożono na klienta. Serwery przechowują jedynie informację o odesłaniach do danych zewnętrznych i pozostawiają klientowi podążanie za nimi. Stanowi to całkowite zaprzeczenie pierwotnej idei protokołu i serwera LDAP. To nowe podejście jest obecnie formalizowane jako LDAPv3.
LDAPv3 jest już zaimplementowany w kilku produktach. Obsługuje go też większość serwerów X.500. Nadal jednak trwają intensywne prace nad rozwojem niektórych jego aspektów np. replikacji (patrz [3]). Niestety nie ma produktów dostępnych bezpłatnie, chociaż cena serwera Netscape nie jest wygórowana (zwłaszcza w porównaniu z pełnymi produktami X.500).

4. Usługa katalogowa w Polsce

Polska przystąpiła do projektu PARADISE w 1992 roku w momencie uruchomienia pierwszych serwerów na UMK w Toruniu. Jeszcze w tym samym roku pieczę na serwisem przejął NASK. Uruchomiony został dedykowany serwer krajowy, zaczęto prace nad rozbudową usługi oraz dostosowywaniem jej do języka polskiego.
W ramach NASK prowadziliśmy zarówno prace rozwojowe jak i badawcze, czego efektem jest ok. 20 prac i raportów prezentowanych na polskich i zagranicznych konferencjach. Wszystkie one są dostępne w archiwum polskiej usługi katalogowej http://ocelot.uni.torun.pl.
UMK, który współzarządza usługą katalogową, trzykrotnie koordynował granty KBN na ładowanie bazy X.500, w wyniku czego polski projekt objął większość środowisk akademickich. Obecnie pracuje 13 serwerów prezentujących dane jednostek regionu. Wyniki ich monitorowania są dostępne pod adresem http://ocelot.uni.torun.pl/Wyniki/polskie_dsa.html (patrz rysunek).
W okresie od 1.01.99 do 6.05.99 bramka WWW-X.500 w Toruniu obsłużyła 61800 zapytań, czyli ok. 490 na dobę. Krajowy serwer X.500 obsługuje ok. 270 połączeń na dobę (są to w większości połączenia

używania systemów X.500 w takich dziedzinach, jak obronność, ośrodki rządowe, transport, a także w bankowości. Dlatego celem usługi katalogowej jest wprowadzenie elastycznych metod replikacji, które będą pozwalały na dużą dowolność konfiguracji replikacji w systemie.

Bibliografia

[1] M. Górecka, T. Wolniewicz, „Obsługa zasobów informacyjno-adresowych za pomocą protokołu LDAP – przegląd dostępnych narzędzi i porównanie z technologią X.500", Miedzeszyn'98

[2] M. Górecka, T. Wolniewicz, „Europejska usługa katalogowa Paradise-NameFlow: perspektywy i zastosowania", Miedzeszyn'99

[3] D. Chadwick, *Understanding X.500. The Directory.* Chapman & Hall 1994 (`http://www.salford.ac.uk/its024/X500.htm`)

[4] D.S. Linthicum, „Finding your way", artykuł w czasopiśmie DBMS, November 1997

[5] A. Silberschatz, H.F. Korth, S. Sudarshan, „DATABASE SYSTEM CONCEPTS", *WCB/McGraw-Hill*, 1998

[6] A.A. Helal, A.A. Heddaya, B.B. Bhargava, „REPLICATION TECHNIQUES IN DISTRIBUTED SYSTEMS", *The Kluwer International Series on Advances in Database Systems*, 1996

[7] R. Lenz, „The virtual-primary-copy approach compared to other approaches with weak consistent data replication"

[8] T. Anderson, Y. Breitbart, H. F. Korth, A. Wool, „Replication, consistency, and practicality: are these mutually exclusive?", SIGMOD'98

[9] Y. Breitbart, H. F. Korth, „Replication and Consistency: Being lazy helps sometimes", *Proceedings of the Sixteenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of Database Systems*, 1997

[10] J. Gray, P. Helland, P. O'Neil, D. Shasha, „The danger of replication and a solution", *Proceedings of the 1996 ACM SIGMOD International Conference on Management of Data*, 1996

[11] S.E. Hardcastle-Kille, *„Replication Requirements to provide an Internet Directory using X.500"*, RFC 1275, November 1991

[12] S.E. Hardcastle-Kille, *„Replication and Distributed Operation extensions to provide an Internet Directory using X.500"*, RFC 1276, November 1991

[13] Data Networks and Open System Communications, „Directory; Information Technology – Open Systems Interconnection – The Directory: Replication", ITU-T Recommendation X.525 (11/93)

[14] Russel Weiser, „LDAP Replication Requirements", October 29, 1998, INTERNET-DRAFT, `draft-weiser-replica-req-02.txt`

[15] John Merrells, Ed Reed, „LDAP Replication Architecture", August 5, 1998, INTERNET-DRAFT, `draft-merrells-ldup-model-01.txt`

[16] Steven Legg, „LDAP Update Reconcilation Procedures", December 24, 1998, INTERNET-DRAFT, `draft-legg-ldup-crp-00.txt`

Oczywiście replikowana informacja ma służyć poprawie efektywności realizacji zleceń, które są odbierane przez system katalogowy. Zarówno encje jak i odsyłacze informacyjne, występujące w ramach repliki mogą być stosowane do generowania wyniku zapytania wysłanego przez użytkownika bazy X.500. Tylko w poniżej wskazanych sytuacjach nie jest możliwe korzystanie z kopii danych:

- odzwierciedlana informacja nie może zostać poddana operacji modyfikacji,
- użytkownik wystawiający zlecenie może zabronić stosowania repliki w celu tworzenia odpowiedzi poprzez parametr „zakaz stosowania kopii" (ang. *don't use copy*) przesłany w ramach argumentów sterowania usługą.

W środowisku globalnej bazy danych, stosującej techniki replikacji na zapytanie może nadejść wiele odpowiedzi pochodzących z serwera głównego (zarządzającego danymi) oraz serwerów utrzymujących wtórne kopie danych. Taki wynik nie będzie satysfakcjonować użytkownika. Możliwe jest oczywiście usunięcie zdublowanej informacji poprzez serwer obsługujący zapytanie bądź przez inteligentny interfejs obsługujący użytkownika. Nie jest to jednak działanie optymalne, gdyż mamy do czynienia ze zbędnym zużyciem zasobów. Kopie danych istnieją w zasobach po to, by skrócić czas niezbędny do uzyskania odpowiedzi. Jeżeli serwer realizuje zapytanie w technice sekwencyjnego wielokrotnego łańcuchowania, to może na postawie odebranych wyników częściowych odpowiednio ustalać argumenty kolejnych zapytań i żądać wyłączenia określonych obszarów drzewa. Jeżeli pracuje w trybie równoległego wielokrotnego łańcuchowania, jedyną metodą uniknięcia duplikowania wyników jest rezygnacja ze stosowania replik. Ważnym aspektem istnienia replik jest, wspomniana wcześniej, możliwość korzystania z nich w procesie analizy nazwy, czyli lokalizacji obiektu na podstawie jego nazwy, dostarczanej przez interfejs użytkowy.

Podsumowując, można stwierdzić, że zdefiniowana w standardzie X.500'93 technika replikacji zasobów daje skuteczne mechanizmy odzwierciedlania danych katalogowych i pozwala tworzyć jednorodne implementacje. Oczywiście nadal pozostaje problemem używanie replikacji w rozwiązaniach heterogenicznych, czyli łączących węzły korzystające z różnego oprogramowania, które w dowolnym stopniu implementuje przedstawione standardy. Dodatkową trudność, o której nie można zapominać, stanowi niespójna definicja wymagań dotyczących kontroli dostępu do zasobów. Dopiero standard X.500'93 zawiera omówienie zagadnień kontroli dostępu do informacji w bazie(wcześniej systemy katalogowe stosowały własne strategie). Prezentowany model definiowania reguł dostępu do zasobów jest bardzo zawiły, a dodatkowo wprowadzone mechanizmy nie są traktowane jako obowiązkowe. W efekcie nie ma pewności, że dwa systemy działające zgodnie ze standardem X.500'93 identycznie obsługują kwestie dostępu do zasobów. Konsekwencje tego są szczególnie uciążliwe właśnie w technice replikacji, która wymaga dobrego określenia reguł korzystania z zasobów.

Ustalone w standardzie X.500'93 reguły replikacji pozostawiają dużą dowolność administratorom systemów. To oni decydują o trybie aktualizacji, częstotliwości przekazywania replik oraz dobierają stosowną strategię (replikacja pełna bądź przyrostowa). Obszar replikacji może być dopasowywany do konkretnych potrzeb, dzięki filtrowaniu encji i atrybutów. Elementem, który pozostaje najmniej zautomatyzowany, jest faza zawarcia porozumienia replikacji, która wymaga synchronizacji działań administratorów dwóch uczestniczących w wymianie replik węzłów.

Według ukazujących się obecnie dokumentów internetowych, intensywnie rozwijający się **standard LDAP** w dużym stopniu przejmie podstawowe założenia dotyczące replikacji w X.500'93. Dostępne już zalecenia precyzują wymagania odnośnie replikacji w protokole LDAP [14], architekturę replikacji [15] oraz w sposób ogólny określają funkcje procedur uzgadniania aktualizacji [16]. Ponieważ prace standaryzacyjne trwają, nie są dostępne produkty implementujące tę postać replikacji w LDAP-ie. Niemniej, warto przyjrzeć się planom. Replikacja w LDAP-ie różni się od zaprezentowanych wcześniej w tym punkcie technik replikacji zasobów katalogowych przede wszystkim tym, że wprowadza się dwie formy replikacji. Pierwsza to metoda tradycyjna, określana dalej nazwą *single-master*, stosowana również w X.500 — dostępna jest jedna główna kopia danych, wszystkie pozostałe kopie traktowane są jako wtórne. Druga forma replikacji zakłada istnienie wielu kopii głównych, jest nazywana *multi-master*. O regułach korzystania z kopii głównych w technice *multi-master* decyduje typ repliki. LDAP definiuje następujące typy replik:

1. Podstawowa (ang. *primary*) – pełna kopia danych, do której powinny być kierowane wszystkie operacje LDAP wymagające silnej spójności zasobów; wśród replik danego kontekstu nazew-

jest nazywany poprzez identyfikację jego encji macierzystej, np. blok danych zawierający wszystkie bezpośrednio podporządkowane dane poziomu c=PL nosi nazwę "c=PL". Blok taki zawiera relatywne nazwy wyróżnione encji bezpośrednio podporządkowanych oraz ich opisy. Główny (ang. *master*) blok EDB składa się z dwóch typów encji. Są to:

1. Encje, którymi DSA zarządza.
2. Kopie encji zarządzanych przez inny serwer, wskazany za pomocą odesłania podporządkowanego. Taka kopia jest utrzymywana automatycznie, dzięki komunikacji z serwerem posiadającym podstawowy blok danych.

Inne serwery mogą przechowywać kopie bloków EDB (tzw. podrzędne EDB, ang. *slave* EDB), które są replikowane w całości bezpośrednio z podstawowego EDB lub z podrzędnego EDB (jeśli mamy do czynienia z wtórnym odzwierciedlaniem danych).

Zastosowanie podejścia, które zaleca dokument RFC1276 i wprowadzenie replikacji w bazie X.500 daje korzyści, które nie są typowe dla wszystkich systemów rozproszonych, lecz wynikają ze specyfiki organizacji zasobów X.500, z ich drzewiastego ustrukturalizowania.

1. Uproszczona jest analiza nazwy encji (ang. *name resolution*), prowadząca do lokalizacji encji w drzewie danych na podstawie jej nazwy, dzięki czemu znacznie podnosi się wydajność.
2. Poprawia się efektywność przeszukiwań, które dotyczą jednego poziomu oraz działań typu „listuj", a także istotnie uproszczona jest implementacja tych operacji. Korzyści wynikają z uniknięcia konieczności kontaktu z licznymi serwerami podporządkowanymi.

Protokół replikacji zdefiniowany w RFC1276 posiada kolejne ograniczenie — zakłada, że stroną inicjującą transfer repliki musi być odbiorca EDB, operacja transmisji ma charakter „ściągania" kopii (*pull-through*). Aktualna replika może być pobierana w określonych odstępach czasowych (domyślnie co 6 godzin) lub jednorazowo, w wyniku jawnego żądania administratora.

Zaletą opisanego mechanizmu replikacji jest prosta implementacja. Podstawową wadą jest niska efektywność, będąca konsekwencją poniższych rozwiązań.

1. Nie jest możliwa obsługa całych poddrzew hierarchicznej bazy informacyjnej, w sytuacji, gdy potrzebne jest powielanie kilku, czy kilkunastu bloków EDB administratorzy muszą wprowadzić odpowiednie, rozbudowane specyfikacje.
2. Nie jest możliwa indywidualna obsługa encji, jeśli dowolny wpis w bloku EDB zmienia się musi zostać odzwierciedlony cały blok EDB.
3. Bloki EDB przesyłane są porcjami tylko w sytuacji serwerów pracujących w domenie Internetu, w innych przypadkach może dochodzić do prób transferu bardzo dużych bloków danych, co często wpływa na obniżenie jakości.
4. Nie jest poprawnie zaimplementowane zabezpieczanie systemu w przypadku pokrywania się operacji transferu replikowanych bloków EDB i modyfikacji danych umieszczonych w tym bloku.

Wyższą wydajność zapewniają techniki inkrementacyjne. Jednak autorzy specyfikacji RFC 1276 uznali, że wykorzystywane metody są wystarczające wobec ówczesnych potrzeb. Zakładali, że kolejne wersje standardu wprowadzą nowe ustalenia i pozwolą na skalowanie modelu.

Rzeczywiście, standard **X.500'93** definiuje w części X.525 ([11]) wyczerpujący, wszechstronny model replikacji. Replikacja jest nazywana w tych rekomendacjach **odzwierciedlaniem, cieniowaniem** (ang. *shadowing*). Standard wymienia również inne sposoby tworzenia dodatkowych kopii informacji, jak np. zastosowanie pamięci podręcznej (*caching*), jednak te metody mogą być realizowane drogą pozaprotokolarną.

Rozwiązanie przyjęte w replikacji w modelu X.500'93 korzysta z osłabionego modelu spójności danych, przedstawionego w drugiej części przeglądu podstawowych technik replikacji. Wśród powodów wyboru takiego modelu wymienia się ponownie argument, że statystyki korzystania z zasobów X.500 wskazują zdecydowaną przewagę zleceń odczytu nad operacjami zapisu. Poza tym, ważną zaletą takiego podejścia jest mniejszy stopień skomplikowania implementacji.

W prezentowanej technice, jest wskazywana kopia główna (ang. *master copy*), czyli miejsce lokalizacji oryginalnych danych. Dane takie są często, może nieco dwuznacznie, nazywane są kopią główną albo kopią podstawową. Inne serwery mogą utrzymywać kopię danych oryginalnych (kopię kopii głównej), czyli kopię wtórną (ang. *shadow copy*). Operacje odczytu mogą (ale nie muszą) korzystać z kopii wtórnych. Operacje zapisu dotyczą zawsze kopii głównej. Następnie zmiany, zgodnie z ustaloną

oparciu o lokalną replikę. Gdy kopia podstawowa ulega uszkodzeniu, kolejna replika, znajdująca się w uporządkowanej liście bezpośrednio powyżej dotychczasowej, staje się bieżącą i w oparciu o nią system kontynuuje swoje działanie. Teoria replikacji określa wiele mechanizmów replikacji opartych na technikach **głosowania** (ang. *voting*) albo **ugody kworum** (ang. *quorum consensous*). Nie stosują one pojęcia kopii wyróżnionej. Zlecenie realizacji określonej operacji, które jest związane, z powodu konieczności nadzoru współbieżności, z zajęciem potrzebnych zasobów, jest przesyłane do wszystkich węzłów zawierających potrzebny element danych. Każda kopia utrzymuje własną pulę reprezentującą zajęte elementy i może przydzielić lub zakazać dostępu do swoich zasobów. Przetwarzanie transakcji musi zostać poprzedzone przegłosowaniem przez większość partnerów prawa do przydzielenia potrzebnych elementów danych. Rodzina protokołów ROWA zdecydowanie faworyzowała operacje odczytu, poza tym nie było tam możliwości tolerowania podziału sieci, pojawiającego się na skutek kłopotów komunikacyjnych. W przypadku strategii opartych na głosowaniu, decyzję o zajęciu zasobów podejmują wszystkie węzły. Mechanizm ten ma swoje wady – występuje tu znaczna ilość komunikatów transmitowanych między poszczególnymi replikami. Dodatkowe utrudnienia wprowadza obsługa awarii, które mogą się zdarzyć w trakcie procesu głosowania. Należy również pamiętać o całej gamie technik mieszanych, które korzystają jednocześnie z metody ROWA lub jej odmian oraz z głosowania i doboru kworum. Istotnym zagadnieniem dla poprawy efektywności opisanych technik silnej spójności jest wprowadzenie możliwości dynamicznego tworzenia reguł obsługi replik — takie rozwiązanie mogłoby uwzględniać specyfikę aktualnej konfiguracji, dostosowywać do typu obsługiwanych operacji i reagować na obciążenie. Przegląd literatury na temat replikacji pokazuje, że jedną z wiodących tendencji jest optymalizowanie podstawowych technik replikacji w celu otrzymania wydajniejszych i bardziej niezawodnych metod.

Zadaniem replikacji jest podniesienie dostępności zasobów oraz poprawa efektywności systemu rozproszonego. Tradycyjne wymagania związane z utrzymywaniem przez cały czas spójnego stanu zasobów w rozproszonych bazach danych są bardzo silne i wprowadzają znaczne obciążenie, zarówno poszczególnych węzłów, jak i sieci komputerowej.

Zaprezentowane powyżej modele replikacji opierają się na transakcyjnym podejściu do zagadnienia replikacji. Narzucają surowe wymagania związane ze spójnością zasobów i niepodzielnością działań na danych. Wśród nowoczesnych strategii, prezentowanych m.in. w pracach [7], [8], [9], [10], coraz częściej pojawiają się techniki, które zezwalają na rozluźnienie potrzeb dotyczących spójności. Takie metody są zazwyczaj dużo bardziej praktyczne, łatwiejsze w implementacji i efektywniejsze w eksploatacji. Wspomniane opracowania zawierają rozbudowane analizy skuteczności i wydajności proponowanych rozwiązań. Należy również zwrócić uwagę, że coraz popularniejsze nowoczesne technologie często uniemożliwiają zapewnienie tradycyjnych warunków pracy w środowisku rozproszonym. Przestaje funkcjonować założenie, że wszystkie węzły są w większości czasu pracy systemu dostępne, a brak łączności z węzłem oznacza jego uszkodzenie. Intensywnie rozwijająca się dziedzina komputerów przenośnych podłączonych do sieci komputerowej (ang. *mobile computing*) powoduje, że zmienia się topologia systemów. Taki węzeł jak np. przenośny komputer może być niedostępny tylko dlatego, że nie jest obecnie włączony, czy nie znajduje się w zasięgu sieci komputerowej. W takiej sytuacji typowe techniki replikacji o charakterze transakcyjnym, realizujące zasadę aktualizacji replik „w każdym miejscu, w każdej chwili, dowolnego elementu danych" nie mogą być wykorzystywane. Aplikacje muszą pozwalać na czasowe występowanie niespójności zasobów. Przykładowo, można dopuścić niezależne wykorzystywanie danych umieszczonych w dwóch częściach sieci, która uległa fragmentacji. W tym kontekście często mówi się o osłabionej, czy ograniczonej spójności replik (ang. *weak consistency*). Najpopularniejszą metodą jest adaptacja przez system żądań z zakresu spójności danych, narzucanych przez konkretną aplikację — z takim właśnie podejściem mamy do czynienia w usługach katalogowych. Natura wielu systemów pozwala na przejściową niespójność danych. Przykładem mogą być systemy, w których gros operacji to odczyt, a operacja zapisu nie musi być natychmiast propagowana do wszystkich replik. Ustala się w takiej sytuacji niezbędny stopień zgodności replik. Dalsze rozróżnienie może dodatkowo podawać, jakiego rodzaju spójność jest zalecana: globalna (z punktu widzenia całego systemu rozproszonego), czy może wystarcza spójność lokalna. Dopuszcza się dwa sposoby aktualizacji replik. Pierwsze podejście, zwane grupowym, ustala, że istnieje zbiór aktywnych replik, a każdy węzeł posiadający kopię danych może aktualizować swoją replikę (strategia ta bywa określana w literaturze metodą wielu kopii głównych, ang. *multimaster*). W drugiej technice, nazywanej metodą jednej kopii głównej (ang. *master*), każdy obiekt danych ma swój węzeł

- **Przyrost zasobów**
  Przyczyną dystrybucji zasobów bazy danych może stać się stopniowy wzrost ilości gromadzonej informacji. Scentralizowane systemy operujące na bardzo dużych bazach danych są nie tylko nieefektywne, ale również bardzo trudne w zarządzaniu.
- **Minimalizacja potrzeby zdalnej komunikacji**
  Jeżeli baza danych jest wykorzystywana w sieci komputerowej, to programy klienckie, nazywane interfejsami dostępowymi są zazwyczaj uruchamiane w odległych lokalizacjach. Przybliżenie zasobów do miejsca, z którego są najczęściej używane redukuje nadmiarową komunikację, wprowadza lokalność aplikacji użytkowych.
- **Wymogi efektywnościowe**
  Istnienie kilku autonomicznych procesorów obsługujących system poprawia efektywność dzięki zrównolegleniu działań. Lokalne komponenty obsługiwane są przez własne aplikacje.
- **Niezawodność i dostępność**
  Rozproszone bazy danych, w szczególności takie, które dysponują zdublowanymi kopiami danych, są często wykorzystywane jako metoda zwiększenia niezawodności oraz dostępności sytemu. Wymaga to jednak stosowania różnorodnych technik wspomagających. Awarie w systemie rozproszonym mogą być, ze względu na jego znacznie większą złożoność i rozbudowanie, częstsze niż w środowisku scentralizowanym, ale ich efekt jest związany wyłącznie z aplikacjami wykorzystującymi dane w uszkodzonym węźle. Awaria całego systemu jest sytuacją bardzo rzadką.

Schemat fragmentacji danych w systemach rozproszonych ([5]) definiuje zbiór fragmentów, które gromadzą łącznie wszystkie atrybuty oraz pełne opisy obiektów globalnej bazy danych. Jest odwzorowaniem, przypisującym poszczególne fragmenty węzłom. Sposób rozłożenia fragmentów musi odpowiadać zadanym wymaganiom, zarówno organizacyjnym, jak i funkcjonalnym. Dla jasności i przejrzystości systemu pożądane jest podporządkowanie się zasadzie tworzenia rozłącznych fragmentów danych. Koncepcja fragmentacji drzewa danych X.500 pomiędzy serwery jest bardzo prosta. Globalne drzewo jest podzielone na poddrzewa, zgodnie z potrzebami dotyczącymi lokalnego administrowania. Wielkość poddrzewa jest dowolna, przy czym każda część musi być pełnym poddrzewem, bez „dziur". Poddrzewo rezyduje w jednym serwerze, który zarządza danym fragmentem globalnego drzewa danych, nie może ono być rozproszone między kilka serwerów przed uprzednim podziałem na kolejne poddrzewa. Jeden serwer może przechowywać dowolną liczbę poddrzew, przy czym każde z poddrzew musi być maksymalne — DSA nie może zawierać dwóch uzupełniających się w kierunku pionowym poddrzew. Poddrzewa w zasobach X.500 są identyfikowane poprzez wyróżnioną nazwę encji umieszczonej w korzeniu danego fragmentu jest ona określana **przedrostkiem kontekstu poddrzewa** (ang. *context prefix*). Z każdym poddrzewem jest powiązany zestaw odsyłaczy informacyjnych (ang. *knowledge references*), wskazujących serwery, które przechowują poddrzewa pionowo przylegające do danego fragmentu drzewa. Takie odesłania są utrzymywane przez serwery i stanowią tzw. metainformację o dystrybucji zasobów. Każde poddrzewo, nie zaczynające się od korzenia globalnego drzewa informacyjnego posiada odesłanie do encji **bezpośrednio nadrzędnej**. Takie poddrzewo, które posiada nie tylko encje końcowe, wskazuje serwery przechowujące poddrzewa położone niżej w strukturze za pomocą odsyłaczy do encji **podporządkowanych**. Poddrzewo zawierające encje, przedrostek kontekstu, pełen zestaw odesłań podporządkowanych oraz odesłanie bezpośrednio nadrzędne to zestaw informacji tworzący **kontekst nazewnictwa** (ang. *naming context*) — jednostkę dystrybucji drzewa informacji między serwery DSA.

3. Techniki replikacji danych w systemach rozproszonych

Przed przystąpieniem do prezentacji replikacji w usługach katalogowych, przyjrzyjmy się typowym, najbardziej popularnym technikom replikacji, które są opisywane w literaturze ([5], [6]). **Replikacja** jest strategią stosowaną w systemach rozproszonych, polegającą na przechowywaniu dodatkowych kopii danych. Kopie takie, zwane **replikami** są zazwyczaj umiejscawiane w różnych węzłach systemu rozproszonego, ich lokalizacja wynika z różnorodnych aspektów funkcjonowania konkretnego systemu. Zastosowanie replikacji w systemie rozproszonym daje duże korzyści. Podstawowe zalety to:

REPLIKACJA W USŁUGACH KATALOGOWYCH X.500 I LDAP A PODSTAWOWE TECHNIKI REPLIKACJI W SYSTEMACH ROZPROSZONYCH

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

Uniwersyteckie Centrum Technologii Sieciowych, UMK
Naukowa Akademicka Sieć Komputerowa NASK
Zakład Rozproszonych Systemów Informacyjnych

Celem artykułu jest prezentacja technik replikacji, stosowanych w usługach katalogowych. Jak każdy system rozproszony, profesjonalnie prowadzona, operacyjna usługa katalogowa może istotnie poprawić swoją efektywność, jeśli umiejętnie zastosujemy replikację. Pierwszy punkt pracy jest krótkim opisem funkcji usługi katalogowej. Więcej informacji można znaleźć w pracy [1] oraz dostępnej w sieci książce na temat X.500 ([3]). W części 2 jest omówione zagadnienie dystrybucji zasobów w zasobach katalogowych. Część 3 prezentuje popularne techniki replikacji i tendencje związane z ich stosowaniem w systemach rozproszonych. Kolejne części prezentują techniki replikacji implementowane w systemach katalogowych.

1. Wprowadzenie

Większość nowoczesnych systemów informatycznych jest umiejscawiania w rozproszonym środowisku sieciowym i korzysta z infrastruktury komunikacji opartej na sieciach komputerowych. Systemy takie zazwyczaj nie używają wyłącznie danych i urządzeń lokalnych, ale również sięgają do różnego rodzaju zasobów sieciowych, takich jak inne aplikacje, zdalne bazy danych, odległe urządzenia, pliki rezydujące na obcych stacjach komputerowych. Ważnym problemem staje się łatwa lokalizacja oferowanych w sieci zasobów. Oprócz adresu konkretnego obiektu zdalnego, często są potrzebne dodatkowe szczegóły na jego temat. Bywa też, że należy zapewnić właściwą kontrolę dostępu do zasobów, by nie dopuścić do naruszenia prawa własności.

Usługa katalogowa jest mechanizmem umożliwiającym lokalizację, identyfikację i korzystanie z zasobów sieciowych. Jest uporządkowanym sposobem klasyfikacji tych zasobów. Wspomaga wyszukiwanie w zawiłym środowisku sieciowym aplikacji, serwerów, użytkowników. Architektura usługi katalogowej stosuje popularny model klient-serwer. Rolę serwera pełni system zarządzający bazą danych, strona kliencka to niezależny lub wbudowany w konkretną aplikację interfejs, korzystający z zasobów katalogowych, np. w celu zautomatyzowania takich zadań jak znalezienie odpowiedniej drukarki sieciowej, czy określenie członków listy dyskusyjnej. Usługa katalogowa może być silnie specjalizowana, jak np. *Domain Name System* lub przeznaczona do różnorodnych, szeroko pojętych zastosowań — przykłady takich systemów to X.500, *Lightweight Directory Access Protocol* — LDAP oraz *Microsoft Active Directory*.

Technologia korzystania przez systemy informacyjne z globalnych zasobów katalogowych została zdefiniowana w międzynarodowych rekomendacjach, wydanych w 1988r. Były one wynikiem prac grupy roboczej CCITT (*Consultative Commitee on International Telegraphy and Telephony*), obecnie ITU-T (*International Telecommunication Union — telecommunication sector*) oraz ISO (*International Standards Organization*). Kolejna wersja tego standardu, sygnowana X.500'93, pojawiła się w 1995 r. Usługa X.500 jest zaprojektowana w warstwie aplikacji siedmiopoziomowego modelu OSI (*Open System Interconnection*). Ta międzynarodowa definicja stała się nie tylko podstawą do tworzenia produktów implementujących X.500, ale również spowodowała rozwój innych technik obsługi globalnych zasobów sieciowych, takich jak np. protokół LDAP. *Lightweight Directory Access Protocol* początkowo rozwijał się jako protokół dostępowy do zasobów X.500 (oryginalny protokół dostępowy X.500, ang. *Directory Access Protocol* — DAP jest skomplikowany i nie daje łatwych mechanizmów tworzenia aplikacji użytkowych). Z czasem LDAP zyskiwał znaczną popularność i rozszerzył swój

bazy dla tysięcy obiektów. Model weryfikowania uprawnień jest typu "co nie jest zakazane jest dozwolone". Pierwotnie założony jest zatem pełen dostęp wszystkich użytkowników do plików.

Ze względu na swą naturę (łatwość pobierania listy wartości dla określonego zleceniodawcy, możliwość sprawdzenia posiadania konkretnego uprawnienia oraz brak ograniczeń co do rodzaju przechowywanych wartości) ACL został również wykorzystany do przechowywania preferencji klienta.

Interfejs pomiędzy Serwerem Usług a Serwerem Preferencji i Autoryzacji został następująco zdefiniowany na poziomie IDL:

```
module RemoteAuthorizationServer
{
        interface RemoteAuthorization
        {
                void setPermission(in string permission);
                boolean checkPermission(in string permission);
                void init(in string principal, in string name);
        };

};
```

Z interfejsu tego korzystają metody `canRead()` i `canWrite()` klasy `RemoteFile`. Zapewnia on co prawda tylko dostęp do List Kontroli Dostępu, ale ze względu na elastyczność mechanizmu ACL daje to możliwość składowania praktycznie dowolnych informacji dotyczących sesji czy też klienta.

W trakcie implementowania biblioteki planowano wykorzystanie DII na styku klient-serwer, jednakże narzuty czasowe oraz zalecenia OMG dotyczące sposobu wołania metod spowodowały zastosowanie modelu "namiastki i szkielety" .

W realizacji wykorzystano ORBACUSA 3.0 - ORBA zgodnego ze standardem CORBA 2.2. ORBACUS jest produktem darmowym dla użytku edukacyjnego i non-profit, występujący w wersji napisanej w C++ i w Javie. W pracy niniejszej wykorzystano wersję napisaną w Javie. Środowiska wykorzystane przy tworzeniu aplikacji (Supercede, VisualAge i JDK) zgodne są ze standardem Java 1.1.6.

6. Podsumowanie

W niniejszym opracowaniu opisano prototyp systemu o architekturze NCA, który miał uzasadnić sensowność konstruowania rozproszonych systemów o zredukowanej funkcjonalności klientów i umożliwiających scentralizowanie zarządzania i konfigurowania klientów. Poprzez zastosowanie dwóch dodatkowych wyróżnionych serwerów specjalizowanych usług uzyskano efekt całkowitej transparentności lokalizacji żądanych usług. Środowiskiem pracy aplikacji klientów jest biblioteka transparentnego dostępu do zdalnych serwerów o semantyce odwołań zgodnej z dotychczasowymi bibliotekami środowiska maszyny wirtualnej JAVY.

W wyniku podjętych prac powstał szkielet systemu, który może być rozbudowywany o dalsze komponenty, na przykład moduły szyfrowania danych lub automatycznego rozpraszania danych (mirroring). Dzięki zastosowaniu dwóch otwartych technologii – języka JAVA i standardu obiektowej komunikacji CORBA rozszerzanie możliwości funkcjonalnych systemu jest stosunkowo proste.

W trakcie prac nad systemem rozważone zostały różne warianty wołania zdalnych metod. Do implementacji została wybrana metoda statyczna, bazująca na modelu "stubs&skeletons", ze względu na narzuty czasowe wnoszone przez metody dynamiczne. W trakcie dalszego rozwoju biblioteki istnieje jednakże możliwość wykorzystania mechanizmów DII/DSI, z tym że

serwera są przekształcane w RIOException, by po przebyciu ORBa być ponownie konwertowane do `java.io.IOException`. Idea ta została zobrazowana na tabeli 1.

Klient	Serwer

Public int read() throws java.io.IOException{
  Try {
  return ris.read();
  } catch (RIOException iox) {
  throw new java.io.IOException();
  }
}
	public int read() throws RIOException {
	  try {
	  return localFileInputStream.read();
	  } catch (java.io.IOException iox) {
	  throw new RIOException();
	  }
	}

Tabela 1 Przekazywanie wyjątków pomiędzy serwerem i klientem

Podczas implementacji zastosowano szablon *fabryki obiektów* (ang. factory design pattern [8]). W modelu tym istnieje jeden obiekt główny (fabryka obiektów), do którego kierowane są żądania tworzenia obiektów. Fabryka tworzy nowy obiekt, po czym zwraca referencje do niego klientowi. Poza prostotą i wydajnością takiej implementacji, zapewnia ona także:

- zapewnienie bezpieczeństwa - klient może być zmuszony do pozyskania autoryzacji przed otrzymaniem referencji do obiektu
- wyrównywanie obciążenia (Load Balancing) - fabryka zarządza pulą obiektów, które mogą reprezentować pewne ograniczone zasoby, i przydziela je według określonego algorytmu
- wielopostaciowość - fabryka może zwracać referencje do różnych implementacji w zależności od żądania klienta

Zastosowany model zapewnia także stałą dostępność serwera, ponieważ obiekt fabryki obiektów jest wywoływany tylko raz podczas uzyskiwania dostępu do zasobu, po czym po przekazaniu referencji do stworzonego obiektu jest gotowy na obsługiwanie kolejnych żądań.

5.1. Serwer Usług (FS)

Serwer Usług jest podstawowym komponentem przedstawianej architektury. Jak widać na poniższym wydruku, uzewnętrznia on poprzez ORBa klasy obsługi plików biblioteki `java.io`, a dokładniej klasy szkieletu usług rozproszonych. Ze względu na brak polimorfizmu w architekturze definiowanej przez standard CORBA, po stronie serwera zdefiniowane jest po jednej metodzie do zapisu i odczytu pliku (`read()` i `write()`) odpowiednio klas `RemoteInputStream` i `RemoteOutputStream`:

```
//RemoteInputStream
public int read() throws RIOException;
[...]

//RemoteOutputStream
public void write(int b) throws RIOException;
```

Aby zapewnić funkcjonalność i zgodność semantyczną, po stronie klienta znajdują się "klasy opakowania" `RemoteFileInputStream` oraz `RemoteFileOutputStream`, które implementują odpowiednio trzy funkcje odczytu i zapisu zgodne z metodami klas `FileInputStream` i `FileOutputStream` biblioteki `java.io`:

Dla poprawnej pracy prototypu niezbędne jest przekazywanie między poszczególnymi węzłami systemu następujących informacji:

1. Żądanie wykonania usługi kierowane do serwera preferencji. Żądanie to następuje w momencie, gdy klient próbuje utworzyć nowy plik lub otworzyć plik już istniejący ulokowany lokalnie lub na jednym z serwerów usług.
2. Serwer preferencji na podstawie charakterystyki danego klienta przekazuje jego żądanie do właściwego serwera usług lub pozwala klientowi ma lokalne wykonanie żadania.
3. Sprawdzenie autoryzacji dostępu - faza I (zapytanie). Po otrzymaniu żądania, Serwer Usług sprawdza, czy dany klient jest uprawniony do określonych operacji na pliku.
4. Sprawdzenie autoryzacji dostępu - faza II (odpowiedź). Serwer Autoryzacji zwraca prawa dostępu dla klienta. Jeśli dany klient nie jest uprawniony do otrzymania żądanej usługi, Serwer Usług generuje odpowiedni wyjątek.
5. Przesłanie danych do/od klienta. W fazie tej następuje właściwe przesłanie danych do/od klienta.

Dla oprogramowania po stronie klienta widoczne są tylko fazy 1 i 5 (ewentualnie pośrednio faza 3 w wypadku gdy klient nie jest uprawniony do korzystania z zasobów) - żądanie dostępu oraz przesłanie danych, natomiast wszystkie pozostałe operacje powinny być wykonywane w sposób automatyczny i niewidoczny dla klienta.

5. Implementacja

Biblioteka `java.io` w wersji 1.1.6, będąca w części punktem wyjścia dla implementacji biblioteki `pl.poznan.put.cs.rio` (zwanej dalej `rio`), definiuje następujące klasy służące składowaniu i pozyskiwaniu danych z urządzeń pamięci masowej:

◊ `File` - reprezentuje plik

◊ `FileDescriptor` - reprezentuje specyficzne dla maszyny struktury odwzorowujące otwarty plik. Jest zaimplementowana jako native (czyli w sposób nieprzenośny) i ze względów bezpieczeństwa nie został uwzględniony.

◊ `FileInputStream` - odzworowuje wejściowy strumień danych

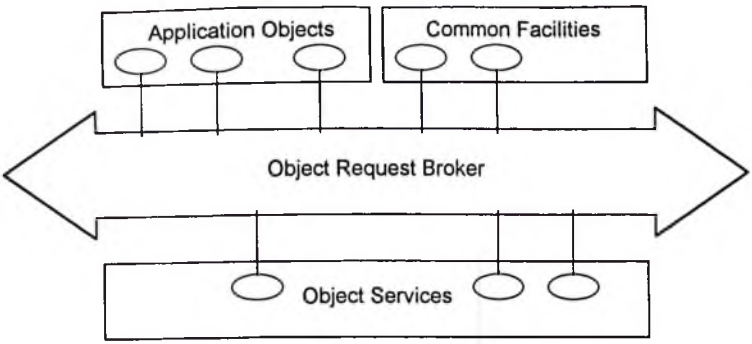
◊ `FileOutputStream` - wyjściowy strumień danych

◊ `FileReader` - klasa będąca ułatwieniem przy odczycie plików znakowych

◊ `FileWriter` - jest ułatwieniem przy zapisie plików znakowych. Podobnie jak klasa poprzednia nie wnosi dodatkowej funkcjonalności, a narzuty czasowe przy tworzeniu wystąpień zdalnych odpowiedników tych klas uczyniły zdalną implementację nieopłacalną.

Obiekty z powyższej listy po uwzględnieniu uwag stały się rdzeniem biblioteki `rio` (na styku klient - FS). Projektowane początkowo klasy Client i ClientAccess na styku FS - AS oraz ClientPreference i Preference na styku FS - PS zostały zastąpione przez ACL (ang. Access Control List - Lista Kontroli Dostępu [9]), bardzo elastyczny mechanizm dający się wykorzystać wbrew nazwie nie tylko do autoryzacji dostępu. Po tej zmianie nastąpiła konwergencja AS i PS, co zaowocowało poza uproszczeniem implementacji także zmniejszeniem opóźnień.

Funkcjonalnie biblioteka została podzielona na dwie współpracujące części: klienta i serwera,. Część kliencka zapewnia zgodność semantyczną z istniejącą biblioteką java.io, natomiast strona serwera zapewnia podstawową funkcjonalność i obsługuje żądania klienta. Obie części



Rys. 1 Model architektury OMA

Narzędziem specyfikacji obiektów komunikujących się poprzez magistralę ORB jest język definicji interfejsu IDL (ang. Interface Definition Language). Język ten umożliwia zdefiniowanie usług udostępnianych przez dany obiekt w sposób niezależny od języka jego implementacji. Dzięki temu komponenty zdefiniowane przy wykorzystaniu IDL są przenośne między językami programowania, platformami sprzętowymi i programowymi oraz sieciami.

IDL jest językiem czysto deklaratywnym, i jako taki nie zawiera żadnych informacji dotyczących implementacji obiektów. IDL definiuje tylko interfejsy aplikacji (ang. API - Application Programming Interface) i umożliwia specyfikację atrybutów obiektów, ich metod i wyjątków, a także określenie hierarchii dziedziczenia. Gramatyka IDL jest podzbiorem gramatyki języka C++ z dodatkowymi elementami umożliwiającymi specyfikację przetwarzania rozproszonego.

Magistrala obiektowa ORB przewiduje kilka rodzajów interfejsów po stronie klientów i serwerów usług:

- Statyczny interfejs wywołań usług za pomocą tzw. *namiastek (*ang. *Stubs*). Namiastki definiują sposób wywołania przez klienta odpowiednich metod serwera. Z punktu widzenia klienta odwołania do serwera są odwołaniami lokalnymi. Namiastki kodują i dekodują komunikatu i ich parametry do ustalonego formatu, po czym przesyłają je do serwera.
- Dynamiczny Interfejs Wywołań (ang. DII - Dynamic Invocation Interface) umożliwia wyszukiwanie wywoływanych metod w trakcie uruchamiania programu. CORBA definiuje interfejsy umożliwiające odnalezienie opisu usług serwera, wygenerowanie parametrów, wykonanie wołania metody i pobranie wyników. Korzystanie z tego interfejsu wiąże się z dodatkowymi narzutami czasowymi.
- Interfejs ORB (ang. ORB Interface) składa się z kilku API do obsługi usług lokalnych, jak np.: zamiana referencji obiektu w łańcuch znaków i na odwrót.
- Szkielety (ang. skeletons), które zapewniają statyczny interfejs do wszystkich usług oferowanych przez serwer. Szkielety, podobnie jak namiastki, są generowane za pomocą kompilatora IDL.
- Dynamiczny Interfejs *Szkieletowy* (ang. DSI - Dynamic Skeleton Interface) zapewnia mechanizm późnego wiązania usług serwerom, które muszą obsługiwać żądania dla klientów nie posiadających namiastek. Mechanizm DII jest szczególnie przydatny przy tworzeniu mostów pomiędzy magistralami ORB.

komputery o ograniczonej do minimum pamięci operacyjnej, dyskowej i wolniejszych procesorach. Część firm komputerowych oferuje w sprzedaży stacje o ograniczonych parametrach jako komputery sieciowe, predestynowane do zastosowania w systemach o architekturze NCA.

Ułatwienie administrowania systemem może zostać osiągnięte poprzez scentralizowanie pielęgnacji oprogramowania implementującego podstawowe funkcje użytkowe systemu. Eksploatowane oprogramowanie zamiast na wszystkich stacjach klienckich utrzymywane jest jedynie na nielicznych serwerach aplikacji. Podejście to gwarantuje ujednolicenie oprogramowania eksploatowanego przez użytkowników systemu niewielkim wysiłkiem administratora. Upraszcza również procedurę autoryzacji dostępu do poszczególnych funkcji systemu.

Z kolei zwiększenie efektywności przetwarzania systemu może zostać osiągnięte w wyniku zmiany rozkładu obciążenia poszczególnych elementów systemu. Komputery personalne nie dysponują wystarczającymi zasobami dla realizacji funkcji interfejsu systemu oraz złożonego i intensywnego przetwarzania danych. W architekturze NCA przetwarzanie danych jest przeniesione ze stacji klienckich na silniejsze jednostki pełniące rolę serwera aplikacji. Klienci są zredukowani do roli przeglądarek dla usług i danych obsługiwanych przez specjalizowane serwery.

W niniejszym opracowaniu przedstawiono projekt i implementację prototypowego systemu o architekturze NCA. Jako platformę programową dla interfejsu oraz funkcji systemu przyjęto język Java. Rolę platformy komunikacyjnej pomiędzy klientem a serwerem usług pełni standard CORBA. Obie te technologie zostały wybrane ze względu na ich przenośność pomiędzy różnymi platformami programowo-sprzętowymi. Funkcjonalność serwera usług miała odpowiadać standardowemu serwerowi plików. W ramach pracy nad prototypem założono stworzenie klasy zdalnego dostępu do systemu plików serwera usług, która semantycznie i funkcjonalnie odpowiadałaby istniejącej klasie `java.io`, przy jednoczesnym zapewnieniu środków kontroli dostępu do plików.

Struktura niniejszego opracowania jest następująca. W rozdziałach drugim i trzecim krótko przedstawiono wykorzystane technologie: język JAVA i architekturę CORBA. Rozdział czwarty zawiera projekt prototypu. Zdefiniowano w nim charakterystykę funkcjonalną poszczególnych modułów systemu. W rozdziale piątym przedstawiono elementy implementacji prototypu. Rozdział szósty zawiera podsumowanie pracy.

2. Przenośny język programowania JAVA

Język JAVA jest obiektowo-zorientowanym językiem programowania ogólnego przeznaczenia. Składniowo jest podobny do języka C++, lecz nie posiada wielu cech, które czyniły ten język złożonym i niebezpiecznym. Od początku język ten był projektowany jako język programowania komputerów połączonych w sieć komputerową. JAVA jest zaprojektowana do pracy na różnych platformach sprzętowo-programowych w sposób umożliwiający bezpieczną wymianę modułów programowych (obiektów) między różnymi węzłami sieci. Aby spełnić te wymagania, skompilowany kod JAVY musi działać na różnych platformach stacji klienckich i zagwarantować klientom bezpieczeństwo uruchamiania *obcych* obiektów.

Elementem składowym języka JAVA jest zbiór predefiniowanych klas systemowych tworzących *wirtualną maszynę JAVY* (ang. Java Virtual Machine - JVM). JVM jest abstrakcyjnym procesorem, który posiada własny zestaw instrukcji. To właśnie ona umożliwia pełną przenoszalność skompilowanych programów JAVY oraz zapewnia bezpieczeństwo uruchamiania obcych aplikacji.

Projekt: Internet dla Lekarzy

Program "Internet dla Lekarzy" (IdL) rozpoczął swoją działalność we wrześniu 1997 roku. Misją programu IdL jest promowanie wykorzystania sieci Internet do celów zawodowych w środowiskach medycznych w Polsce. Cel ten realizowany jest przede wszystkim poprzez upowszechnianie dostępu do sieci Internet wśród osób związanych z medycyną w Polsce, organizację szkoleń w wykorzystaniu Internetu oraz wspieranie i stymulację powstawania polskojęzycznych zasobów medycznych i innych projektów medycznych w sieci Internet.

Na dotychczasową działalność programu złożyły się przede wszystkim dwa konkursy:

- "Kluby Internetowe" - dofinansowanie utworzenia pracowni komputerowej podłączonej do sieci Internet, jej administracji i obsługi, przeprowadzania szkoleń w wykorzystaniu sieci Internet oraz w realizacji własnych projektów w sieci Internet. Klub przeznaczony jest dla osób związanych z medycyna z całego (jak najszerzej rozumianego) regionu jego działania. Dotychczas przyznano dofinansowanie ponad 20 projektom (w Hajnówce, Katowicach, Kraśniku, Krakowie, Legnicy, Lublinie, Łomży, Mielcu, Międzyrzecu Podlaskim, Nisko, Poznaniu, Puławach, Rabce, Suchej Beskidzkiej, Tarnowie, Toruniu, Ustroniu-Zawodziu, Warszawie, Wrocławiu) na łączną sumę około 2 mln. zł;

- "Innowacyjne zastosowania Internetu w Medycynie" oraz "Tworzenie i rozwój medycznych stron WWW, baz danych i innych zbiorów informacji w sieci Internet" - pomoc finansowa w realizacji projektów w nowy sposób wykorzystujących sieć Internet w praktyce medycznej (telemedycyna, telediagnostyka, nauczanie na odległość, edukacja medyczna przez sieć Internet, etc.).

- Dotychczas przyznano dofinansowanie 20 projektom (m.in. w Bytomiu, Gdańsku, Katowicach, Krakowie, Lublinie, Łodzi, Poznaniu, Toruniu, Warszawie – szczegółowy opis dofinansowywanych projektów można znaleźć w sieci Internet pod adresem podanym powyżej) na łączną sumę ponad 800 tys. zł.

W maju 1998 roku dzięki uzyskanej przez nas dotacji Fundacji Bankowej im. Leopolda Kronenberga otwarty został nowy konkurs:

- "Szkolenia w wykorzystaniu Internetu w praktyce medycznej" - dofinansowanie części kosztów organizacji szkoleń dla lekarzy i innych pracowników służby zdrowia. Zakres tematyczny szkoleń musi być bezpośrednio związany z siecią Internet.

  Dotychczas przyznano pięć dotacji: szkolenia w Toruniu (szkolenie 140 osób), Wrocławiu (szkolenie 340 osób), Kaliszu (szkolenie 100 osób) i Żarach (szkolenie 100 osób) oraz cykl 24 prezentacji Internetu w medycynie w instytucjach medycznych na terenie całej Polski (w których wzięło udział ponad 600 osób). Łączna kwota dotacji to ponad 77 tyś. zł.

Planujemy wykorzystanie platformy powyższych konkursów również dla ułatwienia rehabilitacji osób niepełnosprawnych (wspólnie z węzłem projektu Internet dla Niepełnosprawnych), wspierania praktyki lekarza rodzinnego (Serwis Lekarza Rodzinnego w Polsce), oraz poszerzania kontaktów pomiędzy medykami w Polsce i na Zachodzie.

Odnośniki do wspieranych przez nas projektów znajdują się pod adresem:
http://www.batory.org.pl/internet/txt/dotacje.html oraz
http://www.batory.org.pl/internet/dla/lekarzy/

Gmina

- Zrealizowaliśmy projekt regionalny "Internet dla Gminy, Miasta i Wsi" prowadzony przez Wojewódzką Bibliotekę Publiczną w Olsztynie oraz w gminie Jonki, który pokazuje, że Internet na szczeblu lokalnym, dzięki porozumieniu wielu instytucji może stać się doskonałym sposobem promowania gminy, współpracy samorządu z mieszkańcami, nieocenionym narzędziem zdobywania wiedzy (umieszczono terminale w świetlicach bibliotek wiejskich) oraz pracy - zgodnie z umową z urzędem Pracy Urzędu Wojewódzkiego umieszczane są w Internecie oferty pracy.

Czasopisma i Biblioteki

- W drugiej połowie 1997 roku przygotowaliśmy i przeprowadziliśmy dwie edycje warsztatów dla około 40 wydawców małych czasopism o profilu kulturalno-społecznym dotyczących wykorzystania Internetu jako alternatywnego medium publikacji czasopisma. Czasopisma otrzymały ofertę dotycząca wykorzystania darmowego serwera Fundacji,
- Przygotowaliśmy katalog zbierający ofertę ponad 200 „czasopism kulturalnych w Polsce", można go oglądać w sieci Internet pod adresem http://www.batory.org.pl/katalog/
- Obecnie realizujemy zamknięty konkurs dla bibliotek publicznych, którego celem jest podłączenie do Internetu 50 wybranych bibliotek.

Powódź

- Bezzwłocznie i intensywnie włączyliśmy się w pomoc powodzianom, od pierwszych dni powodzi zorganizowaliśmy Internetowy serwis informacyjny w ramach nieformalnego "konsorcjum" z Caritas, Polska Akcja Humanitarna, PCK oraz Wielką Orkiestrą Świątecznej Pomocy,
- W wyniku tych działań powołaliśmy pozarządowy ośrodek informacyjny dla powodzian TRATWA, który obecnie został przeniesiony do Wrocławia i działa pod nazwą „Centrum do spraw katastrof i klęsk żywiołowych – Tratwa" (http://tratwa.ids.pl/),
- Zleciliśmy IdS-owi podłączenie 12 partnerów Tratwy stałymi łączami do Internetu, oraz umożliwiliśmy dostęp do Internetu i przeszkoliliśmy pracowników 12 ośrodków pomocy społecznej, partnerów Tratwy i Ministerstwa Pracy.

Konkurs: „Pszczoły do Ula" – Internet dla Organizacji Pozarządowych

- W 1998 roku opracowaliśmy zasady i przeprowadziliśmy trzy edycje projektu dla Organizacji Pozarządowych "Pszczoły do Ula", którego celem jest wprowadzenie do Internetu organizacji, które dostarczają informacje niezbędne dla rozwoju i funkcjonowania trzeciego sektora (przyznaliśmy dotację ponad 100 instytucjom),

  W ramach konkursu „Pszczoły do Ula" można otrzymać dofinansowanie na :
  - konwersję danych, opracowanie materiałów w wersji html - bazy danych, specjalistyczne serwisy,
  - prowadzenie szkoleń w posługiwaniu się Internetem i opracowywaniu materiałów,
  - unowocześnienie oprogramowania i sprzętu - w wyjątkowych i uzasadnionych przypadkach.

- Współuczestniczyliśmy w tworzeniu kalendarza NGO zbierającego wydarzenia istotne dla sektora pozarządowego w Polsce (http://www.ngo.pl/html/kalendarz.html)

4. Korzyści i zagrożenia

Wprowadzenie usług finansowych do Internetu oznacza nową jakość obsługi klienta. W zamian za rezygnację z osobistego kontaktu z pracownikami banku, klient widzi znaczące obniżenie kosztów transakcyjnych, powodujące pewne oszczędności. W dodatku oferta biura maklerskiego czy banku pozostaje ciągle aktualna. Część tych korzyści jest przekazywana klientom a część akcjonariuszom. W ten sposób bank może osiągnąć przewagę konkurencyjną. Alianse strategiczne są efektem wykorzystania możliwości oferowania klientom transakcji wiązanych.

Do zagrożeń należy konieczność właściwego zaprojektowanie systemu tak, aby z jednej strony był zgodny z istniejącym systemem w banku, a z drugiej strony zapewniał niezbędne bezpieczeństwo. Niezbędna jest ocena obszarów ryzyka systemów informatycznych, na których spoczywa całość odpowiedzialności za zadania banku. Ewentualna awaria może spowodować nie tylko zablokowanie usług lecz również procesy odszkodowawcze ze strony klientów.

Niedocenianym zagrożeniem jest niewłaściwy marketing, który może być tylko zwykłym przedłużeniem dotychczasowej oferty, bez podkreślenia cech właściwych usługom bankowym w Internecie wymienionym w rozdziale 2.

Problem dostępu do Internetu może być w warunkach polskich realną barierą zdobycia wystarczającej liczby klientów. Kolejną kwestią jest przeinwestowanie w nowe technologie, które nie przyczynią się do osiągnięcia wyznaczonych wskaźników rentowności. Należy przed rozpoczęciem projektu uwzględnić tą kwestię.

5. Podsumowanie

Powszechne zastosowanie Internetu w usługach finansowych oznacza kolejną rewolucję, nie tylko finansową, lecz również cywilizacyjno kulturową. Jeszcze nigdy dotąd klienci nie mieli takiego wyboru spośród konkurencyjnych ofert. Oznacza to wprowadzenie nowych usług, również dla nowych klientów z młodszego pokolenia, które potrafi już obsługiwać komputer i żeglować po Internecie, lecz jeszcze nie wie co to jest bank. Właśnie oni będą perspektywicznym rynkiem zbytu usług poprzez Internet.

Powyższe zmiany na pewno wpłyną na zmianę sposobu działania branży, nawet tych banków, które nie zdecydują się na wejście do Internetu. Będą one musiały jasno określić swój rynek i pobierać wyższe prowizje za to, że klient może przyjść do banku, wygodnie usiąść i porozmawiać z kompetentną osobą.

W efekcie nastąpi wkrótce zmiana strategii instytucji finansowych w Polsce. Należy się spodziewać wzrostu bezpośrednich form kontaktu z bankiem: telefonicznie, poprzez home banking czy przez Internet.

- Transakcyjna, czyli działalność operacyjna banku poprzez Internet,
- Płatnicza, w postaci dokonywania przelewów oraz akceptacji pieniądza elektronicznego, np. DigiCash lub CyberCash,
- Realizacji transakcji, poprzez zawarcie w trybie on-line wiążącej umowy kredytowej,
- Monitorowania transakcji, czyli bieżący nadzór nad realizacją zleceń giełdowych, płatniczych, itp.

3. Segmenty rynków finansowych

W 1999 roku zakres działalności finansowej w Internecie obejmuje praktycznie pełen zakres rynków finansowych. Jednakże tempo akceptacji produktów nie jest jednakowe, ponieważ zależy od dużej liczby czynników.

Rynek kapitałowy

Działalność instytucji finansowych w Internecie najszybciej rozwinęła się na rynku kapitałowym. Dotyczy to zarówno rynku wtórnego jak i pierwotnego.

Rynek wtórny

W procesie podejmowania decyzji inwestycyjnych kluczową rolę odgrywa dostęp do bieżącej informacja rynkowej takiej jak notowania akcji, funduszy inwestycyjnych, czy raporty okresowe spółek. Praktycznie każda informacja na powyższy temat znajduje się już w Internecie, na stronach bankowych oraz specjalistycznych, np. giełd papierów wartościowych.

Jednak podstawowym produktem finansowym na rynku bankowych usług detalicznych jest rachunek maklerski. W Polsce jedyna instytucją oferującą taką usługę jest Dom Maklerski Banku Ochrony Środowiska. Oferuje on pełen zakres usług, pobierając niższe prowizje od konkurencji. Za granicą popularnymi biurami maklerskimi są E*Trade i Charles Schwab w USA oraz Consors z Niemiec.

Rynek pierwotny

Ciekawą usługę na rynku polskim prezentuje DM BOŚ dla emitentów papierów wartościowych. Na stronach WWW można znaleźć aktualne prospekty emisyjne spółek wchodzących na giełdę, a także złożyć zamówienie na akcje oferowane w pierwotnym publicznym obrocie papierami wartościowymi. Jest to również informacja dla potencjalnych inwestorów.

Rynek pieniężny

Banki internetowe oferują dwa rodzaje usług na rynku pieniężnym. Pierwszy to instrumenty finansowe z rynku międzybankowego, np. weksle skarbowe USA. Drugi rodzaj usług to oprocentowane rachunki, których oprocentowanie jest tylko pośrednio zależne od tego rynku.

PERSPEKTYWY ROZWOJU USŁUG FINANSOWYCH W INTERNECIE

Adam Kaliszewski*

1. Wprowadzenie

Szybki rozwój technologii internetowych przyczynił się do pierwszych prób wykorzystania sieci w usługach finansowych już w 1995 roku. Od tego czasu kilkaset instytucji finansowych na świecie wdrożyło już zintegrowane systemy informatyczne służące do zawierania transakcji poprzez sieć.

Obecnie można już sobie wyobrazić banki bez oddziałów, wirtualne biura maklerskie, a także kredyt w 2 minuty. Klienci mają coraz lepszy dostęp do konkurencyjnych usług bankowych, co wymusza zmiany w działaniu tej branży.

Wraz z upowszechnianiem się Internetu jako środowiska zawierania transakcji, Unia Europejska zaproponowała zespół norm prawnych, które mają na celu zwiększenie skuteczności prawa i tworzenie bezpiecznych ram działania wirtualnych przedsięwzięć. Również kwestia bezpieczeństwa od strony systemowej i sprzętowej wpływa na potencjalnych klientów banków internetowych.

2. Cechy usług bankowych w Internecie

Usługi bankowe w Internecie mają zdecydowaną przewagę nad usługami tradycyjnymi. Cechuje je:

- Dostępność ogólnoświatowa, czyli możliwość korzystania z usług finansowych w taki sam sposób, na takim samym poziomie w dowolnym miejscu świata,

- Obsługa całodobowa, która nie kosztuje bank więcej niż obsługa w zwykłym czasie pracy. Jest to wynikiem automatyzacji procedur obsługi klienta oraz systemów eksperckich uczestniczących w bezosobowym procesie podejmowania decyzji.

  Banki polskie oferują przeważnie dostępność lokalną lub regionalną, wyłącznie w godzinach urzędowania. Decyzje podejmowane są w sposób tradycyjny, czyli są one podejmowane przez człowieka.

- Elastyczność, czyli łatwość dopasowania oferty konkretnej instytucji finansowej do aktualnej sytuacji rynkowej, czy też wprowadzenia nowych usług i promocji. Koszt drukowania kolorowych broszur czy jest niepotrzebny.

- Niskie koszty wejścia i obsługi, ponieważ zakup technologii informatycznych stanowi koszt zdecydowanie niższy od założenia sieci placówek na terenie regionu, kraju, czy kontynentu. Również koszty transakcyjne są niskie, ponieważ dla klientów bank staje się „samoobsługowy". System banku rejestruje i przetwarza jedynie dane wpisane do systemu

* Adam Kaliszewski jest pracownikiem firmy Arthur Andersen Sp. z o.o. w Warszawie. Poniższy tekst przedstawia wyłącznie poglądy autora. Kontakt z autorem: adam.kaliszewski@pl.arthurandersen.com

używa się jednego z kanałów telewizyjnych leżących w zakresie wysokich częstotliwości (powyżej 700 MHz).

Urządzenia do transmisji danych w sieci telewizyjnej

W centrum transmisji danych, lub przy bardziej rozbudowanej sieci w poszczególnych hubach optycznych, znajdują się urządzenia służące do zamiany sygnału z kodowania właściwego dla telewizji (QPSK itp.) na kodowanie stosowane w sieciach komputerowych (podstawowym jest Ethernet, choć urządzenia typu modem centralny umożliwiają transmisję pakietów również w innych standardach). Urządzenia tego typu nazywane są bramkami sieci, od ich wydajności zależy przepustowość sieci. Urządzenia starszych generacji umożliwiały przysyłanie sygnałów z szybkością około 4 Mbit/s, obecnie stosowane urządzenia umożliwiają przesył sygnału w kilku kanałach, każdy o przepustowości 10baseT, np. Aster City stosuje urządzenia o przepustowości: 30 Mbit/s w dół (w kierunku do odbiorcy) oraz 2,5 Mbit/s w górę. Bramka sieci współpracuje z modemami kablowymi zainstalowanymi u końcowych odbiorców regulując parametry pracy modemów. Urządzenia stosowane w Aster City dla przypadku odbiorców indywidualnych są asymetryczne z tego powodu, iż nasi klienci odbierają więcej informacji niż wysyłają.

Do niedawna urządzenia do transmisji danych produkowane przez poszczególne firmy były niekompatybilne ze sobą, a zatem wybór urządzenia centralnego określał również dostawcę urządzeń końcowych. W ostatnim czasie nastąpił znaczny wzrost zainteresowania ofertą telewizji kablowych, zwłaszcza w USA, ale również i w Europie. Spowodowane to jest znacznie większą przepustowością sieci telewizyjnych w stosunku do sieci telefonicznych. W związku z tym na rynku zaczęły pojawiać się rozwiązania wielu firm znanych z technologii tradycyjnie związanych z telekomunikacją i rynkiem sieci komputerowych – np. Cisco, 3Com i szereg innych. Większość producentów modemów kablowych przyjęła wspólny standard – zwany jako DOCSIS. W ramach tego standardu urządzenia centralne mają możliwość kontrolowania parametrów pracy modemów klienckich. Modem kliencki po włączeniu do sieci komunikuje się z modemem centralnym uzyskując od niego informację typu częstotliwość pracy itd. W ramach standardu DOCSIS możliwe jest też wprowadzenie szyfrowania transmisji – pozwala to na uniknięcie znanego problemu podsłuchiwania w sieciach telewizji kablowej. Dodatkowo standard ten wprowadza pewne elementy gwarantowanej jakości usług (tzw. Quality of Service – QoS) umożliwiając określenie przepustowości modemu klienckiego i co niemniej ważne wielu producentów oferuje urządzenia końcowe (modemy kablowe) zgodne ze standardem tym samym klient ma możliwość wyboru najbardziej mu odpowiadającego urządzenia.

Modemy centralne obsługują typowo około 1000 końcówek. Przy większej liczbie abonentów przemieszcza się je na niższy poziom – bliżej odbiorców – np. do węzłów optycznych. Przy bardzo rozbudowanej sieci modemy centralne mogą obsługiwać wybrane nitki światłowodowe prowadzące do osiedli.

Ewolucja sieci telewizyjnej w kierunku sieci telekomunikacyjnej

Pojedynczy modem centralny wymaga pasma 30 Mbit/s w dół i obsługuje typowo około 500 – 1000 odbiorców. Przy małej liczbie abonentów do świadczenia usługi transmisji danych wystarczy jeden modem centralny pracujący w jednym paśmie telewizyjnym. Wraz ze wzrostem liczby modemów i wzrostem ruchu w sieci takie rozwiązanie staje się niewystarczające. Można w takiej sytuacji wykorzystać kolejne kanały telewizyjne do

końcowymi punktami (protokołem takim jest np. RSVP). W takim kanale pakiety mogą płynąć ze stabilną prędkością i niewielkimi opóźnieniami.

Dynamiczne rezerwowanie pasma w Internecie jest jednak jeszcze bardzo obciążające dla routerów i dlatego nie może być stosowane przy większych przepływnościach.

Rozwiązywania problemów ciąg dalszy, czyli oferta NASK.

We wrześniu 1998 roku sieć NASK uzyskała zagraniczne połączenie naziemna 155Mbps. Jest ono zrealizowane w technologii ATM i stanowi podstawę do oferowania kwalifikowanych usług, takich jak Internet z gwarancją serwisu.

Dla dużych operatorów i klientów zestawiamy sieci korporacyjne o zasięgu krajowym i międzynarodowym stanowiące podstawę do budowy sieci Intranet z gwarancją serwisu. W sieci takiej przesyłany może być zarówno głos jak i transmisja wideo jednocześnie z danymi np. wewnętrznego serwera WWW.

Jako rozwiązanie w pełni internetowe oferujemy dostęp do nieobciążonych łącz szkieletowych sieci Internet poprzez ściśle zdefiniowany i wydzielony kanał. Od użytkownika zależy, czy ten kanał będzie niezbyt mocno obciążony, co pozwala nazywać to połączenie QoS Internet.

W miarę postępu prac standaryzacyjnych zamierzamy wprowadzać do sieci możliwość stosowania protokołów rezerwacji pasma, co pozwoli końcowemu użytkownikowi detalicznemu na korzystanie z zalet QoS Internet.

Podsumowując Internet z gwarancją usług jest już rzeczywistością. Stosowanie go pozwala na ujednolicenie medium transmisyjnego dotychczasowych usług telekomunikacyjnych i na wprowadzanie nowych, bardziej inteligentnych. W ten właśnie sposób Internet zmienia nasze życie. Przynajmniej od strony dostępu do informacji.

INTERNET Z GWARANCJĄ USŁUG (QoS INTERNET)

Andrzej Skrzeczkowski

NASK

We współczesnym Internecie pojawia się coraz więcej zasobów, jest coraz więcej komputerów, przenoszone jest coraz więcej informacji. Razem z Internetem rosną również oczekiwania wobec niego. Współczesny użytkownik chce nie tylko, żeby jego poczta elektroniczna działała prawidłowo i strona WWW pojawiała się szybko na ekranie. Oczekuje nowych usług – chciałby słuchać radia z Internetu, oglądać wybrany film, czy wreszcie móc porozmawiać i zobaczyć się z kimś daleko. Bardziej wymagający użytkownik będzie oczekiwał, że Internet połączy wiele komputerów w celu dokonania skomplikowanych obliczeń, czy pozwoli mu śledzić i kontrolować różne procesy zachodzące w czasie rzeczywistym. Wszystkie te oczekiwania może rozwiązać jedynie Internet z gwarancja usług – QoS Internet.

Wymagające aplikacje.

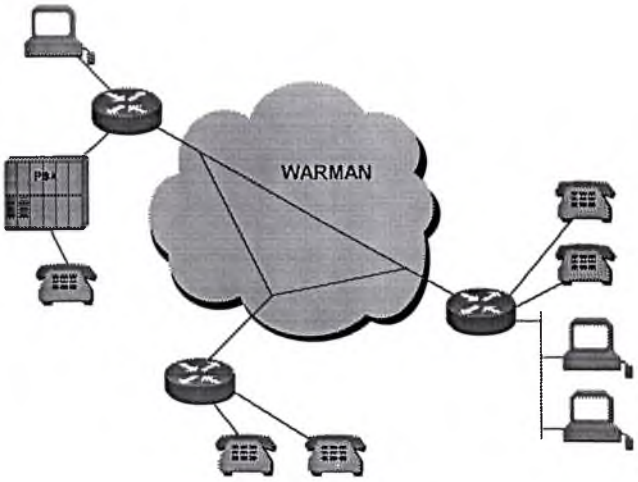
Opisany we wstępie obraz oczekiwań użytkownika byłby niekompletny bez przedstawienia kilku z wielu „wymagających" aplikacji powoli torujących sobie drogę we współczesnym Internecie.

Pierwszą ich grupą są systemy rozgłoszeniowe transmisji multimedialnej w Internecie. Systemy te na żądanie użytkownika wysyłają do niego ciąg pakietów z zawartą w nich transmisją wideo i audio (będzie to albo film na żądanie, albo bezpośrednia transmisja z jakiegoś wydarzenia, albo prosty podgląd z kamery na szczycie wieżowca pozwalający na zorientowanie się w sytuacji drogowej w mieście). Systemy te mogą sobie pozwolić na wyświetlanie obrazu i przekazywanie dźwięku z np. 15 sekundowym opóźnieniem. Dzięki zastosowaniu odpowiednio dużych buforów aplikacje te nie obawiają się dużych i zmiennych opóźnień i tolerują nawet chwilowe zaniki transmisji. Jedyne wymaganie to odpowiednio duże dostępne średnie pasmo. To jedyne wymaganie we współczesnym Internecie nie jest spełnione przez cały czas i wszędzie, a to oznacza niedostępność tej usługi dla dużej liczby użytkowników.

Dużo bardziej wymagającymi aplikacjami są systemy transmisji dwustronnej dźwięku i obrazu przez Internet, takie jak „telefon" Internetowy czy wideokonferencja. Dla tej usługi opóźnienia rzędu 200ms. są już krytyczne. Aplikacje wymagają więc od Internetu bardzo dobrych parametrów transmisyjnych (duże pasmo i małe, najlepiej stałe opóźnienie). Powszechne użycie takich systemów w dotychczasowej strukturze Internetu jest niemożliwe.

Równie wrażliwymi na jakość transmisji są systemy synchronizujące obliczenia i działające w czasie rzeczywistym. W ich przypadku najgroźniejsze są długie przerwy lub duże opóźnienia transmisji. Takie kłopoty z przesyłaniem danych drastycznie zmniejszają wydajność lub wręcz uniemożliwiają pracę systemów reagujących na wydarzenia.

Masowe wykorzystanie opisanych wyżej aplikacji we współczesnym Internecie nie jest na razie możliwe. Jakie są tego przyczyny opiszę poniżej.



Rys. 9

III. Dostęp do Internetu.

Kolejną usługą świadczoną przez sieć WARMAN jest dostęp do Internetu. Jest to usługa o największej ilości klientów i najbardziej znana, dlatego w części opisowej wszelkie warianty przedstawione zostały jedynie skrótowo.

1. Łącza dodzwaniane (Dial-up)

- nowe możliwości:

- modemy **56 kb/s** zgodne z **V.90** i **K56flex**,
- dostęp poprzez **ISDN 64 kb/s**.

Po dodzwonieniu się do serwera komunikacyjnego możliwe są do uzyskania następujące typy pracy:

- protokół PPP z dynamicznym przyznaniem adresu IP i możliwością pełnego korzystania z Internetu.
- dostęp terminalowy z możliwością wykonania telnetu na maszynę atos.warman.com.pl, będącą serwerem kont i poczty dla użytkowników

2. Łącza stałe.

a) asynchroniczne

- przepustowość do 115 kb/s,
- protokoły PPP, SLIP.

b) synchroniczne

Sieć WARMAN może oferować zestawienie wideokonferencji najwyższej jakości, będącej transmisją sygnału telewizyjnego w systemie PAL. Źródłem sygnału mogą być kamery wideo (wysokiej jakości lub popularne domowego użytku), natomiast odbiornikami mogą być tradycyjne telewizory lub rzutniki przystosowane do odbierania sygnału PAL. Dźwięk przesyłany jest stereofonicznie 16-bitowo/22kHz. Technologia ta zależnie od wymaganej jakości obrazu zajmuje od 5 do 20 Mb/s.

Następnym proponowanym sposobem realizowania wideokonferencji jest zastosowanie sprzętu zgodnego ze standardem H.320.

Wideokonferencje tego typu realizowane mogą być w oparciu o łącza dzierżawione (urządzenia posiadają porty V.35, V.36, itp.) lub o komutowane łącza ISDN'owe. Sumaryczna przepustowość łącza może wynosić od 128 do 384 kb/s w zależności od wymaganej jakości. Jako łącza dzierżawione służyć mogą kanały E1 WARMAN'a obsadzone odpowiednimi konwerterami dopasowującymi pasmo transmisji.

W celu zrealizowania wideokonferencji wielopunktowej należy wykorzystać mikser (mostek wideokonferencyjny) będący punktem centralnym takiego układu. Mostek będący na wyposażeniu NASK'u i podłączony do struktury WARMAN'a może obsłużyć jednocześnie kilka wielopunktowych wideokonferencji. Przy pomocy miksera jesteśmy w stanie łączyć różnego typu urządzenia podłączone przy pomocy różnych mediów.

Możemy wyodrębnić trzy grupy sprzętu realizującego ten typ wideokonferencji:
- wyspecjalizowane zestawy zapewniające wysoką jakość odbioru,
- zestawy oparte na komputerach osobistych,
- wideotelefony.

Wyspecjalizowane zestawy dają możliwość skierowania obrazu na odbiornik telewizyjny lub rzutnik. Mogą być do nich podłączone zdalnie sterowane kamery o zmiennym powiększeniu, specjalne szerokokątne kamery do przekazywania widoku dokumentów, zestawy mikrofonowe dla obsługi większego gremium rozmówców oraz mikrofony kierunkowe do automatycznego nakierowywania kamery na mówcę. Wyspecjalizowane zestawy nadają się dobrze do realizacji wideokonferencji z udziałem większej ilości osób na sali.

Zestawy oparte na komputerach osobistych dają raczej gorszą jakość, jednakże oferują dodatkowe możliwości w postaci wspólnej pracy nad dokumentem.

Wideotelefony dają zdecydowanie najmniejsze możliwości, ale za to nie wymagają wyspecjalizowanej obsługi i są najłatwiejsze do zainstalowania.

Kolejnym rozwiązaniem wideokonferencyjnym może być zastosowanie innego protokołu z tej samej rodziny, a mianowicie H.323. Sprzęt tego typu pozwala na nawiązanie wideokonferencji poprzez sieć LAN. Rozwiązania takie z reguły bazują na komputerach osobistych. Istnieją jednakże moduły pozwalające na konwersję H.320 na H.323 i podłączenie dużych wyspecjalizowanych zestawów do sieci LAN.

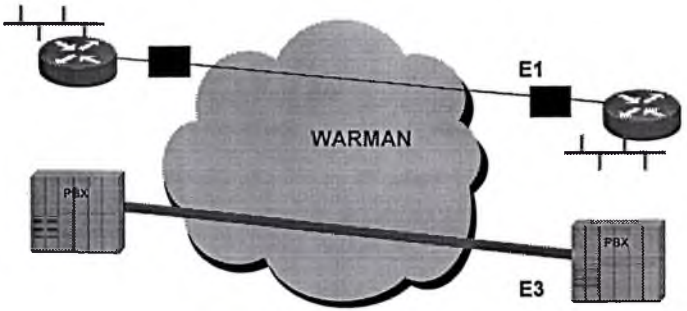
Dodatkową elastyczność można osiągnąć poprzez instalację bramek pozwalających na jednoczesne połączenie kilku sesji wideokonferencyjnych działających częściowo na sieci lokalnej (H.323), a częściowo na łączach dzierżawionych lub komutowanych (H.320).

realizowanie usługi wielopunktowej, polegającej na wydzieleniu z linii E1 kanałów 64 kb/s i skierowanie ich indywidualnie do różnych portów docelowych.

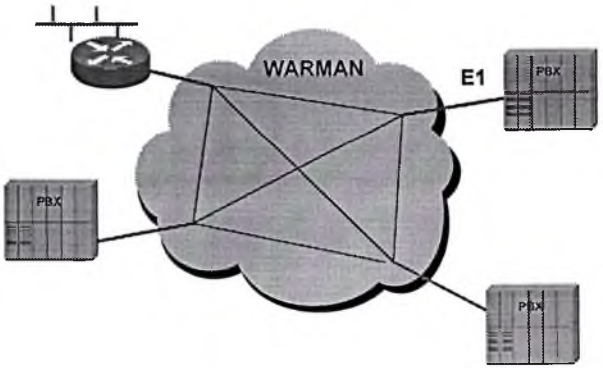
Możliwe jest zestawienie kanału cyfrowego do portu znajdującego się w Sztokholmie.

specyfikacja portów:

- E1 - symetryczne lub asymetryczne (120 lub 75 om), stryk DB15,
- E3 - asymetryczne 75 om.



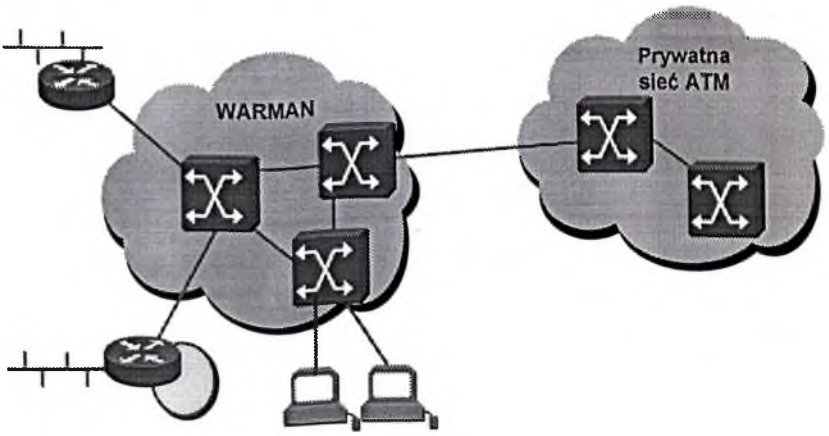
Rys. 5
Kanały cyfrowe



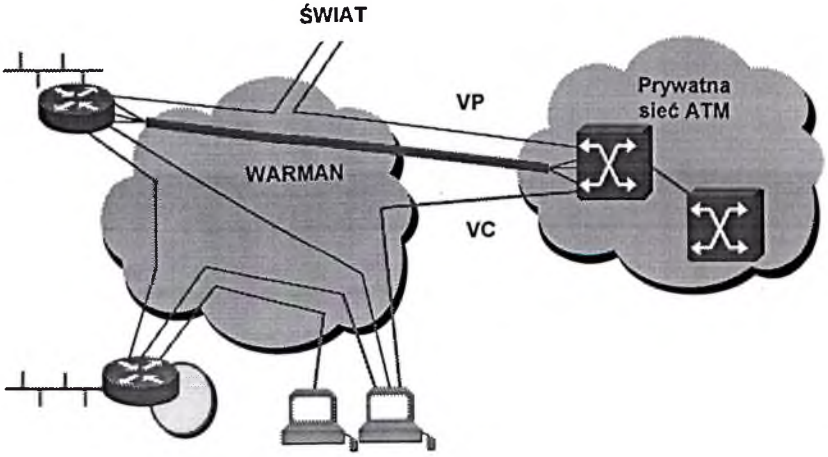
Rys. 6
Kanały cyfrowe z wydzieleniem szczelin 64 kb/s

4. Prywatne sieci typu Ethernet.

Struktura sieci WARMAN umożliwia rozpięcie klasycznej sieci ethernet na obszarze całego miasta. Pomiędzy lokalnymi segmentami sieci ethernet znajduje się wirtualny bridge



Rys. 2
Schemat podłączania stacji roboczych/serwerów, routerów i switch'y prywatnych do sieci WARMAN - łącza fizyczne



Rys. 3
Schemat podłączania stacji roboczych/serwerów, routerów i switch'y prywatnych do sieci WARMAN - kanały wirtualne VP i VC.

2. Prywatne sieci Frame Relay.

Sieć taka jest prywatną siecią Frame Relay rozpiętą na ATM'owym szkielecie sieci WARMAN. Z punktu widzenia użytkownika jest to normalna siec Frame Relay z konfigurowalnymi parametrami takimi jak CIR i EIR, z możliwością zestawienia wielu

USŁUGI W SIECI NASK

Rafał Klauzo

NASK

Najbardziej znaną i popularną usługą w sieci NASK jest dostęp do Internetu. W obecnej chwili nie jest to już tak ciekawa usługa jak było to kilka lat temu. Inną usługą świadczoną przez NASK od dawna, a adresowaną do odbiorcy o całokowicie innych wymaganiach są sieci korporacyjne, zarówno o zasięgu mejskim, krajowym jak i międzynarodowym. Sieci te mogą być realizowane w różnych technologiach w zależności od specyficznych potrzeb klienta.

Kolejną grupę usług stanowią usługi multimedialne polegające na przesyle głosu i obrazu bazując na sieciowej infrastrukturze NASK'u.

I. Sieci korporacyjne.

Metropolitalna sieć WARMAN umożliwia realizację zamkniętych sieci wydzielonych (sieci korporacyjnych). Realizacja tych sieci oparta jest na technologii ATM, jednakże z zewnątrz sieci te mogą wyglądać jak sieć Frame Relay, rozciągnięty po całym mieście ethernet, prywatna sieć ATM z wydzielonym pasmem lub zestaw kanałów cyfrowych.

Na jednej bazie, jaką jest WARMAN, może jednocześnie funkcjonować wiele prywatnych, odseparowanych od siebie sieci wirtualnych. Sieć korporacyjna może zapewniać użytkownikowi równoprawną łączność pomiędzy kilkoma jego lokalizacjami (np. ethernet) lub w przypadku najprostszym może łączyć dwa punkty kanałem cyfrowym.

Sieci korporacyjne oparte na sieci WARMAN, będąc sieciami wirtualnymi, z punktu widzenia ich użytkownika wyglądają jak jego własna prywatna sieć.

Z uwagi na połączenia z siecią rozległą NASK oraz sieciami innych operatorów (w tym zagranicznych) omawiane sieci wirtualne mogą mieć połączenia z lokalizacjami w całej Polsce jak i na świecie lub być częścią ogólnopolskich jak i międzynarodowych sieci korporacyjnych. W ramach połączeń ogólnopolskich oferujemy połączenia oparte na Frame Relay, natomiast połączenia zagraniczne mogą być realizowane jako Frame Relay, ATM lub kanały cyfrowe.

Bazując na sieciach korporacyjnych możemy zaoferować usługi dodatkowe polegające na przesyłaniu dźwięku i obrazu. W sieciach takich można realizować prywatne połączenia telefoniczne jak i wideokonferencje. Przesył obrazu w czasie rzeczywistym można zrealizować na kilka sposobów w zależności od stawianych wymagań (od połączeń realizowanych przy pomocy komputerów osobistych do wyspecjalizowanych systemów i przesyłu standardowego sygnału telewizyjnego w systemie PAL). Realizowane mogą być także wideokonferencje o zasięgu międzynarodowym.

ŁĄCZNOŚĆ MIĘDZYNARODOWA NASK

Roman Adamiec

NASK

Masowe zastosowanie komputerów w zarządzaniu przedsiębiorstwami, globalny charakter prowadzonych przez nie interesów oraz spadek kosztów transmisji danych spowodował ustalenie się trendów na rynku transmisji danych w skali międzynarodowej. Wprawdzie można tutaj wyodrębnić zarówno typowe potrzeby użytkowników jak i typowe usługi – jednakże zagadnienie to wykracza daleko poza sektor tzw. usług masowych czy standardowych.

Transmisja danych komputerowych pomiędzy oddziałami firmy zlokalizowanymi w różnych regionach świata przechodziła charakterystyczną ewolucję. Na samym początku próbowano wykorzystać do tego celu Internet. Ze względu na brak gwarancji przesłania informacji oraz dosyć dużą podatność na ingerencję osób niepowołanych, popularność tego podejścia do wymiany danych wewnątrz firmy systematycznie malała. Pierwotnie wywołało to zwiększoną popularność dedykowanych połączeń – na początku przeważnie satelitarnych – a następnie sieci pojawienie się VPN (*Virtual Private Network*), sieci korporacyjnych o zasięgu międzynarodowym.

Współczesne rozwiązania VPN:

- mają charakter globalny.
  Dzięki umowom z firmami zajmującymi się transmisją danych na skalę międzynarodową, możliwe jest zestawianie dla abonentów kanałów logicznych do dowolnych miejsc na świecie.

- są modułowe.
  Możliwe jest uzupełnienie podstawowej usługi VPN - kanałów logicznych - o elementy dodatkowe, takie jak połączenia lokalne, urządzenie końcowe po stronie abonenta, dostęp do Internet-u

- są elastyczne.
  W odróżnieniu od dedykowanych połączeń (np. satelitarnych) możliwa jest szybka rekonfiguracja VPN taka jak zmiana gwarantowanej przepustowości, zmiana lokalizacji czy zmiana parametrów kanału logicznego. Niejednokrotnie sprowadza się to do ustawienia nowych parametrów połączenia w systemie zarządzania operatora.

- mają charakter rozwiązań „pod klucz".
  Operator wydzielonej sieci przejmuje na siebie odpowiedzialność za działanie całego rozwiązania, nie tylko jego poszczególnych elementów. Dzięki temu abonent nie jest obciążony koniecznością posiadania wysokowykwalifikowanej kadry dedykowanej do obsługi połączeń teleinformatycznych.

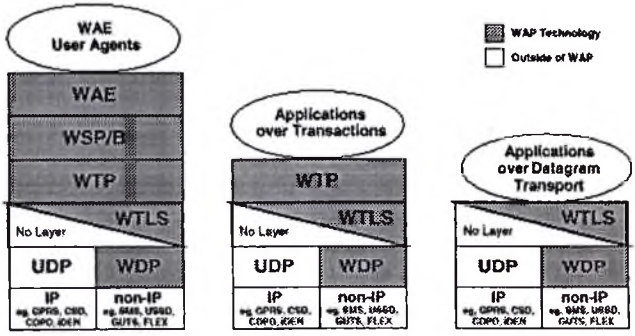
Bezprzewodowy protokół datagramowy WDP (*Wireless Datagram Protocol*) jest protokołem warstwy transportowej pracującym nad przenoszącymi dane nośnymi pracującymi zgodnie z określonym standardem telefonii bezprzewodowej. Podstawową usługą transportową WDP jest stała usługa świadczona wyższej warstwie w postaci przezroczystego kanału poprzez jedną z dostępnych nośnych.

Ponieważ protokół WDP stosuje wspólny interfejs do warstw wyższych zabezpieczenia, transportu i aplikacji, to warstwy te mogą pracować niezależnie od typu sieci bezprzewodowej. Adaptacja protokołu do typu sieci bezprzewodowej jest wymagana jedynie w warstwie transportowej. Lista obecnie obsługiwanych przez WDP typów sieci jest pokazana na rysunku 5.

8. Przykładowe struktury WAP

Technika WAP jest przygotowana do stosowania aplikacji i świadczenia usług nie uwzględnionych w dokumentach WAP Forum. Na rysunku 6 przedstawiono możliwe rejestry protokołów.

Rejestr z lewej strony przedstawia typową pełną aplikację WAP. Rejestr środkowy jest charakterystyczny dla usług transmisyjnych z zabezpieczeniem lub bez zabezpieczenia. Rejestr prawy jest charakterystyczny dla aplikacji i usług korzystających jedynie z transmisji datagramowej z zabezpieczeniem lub bez zabezpieczenia.



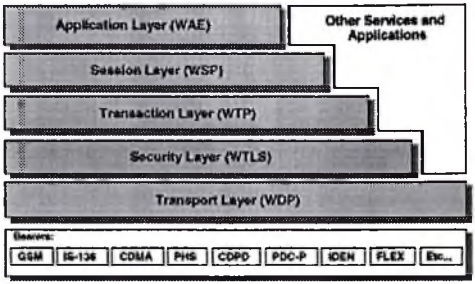
Rys. 6. Rejestry protokołów WAP

9. Podsumowanie

Obserwacja rozwoju metod dostarczania usług internetowych do ruchomych terminali skłania do stwierdzenia, że w tym obszarze na przestrzeni ostatniego roku poczyniono duży postęp. Od identyfikacji problemów występujących podczas transmisji danych w łączu radiowym do opracowania standardu opisującego protokół, który w znacznym stopniu redukuje niekorzystny wpływ omawianych na początku referatu czynników upłynął bardzo krótki okres czasu. Nie wszystko jednak w tym obszarze zostało już opracowane i ujednolicone. Do opracowania pozostało szereg zagadnień, m.in.: protokół transportowy zorientowany połączeniowo, integracja kart SIM, możliwość zdalnego wprowadzania bibliotek skryptów,

7. Elementy składowe architektury WAP

Architektura WAP dostarcza elastycznego, skalowalnego środowiska do rozwoju aplikacji przeznaczonych dla terminali ruchomych. Osiągnięto to poprzez warstwową strukturę protokołu przedstawioną na rysunku 5.



Rys. 5. Struktura warstwowa protokołu WAP

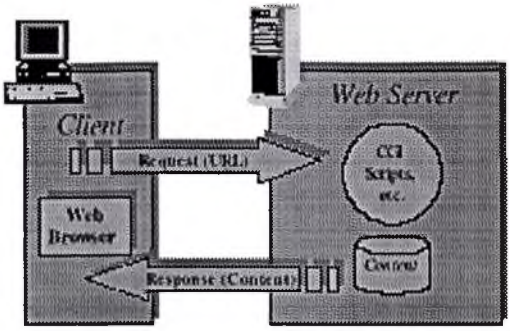
Środowisko aplikacji bezprzewodowych WAE (*Wireless Application Environment*) zostało zbudowane przy wykorzystaniu technik zapożyczonych ze środowiska WWW i środowiska telefonii bezprzewodowej. Podstawowym warunkiem spełnianym przez WAE jest możliwość tworzenia przez operatorów i podmioty świadczące usługi aplikacji i usług, które mogą pracować w skuteczny sposób na wielu platformach sprzętowych. Środowisko aplikacji bezprzewodowych obejmuje również środowisko mikroprzeglądarki, które musi spełniać następujące funkcje:

- stosować język WML (*Wireless Markup Language*) - prosty język, podobny do HTML, który został zoptymalizowany z punktu widzenia zastosowań w terminalach przenośnych,
- wykorzystywać skrypt WML, który jest podobny do skryptu języka Java (*JavaScript*),
- współpracować z aplikacjami telefonii bezprzewodowej WTA (*Wireless Telephony Application*) - w celu realizacji usług telefonicznych i obsługi programowego interfejsu WTAI (*Wireless Telephony Application Interface*),
- prezentować dane zgodnie z odpowiednim formatem strony (*Content Format*), stanowiącym zbiór dobrze zdefiniowanych formatów dotyczących prezentacji rysunków, danych z książki telefonicznej i informacji kalendarzowych.

Bezprzewodowy protokół warstwy sesji WSP (*Wireless Session Protocol*). Protokół ten dostarcza warstwie aplikacji WAP interfejs logiczny dla dwóch usług sesyjnych. Pierwsza z nich jest usługą zorientowaną połączeniowo pracującą ponad warstwą protokołu transmisyjnego WTP (*Wireless Transaction Protocol*). Druga jest usługą bezpołączeniową pracującą ponad warstwą protokołu usług datagramowych WDP (*Wireless Datagram Protocol*) z opcją bezpieczeństwa włączoną (*secure*) lub wyłączoną (*non-secure*).

Obecnie protokół warstwy sesji składa się z usług przystosowanych do przeglądania aplikacji WSP/B i zapewnia:

- funkcjonalność i semantykę wraz z kodowaniem w łączu radiowym zgodną z HTTP/1.1,
- długotrwałe podtrzymanie aktywności sesji,
- możliwość zawieszenia i wznowienia oraz migracji sesji,

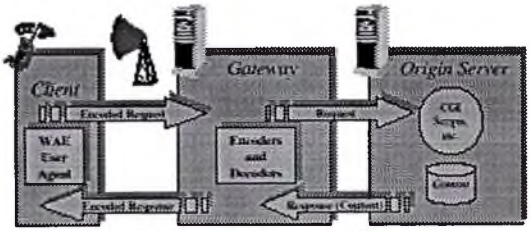


Rys. 2. Model dostępu do sieci WWW

• serwer proxy (*proxy*) - będący programem pośredniczącym, realizującym zarówno zadania serwera, jak i klienta w celu obsługi zapytań w imieniu klienta. Serwery proxy lokalizuje się zazwyczaj pomiędzy klientami i serwerami nie mającymi bezpośredniego połączenia z siecią, np. poprzez serwer zabezpieczający (*firewall*). Zapytania są obsługiwane przez serwer proxy lub przepuszczane do innych serwerów po translacji, jeśli zachodzi jej konieczność. Serwer proxy musi mieć zaimplementowane funkcje zgodne ze specyfikacją WWW, obsługujące zapytanie pochodzące od klienta i serwera.

• gateway - pracujący jako serwer pośredniczący dla innych serwerów. W odróżnieniu od serwera proxy, gateway otrzymuje zapytania tak, jak by był źródłowym serwerem w odniesieniu do przychodzącego zapytania. Klient wysyłający zapytanie może nie wiedzieć, że komunikuje się z gatewayem.

Strukturę modelu WAP pokazano na rysunku 3.



Rys. 3. Model dostępu do sieci WWW zgodny z protokołem WAP

Dostęp do sieci WWW przy wykorzystaniu WAP jest bardzo podobny do klasycznego modelu dostępu. Dzięki temu utrzymuje się wypróbowaną architekturę dostępu, znane rozwiązania i narzędzia nie wymagają zmian. Optymalizację i rozszerzenie dokonano z myślą o lepszym dopasowaniu do charakterystyk środowiska łączności radiowej. Tam, gdzie można było, zaadoptowano istniejące standardy lub użyto ich jako punkt wyjścia do rozwiązań opracowanych dla środowiska WAP.
Zawartość strony i aplikacje zgodne z protokołem WAP są definiowane w podobny sposób jak dla sieci WWW. Zawartość strony jest transportowana przy użyciu zbioru standardowych protokołów komunikacyjnych opartych o protokół komunikacyjny WWW. Mikroprzeglądarka

- względnie duża bitowa stopa błędu (10^{-3}),
- występujące znacznie częściej niż w łączach przewodowych przerwania połączeń.

Wpływ tych czynników ograniczających współpracę sieci komórkowej ze stacjonarną siecią transmisji danych można zminimalizować stosując architekturę klient - mediator - serwer zamiast klasycznej architektury klient - serwer. Mediator jest odpowiedzialny za komunikację między punktami końcowymi, która częściowo odbywa się w łączu stacjonarnym, a częściowo w łączu radiowym. Jest on odpowiedzialny za sterowanie przepływem danych w łączu heterogenicznym i zapewnienie użytkownikowi nadrzędnej kontroli. Architektura klient - mediator - serwer umożliwia:

- uzyskanie bardziej efektywnego wykorzystania ograniczonego widmowo kanału i zwiększenie tolerancji na błędy oraz poprawę działania,
- pozostawienie niezmienionej architektury TCP/IP w sieci stacjonarnej, aby nie zachodziła konieczność wymiany aplikacji sieciowych i protokołów w komputerach dołączonych do sieci stacjonarnej (hostach),
- stosowanie zaawansowanego sterowania transmisją w zawodnym i względnie drogim łączu radiowym,
- dostarczenie interfejsów dla oprogramowania aplikacyjnego, umożliwiających nowym apli-kacjom użytkownika współpracę z istniejącymi usługami świadczonymi przez stacjonarne komputery w sieci (hosty).

Spodziewając się rosnącego zainteresowania dostępem do Internetu grupa firm, w tym: Nokia, Unwired Planet, Ericsson i Motorola powołały do życia WAP (*Wireless Application Protocol*) Forum. Celem tego Forum jest opracowanie jednolitej, otwartej, uniwersalnej i ogólnie akceptowalnej specyfikacji, umożliwiającej tworzenie i udostepnienie abonentom sieci bezprzewodowych usług poprzez Internet.

4. Sieć GSM

Standard GSM wymaga dla przeźroczystej transmisji danych bitowej stopy błędu w interfejsie radiowym nie większej niż 10^{-3}. Podczas transmisji danych w trybie nieprzeźroczystym stosuje się dodatkową korekcję błędów na poziomie protokołu łącza radiowego RLP (*Radio Link Protokol*). Metoda korekcji została zapożyczona z protokołu HDLC i stosuje selektywne powtórzenia (transmisja z potwierdzeniem) [4] umożliwiające redukcję bitowej stopę błędu do wartości nie przekraczającej 10^{-8} dla danych transmitowanych w trybie „nieprzezroczystym". Oczywiście zostało to okupione zwiększeniem opóźnienia oraz zmianą szybkości transmisji w zależności od warunków propagacji. W warunkach dużej stopy błędu (transmisja przezroczysta) lub dużych opóźnień (transmisja nieprzeźroczysta) protokoły transportowe, takie jak TCP, nie są zbyt wydajne.

5. Protokoł TCP

Badania prowadzone w radiowych sieciach komputerowych WLAN (*Wireless Local Area Network*) wykazały, że protokoł TCP nie jest w nich wydajny. Te same efekty zaobserwowano w systemie GSM.
Protokoł transportowy danych TCP (czwarta warstwa) stosowany w sieci Internet ma wbudowane dwa samokontrolujące się mechanizmy:

- obsługę natłoku,
- obsługę błędów.

Mechanizmy te w środowisku łącza radiowego powodują mało skuteczne wykorzystanie kanału radiowego oraz ograniczenie jego pojemności.

DOSTĘP DO INTERNETU POPRZEZ BEZPRZEWODOWE TERMINALE

Daniel J. Bem, Ryszard J. Zieliński

Politechnika Wrocławska, Instytut Telekomunikacji i Akustyki
Wybrzeże St. Wyspiańskiego 27, 50-370 Wrocław
tel.:(71) 214 998, faks: (71) 223 473

e-mail: Dick@zr.ita.pwr.wroc.pl

1. Wprowadzenie

Bardzo szybki rozwój systemów telefonii komórkowej w ostatnich latach zarówno pod względem ilościowym, jak również technicznym, spowodował, że coraz większa liczba użytkowników próbuje z powodzeniem wykorzystać telefon komórkowy nie tylko jako urządzenie świadczące usługi głosowe, ale także jako urządzenie do transmisji danych. W Europie na czołowe miejsce wysunął się system GSM, który umożliwia transmisję dźwięku i danych. W ślad za nim podąża system DCS, identyczny pod względem architektury, ale pracujący w wyższym i szerszym zakresie częstotliwości. Jest on zatem bardziej pojemny. Systemy te są instalowane również w innych częściach świata: w Azji, Australii i Ameryce tworząc jednolitą i szeroko dostępną platformę dostępu do stacjonarnej sieci telefonicznej, a poprzez nią do zasobów informatycznych określonej firmy lub sieci komputerowej. Dostęp ten pod względem jakości ustępuje jednak dostępowi poprzez łącza przewodowe ze względu na dużo gorsze parametry łącza radiowego w stosunku do łącza przewodowego. Czy można zmniejszyć wpływ tych mniej korzystnych uwarunkowań i uzyskać podobną jakość dostępu do Internetu poprzez sieć GSM? Odpowiedź na to pytanie można znaleźć w dalszej części referatu.

2. Ogólna koncepcja ruchowego systemu z usługami multimedialnymi

Wykorzystanie systemu GSM jako sieci dostępowej do różnorodnego typu usług świadczonych przez sieci stacjonarne jest częścią ogólnej koncepcji stworzenia globalnego ruchowego systemu dostępu do usług multimedialnych GMM (*Global Multimedia Mobility*) [2]. Architektura tego typu systemu musi spełnić następujące wymagania:

- poradzić sobie z różnorodnością usług,
- umożliwić świadczenie usług przez wielu różnorodnych operatorów sieciowych i przez wiele firm usługowych od wielkich międzynarodowych korporacji zaczynając, a kończąc na małych firmach lokalnych,
- umożliwić dostęp do tych samych aplikacji poprzez różnego rodzaju terminale,
- oferować usługi w różnorodnych środowiskach w zależności od lokalnych warunków.

W strukturze systemu możemy wyróżnić urządzenia abonenckie (*Terminal Equipment*), sieć dostępową, sieć kręgosłupową (*Core Transport Network*) oraz aplikacje świadczące różnorodne usługi. Poszczególne elementy są oparte na już istniejących lub dopiero opracowywanych technikach. Koncepcję modelu tego systemu z wyróżnioną częścią dotyczącą systemu GSM jako dostępu do Internetu przedstawiono na rysunku 1.

Parametry terminali abonenckich w systemie SkyBridge

Parametr	Abonent indywidualny	Abonent instytucjonalny
Średnica anteny	<50 cm	60 - 100 cm
Maksymalna przepływność (nadawanie)	2 Mb/s	*n*×2 Mb/s
Maksymalna przepływność (odbiór)	20,5 Mb/s	*n*×20,5 Mb/s
Moc	<2 W	<2 W

Wstępne prace projektowe systemu SkyBridge rozpoczęto na początku lat 90. Do końca roku 1998 zostaną zakończone prace konstrukcyjne i projektowe. Następnie rozpocznie się produkcja elementów składowych segmentu kosmicznego i segmentu naziemnego. Umieszczenie na orbicie pierwszych satelitów jest przewidziane po roku 2000. Komercyjna eksploatacja systemu ma się rozpocząć w roku 2002.

Bibliografia

1. Ananasso F., Priscoli F., *The Role of Setellites in Personal Communication Services*, IEEE J. Select. Areas Commun. Vol.13. February 1995.
2. Bem D.J., Janiszewski J.M., *Systemy komunikacji osobistej*, materia³y Krajowego Sympozjum Telekomunikacji KST'95, Bydgoszcz 6-8 wrzeœnia 1995, tom A, s. 32-58.
3. Christensen J., *WRC-95. Results Related to Satellite Communications*, Via Satellite, February, 1996.
4. Clark D.J., *Personal Communications Service in Fixed and Mobile Networks*: Proc. of the Internat. IEE Conf. on Telcom., Manchester, 1993.
5. *Draft ERC Decision on the Harmonised Use of Spectrum for Satellite Personal Communications Services (S-PCS) Operating Within the Bands 1610 - 1625,5 MHz, 2483,5 - 2500 MHz, 1980 - 2010 MHz and 2170 - 2200 MHz*, ERC/PT 22 (S-PCS), Copenhagen, October 15 - 17 , 1996.
6. ETSI, ETR 093, *Satellite Earth Stations (SES); Possible European Standardisation of Certain Aspects of Satellite Personal Communications Networks (S-PCN)*, Phase 1 report, September 1993.
7. Gasparollo L., *The Globalstar System: A Complement to Terrestrial Mobile Networks*, Proceedings of the Second European Workshop on Mobile/Personal Satcoms (EMPS'96), 9 - 11 October, Roma, 1996.
8. Gilhousen K.S., Jacobs I.M., Padovani R., Viterbi A.J., Weaver L.A., Wheatley C.E., *On the Capacity of a Cellular CDMA system*, IEEE Trans. Vehicular Techn., Vol. 40, May 1991, pp. 303-311.
9. Gilhousen K.S., Padovani R., *Increased Capacity Using CDMA for Mobile Satellite Communications*, IEEE J. Select. Areas Comm., Vol.8. May 1990.
10. Graudenzi R., Graudenzi F., *Advances in Satellite CDMA Transmission for Mobile and Personal Communications*, Proc. of The IEEE, Vol. 84, January 1996.
11. Kajiwara, *Mobile Setellite CDMA System Robust to Doppler Shift*, IEEE Trans. on Veh. Techn., Vol 44, August 1993.
12. Maral G., Bousquet M., *Satellite Communications Systems*, Wiley&Sons, 1993.
13. Maral G., *Low Earth Orbit (LEO) Satellite Systems*, CEI-Europe, Spain, 1993.
14. Mazzella M., Cohen M. Rouffet D., Louie M., Gilhousen K.S., *Multiple Access Techniques and Spectrum Utilisation of the Globalstar Mobile Satellite System*, IEE Conference on Telecommunications, Manchester,1993, pp. 306-311.
15. Monsen P., *Multiple Access Capacity in Mobile User Satellite Systems*, IEEE J. Select. Areas Comm., Vol.13. February 1995
16. Pickholtz R.L., *Communications by Means of Low Earth Orbiting Satellites*, Modern Radio Science 1996, URSI, Oxford University Press, 1996, pp.133-150.
17. Prasad R., *Performance Analysis of Mobile Packet Radio Networks in Real Channels with Inhibit multiple Access*, IEEE trans. Comm., Vol. 26, October 1991, pp. 1405-1413.

Każdy satelita jest węzłem komutacyjnym połączonym z ośmioma satelitami: czterema na tej samej orbicie (dwa wcześniejsze i dwa późniejsze) i po jednym na każdej z dwóch sąsiednich orbit. Układ połączeń ma formę siatki i zapewnia konfigurację sieci odporną na awarie i lokalne przeciążenia.

Zmiany natężenia ruchu telefonicznego w sieci powodują ustawianie się kolejek pakietów na satelitach, co wydłuża czas oczekiwania na retransmisję do następnego satelity. Ten, jak i inne czynniki są brane pod uwagę przy zestawianiu połączenia. Decyzje są podejmowane w każdym węźle komutacyjnym (satelicie) stosując adaptacyjny algorytm marszrutowania. Algorytm ten korzysta z informacji rozprzestrzenianej w sieci przez każdego satelitę, na podstawie której określa się obciążenie sieci i dokonuje wyboru trasy o najmniejszym opóźnieniu. Pakiety tego samego połączenia mogą podążać różnymi drogami przez sieć. Każdy węzeł niezależnie marszrutuje pakiet wzdłuż trasy, która aktualnie oferuje najmniejsze opóźnienie do miejsca przeznaczenia. Terminal lub adapter w miejscu docelowym, jeśli jest taka potrzeba, porządkuje pakiety by wyeliminować efekty opóźnień czasowych. Rozległe i szczegółowe badania sieci i algorytmu marszrutowania wykazują, że dla długiej trasy całkowite opóźnienie między punktami końcowymi jest często mniejsze niż w lądowym połączeniu światłowodowym tych samych punktów.

W systemie można stosować zarówno terminale ruchome, jak i stacjonarne. Terminale stacjonarne nie są ograniczone mocą lub rozmiarem anteny. Terminale stacjonarne wykorzystują kanał o podstawowej przepływności 16 kb/s i dodatkowo 2 kb/s do sygnalizacji i sterowania. Mogą one być multipleksowane do przepływności 2 Mb/s. Podstawowa przepływność zapewnia jakość kodowania mowy taką jak w lądowych systemach cyfrowych (64 kb/s). Podstawowa przepływność umożliwia zastosowanie w sieci modemów o szybkości transmisji 4,8 kb/s. Zwielokrotnienie przepływności kanału podstawowego umożliwia tworzenie kanałów n×64 kb/s i realizację usług ISDN.

Terminale stacjonarne są wyposażone w anteny o średnicy około 25 cm, ustawione w ustalonej pozycji. Należy się spodziewać, że przeważająca liczba stacjonarnych terminali będzie połączona ze standardową siecią telefoniczną lub siecią ISDN. Możliwe jest stosowanie terminala grupowego, który umożliwia uzyskanie dostępu do sieci małym wsiom lub komunikację abonentów używających niedrogich telefonów bezprzewodowych.

Terminale ruchome są małe i lekkie, podobne do obecnie stosowanych w naziemnych sieciach komórkowych. Działają one przy małym poziomie mocy i używają anten niskoprofilowych (np. mikropaskowych). Ruchomy terminal wykorzystuje pojedynczy kanał o podstawowej przepływności 16 kb/s plus 2 kb/s do sygnalizacji i sterowania, który umożliwia transmisję mowy, transmisję modemową (4,8 kb/s), transmisję danych o przepływności 16 kb/s i trasmisję faksów. Zastosowanie małej anteny wymaga zastosowania w terminalu ruchomym większej energii na bit niż w terminalu stacjonarnym.

Obszar obsługiwany przez satelitę jest złożony z przylegających do siebie komórek, analogicznie jak w naziemnych systemach komórkowych. Wiązka antenowa satelitów przemieszcza się nad powierzchnią Ziemi z prędkością około 25 tysięcy km/h. Gdyby obszar komórki przesuwał się wraz z wiązką satelitarną, to terminal pozostałby w niej zaledwie przez kilka sekund, a częste przekazywanie rozmów zwiększyłoby koszty użytkowania systemu. W systemie Teledesic przekazywanie rozmów jest zminimalizowane przez zastosowanie komórek stacjonarnych, tzn. przypisanych do określonego obszaru na powierzchni Ziemi. Podczas ruchu nad powierzchnią Ziemi satelita kieruje swoje wiązki antenowe w miejsca stacjonarnych komórek, wewnątrz jego obszaru pokrycia. Częstotliwości i szczeliny czasowe są przypisane do każdej komórki i są przydzielane przez satelitę aktualnie obsługującego daną komórkę. Jak długo terminal pozostaje w obszarze komórki, tak długo zachowuje przydzielony mu na czas

Opłaty za usługi są bardzo wysokie. Na przykład w listopadzie 1998 roku koszt 1-minutowej rozmowy wynosił od 2,5 USD dla rozmowy zainicjowanej i kończącej się w Japonii do 10,2 USD dla rozmowy zainicjowanej w Ameryce Łacińskiej i kończącej się w Chinach. Średnio koszt 1-minutowej rozmowy wynosił 5 USD.

Przewiduje się, ¿e g³ówn¹ grup¹ abonentów systemu bêd¹ ludzie biznesu zmuszeni do czêstego podró¿owania. Za³o¿eniem jest, ¿e maj¹ oni w prosty sposób uzyskaæ takie same us³ugi, jakie s¹ im dostêpne w biurze. Ponadto oczekuje siê, ¿e potencjalnymi klientami systemu bêd¹ administracje krajów rozwijaj¹cych siê, które w ten sposób mog¹ zniwelowaæ ró¿nice w dostêpnoœci do systemów ³¹cznoœci bez koniecznoœci budowania dodatkowej infrastruktury telekomunikacyjnej.

W koñcu roku 1998 system Irydium mia³ 3000 abonentów. Nie jest to du¿a liczba, jeœli weŸmie siê pod uwagê, ¿e 2000 spoœród nich bra³o udzia³ w tescie *beta*. Operator systemu spodziewa siê, ¿e liczba abonentów wzroœnie do 500000 w koñcu 1999 roku i system oka¿e siê dochodowym na pocz¹tku roku 2000.

Globalstar jest systemem umożliwiającym transmisję fonii, danych, faksymili oraz określanie położenia. Zastosowano w nim kodową metodę dostępu wielokrotnego (CDMA - ang. *Code Division Multiple Access*), opatentowaną przez firmę Qualcomm Inc. Umożliwia ona korzystanie z tego samego kanału częstotliwościowego przez wielu użytkowników, zapewniając jednocześnie łatwe uzyskanie kompatybilności z innymi systemami stosującymi inne metody dostępu, np. podział czasu (TDMA - ang. *Time Division Multiple Access*), stosowany w systemie GSM.
W części naziemnej Globalstar ma korzystać z istniejącej infastruktury sieci komórkowych i publicznej sieci telefonicznej. Ma to być atutem systemu, gdyż zmniejsza koszty związane z budowaniem własnych łączy między adapterami międzysieciowymi. Z założenia system ma być uzupełnieniem istniejących systemów, zapewniając łączność tam, gdzie do tej pory jej nie było.
System składa się z konstelacji 48 satelitów umieszczonych na niskich orbitach, co umożliwia uzyskanie globalnego pokrycia. Wszystkie funkcje związane z przetwarzaniem i dystrybucją sygnałów są realizowane w części naziemnej systemu. Dzięki temu możliwe będzie zbudowanie tanich, niezawodnych satelitów.

Tabela 3

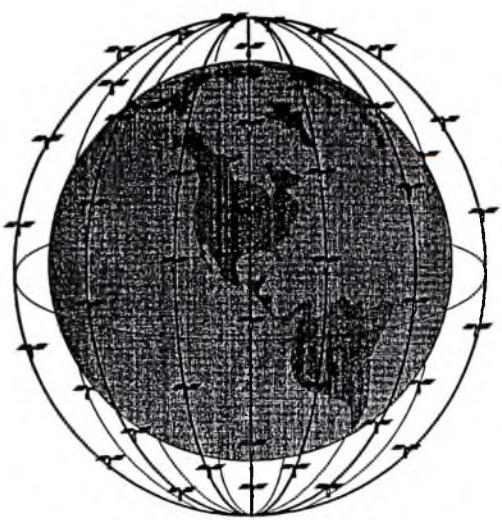
Podstawowe parametry systemu S-PCN Globalstar

Liczba satelitów	48 + 8 zapasowych
Liczba orbit	8
Inklinacja orbit	52^0
Wysokość orbity	1410 km
Okres obiegu	114 min
Okres widzialności satelity	16,4 min
Technika dostępu	CDMA/FDMA/FDD
Liczba wiązek na satelicie	16
Całkowita liczba wiązek	768
Średnica komórki	5850 km
Usługi:	
transmisja głosu	adaptacyjna 2,4/4,8/9,6 kb/s
transmisja danych	7,2 kb/s
faks	
przywoływanie	
krótkie wiadomości	

miał się składać się z 77 satelitów okrążających Ziemię na niskich orbitach. Przyrównano system do atomu, którego jądro okrąża 77 elektronów i dlatego nadano mu nazwę Irydium, pierwiastka o liczbie atomowej 77. Pomysłodawcą systemu była znana amerykańska firma Motorola. Oprócz Motoroli w realizację projektu jest zaangażowanych wiele organizacji: BCE Mobile of Canada, China Great Wall Industry Corp., Iridium Africa Corp., Iridium Andes-Carnibe of Venezuela, Iridium India Ltd., Iridium Middle East Corp., Khrunichev Enterprise, Lockheed of the USA, Nippon Iridium Corp. of Japan, Raytheon Company of the USA, Sprint of the USA, STET of Italy, Pacific Iridium Telecom Company of Taiwan, Thai Satellite Com-munications Co. Ltd. of Thailand.

W trakcie prac projektowych okazało się, że można zmniejszyć liczbę satelitów w systemie do 66 (+6 zapasowych). Nie zmieniono jednak nazwy systemu, ponieważ łacińska nazwa pierwiastka o liczbie atomowej 66 - dysprosium kojarzy się ze "złym podejściem". Satelity są rozmieszczone równomiernie na sześciu orbitach o wysokości 780 km. Kąt inklinacji orbit wynosi $86{,}4^0$ (rys. 1). Satelita obiega Ziemię w ciągu 100 minut i 28 sekund. Okres widzialności satelity wynosi 11,1 minuty.

Satelity o trójosiowej stabilizacji (rys. 2) mają 13 m długości i 4 m szerokości. Ich masa wynosi 689 kg. Są one produkowane przez firmy Motorola i Lockheed-Martin. Pierwsze pięć satelitów umieszczono na orbitach 5 maja 1997 roku. Kolejne satelity umieszczano na orbitach w odstępach kilkutygodniowych za pomocą rakiet: McDonnel Douglas Delta II (5 satelitów za każdym startem), Kruniczev Proton (7 satelitów za każdym startem), Long March 2 C (2 satelity za każdym startem). 17 maja 1998 roku rakieta Delta wyniosła na orbity ostatnie pięć satelitów kompletując konstelację Irydium. Czas życia satelity ocenia się na 8 lat, mimo to dokonano już wymiany kilku satelitów.



Rys. 1. Konstelacja satelitów Irydium

$$t_o = \frac{L}{c} = \frac{10354 \text{ km}}{300000 \frac{\text{km}}{\text{s}}} = 0{,}0345 \text{ s} = 34{,}5 \text{ ms},$$

a dla satelity na niskiej orbicie (H = 780 km)

$$t_o = \frac{L}{c} = \frac{780 \text{ km}}{300000 \frac{\text{km}}{\text{s}}} = 0{,}0026 \text{ s} = 2{,}6 \text{ ms}.$$

Tłumienie sygnału o częstotliwości 2 GHz na trasie Ziemia (punkt podsatelitarny) - satelita wynosi 189,5 dB dla satelity geostacjonarnego (H = 35786 km), 178,8 dB dla satelity na średniej orbicie (H = 10354 km) i 156,3 dB dla satelity na niskiej orbicie (H = 780). Oznacza to, że przy ustalonych pozostałych warunkach, moce nadajników współpracujących z satelitą niskoorbitowym, średnio-orbitowym i geostacjonarnym mają się do siebie jak: 1 : 178 : 2090.

5. Zakresy częstotliwości

Zainteresowanie systemami telekomunikacyjnymi z satelitami na orbitach innych niż geostacjonarna spowodowało konieczność przydzielenia im odpowiednich zakresów częstotliwości. Przydziału dokonano podczas Światowej Administracyjnej Konferencji Radiowej WARC-92, która odbyła się w Hiszpanii w 1992 roku. Systemy satelitarne pracujące na niskich orbitach określa się mianem LEO. Obecnie pojęcie to rozszerzono na systemy pracujące na orbitach innych niż orbita geostacjonarna (NGSO - ang. *Non GeoStationary Orbit*).

Podczas konferencji WARC-92 systemy LEO podzielono na dwie klasy (tab. 1):

- systemy pracujące przy częstotliwościach poniżej 1 GHz, które nazwano małymi LEO (ang. *small LEO*),
- systemy pracujące przy częstotliwościach powyżej 1 GHz, które nazwano dużymi LEO (ang. *big LEO*).

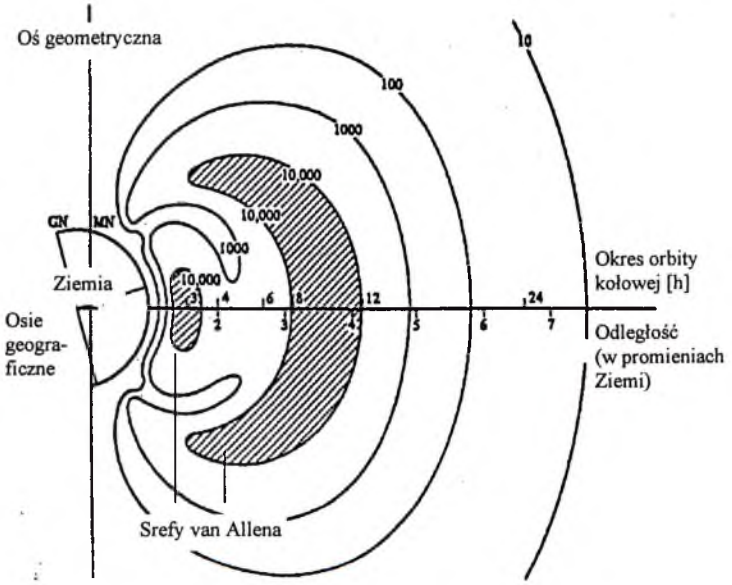
Tabela 1

Niskoorbitowe satelitarne systemy telekomunikacyjne

Typ	Małe LEO	Duże LEO	Szerokopasmowe LEO
Przykłady	Orbcomm VITA	Iridium Globalstar ICO	Teledesic SkyBridge
Współpraca z systemami naziemnymi	Systemy przywoławcze	Systemy komórkowe	Systemy światłowodowe
Zakres częstotliwości	<1GHz	1 - 3 GHz	20/30 GHz (Teledesic) 11/14 GH (SkyBridge)

Uregulowania obowiązujące po WARC-92 nie zadawalały żadnego z przyszłych operatorów systemów. Zarówno ITU, jak i organizacje lokalne: FCC (ang. *Federal Communications Commission*) w USA, CEPT (franc. *Conférence Européenne des Postes et*

Orbity systemów S-PCN wybiera się w taki sposób, aby leżały one poza strefami van Allena. Strefy te są obszarami bardzo silnego promieniowania jonizującego, które może powodować uszkodzenia elementów elektronicznych, zwłaszcza umieszczonych na lekkich, nieekranowanych satelitach. Przebywanie wewnątrz stref van Allena przez dłuższy czas powodowałoby skrócenie czasu życia satelity. Z tego powodu satelity na niskich orbitach są umieszczone poniżej pierwszej strefy van Allena, a satelity na orbitach średnich są umieszczane na wysokościach pomiędzy pierwszą i drugą strefą van Allena.



Rys. 2. Względny poziom promieniowania jonizującego w otoczeniu Ziemi (strefy van Allena)

W systemach satelitarnej telekomunikacji osobistej stosuje się następujące typy orbit.

LEO-i - (ang. *Low Earth Orbit - inclined*) - orbity niskie nachylone. Orbity o stałym kącie inklinacji $i \in (0, 90^0)$. Ponieważ wszystkie orbity konstelacji mają ten sam kąt inklinacji, konstelacje te nazywa się konstelacjami rozetowymi. Wymagana liczba satelitów potrzebnych do obsłużenia całego założonego obszaru zależy od wysokości orbity oraz minimalnego kąta elewacji dopuszczanego przez system. Ten typ orbit jest w stanie zapewnić łączność globalną. Orbity LEO-i mogą być kołowe i eliptyczne, jednak w systemach S-PCN stosuje się tylko orbity kołowe.

LEO-p - (ang. *Low Earth Orbit - polar*) - niskie orbity biegunowe. Kąt inklinacji tych orbit wynosi 90^0. Liczba wymaganych satelitów jest, podobnie jak dla orbit LEO-i, zależna od wysokości orbity oraz minimalnego kąta elewacji i, podobnie jak w przypadku orbit LEO-i, w systemach S-PCN stosuje się tylko orbity kołowe.

- poufnością.

Usługi personalne realizuje się przez wprowadzenie kart osobistych. Po umieszczeniu karty w terminalu następuje jego personalizacja. Umożliwia to uzyskanie połączenia (dostarczenie wiadomości) do konkretnego abonenta. System umożliwia abonentowi korzystanie z usług, do których ma dostęp i za które ponosi opłaty. W ten sposób z jednego terminala może korzystać wiele osób, przy czym na czas umieszczenia w nim karty identyfikacyjnej jest on terminalem osobistym danego abonenta.

Personalizacja usług dokonuje się w ramach obecnie eksploatowanych systemów przywoławczych, komórkowych i bezprzewodowych. Konieczna jest jednak integracją systemów w jeden system o zasięgu światowym. Stwarza to pewne problemy, stąd rozważa się przygotowanie systemów przyszłościowych realizujących taką koncepcję. Należy zwrócić uwagę, że abonent osobistego systemu komunikacyjnego powinien być zawsze osiągalny, niezależnie od tego, w zasięgu jakiej sieci może się znaleźć.

Problemy związane z przygotowaniem trzeciej generacji systemów telekomunikacyjnych są dyskutowane przez organizacje międzynarodowe zajmujące się normalizacją. Koncepcje takich systemów są przygotowywane przez ETSI[2)] oraz ITU[3)]. W ETSI specjalna grupa zajmująca się systemami ruchowymi przygotowuje projekt uniwersalnego systemu telekomunikacji ruchowej UMTS (ang. *Universal Mobile Telecommunication System*). Przyjęte kierunki rozwoju są zgodne z propozycjami ITU, który przygotowuje koncepcję przyszłościowego publicznego systemu ruchowej telekomunikacji lądowej FPLMTS (ang. *Future Public Land Mobile Telecommunications System*), ostatnio określanego jako system IMT-2000 (ang. *International Mobile Telecommunications - 2000*). Obie koncepcje zmierzają do przygotowania systemu komunikacji z abonentami przemieszczającymi się po całym świecie. W obu pojawia się idea wykorzystania systemów satelitarnych jako jednego z elementów takich sieci. Jednym z istotnych powodów, jakie zdecydowały o zainteresowaniu systemami satelitarnymi jest to, że dają one możliwość uzyskania kompatybilnego standardu światowego. Zadaniem takich systemów musi być uzupełnienie pokrycia uzyskiwanego dzięki zastosowaniu systemów lądowych (komórkowych i bezprzewodowych).

2. Satelitarne systemy komunikacji osobistej

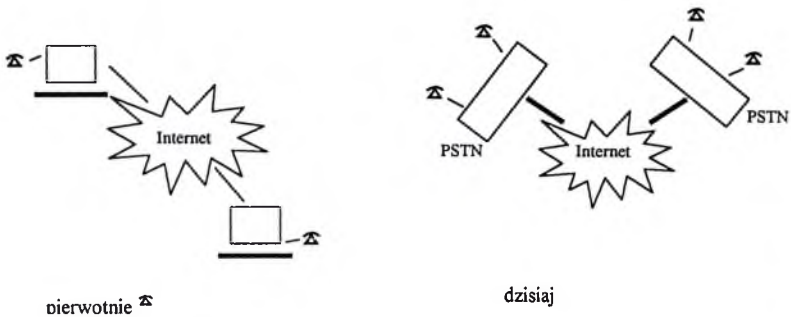
Od kilku lat promuje się różne koncepcje satelitarnych systemów komunikacji osobistej S-PCN (ang. *Satellite Personal Communication Network*). Pierwszy z tych systemów został uruchomiony w listopadzie ubiegłego roku. W systemach satelitarnych (rys. 1) wyróżnia się dwa człony: kosmiczny i naziemny. Człon kosmiczny tworzy pewna liczba satelitów (zależna od systemu), które mogą być umieszczone na różnorodnych orbitach. W opracowywanych obecnie systemach liczba satelitów zawiera się od kilku do kilkuset. Człon naziemny musi spełniać dwie funkcje. Pierwszą jest zapewnienie możliwości komunikowania się abonentów za pomocą terminali, które mogą być urządzeniami montowanymi w pojazdach, przenośnymi lub kieszonkowymi.

Człon naziemny spełnia także inne funkcje. Jedna z nich jest związana z funkcją telekomunikacyjną systemu. System ma stacje naziemne, nazywane adapterami międzysieciowymi (ang. *gateway*), które zapewniają połączenie abonentów z publiczną siecią telekomunikacyjną. W zależności od typu systemu takich stacji może być od kilku, aż do co najmniej jednej stacji w każdym kraju. Innym zadaniem członu naziemnego jest zarządzanie siecią, sterowanie oraz pomiary telemetryczne konstelacji satelitów. Do tego celu stosuje się

[2)] European Telecommunications Standards Institute - Europejski Instytut Standardów Telekomunikacyjnych
[3)] International Telecommunication Union - Międzynarodowy Związek Telekomunikacyjny

standardowej praktyki w sieciach TCP/IP, gdzie efektywność przesyłania danych osiągana jest głownie przez przesyłanie maksymalnie długich pakietów. Ponieważ powszechnie stosowane do transmisji TCP/IP techniki i urządzenia są projektowane z uwzględnieniem tej prawidłowości - w wypadku masowego obciążenia sieci transmisją głosu istnieje obawa przeciążenia urządzeń do transmisji TCP/IP (router-ów), generalnie nieprzystosowanych do konieczności obróbki dużych ilości krótkich pakietów.

Masowość stosowania techniki VoIP zaowocowała pewnymi trendami w rozwoju rynku oraz urządzeń. Można to zaobserwować porównując typowe zastosowania.



pierwotnie dzisiaj

Reasumując, technika VoIP - pomimo podobieństwa ze strony końcowego użytkownika - różni się znacznie od klasycznej telefonii. Podstawową cechą odróżniającą te dwie techniki jest fakt iż ta pierwsza jest specyficzną formą przesyłania danych (pakietów TCP/IP) pomiędzy określonymi punktami podczas w odróżnieniu od komutacji połączeń głosowych. Dlatego, w warstwie technicznej VoIP skupia się na różnorodnych technikach adaptujących medium transmisyjne (protokół TCP/IP) do potrzeb transmisji głosu, natomiast w warstwie użytkowej pozostawia klasycznej telefonii komutację połączeń wychodzących od użytkowników, skupiając się na transmisji zagregowanych kanałów TCP/IP służących do połączeń głosowych.

[D]. Deng, H.; Gong, L.; Lazar, A. 1995: ``Secure Data Transfer in Asynchronous Transfer Mode Networks". In: Proceedings of IEEE Globecom `95, Singapore, November 1995.
[E]. ATM Forum 1996: ``Integrated Local Management Interface (ILMI) Specification Version 4.0", ATM Forum 1996
[F]. ATM Forum 1996: ``Private Network-Network Interface Specification Version 1.0", ATM Forum 1996
[G]. Varadharajan, V; Shankaran, R.; Hitchens, M. 1997: ``Security Issues in Asynchronous Transfer Mode". Proceedings of Second Australasian Conference, ACISP`97, Sydney July 1997, Springer, 1997.
[H]. H. Dutton and P. Lenhard, "Asnchronous Transfer Mode (ATM) Technical Overview", 2nd Ed., Prentice Hall, 1995
[I]. T. M. Chen, and S. S. Liu, "ATM Switching Systems", Artech House, INC., 1995
[J]. ATM Forum Technical Committee, UNI Signalling 4.0 Security Addendum (btd-sig-sec-01.02, baseline text), September 1997
[K]. ATM Forum Technical Committee, ATM Security Specification Version 1.0 (str-sec-01.02 - Straw Ballot in April 98), February 1998
[L]. ATM Forum Technical Committee, UNI Signalling 4.0, July 1996
[M]. Laubach, M., Classical IP and ARP over ATM, RFC 1577, 1993
[N]. Armitage, G., Support for Multicast over UNI 3.0 /3.1 based ATM Networks, RFC 2022, 1996
[O]. Luciani, J., et al, NBMA Next Hop Resolution Protocol (NHRP), INTERNET DRAFT (draft-ietf-rolc-nhrp-15.txt), 1998
[P]. Armitage, G., et al, Security issues for the ATMARP protocol, INTERNET DRAFT (draft-armitage-ion-sec-arp-00.txt), 1997
[Q]. Armitage, G., Security issues for ION protocols, INTERNET DRAFT (draft-armitage-ion-security-01.txt), 1997

NHRP posiada te same defekty związane z uwierzytelnianiem w warstwach wyższych jakie zostały przedstawione w poprzednich przykładach. Dodatkowo istnieje tutaj poważny problem wynikający z zasady działania NHS (ang. Next Hop Server), który akceptuje połączenia z dowolnego adresu (należącego do tej samej lub innej podsieci). Dodatkowo w połączeniu z protokołami MARS można łatwo przeciążyć serwer NHS poprzez wielokrotnie generowane żądania. Standardy, które zostały zaproponowane przez ATM Forum takie jak MPOA (ang. Multi Protocol Over ATM) czy LANE (ang. LAN Emulation) posiadają dokładnie te same słabości jak przedstawione wcześniej rozwiązania. W obydwu przypadkach serwery akceptują wywołania klienta, przyjmują informację, którą podaje klient i obsługują go zgodnie z zapytaniem w wywołaniu usługi (np. podają nazwy i adresy innych klientów). W LANE wersja 2 wprowadzono podstawowy mechanizm kontroli dostępu (oparty o adresy NSAP strony wywołującej). Mechanizm ten jest stosowany na serwerach konfiguracji LANE. W protokole MPOA nie przewidziano jakichkolwiek mechanizmów bezpieczeństwa.

Zastosowanie w sieciach techniki ATM wymaga rozpatrzenia zagadnień związanych z ich bezpieczeństwem. Sieci ATM są oparte na koncepcji wirtualnych połączeń komutowanych i komórek o ustalonych długościach, będących przeciwieństwem do „odziedziczonych sieci" (ang. „legacy networks") pracujących w trybie bezpołączeniowych i rozsiewczym (ang. broadcasting) opartych o wspólne medium. Technika ATM związana jest z rozwojem protokołów takich jak ILMI (ang. 'Integrated Local Management Interface') [e] czy P-NNI (ang. 'Private Network-Network Interface') [f]. Specyfikacje tych protokołów nie zostały jeszcze poddane dokładnej analizie bezpieczeństwa.
Aby wykorzystać protokół IP w sieciach ATM należy wprowadzić dodatkowe usługi, takie jak np. serwer ATMARP. Powoduje to powstanie nowych niebezpieczeństw, które muszą być sprawdzone zanim można będzie użyć „Classical IP over ATM" w warunkach zagrożenia bezpieczeństwa transmisji. Zwykle w sieciach używa się kryptografii, aby potwierdzić autentyczność, zapewnić integralność i poufność. Integracja mechanizmów kryptografii w sieciach ATM jest obecnie przedmiotem badań [d],[g] ale żaden z tych mechanizmów nie został unormowany.
W opracowaniu „ Securing Classical IP over ATM Networks" [c] przedstawiono szereg szczegółowych zagrożeń związanych z transmisją IP przez ATM. Zaproponowano jednocześnie wykorzystanie możliwości filtracji ruchu poprzez listy dostępu w warstwie ATM jako ochronę przed zagrożeniami związanymi z obejściem zabezpieczeń w warstwie IP.
Listę typowych zagrożeń można przedstawić następująco:

- Oszukiwanie protokołu IP dla połączeń ATM z wykorzystaniem słabości protokołu ATMARP;
- „Blokowanie usługi" przez zajęcie adresu IP na serwerze ATMARP;
- Ataki typu „człowiek wewnątrz" (ang. Man in the Middle) - możliwość zarejestrowania się w sieci wirtualnej pozwala na atak nawet z odległych sieci;
- „Blokowanie usługi" transmisji IP (transmisja UBR) przez zajęcie pasma usługami typu CBR;
- „Blokowanie usługi" przez zajęcie wszystkich możliwych połączeń wirtualnych;
- Ataki wykorzystujące protokół ILMI - pozwalają na określenie adresów obowiązujących w obrębie sieci ATM;
- Ataki na przełączniki sieciowe wykorzystujące słabość protokołu P-NNI.

6. Wnioski

Użycie protokołu IP w sieciach ATM wiąże się z kilku interesującymi problemami związanymi z bezpieczeństwem. Ryzyko ataków typu „oszukanie" protokołu IP jest bardzo

podstawie etykiety jest zdefiniowany w specyfikacji, jednak dopuszczalna jest implementacja innych mechanizmów.

- **Usługi bezpieczeństwa w płaszczyźnie kontroli**

W płaszczyźnie kontroli zdefiniowane są jedynie funkcje uwierzytelniania i integralności danych. Poufność i inne mechanizmy bezpieczeństwa będą zawarte w następnych wersjach specyfikacji. Usługa uwierzytelnienie i integralność danych jest realizowana dla każdego z osobna elementu sygnalizacji, przez nałożenie usług uwierzytelniania i integralności z płaszczyzny użytkownika na sygnalizację łączącą w warstwie adaptacyjnej dwa podmioty sygnalizacji.

Poza wymienionymi usługami podstawowy zestaw usług jest uzupełniony przez następujące specyfikacje:

- **Bezpieczna wymiana danych i negocjacja opcji bezpieczeństwa**

Dwa mechanizmy dotyczące przesyłania informacji związanych z bezpieczeństwem są opisane w specyfikacji: wymiana komunikatów w ramach sygnalizacji UNI 4.0 (zobacz [l]) i wewnątrzpasmowa wymiana komunikatów (oznacza to, że komunikaty są wymieniane wewnątrz połączenia wirtualnego użytkownika po zestawieniu połączenia z wykorzystaniem normalnej sygnalizacji). Wybór mechanizmu przesyłania jest zależny od „agenta bezpieczeństwa" (ang. Security Agents), co wynika z rodzaju usługi bezpieczeństwa. Agent jest lokowany (zgodnie z terminologią bezpieczeństwa) jako logiczny element w płaszczyźnie użytkownika - w przypadku użycia sygnalizacji- lub na zewnątrz płaszczyzny kontroli w przypadku użycia negocjacji wewnątrz pasma. Usługi bezpieczeństwa w płaszczyźnie kontroli są dostępne tylko w sygnalizacji UNI 4.0. Bezpieczna wymiana komunikatów może być wykonana w postaci dwu lub trójstronnych protokołów. Negocjacja parametrów usług bezpieczeństwa jest możliwa tylko poprzez trójstronną wymianę. **W sygnalizacji UNI 4.0 zdefiniowano protokoły do wymiany dwustronnej.** Każdy algorytm jest związany z „punktem kodowym" (ang. codepoint) używanym do jego identyfikacji w procesie negocjacji opcji bezpieczeństwa. Wszystkie opisane mechanizmy i protokoły używają elementów informacyjnych usług bezpieczeństwa SSIE (ang. Security Services Information Element), które są opisane w omawianym dokumencie. Owe SSIE przenoszą wszystkie parametry związane z bezpieczeństwem. Są przesyłane w komunikatach sygnalizacji związanych z konfiguracją (ang. SETUP) i generacją połączenia (ang. CONNECT) dla połączeń typu punkt - punkt. W połączeniach punkt -wiele punktów wykorzystywane są komunikaty dołączenia do grupy (ang. ADD PARTY) i potwierdzenia dołączenia do grupy (ang. ADD PARTY ACKNOWLEDGE). Dla negocjacji wewnątrzpasmowej zdefiniowany jest protokół trójstronny z nowo utworzonym komunikatem związanym z potwierdzeniem połączenia (ang. CONNECT ACKNOWLEDGE).

- **Wymiana kluczy**

Jest realizowana przy użyciu algorytmów symetrycznych i asymetrycznych w celu szyfrowania i uwierzytelniania.

- **Aktualizacja klucza sesji**

Jest realizowana przez protokół, który wykorzystuje komórki OAM (ang. Operations, Administration and Management) przesyłane razem z danymi użytkownika do wymiany nowego klucza sesji z drugą stroną oraz do sygnalizacji momentu użycia nowego klucza. Używane są strumienie komórek typu F4 i F5 OAM odpowiednio dla wirtualnych łączy i ścieżek. Proces aktualizacji i zmiany kluczy jest realizowany niezależnie dla każdego kierunku.

- **Certyfikacja**

Tabela B. Wyszczególnienie ogólnych zagrożeń oraz wymagań funkcjonalnych w zakresie zabezpieczeń.

Podstawowe zagrożenia	Zasadnicze wymagania funkcjonalne bezpieczeństwa								
	Weryfikacja tożsamości	Kontrola dostępu oraz upoważnienie	Ochrona poufności	Ochrona integralności	Bezwzględna odpowiedzialność	Zapis zdarzeń	Raportowanie o alarmach	Audyt	Przywracanie bezpieczeństwa /zarządzanie bezpieczeństwem
Maskarada	tak					tak	tak	tak	tak
Podsłuch		tak	tak						tak
Nieupoważniony dostęp	tak	tak	tak			tak	tak	tak	tak
Utrata lub uszkodzenie przekazywanych informacji				tak			tak		tak
Zaprzeczenie					tak	tak		tak	tak
Fałszerstwo					tak	tak		tak	tak
Blokowanie usługi		tak				tak	tak	tak	tak

Tabela C. Wskazanie wymagań funkcjonalnych w zakresie bezpieczeństwa i usług bezpieczeństwa

Wymagania funkcjonalne bezpieczeństwa	Usługa bezpieczeństwa
Weryfikacja tożsamości	*Uwierzytelnianie użytkownika* *Uwierzytelnianie równoprawnych podmiotów* *Uwierzytelnienie pochodzenia danych*
Kontrola dostępu i upoważnienie	*Kontrola dostępu*
Ochrona poufności — Dane przechowywane	*Kontrola dostępu*
Ochrona poufności — Dane przesyłane	*Poufność*
Zabezpieczenie nienaruszalności danych — Dane przechowywane	*Kontrola dostępu*
Zabezpieczenie nienaruszalności danych — Dane przesyłane	*Integralność*
Bezwzględna odpowiedzialność	*Niezaprzeczalność*
Rejestracja zdarzeń	*Alarm bezpieczeństwa, stała kontrola i odzyskiwanie*
Raportowanie o alarmach	*Alarm bezpieczeństwa, stała kontrola i odzyskiwanie*
Audyt	*Alarm bezpieczeństwa, stała kontrola i odzyskiwanie*
Przywracanie bezpieczeństwa /Zarządzanie bezpieczeństwa	

„ATM Security Framework 1.0" definiuje wyłącznie podstawową listę usług bezpieczeństwa, inne możliwe usługi (np. „wykrywanie blokady usług") mogą wynikać z poniższej listy.

interpretację wymagań funkcjonalnych w zależności od płaszczyzny działania i usług wspierających. Pełna interpretacja będzie zawarta w następnych wersjach dokumentu.

W „ATM Security Framework 1.0" zdefiniowano najważniejsze elementy bezpieczeństwa:

- **Poufność** - poufność gromadzonych i przenoszonych informacji,
- **Integralność danych** - ochrona gromadzonych i przenoszonych informacji,
- **Odpowiedzialność** - odpowiedzialność za wszystkie wywołania usług sieci ATM oraz za cały zakres działania systemu zarządzania siecią ATM; każdy podmiot powinien być odpowiedzialny za każde wszczęte działanie, oraz
- **Dostępność** - wszystkie upoważnione podmioty powinny mieć zapewniony poprawny dostęp do zasobów udostępnianych przez ATM.

W analizie zagrożeń sieci ATM „ATM Security Framework 1.0" proponuje uwzględnić następujące zamierzone zagrożenia:

- **Maskarada („oszustwo")** - udawanie przez kogoś, że jest kimś innym.
- **Podsłuchiwanie** - złamanie poufności przez śledzenie połączeń
- **Nieupoważniony dostęp** - podmiot zdobywa dostęp do danych z naruszeniem polityki bezpieczeństwa.
- **Utrata lub uszkodzenie informacji** - integralność przekazywanych danych jest naruszona przez usunięcie, wstawienie, modyfikację, zmianę kolejności, powtarzanie lub nieupoważnione opóźnianie.
- **Zaprzeczenie** - podmiot uczestniczący w wymianie danych zaprzecza temu zdarzeniu.
- **Fałszerstwo** - podmiot fabrykuje informacje i zgłasza pretensje, że informacje otrzymane zostały od innego podmiotu lub wysłane do innego podmiotu.
- **Blokowanie usług** - pojawia się wtedy, gdy podmiot realizuje błędnie swoje funkcje lub uniemożliwia innym jednostkom pełnienie ich funkcji. To zagrożenie może obejmować odmowę dostępu do usług ATM oraz blokadę transmisji z powodu przeciążenia sieci ATM lub jej części składowych.

W tabeli (tabela a) przedstawiono relacje pomiędzy zagrożeniami i elementami bezpieczeństwa. Słowo „tak" w odpowiedniej pozycji tabeli oznacza, że istnieje zdefiniowane zagrożenie mogące naruszyć odpowiedni element bezpieczeństwa.

Tabela A. Wyszczególnienie elementów i zagrożeń

	Podstawowe zagrożenia						
Główne elementy bezpieczeństwa	Maska-rada	Podsłuch	Nieupo-ważniony dostęp	Utrata lub uszkodzenie przekazywa-nych informacji	Zaprze-czenie	Fałszer-stwo	Blokowa-nie usług
Poufność	tak	tak	tak				
Integralność danych	tak		tak	tak		tak	
Odpowiedzialność	tak		tak		tak	tak	
Dostępność	tak		tak	tak			tak

Według „ATM Security Framework 1.0" jako zasadę można przyjąć, **że otwarte środowiska sieciowe, w zakresie bezpieczeństwa wymagają mechanizmów silniejszych niż zamknięte środowiska sieciowe.** W zamkniętych środowiskach, wystarczający poziom bezpieczeństwa można otrzymać środkami organizacyjnymi.

BEZPIECZEŃSTWO W SIECIACH ATM

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

Od kilku lat w sieciach teleinformatycznych coraz częściej stosowana jest technika ATM (ang. Asynchronous Transfer Mode). Protokół ATM znajdziemy w sieciach teleinformatycznych publicznych operatorów telekomunikacyjnych, banków, agent rządowych itp. czyli wszędzie tam, gdzie wymagany jest wysoki poziom bezpieczeństwa transmitowanych danych. Wraz z upowszechnieniem ATM-u istotne jest utrzymanie odpowiedniego poziomu bezpieczeństwa. Niniejszy artykuł przedstawia aktualny stan unormowań w zakresie bezpieczeństwa w sieciach ATM. Definiuje podstawowe zagrożenia. Na przykładzie rozwiązania „IP over ATM" zilustrowane są zagrożenia jakie niesie stosowanie protokołu IP w sieciach ATM [a].

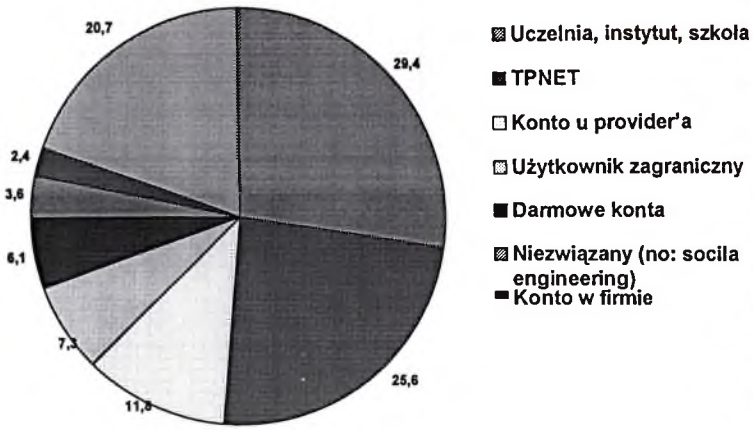
2. Bezpieczna transmisja w sieci ATM

ATM (ang. Asynchronous Transfer Mode) jest standardem asynchronicznego trybu transmisji w którym transmisja jest poprzedzona zestawieniem połączenia. Przed rozpoczęciem transmisji pomiędzy abonentami zestawiany jest kanał wirtualny w sposób statyczny lub dynamiczny. W ATM-ie host jest dołączony do sieci poprzez przełączniki (ang. switches). Mimo że abonenci mogą przesyłać dane o różnej długości, wewnątrz sieci ATM dane przesyłane są w porcjach o stałej długości nazywanych komórkami. Komórka posiada nagłówek o długości 5 oktetów i obszar użytkowy o długości 48 oktetów. Przełączanie komórek odbywa się na podstawie informacji zawartej w nagłówku po trasie ustalonej w procesie zestawiania połączenia. To rozwiązanie pozwala na bardzo szybkie przenoszenie komórki przez przełączniki. W sieci ATM możliwa jest transmisja z zachowaniem gwarantowanej jakości usług QoS (ang. Quality of Service).

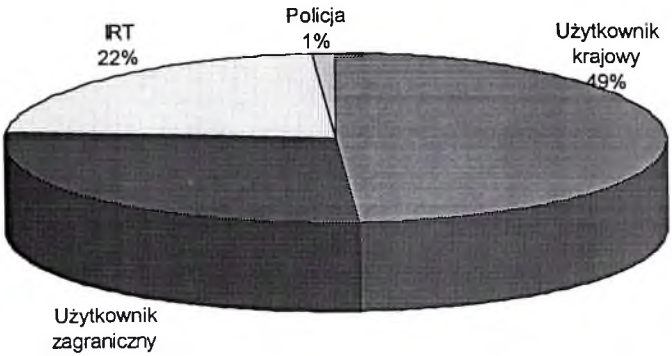
Sieć ATM może być zbudowana z wykorzystaniem pewnego podzbioru funkcjonalnego usług ATM - np.: CBR i PVC (stała prędkość bitowa i trwałe połączenie wirtualne), brak elementów kontroli jakości (QoS), brak sygnalizacji - lub z pełną implementacją funkcji zawartych w tej technice. W przypadku statycznie zestawianych połączeń (PVC) bez użycia sygnalizacji na interfejsie użytkownika zagrożenia są zbliżone do spotykanych w liniach dzierżawionych. W przypadku zastosowania sygnalizacji koniecznej do realizacji zaawansowanych usług w sieci ATM problem bezpieczeństwa staje się bardzo ważny. Zastosowanie odpowiednich mechanizmów bezpieczeństwa staje się koniecznością.

Początkowo ATM był dedykowany dla szerokopasmowych sieci z integracją usług (B-ISDN ang. Broadband Integrated Services Digital Network) w celu umożliwienia transmisji informacji o różnych formach (głos, wizja, dane itp.) poprzez sieć telekomunikacyjną. Jednak stosowanie ATM-u nie jest ograniczone jedynie do B-ISDN. ATM jest najczęściej wykorzystywany w celu uproszczenia infrastruktury sieciowej z wieloma połączeniami sieciowymi. Szczegóły dotyczące techniki ATM można znaleźć w wielu opracowaniach (np.[h],[i]). Najważniejszą organizacją zajmującą się problematyką sieci ATM jest obecnie ATM Forum zrzeszające większość producentów urządzeń, oprogramowania oraz operatorów sieci telekomunikacyjnych. Organizacjami dostarczającymi standardów dla telekomunikacji są

Wykres nr 3. Procentowy rozkład źródła ataków, 1998.



Wykres nr 4. Procentowy rozkład źródła zgłoszenia ataków, 1998.



pojedynczych komputerów. Ogólnodostępność oprogramowania służącego do skanowania, często reklamowanego pod hasłem „sprawdź bezpieczeństwo swojego komputera" niewątpliwie poważnie przyczyniło się do popularności tego typu ataku. Również niezwykle łatwy atak na serwer z wykorzystaniem oprogramowania typu *common gateway interface* (CGI) sprawiło, że wśród zgłoszonych incydentów wiele było tych, które wskazywały na chęć przejęcia istotnych informacji przez intruza w ten właśnie sposób.

Źródło ataków

Tak jak było już wspomniane wcześniej prym w tej kategorii wiedzie środowisko akademickie. Nie jest to zjawiskiem nowym w odróżnieniu do tego co dotyczy sieci TPNET. „Darmowy" dostęp do sieci stał się w zeszłym roku doskonałym sposobem na ukrycie swojej tożsamości, przynajmniej zdaniem intruzów. Aktywna działalność CERT NASK, poparta zdecydowanym głosem środowiska internautów, niewątpliwie przyczyniła się do ograniczenia tego zjawiska, czego efekty są już widoczne. W strukturach TP S.A. powstał dedykowany zespół odpowiedzialny za tego typu przypadki, uruchomiono procedury organizacyjne i techniczne, które prowadzą do zdecydowanego ograniczenia zjawiska. Także współpraca z firmami udostępniającymi na swych serwerach darmowe konta dla internautów niewątpliwie przyniosła efekty, które widać w niewielkiej ilości incydentów powiązanych właśnie z darmowymi kontami.

Efekt ataków

Wśród zarejestrowanych ataków więcej jest tych, które wg zgłaszających zostały skutecznie odparte, niż tych które skończyły się przejęciem przez intruza praw administratora systemu. Potwierdza to fakt, że tylko nieliczne incydenty zgłaszane są do oficjalnych statystyk, i rzadko, kto chce się przyznawać do tego, że jego sieć została skutecznie zaatakowana. Jest to zjawisko ogólnoświatowe.

Niestety największy procent odnosi się do sytuacji, w której poszkodowany nie jest w stanie ustalić poniesionych strat i często nie ma na to już szans gdyż system, który musi działać w trybie natychmiastowymi jest reinstalowany.

Cel ataku i źródło zgłoszenia

Większość, blisko 80%, zgłaszanych do CERT NASK incydentów pochodzi od niezależnych użytkowników sieci, głównie przedstawicieli firm i instytucji. Pozostałe, niewiele ponad 20% zgłoszeń pochodzi od instytucji, które w swojej działalności zajmują się walką z przestępczością komputerową, czyli innych zespołów reagujących (IRT) lub Policji, ze zdecydowanym wskazaniem na te pierwsze.

Wśród poszkodowanych dokładnie 50 % jest użytkowników zagranicznych i 50 % użytkowników polskiej sieci Internet. Na negatywne oddziaływanie intruzów bardziej uczuleni wydają się być użytkownicy zagraniczni. Przyczyną takiego stanu rzeczy jest z jednej strony większa wrażliwość użytkownika zagranicznego na nieuprawnioną działalność intruzów, zaś z drugiej dotychczasowe przekonanie o bezkaralności i często anonimowości intruza jakie panuje wśród polskich internautów. Na szczęście opinia ta się zmienia, na co wpływ ma bardziej szczegółowa kontrola dostępu (funkcja rozliczalności) wśród polskich provider'ów (w szczególności chodzi tu o TP S.A.) oraz wprowadzenie nowego kodeksu karnego, który w większym stopniu daje szansę dochodzenia krzywd na drodze prawnej.

Z pozytywnych zmian zaobserwowanych w ramach naszej działalności jest powstawanie w ramach struktur firmowych zespołów lub osób ospowiedzialnych za sprawy bezpieczeństwa teleinformatycznego. Wskazuje to poniekąd podstawową rolę dla zespołów reagujących, takich jak CERT NASK, wydaje się nim być koordynacja w wymianie iinformacji między zainteresowanymi, ze szcególnym uwzględnieniem spraw międzynarodowych.

- *Oprogramowanie agenta (Keon Agent)*

Aplikacje na serwerach objętych systemem bezpiecznego dostępu muszą zostać wyposażone w pewien sprzęg pozwalający na komunikację z użytkownikiem posługującym się oprogramowaniem Keon Desktop. Możliwość praktycznego wdrożenia systemu tkwi w ilości standardowych modułów pozwalających na komunikację z wieloma systemami i aplikacjami różnych producentów (np. bazy danych Oracle,Informix, Sybase, SAP, protokoły HTTP, telnet, systemy operacyjne – np. rozmaite odmiany UNIX-a, NT). Keon Agent spełnia te warunki a ponadto zapewnia też mocne uwierzytelnienie (OTP, two factor authentication itp.)

- *Serwer Bezpieczeństwa (Keon Security Server)*

Oprogramowanie Keon Security Server zapewnia centralną kontrolę nad procesami dostępu do zasobów w sieci. Serwer obsługuje zarządzanie strukturą klucza publicznego (ang. PKI – Public Key Infrastructure) w standardzie X.509 służącą do wykorzystania certyfikatów kluczy publicznych użytkowników jako informacji uwierzytelniającej (ang. credentials) w procesie identyfikowania i uwierzytelniania użytkowników a także w czasie szyfrowania sesji dostępu do zdalnych systemów i aplikacji.

Certyfikaty użytkowników mogą być przechowywane na dyskietkach bądź dyskach w postaci zaszyfrowanych plików bądź na kartach inteligentnych. Dostęp do kluczy prywatnych użytkowników jest chroniony hasłem dynamicznym systemu OTP sprzężonym z Serwerem Bezpieczeństwa.

Usługi katalogowe (LDAP) sprzężone z PKI zapewniają ułatwioną dystrybucję i zarządzanie certyfikatami. (Użytkownik ma możliwość łatwego uzyskania swych „credentials" przy pomocy swego komputera dostepowego do sieci -np. desktop PC- a administrator możliwość np. sprawnego centralnego unieważniania certyfikatów użytkowników.

Wbudowany w Keon Security Server serwer certyfikatów ma możliwość współpracowania z dowolnymi certyfikatami X.509 wydanymi przez inne Urzędy ds. Certyfikatów (ang. Certification Authority).

Dodatkowo prawa dostępu dla użytkowników / grup użytkowników są kontrolowane z jednego miejsca (konsola Serwera Bezpieczeństwa) podobnie jak poziom bezpieczeństwa komputerów w całej sieci. Serwer Bezpieczeństwa posiada swą replikę.

W środowisku Keon jest więc możliwe zapewnienie bezpiecznego dostępu do aplikacji np. SAP, Oracle, Sybase, PeopleSoft oraz wykorzystywanie wszelkich aplikacji opartych na idei otwartego PKI jak np. poczta elektroniczna (SMIME), aplikacji opartych na WWW (SSL) czy wirtualnych sieci prywatnych VPN opartych o standard IPSec. W tym celu można wykorzystywać certyfikaty generowane przez system Keon lub dowolne certyfikaty wydawane na świecie (np. VeriSign).

czy dyskietkach ich ochrona realizowana poprzez statyczne hasło z reguły jest nieskuteczne.

Ta forma przechowywania kluczy jest też dość niewygodna. Coraz częściej więc stosuje się do tego celu karty inteligentne, w których chipie zapisuje się klucze i certyfikaty (dostęp do których jest chroniony poprzez PIN przesyłany z klawiatury do czytnika) lub karty inteligentne kryptograficzne, w których klucz prywatny w ogóle nie opuszcza karty zapewniając tym samym maksymalne bezpieczeństwo.

Karty inteligentne są bardzo wygodne w użyciu pod warunkiem, że komputer „desktop" jest wyposażony w odpowiedni czytnik.

Odmianą fizycznej karty inteligentnej jest tzw. wirtualna karta inteligentna, która jest niczym innym jak zestawem kluczy i certyfikatów użytkownika przechowywanych na serwerze sieciowym. W takim przypadku dostęp do klucza prywatnego nie może być chroniony za pomocą statycznego hasła, które można podsłuchać w sieci. W takim przypadku stosuje się więc systemy haseł dynamicznych, jednorazowych a więc systemy OTP. Użytkownik jest wyposażony w token sprzętowy, który nie wymaga czytnika a więc można zeń korzystać w każdych warunkach. Token sprzętowy generuje hasło jednorazowe, które umożliwia dostęp do klucza prywatnego i dalsze jego stosowanie – podobnie jak w każdym innym przypadku.

Systemy OTP

W każdym systemie wielodostępnym istnieje problem zapewnienia skutecznej identyfikacji i weryfikacji użytkownika na etapie zezwalania dostępu do określonych zasobów (np.logowanie do sieci, logowanie do systemu operacyjnego komputera, dostęp do aplikacji, dostęp do plików i katalogów np. WWW).

Sieci lokalne, korporacyjne, intranety, extranety, VPN-y i inne typy sieci obfitują w systemy o różnym przeznaczeniu gdzie niezwykle istotne jest rozgraniczenie praw dostępu (np. blokowanie dostępu z zewnątrz do serwerów intranetowych, ograniczenie dostępu do niektórych aplikacji.

Tradycyjne systemy haseł nie są już obecnie traktowane jako wystarczające ze względu na powszechnie występujące przypadki podsłuchiwania, podpatrywania, wykradania, łamania haseł. Coraz częściej wykorzystywane są metody typu OTP (One Time Password), w których w sposób programowy lub sprzętowy (użytkownik zostaje wyposażony w kartę/token generujący hasła ważne tylko jeden raz) realizowana jest zasada jednorazowego hasła dostępu: hasło raz użyte jest „zużyte". Co pod względem bezpieczeństwa jest do zaakceptowania to ze względów użytkowych może posiadać pewne wady. W tym wypadku użytkownik, który miałby mieć precyzyjnie określone i egzekwowane prawa dostępu do wielu systemów, aplikacji w środowisku pracy w sieci musiałby za każdym razem , kiedy stara się uzyskać dostęp do określonego zasobu - podawać hasło. Jeśli system haseł dostępu jest tradycyjny – użytkownika zmusza się do pamiętania kilku, kilkunastu czy kilkudziesięciu różnych haseł - co jest trudne i zazwyczaj powoduje zagrożenia bezpieczeństwa (jedno hasło do wszystkich zasobów, hasła zbyt proste, hasła zapisywane w widocznych miejscach). Jeśli system haseł dostępu jest dynamiczny (OTP) użytkownik haseł pamiętać nie musi - jednak częste wprowadzanie haseł w czasie pracy również może być uciążliwe.

Automatyczna kontrola okresu ważności kluczy
Ręczne zarządzanie procesem kontroli okresu ważności kluczy jest z pewnością przyczyną małej skalowalności rozwiązania. Dlatego zautomatyzowanie tego procesu wydaje się być kluczowym problemem w realizowaniu funkcji kontroli okresu ważności certyfiaktu.

Standardy PKI

Zastosowanie standardów w strukturze PKI pozwala na współprace pomiędzy wieloma strukturami PKI i na korzystanie z PKI w wielu aplikacjach. Standardy PKI można podzielić na dwie grupy: na standardy poziomu użytkownika i na standardy dla samego PKI. Standardy PKI są konieczne dla:

- Procedury rejestracji
- Formatów certyfikatów
- Formatów CRL
- Formatów dla informacji o rejestracji certyfikatu (wystąpienie o certyfikat i wydanie certyfikatu)
- Formatów podpisów cyfrowych
- Protokołów typu *challenge/response*

Próbę zestandaryzowania funkcji PKI podjęła grupa robocza o nazwie IETF (Internet Engineering Task Force), znana również jako grupa PKIX (PKI dla certyfikatów X.509)

Standard PKIX

Cztery podstawowe składniki modelu PKIX to:

- Użytkownik
- CA
- RA
- „składnica" certyfikatów

Standardy składników PKIX
Specyfikacja PKIX oparta jest na dwóch innych standardach: X.509 Międzynarodowego Związku Telekomunikacji (International Telecommunication Union - ITU) i Standardów Kryptografii Klucza Publicznego (Public Key Cryptography Standards – PKCS) autorstwa RSA Data Security. Istnieją trzy najważniejsze standardy PKCS:
PKCS#7 – „Cryptographic Message Syntax Standard"
PKCS#10 – „Certyficate Request Syntax Standard"
PKCS#12 – „Personal Information Exchange Syntax Standard"

Standardy bezpieczeństwa współpracujące z PKI
Większość najważniejszych standardów w dziedzinie bezpieczeństwa teleinformatycznego jest tak zaprojektowanych aby umożliwić współpracę z PKI. Wśród tych standardów są takie jak:

SSL – Secure Socket Layer
TLS – Transport Layer Security
S/MIME – Secure Multipurpose Internet Mail Ex-tensions
SET – Secure Electronic Transactions
IPSEC – IP Security

Funkcje PKI

Podstawowymi funkcjami PKI jest wydawanie certyfikatów, odwoływanie ich, tworzenie i publikowanie CRLs, przechowywanie i odzyskiwanie certyfikatów, oraz zarządzanie okresem ważności certyfikatu.

Funkcje jakie ma do spełnienia PKI zawarte są poniżej.

Wydawanie certyfikatów
CA wydaje (podpisuje) certyfikat. Poprzedzone jest to procesem identyfikacji zgłaszającego się o wydanie takiego certyfikatu. Pozytywne rozpatrzenie zgłoszenia kończy się wydaniem certyfikatu wraz z datą jego rozpatrywania.

Odwoływanie certyfikatów
Certyfikat może stać się nieważny przed oficjalną datą jego wygaśnięcia. Przyczyną tego może być na przykład zmiana nazwiska pracownika lub utrata kontroli na prywatnością klucza prywatnego. W takich przypadkach CA odwołuje certyfikat poprzez umieszczenie jego numeru seryjnego na następnej publikowanej CRL.

Tabela 1. Funkcje Infrastruktury Klucza Publicznego (PKI)

FUNKCJA	OPIS	IMPLEMANTACJA
Rejestracja użytkowników	Zbieranie informacji o użytkownikach i ich weryfikacja	Funkcja CA, lub oddzielnego RA
Wydawanie certyfikatów	Tworzenie certyfikatów w odpowiedzi na zgłoszenie użytkownika lub administratora	Funkcja CA
Odwoływanie certyfikatów	Tworzenie i publikowanie CRLs	Oprogramowanie administracyjne CA
Przechowywanie i uaktualnianie certyfikatów i CRLs	Udostępnianie autoryzowanym użytkownikom dogodnego dostępu do bazy certyfikatów	Miejsce przechowywania certyfikatów i CRLs jest bezpieczne, dostępne przy pomocy protokołu LDAP
Potwierdzanie certyfikatów w oparciu o ustaloną politykę	Badanie certyfikatu w oparciu o wszystkie napotkane elementy certyfikacji i potwierdzenie lub zaprzeczenie ważności certyfikatu	Funkcja CA
Oznaczanie czasu	Oznaczanie każdego certyfikatu datą ważności	Funkcja CA lub dedykowanego do tego zadania Serwera Czasu (Time Server – TS)
Zarządzanie okresem ważności certyfikatu	Uaktualnianie, archiwizacja i przechowywanie kluczy	Zautomatyzowane poprzez oprogramowanie lub przeprowadzane ręcznie

Przechowywanie i uaktualnianie certyfikatów i CRLs
Typowym sposobem realizacji tej funkcji jest umożliwienie, w oparciu o protokół LDAP, dostępu do certyfikatów i CRLs. Inne opcje realizacji tej funkcji oparte mogą być o protokoły X.500, HTTP, FTP i pocztę elektroniczną.

IFRASTRUKTURA KLUCZA PUBLICZNEGO (PKI) NA POTRZEBY BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH

Krzysztof Silicki, Mirosław Maj

Wstęp

Zmiany jakie nastają w dziedzinie biznesu elektronicznego wymuszają zmiany jakie są konieczne w w zapewnieniu bezpieczeństwa teleinformatycznego firm korzystających ze struktury teleinformatycznej.

Na przykład, poczta elektroniczna nie jest już tylko nośnikiem prostych informacji lecz również stała się medium dla przekazywania informacji finansowych. Witryna internetowa nie jest już tylko formą prezentacji firmy, ale również sposobem na prowadzenie dystrybucji produktów i realizacji handlu elektronicznego (*e-commerce*). Prywatne sieci wirtualne (VPN – Virtual Private Network) pozwalają na ekspansję sieci korporacyjnych w oparciu sieć Internet.

Bezpieczna poczta elektroniczna, dostęp do witryny internetowej, handel elektroniczny, VPN-y i ekstranety wymagają silnych narzędzi bezpieczeństwa takich jak poufność, uwierzytelnienie, kontrola dostępu, integralność danych i rozliczalności. Certyfikaty cyfrowe i szyfrowanie w oparciu o mechanizm klucza publicznego są niewątpliwie kluczowymi elementami w tej dziedzinie. Ocenia się, że wiele wielkich organizacji wykorzysta kryptografię klucza publicznego i certyfikaty w swoich firmach w przeciągu kilku następnych lat.

Kryptografia klucza publicznego wymaga Infrastruktury Klucza Publicznego (PKI) dla zarządzania cyfrowymi certyfikatami i kluczami szyfrującymi dla osób, programów i systemów.

Co to jest kryptografia klucza publicznego ?

Aplikacje realizujące szyfrowanie w oparciu o klucz publiczny wykonują:

- Szyfrowanie danych w celu zapewnienia ich poufności
- Podpisy cyfrowe dla zapewnienia niezaprzeczalności i weryfikacji integralności danych
- Certyfikaty dla uwierzytelnienia osób, aplikacji i serwisów oraz dla zapewnienia kontroli dostępu (uwierzytelnienia)

Wyróżnia się dwa podstawowe rodzaje kryptografii: *kryptografia symetryczna i kryptografia klucza publicznego.*

W *kryptografii symetrycznej*, zarówno nadawca jak i odbiorca używają tego samego klucza do szyfrowania i odszyfrowania informacji. Powoduje to sytuację, w której wielu użytkowników zmuszonych jest do posiadania tego samego klucza co niewątpliwie osłabia poziom bezpieczeństwa rozwiązania.

Kryptografia klucza publicznego, w odróżnieniu od *kryptografii symetrycznej*, wykorzystuje parę kluczy:

większości jednostek budżetowych, optymalne jest rozlicznie ryczałtowe, według planu kosztów, w drugim, trzecim i czwartym kwartale bieżącego roku, natomiast korekta powinna następować w pierwszym kwartale roku następnego.

Ogólny koszt działania sieci można określić w dwojaki sposób. Jeżeli wyposażenie sieci nie jest jednolitą własnością i koszty jej utrzymania są ponoszone przez nie jeden podmiot, koszt działania sieci jest sumą kosztów ponoszonych przez te podmioty. Jeżeli całość środków jest własnością operatora lub jest postawiona do jego dyspozycji, koszt sieci w całości rejestruje operator. Opowiadamy się za drugim wariantem, który naszym zdaniem zapewnia lepszą dyscyplinę rzeczową i finansową i pozwala na jednoznaczne obciążenia odpowiedzialnością za działanie sieci.

Rozliczenie kosztów utrzymania sieci mogłoby odbywać się według następujących zasad:

I. Ustalanie kosztu

1. Za podstawę rozliczenia kosztów utrzymania sieci szkieletowej uznaje się całkowity koszt utrzymania sieci zaksięgowany u współpracujących ze sobą użytkowników. W tym celu w systemach księgowych zarówno użytkowników zostaną założone wyodrębnione rachunki, na których będą zapisywane wszystkie koszty ponoszone na rzecz utrzymania sieci.
2. Rozliczanie kosztów będzie następowało w okresach kwartalnych. Podstawą rozliczeń w trzech kwartałach każdego roku będzie uzgodniony plan kosztów utrzymania sieci. W czwartym kwartale nastąpi korekta stosownie do rzeczywiście poniesionych kosztów.

II. Podział kosztów

1. Podział kosztów pomiędzy umawiające się strony następuje proporcjonalnie do sumy przepustowości portów, poprzez które każda ze stron deklaruje wykorzystanie sieci szkieletowej. Strony ponoszą również solidarnie (proporcjonalnie) koszty utrzymania portów nadmiarowych w sieci.
2. W przypadku pojawienia się strony nieobjętej porozumieniem postępuje się podobnie.

III. Rozliczenie kosztów

1. Wpływy i wydatki każdej ze stron określa się jako różnicę pomiędzy kosztem obliczonym oraz rzeczywiście poniesionymi wydatkami na utrzymanie sieci.
2. Rozliczenie musi uwzględniać aktualnie obowiązujące przepisy w zakresie opodatkowania podatkiem VAT.

IV. Rozbudowa sieci

1. Rozbudowa sieci odbywa się ze środków inwestycyjnych operatora sieci lub w formie bez inwestycyjnej poprzez dzierżawę lub wynajem wyposażenia.
2. W przypadku konieczności poniesienia wydatków inwestycyjnych przekraczających możliwości operatora od żądającego rozbudowy żąda się przedpłacenia kosztów utrzymania sieci.

Osobnym problemem jest opodatkowanie VAT. Generalne rozwiązania polegające na rozliczeniu kosztów mogłoby przyczynić się do uniknięcia podatku. Jednak wszystkie zakupywane z zewnątrz dostawy i usługi byłyby droższe o ten podatek, który nie mógłby być rozliczony z Urzędami Podatkowymi. Jest to szczególnie niekorzystne w fazie inwestowania, gdy suma zwracanego podatku zasadniczo przekracza podatek wpłacany do Urzędów Skarbowych. Uważamy, że właściwszą drogą jest zabieganie o zwrot VAT dla instytucji budżetowych, gdzie jałowy obrót pieniędzmi ze budżetu (na zapłacenie VAT) i do budżetu (VAT zapłacony) podnosi tylko ogólne wydatki, chociażby na obsługę tego obrotu.

Rozważono trzy warianty finansowania przedsięwzięcia: ze środków własnych, za pomocą kredytu oraz poprzez wynajem wyposażenia.

Finansowanie inwestycji ze środków własnych jest łatwe oraz proste w realizacji. Jednak ten wariant finansowania ma kilka podstawowych wad. Po pierwsze zawsze występują

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 chociaż w części wdrożone. Na pewno nie w pełnej skali potrzeb, ale w stopniu zapewniającym nieporównywalne bezpieczeństwo sieci w porównaniu z bezpieczeństwem systemów tradycyjnych.

W tym miejscu należałoby przejść do rozważania problemu organizacji potrzebnej dla utrzymania systemu w sprawności. Niestety za szybkim postępem technologicznym, przenoszonym z innej niż polska rzeczywistości nie idzie w parze postęp organizacyjny oraz zmiany w sposobie myślenia. A nie jest tak, że tymi samymi metodami organizacyjnymi i przy pomocy podobnej kadry można eksploatować systemy tradycyjne i nowoczesne. Ta teza nie wymaga chyba udowodnienia.

Realizacja przedsięwzięcia polegająca na budowie, operowaniu i odpowiedniej ciągłej modyfikacji systemu łączności Państwa wymaga woli politycznej zapewniającej finansowanie i użytkowanie systemu ponad podziałami. Realizacja przedsięwzięć cząstkowych przez każdego zainteresowanego osobno jest nierealna. Zakładając hipotetycznie, że znajdą się odpowiednie środki finansowe, to nie spotkają się one z odpowiednią kwalifikowaną mocą wykonawczą. Na świecie tak jak w Polsce występuje ostry deficyt kadr w tej dziedzinie, a zwłaszcza kadr z odpowiednim doświadczeniem oraz odpowiednio zorganizowanych.

Jak uzasadniałem poprzednio utrzymanie sieci wymaga istnienia Operatora tej sieci odpowiedzialnego za jej działanie i rozwój. Nie ulega wątpliwości, że Operator ten powinien być pod całkowitą kontrolą Państwa. Jednak formy organizacyjne Operatora, realizacja nadzoru oraz metody uzyskiwania środków na działanie mogą być różne.

Operator może być zorganizowany jako jednostka budżetowa jak to tradycyjnie było w podobnych dziedzinach. Zaletą takiego rozwiązania jest administracyjna podległość jednostki i jej personelu. Wadami małą sprawność wynikająca z systemu organizacyjnego oraz nie odpowiednia reprezentacja interesów użytkowników. W systemie administracyjnym pracownik musi pełnić wyznaczone role w ramach określonych przepisów. W nowoczesnych systemach telekomunikacyjnych dąży się do zautomatyzowania wszystkiego co rutynowe i dające się uporządkować. Rola obsługi sprowadzana jest do rozwiązywania sytuacji nietypowych wymagających inicjatywy i indywidualnego podejścia do rozwiązywanych problemów. Następuje sprzeczność odpowiedzialności formalnej wynikającej z systemu organizacyjnego oraz potrzebnej odpowiedzialności rzeczowej (za wynik) wynikającej z rodzaju wykonywanej pracy. W takiej sytuacji jednostka budżetowa w dużej części zamienia się w kanał finansowania bardziej sprawnych jednostek gospodarczych. System podległości jednostki budżetowej zapewnia realizację interesów jednostek nadrzędnych, podczas gdy system powinien zapewnić realizację potrzeb wielu jednostek prawnie niezależnych.

Przeciwstawną formą organizacyjną Operatora jest przedsiębiorstwo jednoosobowej spółki Skarbu Państwa. Zaletą takiej formy organizacyjnej jest sprawność, odpowiedzialność za wyniki oraz łatwość wszelkiego rodzaju form rozliczeń. Również nadzór nad realizacją poprzez reprezentującą interesy użytkowników Radę Nadzorczą pewny i prawnie silnie umocowany. Wad a rozwiązania jest brak tradycji w tym zakresie, szereg irracjonalnych uprzedzeń oraz możliwość nadużywania atrakcyjnych stanowisk.

Jego zadaniem jest przygotowanie projektów, zorganizowanie dostaw oraz realizacja procesów wykonawczych.
Zespól zajmujący się optymalizacją działania sieci działa w oparciu o istniejące wyposażenie oraz istniejącą topologię sieci. Jego zadania wynikają z długo i krótkookresowych potrzeb eksploatacyjnych. Na przykład w przypadku ważnych wizyt trzeba przygotować czasową konfiguracją sieci w związku ze zmianami okresowymi w rozłożeniu ruchu w sieci, na skutek zmiany wagi poszczególnych węzłów sieci trzeba zmienić układ połączeń stałych i awaryjnych i tak dalej. Również obserwacja działania sieci lub długotrwałe awarie łącz wymagają czasowych zmian relacji i tym samym zmiany konfiguracji logicznej sieci.
Zespól serwisu zajmuje się zapobieganiem i usuwaniem skutków awarii w sieci, prowadzeniem odpowiednich magazynów i tym podobnymi sprawami zapewniającymi możliwe krótki stany awarii w sieci.
Każda z wymienionych warstw potrzebuje innego rodzaju realizatorów. Rozbudowa sieci wymaga zastanowienia, dokładnego projektowania i dłuższego czasu na realizację. Kadra obsługująca tego rodzaju działania wymaga wysokich kwalifikacji zawodowych, nie musi jednak mieć kwalifikacje do szybkich reakcji w sytuacjach niedoczasu.
Działania opisane w warstwie drugiej są podobne, ale wymagają większych zdolności analitycznych oraz znacznie krótszych okresów realizacji - normalnie w ciągu dni lub godzin. Z tego powodu kadra poza wybitnymi kwalifikacjami zawodowymi musi mieć zdolność działania w warunkach ograniczonego stresu w warunkach kooperacji z użytkownikami i obsługą eksploatacji w terenie.
Usuwanie awarii odbywa się w warunkach skrajnie stresujących przy szerokiej kooperacji z użytkownikami i obsługą eksploatacji w terenie. Ograniczony czas nie pozwala na głębsze analizy wobec czego usuwanie awarii powinno odbywać się zgodnie z wcześniej przygotowanymi scenariuszami. Kwalifikacje kadry są inne niż w poprzednio opisanych, ponieważ na pierwsze miejsce wysuwają się kwalifikacje do pracy w warunkach stresu, natomiast kwalifikacje zawodowe mają istotne, ale mniejsze znaczenie.
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.

wykorzystywać różne media od połączeń przewodowych, przez wiązki radiowe, podczerwieni itp.
Może również wystąpić przeciążenie sieci
Przeciążenie sieci wobec istniejących obecnie i dających się przewidzieć w przyszłości ograniczeń finansowych jest wysoce prawdopodobne. Zwłaszcza, jeżeli 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.
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.
Zdarzać się również będą 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.

5. Rozwiązania organizacyjne

Zapewnienie sprawnego działania systemu telekomunikacyjnego wymaga funkcjonowania dwóch rodzajów służb nazwanych tutaj służbami eksploatacji zajmującymi się kierowaniem i nadzorem nad funkcjonowaniem sprawnie funkcjonujących instalacji oraz służb utrzymania sieci zajmujących się rozbudową, modyfikowaniem i serwisem awaryjnym. Działanie tych służb jest ściśle ze sobą powiązane jednak tryb pracy oraz wymagane kwalifikacje odmienne. Z tego powodu służby te zostały opisane osobno.
Eksploatacja sieci może być rozpatrzona na trzech lub czterech poziomach. Poziom podstawowy obejmuje dyżurną obsługę węzła telekomunikacyjnego oraz dyżurującego operatora obsługującego szeroko rozumiane awizo. Poziom ten może być wspierany przez

- Na terenie wielu obiektów istnieją zakończenia pozostałe po pilotowej sieci KSŁ. Według naszych informacji istnieje również międzymiastowe wyposażenie tej sieci. Istnieje możliwość wynajmu części przepustowości tej sieci na preferencyjnych warunkach oraz przy zachowaniu jej podwyższonej niezawodności. Wadą tej sieci jest brak odpowiedniego wyposażenia teletransmisyjnego zapewniającego wysoką jej niezawodność.

Najważniejszym problemem jest znalezienie obiektów, w których mogłyby zostać zlokalizowane węzły sieci łączności Państwa. Prawie wszystkie obiekty wykorzystywane obecnie do podobnych celów, które w przyszłości mogłyby być wykorzystane dla potrzeb przedsięwzięcia nie spełniają wymogów odpowiedniej ochrony. Postępujący szybko rozwój techniczny powoduje doskonalenie również narzędzi służących do przechwytywania informacji, przełamywania ochrony, skutecznego ataku na obiekty itp. Spełnienie podstawowych wymogów przy obecnym poziomie wiedzy wymaga dokonywania kosztownych adaptacji oraz uregulowania wielu kwestii prawnych. W każdym razie wydaje się rozsądniejszą metodą adaptowanie istniejących obiektów niż budowanie ich od nowa, również ze względu na oszczędność czasu.

Wykorzystanie infrastruktury dla sieci łączności Państwa powinno zakładać, że:

a) Wszystkie kierunki przesyłania powinny mieć alternatywne drogi przesyłania:

- pomiędzy węzłami sieci szkieletowej powinny istnieć co najmniej dwie dodatkowe drogi przesyłania, w sieci regionalnej co najmniej 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.

4. Rozwiązania techniczne

Wszystkie obiekty objęte analizowanym przedsięwzięciem powinny być wyposażone, chociaż w różnym stopniu w urządzenia;

- Centrale komutacji połączeń wraz z wyposażeniem abonenckim,
- Urządzenia teletransmisyjne,
- Urządzenia teleinformatyczne,
- Siłownie telekomunikacyjne,
- Lokalne systemy zarządzania zasobami.

Wszystkie wyżej wymienione wyposażenia tworzą zintegrowane systemy teletransmisyjne poddane centralnemu nadzorowi i sterowaniu. Podstawowe systemy instalowane w węzłach powinny być powielane. Tym samym dostawcy i instalatorzy systemów powinni być ci sami. W tej celowym jest ustanowienie jednego generalnego realizatora systemu.

W referacie przewiduje się następujące środki przeciwdziałania uszkodzeniom wyposażenia sieciowego:

a) Całe wyposażenie sieciowe powinno być zlokalizowane w odpowiednio wyposażonych pomieszczeniach zapewniających normatywne warunki pracy urządzeń sieci, zasilanie

- nie utrwaliły się obyczaje i normy regulujące współudział w ponoszeniu kosztów za świadczenie usług w zamkniętej grupie użytkowników wybudowanego systemu.

W krótkim referacie nie sposób 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 sieci budowanych i operowanych przez NASK oraz ze współudziałem NASK.

Atak na sieć może dotyczyć przechwycenia informacji użytkownika lub uniemożliwić przesłanie tych informacji. Przechwytywanie informacji wymaga uzyskania dostępu do 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 lub więcej przechwycenie informacji wymaga urządzeń o wielkiej pojemności pamięci, 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.

Ochronę sieci można rozważać w trzech aspektach: ochrona niezawodności, ochronę informacji użytkownika oraz ochronę przed niepowołanym dostępem do sieci. Wszystkie aspekty ochrony sieci należy 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.

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:

- 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. Konieczna infrastruktura

Sieć telekomunikacyjne dla potrzeb Państwa nie powinna być siecią podstawową budowaną z przeznaczeniem tylko dla własnych potrzeb. Istnieją co najmniej trzy powody, dla których takie rozwiązanie jest niecelowe:

- Sieć dedykowana jest łatwa do zaatakowania przez swoje wydzielenie, a co za tym idzie łatwość identyfikacji,

Zestawienie ważniejszych aktów prawnych związanych z problematyką budowy bezpiecznych węzłów teleinformacyjnych.

1. Ustawa z dnia 7 lipca 1994r. Prawo Budowlane.
2. Zarządzenie Ministra Gospodarki Przestrzennej i Budownictwa z dnia 15 grudnia 1994r. w sprawie dziennika budowy oraz tablicy informacyjnej.
3. Zarządzenie Ministra Gospodarki Przestrzennej i Budownictwa z dnia 30 grudnia 1994r. w sprawie szczegółowego zakresu i formy projektu budowlanego.
4. Ustawa z dnia 23 listopada 1990r. o łączności.
5. Rozporządzenie Ministra Łączności z dnia 16 lipca 1993r. w sprawie wymagań technicznych i eksploatacyjnych oraz warunków wzajemnej współpracy urządzeń, linii i sieci telekomunikacyjnych zakładanych i używanych na terytorium Rzeczypospolitej Polskiej.
6. Rozporządzenie Ministra Łączności z dnia 21 kwietnia 1995r. w sprawie warunków technicznych zasilania energią elektryczną obiektów budowlanych łączności.
7. Rozporządzenie Ministra Łączności z dnia 10 października 1995r. w sprawie samodzielnych funkcji technicznych w budownictwie telekomunikacyjnym.
8. Rozporządzenie Ministra Łączności z dnia 16 marca 1994r. w sprawie obowiązków stosowania polskich norm i norm branżowych z dziedziny łączności.
9. Rozporządzenie Ministra Przemysłu z dnia 8 października 1990r. w sprawie warunków technicznych jakim powinny odpowiadać urządzenia elektroenergetyczne w zakresie ochrony przeciwpożarowej.
10. Rozporządzenie Ministra Spraw Wewnętrznych z dnia 3 listopada 1992r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów.
11. Rozporządzenie Ministra Łączności z dnia 31 maja 1993r. w sprawie określenia systemów telekomunikacyjnych, zakładanych i używanych na terytorium Rzeczypospolitej Polskiej.
12. Ustawa z dnia 22 stycznia 1999r. o ochronie informacji niejawnych.
13. Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999r. w sprawie wymagań bezpieczeństwa systemów i sieci teleinformacyjnych.

Państwo nasze zdecydowało, że systemy i sieci teleinformatyczne służące do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych stanowiących tajemnicę państwową, podlegają szczegółowej ochronie przed nieuprawnionym ujawnieniem tych informacji, a także przed możliwością przypadkowego lub świadomego narażenia ich bezpieczeństwa.

Ponieważ wytwarzanie, przechowywanie, przetwarzanie i przekazywanie informacji niejawnych stanowiących tajemnicę państwową wymaga certyfikatu wydanego przez właściwą służbę ochrony państwa (Art. 62 pkt.1 w/w ustawy) - to w rozumieniu tego zapisu cały proces przygotowania budowy i jej realizacji poddany musi być rygorom wynikającym z tej ustawy.

Oznacza to, że zarówno przedsiębiorstwa jak i jednostki badawczo-rozwojowe uczestniczące w procesie projektowym i budowlanym, z wykonaniem, którego łączy się dostęp do informacji niejawnych stanowiących tajemnicę - mają obowiązek ochrony tych informacji.

To czy mają odpowiednią zdolność do ochrony tych informacji, ma wykazać prowadzone przez służby ochrony państwa postępowanie sprawdzające. Postępowanie to prowadzone jest na podstawie kwestionariusza bezpieczeństwa przemysłowego.

Postępowaniu podlegają:

- osoby zajmujące stanowiska związane z kierowaniem, wykonywaniem umowy lub jej bezpośrednią realizację u przedsiębiorcy lub jednostce badawczo-rozwojowej
- osoby, które w imieniu wspomnianych wyżej podmiotów uczestniczą w czynnościach zmierzających do zawarcia umowy , jeżeli są one związane z dostępem do informacji niejawnych
- osoby zatrudnione w procesie ochrony.

Potwierdzeniem zdolności do uczestnictwa w procesie budowy bezpiecznego systemu teleinformacyjnego jest świadectwo bezpieczeństwa przemysłowego wydane przez stosowne służby ochrony państwa.

Podstawowe wymagania odnośnie bezpieczeństwa systemów i sieci teleinformatycznych służących do wytwarzania, przetwarzania, przechowywania i przekazywania informacji niejawnych zawarte są w Rozporządzeniu Prezesa Rady Ministrów z dnia 25 lutego 1999r.

W myśl tego rozporządzenia bezpieczeństwo teleinformatyczne zapewnia się przez:

- ochronę fizyczną,
- ochronę elektromagnetyczną,
- ochronę kryptograficzną,
- bezpieczeństwo transmisji,
- kontrolę dostępu do urządzeń, systemu lub sieci teleinformatycznych.

Opracowując program funkcjonalno-użytkowy dla bezpiecznego systemu teleinformacyjnego przygotować musimy zatem szczegółowe wymagania bezpieczeństwa.

Istotnym ich elementem będą:

- lokalizacja,
- typ wykorzystywanych w nim urządzeń oraz oprogramowania,
- sposób realizowanych połączeń wewnętrznych i zewnętrznych,
- konfiguracja sprzętowa,

Ponadto projektant ma obowiązek zapewnić sprawdzenie projektu przez osobę posiadającą uprawnienia budowlane do projektowania bez ograniczeń, w odpowiedniej specjalności. Obowiązek ten nie dotyczy obiektów o małym stopniu złożoności nie stwarzających zagrożenia dla użytkowników i otoczenia.

Projektantowi przysługuje jednocześnie prawo do:

- wstępu na teren budowy i dokonywania zapisów w dzienniku budowy dotyczących jej realizacji
- żądania wpisem do dziennika budowy wstrzymania robót budowlanych w razie:
  1. stwierdzenia możliwości powstania zagrożenia,
  2. wykonywania robót niezgodnie z projektem.

Do obowiązków kierownika budowy należy:

- protokolarne przyjęcie od inwestora i odpowiednie zabezpieczenie terenu budowy wraz z znajdującymi się na nim obiektami budowlanymi, urządzeniami technicznymi i stałymi punktami osnowy geodezyjnej oraz podlegającymi ochronie elementami środowiska przyrodniczego i kulturalnego,
- prowadzenie dokumentacji budowy,
- zapewnienie geodezyjnego wytyczenia obiektu oraz zorganizowanie i kierowanie budową obiektu budowlanego w sposób zgodny z projektem i pozwoleniem na budowę, przepisami i obowiązującymi Polskimi Normami oraz przepisami bezpieczeństwa i higieny pracy,
- wstrzymanie robót budowlanych w przypadku stwierdzenia możliwości powstania zagrożenia oraz bezzwłoczne zawiadomienie o tym właściwego organu,
- zawiadomienie inwestora o wpisie do dziennika budowy dotyczącym wstrzymania robót budowlanych z powodu wykonania ich nie zgodnie z projektem,
- realizacje zaleceń wpisanych do dziennika budowy,
- zgłoszenie inwestorowi do sprawdzenia lub odbioru wykonanych robót ulegających zakryciu bądź zanikających oraz zapewnienie dokonania wymaganych przepisami lub ustalonych w umowie prób i sprawdzeń urządzeń technicznych,
- przygotowanie dokumentacji powykonawczej obiektu budowlanego,
- zgłoszenie obiektu budowlanego do odbioru odpowiednim wpisem do dziennika budowy oraz uczestnictwie w czynnościach odbioru, a także przekazanie inwestorowi oświadczenia o:
  1. zgodności wykonania obiektu z projektem i warunkami pozwolenia na budowę, a także przepisami i obowiązującymi normami,
  2. doprowadzenie do należytego stanu i porządku terenu budowy (budynku lub lokalu).

Kierownik budowy ma prawo:

- wystąpienia do inwestora o zmiany w rozwiązaniach projektowych, jeżeli są one uzasadnione koniecznością zwiększenia bezpieczeństwa realizacji robót lub usprawnienia procesu budowy
- ustosunkowania się w dzienniku budowy do zaleceń w nim zawartych.

Do podstawowych obowiązków inspektora nadzoru inwestorskiego należy:

- reprezentowanie inwestora na budowie przez sprawowanie kontroli zgodności jej realizacji z projektem i pozwoleniem na budowę, przepisami i obowiązującymi normami,

3. Zadania operatora systemów łączności dla potrzeb kierowania państwem.

Eksploatacja i utrzymanie systemów łączności dla potrzeb kierowania państwem jest zadaniem bardzo skomplikowanym. Z jednej strony konieczna jest wysoka niezawodność działania sieci telekomunikacyjnej oraz jej ochrona, z drugiej bardzo duży zasób wiedzy oraz duża elastyczność organizacyjna i finansowa, aby tę niezawodność zapewnić.

Sieć poprzez swoją technologię posiada dużą odporność na błędy działania operatorów i użytkowników oraz odporność na zakłócenia w wyniku awarii czy działania chwilowych czynników zewnętrznych. Ta odporność wynika z jednolitości systemu zarządzania działania sieci (system automatyczny) i wynikającą z tego centralizację operatora. Z drugiej strony usuwanie przyczyn powodujących błędy jest konieczne, bowiem automatyczne czy półautomatyczne ich usunięcie zmniejsza prawdopodobieństwo automatycznego usunięcia następnej awarii czy zakłócenia. Działania z tym związane muszą przebiegać w terenie, daleko od centrum zarządzania i jak już wspomniano wymagają odpowiednich kwalifikacji.

Z usług telekomunikacyjnych sieci dla potrzeb kierowania państwem będzie korzystać wiele podmiotów, które dają się pogrupować ze względu na charakter działalności oraz rodzaj jej finansowania. Operowanie siecią dla tych grup użytkowników powinno być wyspecjalizowane. Ponadto występowanie wielu podmiotów po stronie operatorów jak i po stronie użytkowników uzasadnia konieczność regulowania wzajemnych zobowiązań i uprawnień przy pomocy umów cywilno - prawnych. To znaczy, że użytkownik zamienia się w abonenta usług sieci telekomunikacyjnej, który ma jasno określone, drogą regulaminów, cenników i szczegółowych regulacji umownych, swoje prawa i obowiązki.

Do powołania operatora "strategicznego" niezbędne są decyzje polityczne oraz gwarancje finansowania (przynajmniej w początkowym okresie funkcjonowania urzędu) jako wydzielona pozycja w budżecie.

Jest to tradycyjne działanie w ramach jednostek budżetowych. Metoda ta zawiera istotne zabezpieczenia ale sprawność jej jest ograniczone. W przypadkach budowy systemów dla potrzeb kierowania państwem występuje konieczność zlecania dużej części prac jednostkom posiadającym znacznie większą elastyczność organizacyjną.

Szczególnie trudne lub wręcz niemożliwe jest zapewnienie w systemie budżetowym odpowiedniego systemu wynagrodzeń dla specjalistów z dziedziny telekomunikacji..

Drugim przeciwstawnym przykładem jest budowa systemów i utrzymanie ich przez jednostkę typu gospodarczego posiadającą odpowiednie certyfikaty bezpieczeństwa. Rozwiązanie coraz powszechniejsze na świecie, w Polsce budzi jeszcze wiele zastrzeżeń o charakterze politycznym lub wręcz abstrakcyjnym.

Trzecim rozwiązaniem jest działanie poprzez jednostki o charakterze pośrednim jak zakłady budżetowe, agencje itp.

Jednostki tego typu nie posiadają sprawności jednostek gospodarczych, ale finansowane częściowo z budżetu, a częściowo z działalności gospodarczej, mogłyby stanowić podstawę do powołania operatora "strategicznego".

Przedstawione w niniejszym referacie problemy i uwarunkowania ukierunkowywują działania jakie należy podjąć w celu zapewnienia sprawnej łączności dla potrzeb kierowania państwem.

Warszawa - maj 1999 rok.

- pomieszczenia chronione powinny być zabezpieczone przed podglądem
- i podsłuchem akustycznym;
- pomieszczenia dla obsług operatorskich systemu zarządzania i utrzymania powinny być bezwzględnie oddzielone od pomieszczeń stacyjnych. System ten powinien być wyposażony w narzędzia i techniki logiczne chroniące przed nieupoważnionym dostępem;
- w skład systemu kryptograficznego (utajniającego) powinny wchodzić:
  - indywidualne urządzenia utajniające, instalowane w stacjach abonenckich,
  - grupowe urządzenia utajniające, instalowane w urządzeniach stacyjnych,
- system kryptograficzny powinien umożliwiać :
  - utajnianie rozmów telefonicznych, transmisji danych i innych form korespondencji,
  - utajnianie traktów między węzłami (utajnianie grupowe - grupowe urządzenie utajniające powinno pracować dupleksowo z szybkością od 64 kbit/s do 2048 kbit/s).
- w systemie powinien być wykorzystywany sprzęt charakteryzujący się niskim poziomem emisji ujawniającej;
- w systemie instalacja abonencka i zasilania powinny być zabezpieczone przed ulotem elektromagnetycznym.

2.5. System zarządzania i utrzymania.

- podstawowe funkcje systemu zarządzania i utrzymania systemu łączności:
  - zarządzanie uszkodzeniami (obsługa alarmów, lokalizacja i usuwanie skutków uszkodzeń, powodowanie działań naprawczych, uruchamianie testów diagnostycznych);
  - zarządzanie konfiguracją, możliwość rekonfiguracji elementów systemu, przyjmowanie nowych elementów systemu do zarządzania;
  - zarządzanie bezpieczeństwem tj. bezpieczeństwem systemu zarządzanego, bezpieczeństwem w systemie zarządzania i utrzymania, zarządzanie utajnianiem;
  - zarządzanie usługami (utrzymywanie aktualnego spisu abonentów, dołączanie i odłączanie abonentów, przyznawanie i odwoływanie uprawnień abonentom, tworzenie statystyk dla abonentów i usług);
  - zarządzanie ewentualnymi opłatami (gromadzenia danych taryfikacyjnych i ich przetwarzanie);
  - system zarządzania i utrzymania powinien posiadać scentralizowaną architekturę wieloszczeblową natomiast realizować swoje zadania
  - w sposób rozproszony;
  - w systemie powinna być zapewniona możliwość zmiany konfiguracji systemu (włączanie do systemu nowych urządzeń, wyłączenie
  - z systemu urządzeń, zmiany statusu urządzeń) bez przerw w łączności;
  - powinna być zapewniona możliwość automatycznego wykrywania
  - i wyizolowana uszkodzonego elementu;
  - powinna być zapewniona możliwość organizowania rezerwowych dróg dla przekazywania danych do ośrodków zarządzania i utrzymania.

2.6. Usługi dostarczane przez system.

- wszyscy użytkownicy powinni mieć docelowo możliwość standardowej komunikacji w czterech kategoriach: fonia, dane, tekst i obraz:

- naczelny dowódca;
- dowódca wojsk lądowych;
- dowództwa okręgów wojskowych i rodzajów sił zbrojnych;
- dowództwa związków operacyjnych, taktycznych, oddziałów i pododdziałów.

2. Wymagania na zintegrowany system łączności.

Planowany zintegrowany system łączności powinien zapewnić bezpieczny i niezawodny obieg informacji organom władzy i administracji państwowej, organom bezpieczeństwa wewnętrznego oraz innym użytkownikom realizującym szczególnie ważne zadania na rzecz bezpieczeństwa państwa, kryzysu i wojny.

Wychodząc z powyższego wymagania stawiane systemowi łączności sformułowane powinny zostać w następującym układzie tematycznym:

- struktura systemu,
- sieć transmisyjna,
- sieć komutacyjna,
- bezpieczeństwo systemu łączności,
- system zarządzania i utrzymania ,
- usługi dostarczane przez system,
- podsystem dostępu radiowego,
- odtwarzanie naruszonego systemu łączności,
- współpraca z innymi sieciami telekomunikacyjnymi.

2.1. Struktura systemu.

- struktura projektowanego systemu łączności powinna być dostosowana do struktury systemu kierowania państwem;
- architektura sieci musi być dostatecznie elastyczna i podatna na zmiany warunków funkcjonowania i potrzeb użytkowników bez konieczności zmiany jej struktury;
- system łączności powinien zapewniać możliwość współpracy z innymi sieciami telekomunikacyjnymi;
- system łączności powinien być kompatybilny z międzynarodowymi systemami łączności, w tym rządowymi, bezpieczeństwa i porządku publicznego, militarnymi i ratownictwa;
- w zależności od przeznaczenia (liczby abonentów) węzły łączności powinny być projektowane i budowane z podziałem na różne kategorie;
- węzły powinny mieć strukturę zdecentralizowaną o sterowaniu rozproszonym. Każdy węzeł powinien być przystosowany do tranzytowania połączeń;
- węzły łączności powinny umożliwiać dowiązywanie się grup abonentów za pomocą mobilnych środków łączności;
- system powinien zapewnić możliwość współpracy z abonentami w ruchu (radiodostęp).

2.2. Sieć transmisyjna.

- system transmisyjny powinien mieć status sieci priorytetowej;
- powiązanie węzłów łączności pomiędzy sobą powinno opierać się na cyfrowej sieci teletransmisyjnej wykorzystującej docelowo jako medium fizyczne wyłącznie

badawczo - rozwojowych oraz obywateli. W świetle tej ustawy można przyjąć, że ***polityka bezpieczeństwa teleinformatycznego, obejmująca bezpieczeństwo systemów i sieci teleinformatycznych jednostki organizacyjnej, stanowi uporządkowany zbiór praw, zasad i metod postępowania, regulujących procedury bezpiecznego działania na informacjach wytwarzanych, przetwarzanych, przechowywanych i przekazywanych, zachowując ich niejawność (stosownie do kompetencji) dostępność i integralność, a także ochronę osób i materiałów, osiąganych w wyniku działań naukowych, parlamentarnych, administracyjnych, technicznych i fizycznych.***

Ta obszerna, lecz z pewnością nie wyczerpująca problem definicja jest wykładnią do rozpisania zadań wykonawczych dla organów odpowiedzialnych za ich realizację na odpowiednich poziomach - celem zapewnienia sprawnego a zarazem bezpiecznego kierowania państwem.

Sprawność systemu kierowania państwem w dużej mierze zależy od posiadanego systemu łączności, funkcjonującego zarówno w czasie pokoju, jak i w okresie zagrożenia (kryzysu) i wojny.

W czasie pokoju system łączności powinien zapewnić sprawne funkcjonowanie wszystkich ogniw systemu kierowania państwem, zachowując możliwość bezkolizyjnego przejścia na wzmożony reżim pracy w stanach nadzwyczajnych.

W okresie zagrożenia bezpieczeństwa państwa (kryzysu) i wojny warunki funkcjonowania systemów łączności ulegają radykalnym zmianom ze względu na to że:

a) po pierwsze - może stać się on obiektem bezpośredniego ataku przeciwnika i tym samym mogą ulec znacznemu zmniejszeniu jego możliwości;

b) po drugie - wzrośnie obciążenie większości elementów i ogniw systemu, bowiem w okresie tym szczególnego znaczenia nabiera kompleksowe i wiarygodne informowanie o zasobach gospodarki narodowej (potencjale gospodarczym) oraz potencjale sił zbrojnych własnego państwa jak również potencjale przeciwnika, warunkach bezpieczeństwa i ochrony struktur państwa i ludności a także o decyzjach związanych z obronnością. W czasie wojny nasila się proces informacyjny, wzrastają wymagania wobec tajności i sprawności pozyskiwania, przetwarzania i przekazywania informacji przy prawdopodobnym zmniejszeniu możliwości systemu łączności w wyniku zniszczenia części jego infrastruktur.

W okresie zagrożenia bezpieczeństwa państwa kryzysami niemilitarnymi (ekologicznymi - nadzwyczajne zagrożenia środowiska, społecznymi - zagrożenie ładu i porządku publicznego) system łączności powinien być tak zbudowany aby można było stworzyć możliwości funkcjonowania systemu kierowania w sytuacjach kryzysowych na szczeblu państwa, regionu lub nawet powiatu. Dla potrzeb sztabów kryzysowych należy umożliwić bezkolizyjne przekazywanie znacznej ilości informacji sytuacyjnych i decyzyjnych szczególnie w układach funkcjonalnych ogniw polityczno - administracyjnych i społecznych oraz ochronno - obronnych.

W tej sytuacji należy przewidywać znaczne skumulowanie się ilości przekazywanej informacji w określonym przedziale czasu i na określonych kierunkach (obszarach).

W razie wystąpienia zagrożeń bezpieczeństwa państwa przewiduje się wprowadzenie - zależnie od rodzaju zagrożenia - stosownych stanów nadzwyczajnych:

- wojennego;
- wyjątkowego;
- klęski żywiołowej,

w czasie których następuje bądź to reagowanie na dane zagrożenie siłami i środkami czasu "P" utrzymywanymi w stałej gotowości do działania, bądź też rozwija się dodatkowe siły i środki, w tym włącznie z uruchomieniem mobilizacji sił zbrojnych i gospodarki narodowej.

człowieka. W coraz większym stopniu stajemy się wszyscy uzależnieni od tych systemów. Jak słusznie zauważył P. Tyrrell[12] rozwój telekomunikacji w XX wieku można porównywać do analogicznej rewolucji przemysłowej przełomu XIX i XX wieku, a historia łączności jest odbiciem historii transportu. Powoli systemy komputerowe przejmują kontrolę nad naszym życiem. Korzystamy z nich w pracy i w domu. Sterują procesami produkcyjnymi, przyśpieszają obrót handlowy i wypierają pieniądz kruszcowy. Wraz z rozwojem nowych technologii zwiększa się też zagrożenie ze strony tych technik dla człowieka. Wielokrotnie podkreślał to w swoich felietonach publikowanych w „PC Magazine po polsku" znany pisarz Stanisław Lem stwierdzając, że „pociąg ludzi do zła ujawnia się szczególnie tam, gdzie pojawia się nowa technologia". Symptomatyczna i potwierdzająca tą tezę jest informacja Steve Kirscha z firmy "Infoseek" wygłoszona na kongresie "Internet World" w Berlinie, iż na dwadzieścia najczęściej zadawanych pytań w ich wyszukiwarce - tylko trzy z nich nie były związane z seksem.

Przedstawione w niniejszym opracowaniu tezy z całą pewnością nie prezentują całości zagadnienia. Jednakże w ocenie autora przekazanie wiedzy chociażby w sposób wycinkowy jest niezmiernie potrzebne w dobie tak szybkich przemian technologicznych. Należy bowiem pamiętać, że życie nie lubi próżni. Zasadą znaną od wieków jest to, iż to przestępcy pierwsi wykorzystują nowoczesne technologie a organy ścigania zawsze są o krok za nimi.

[12] P. Tyrrell: Internet: anioł – przewodnik czy diabeł – oszust?, „Internet Security" wkładka w „Internet Devoloper" 1998, nr 2, s. 3 – 5;

programu komputerowego, to czyn taki narusza zarówno dyspozycję art. 293 w zw. z art. 291 § 1 k.k., jak i art. 118 ust. 1 upapp. Jeżeli natomiast sprawca działa bez zamiaru osiągnięcia korzyści majątkowej, bądź gdy przedmiotem wykonawczym przestępstwa jest zapis programu, którego pliki sprawca instaluje lub przyjmuje na przechowanie we własnym komputerze albo pomaga do zbycia lub ukrycia programu za pośrednictwem sieci komputerowej i założonego przez siebie albo należącego do innej osoby BBS-u, wtedy w grę wchodzi wyłącznie możliwość pociągnięcia go do odpowiedzialności karnej na podstawie art. 293 k.k.[11]

Należy dodać, że za paserstwo programu komputerowego każda z ustaw przewiduje inne zagrożenie karne (art. 293 w zw. z art. 291 § 1 k.k. - karę pozbawienia wolności od 3 miesięcy do lat 5, natomiast art. 118 ust. 1 upapp - karę grzywny, karę ograniczenia wolności lub karę pozbawienia wolności do lat 2). Ponadto k.k. przewiduje ściganie tego przestępstwa z urzędu, zaś art. 122 upapp - w trybie oskarżenia prywatnego.

Chociaż przepis art. 293 k.k. dotyczy wyłącznie paserstwa programu komputerowego, podczas gdy art. 118 ust. 1 upapp chroni także inne utwory oraz artystyczne wykonania, fonogramy i wideogramy, to jednak w porównaniu z art.118 ust. 1 upapp dyspozycja art. 293 k.k. nie zawiera żadnych dodatkowych znamion bliżej określających istotę paserstwa programu komputerowego.

Nabycie, jako forma paserstwa programu komputerowego może mieć dwojaką postać. W sytuacji, gdy dotyczy nośnika pirackiej kopii programu komputerowego - wiązać się będzie z uzyskaniem przez nabywcę władztwa nad nośnikiem, oczywiście bez uzyskania tytułu własności do utrwalonego na nim programu. O rozmiarach osiągniętej w ten sposób przez pasera korzyści majątkowej decyduje jednak wartość programu a nie nośnika. Jeżeli paserstwo programów komputerowych dotyczy mienia znacznej wartości, sprawca ponosi surowszą odpowiedzialność na podstawie art. 294 § 1. W przypadku, gdy przedmiotem paserstwa jest tylko zapis programu - nabycie jest równoznaczne ze skopiowaniem zapisu pirackiej wersji programu komputerowego, udostępnionego paserowi przez inną osobę. Może to nastąpić za pośrednictwem tzw. BBS-u, serwera sieciowego, który zapewnia usługę FTP lub serwera WWW.

Art. 293 § 2 k.k. przewiduje możliwość orzeczenia przepadku rzeczy określonej w § 1 tego artykułu (tj. programu komputerowego), chociażby nie stanowiła ona własności sprawcy. Orzeczenie przepadku komputera wobec sprawcy czynu określonego w art. 293 § 2 k.k. jest więc możliwe, gdy chodzi o taką postać paserstwa programów komputerowych, jaką jest pomoc do zbycia tych programów. Przykładem takiej sytuacji może być posadowienie na komputerze włączonym do Internetu strony WWW zawierającej ofertę sprzedaży wysyłkowej komercyjnych programów komputerowych „po super atrakcyjnej cenie".

Paserstwo nieumyślne programu komputerowego

Nowy kodeks karny - w odróżnieniu od ustawy o prawie autorskim - przewiduje także odpowiedzialność za nieumyślne paserstwo programu komputerowego. Rozwiązanie to niewątpliwie ułatwi udowodnienie winy i doprowadzenie do skazania za przestępstwo (ścigane z urzędu) każdego, komu będzie można wykazać, że wszedł w posiadanie prawnie chronionego programu komputerowego bez uzyskania licencji na jego używanie.

Przypisanie indywidualnej odpowiedzialności wymaga wykazania osobie podejrzanej, że cechy programu lub okoliczności, w jakich doszło do jego uzyskania powinny były wywołać w niej wątpliwości co do trafności przekonania o legalnym pochodzeniu tego programu. Część pirackiego oprogramowania, która jest podrabiana profesjonalnie, łącznie z fałszowaniem znaków towarowych, hologramów i umów licencyjnych, może nie dawać podstaw do postawienia zarzutu paserstwa programu komputerowego jego nabywcy, w szczególności, jeśli są to programy nabyte w specjalistycznym sklepie, którego właściciel dba o zachowanie wszelkich pozorów legalności prowadzonej przez siebie działalności.

Przedmiotem czynności wykonawczej nieumyślnego paserstwa programu komputerowego może być zarówno materialna jak i wyłącznie cyfrowa postać tego programu.

---

[11] A. Adamski, Przestępstwa..., wyd. cyt.

kryminalizujących tzw. piractwo komputerowe przepisów ustawy z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. Nr 24, poz. 83), które zostały utrzymane w mocy przez ustawę z dnia 6 czerwca 1997 r. przepisy wprowadzające kodeks karny (Dz. U. Nr 88, poz. 554).

Karalność oszustwa komputerowego

art. 287

Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody bez upoważnienia wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub zmienia, usuwa albo wprowadza nowy zapis na komputerowym nośniku informacji,

podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Istota przestępstwa określonego w art. 287 § 1 k.k. polega na usiłowaniu uzyskania korzyści lub spowodowania szkody, co ma ułatwić dowodzenie w procesie karnym jego znamion.[8] Dokonanie oszustwa komputerowego zachodzi „już w momencie wpłynięcia na automatyczne przetwarzanie danych, wprowadzenia nowego zapisu na komputerowym nośniku informacji itp., tj. zanim nastąpiło przesunięcie w sferze majątkowej (powstanie zamierzonej szkody)."[9]

Zakres penalizacji art. 278 k.k. jest bardzo szeroki, co wynika z określenia funkcji czasownikowej dyspozycji tego przepisu zwrotem „wpływa". Przepis mówi o wpływaniu na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji przez osobę do tego nieupoważnioną. Chodzi zatem o ingerencję takiej osoby w funkcjonowanie systemu przetwarzania danych. Tego rodzaju sytuację można natomiast traktować jako naruszenie integralności, poufności lub dostępności danych i systemów komputerowych (teleinformatycznych), której celem - w przypadku art. 278 k.k. - jest osiągnięcie korzyści majątkowej lub wyrządzenie szkody innej osobie. Przemawia za tym szereg podobieństw w sposobie określenia strony przedmiotowej przestępstw przeciwko ochronie informacji (art. 267, 268 i 269 k.k.) i oszustwa komputerowego (art. 278 k.k.). Przełamywanie elektronicznych zabezpieczeń informacji, o którym mówi art. 267 § 1 k.k., albo posługiwanie się urządzeniem specjalnym w celu uzyskania zastrzeżonej informacji (art. 267 § 2 k.k.) jest formą „wpływania" na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji. Stanowi więc zachowanie wypełniające także znamiona ustawowe art. 278 k.k.

Oszustwa komputerowe wraz z rozwojem w Polsce Internetu dokonywane są coraz częściej. Dotyczą one głównie czynów na szkodę międzynarodowych systemów kart płatniczych (transakcje w sklepach internetowych).

Karalność paserstwa programów komputerowych

Norma art. 293 § 1 k.k. nakazuje odpowiednie stosowanie przepisów dotyczących paserstwa rzeczy uzyskanej za pomocą czynu zabronionego do programu komputerowego.
Przepis ten uznaje możliwość popełnienia paserstwa programu komputerowego zarówno z winy umyślnej (art. 291 k.k.) jak i nieumyślnej (art. 292 k.k.).

Art. 293.

§ 1. Przepisy art. 291 i 292 stosuje się odpowiednio do programu komputerowego.

§ 2. Sąd może orzec przepadek rzeczy określonej w § 1 oraz w art. 291 i 292, chociażby nie stanowiła ona własności sprawcy.

oszustwo komputerowe, [w:] Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Materiały z konferencji naukowej, Poznań 20-22.04.1994 r. (pod red. A. Adamskiego), Toruń 1994,s. 136 .

[9] Tamże, s. 137.

Indywidualnym przedmiotem ochrony przestępstwa z art. 267 § 2 k.k. jest **poufność informacji**. Omawiany przepis sankcjonuje wszelkie działania zmierzające do naruszenia prawa do wyłącznego dysponowania określonym rodzajem informacji. W odróżnieniu od przepisu § 1 art. 267 k.k., mamy tu do czynienia z przyjęciem bardziej zobiektywizowanego kryterium karalności, jakim jest zakładanie urządzeń technicznych lub posługiwanie się nimi w celu uzyskania zastrzeżonych rodzajów informacji. Karalne jest nie tylko zakładanie lub posługiwanie się w tym celu wspomnianymi urządzeniami, lecz także uzyskiwanie przy ich pomocy informacji przez osoby do tego nieuprawnione.

Poufność rozmów i innych form interpersonalnego porozumiewania się jest tylko jednym z elementów przedmiotu ochrony przestępstwa z art. 267 § 2 k.k. Przepis ten może być też podstawą sankcjonowania rozmaitych form ingerencji w życie prywatne i swobodne korzystanie z mieszkania, np. przez inwigilację przebywających w nim osób przy użyciu urządzeń optycznych, akustycznych, nokto - i termowizyjnych lub elektronicznych. Inwigilacja może polegać na przechwytywaniu informacji przesyłanych przy pomocy urządzeń telekomunikacyjnych albo na podsłuchu lub podglądzie elektronicznym bezpośrednim (ang. *bugging*), prowadzonym przy użyciu mikrofonów, kamer lub nadajników radiowych umieszczonych zarówno wewnątrz lokalu, jak i przy wykorzystaniu urządzeń znajdujących poza lokalem (np. mikrofonów kierunkowych, skanerów do przeszukiwania częstotliwości fal radiowych, satelitów)[5].

Istnieje duże ryzyko naruszenia poufności informacji przetwarzanej elektronicznie i przesyłanej sieciami komputerowymi. Wiąże się ono z możliwością podsłuchu transmisji teleinformatycznych wieloma metodami. Niestety koszty ujawniania takich zdarzeń są bardzo wysokie i na dzień dzisiejszy praktycznie nie ujawniane.

Karalność niszczenia danych lub programów komputerowych oraz sabotażu komputerowego

art.268

§ 1.

Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2.

Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca

podlega karze pozbawienia wolności do lat 3.

§ 3.

Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową,

podlega karze pozbawienia wolności do lat 5.

art. 269 § 1.

Kto, na komputerowym nośniku informacji, niszczy, uszkadza, usuwa lub zmienia zapis o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji lub funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej albo zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich informacji,

podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

art. 269 § 2.

Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji

[5] A. Adamski: "Przestępstwa komputerowe w nowym kodeksie karnym", Departament Kadr i Szkolenia Ministerstwa Sprawiedliwości 1998,

komputerowej,

c/ przełamanie zabezpieczeń elektronicznych, magnetycznych lub innych specjalnych.

W ujęciu art. 267 § 1 k.k. „otwarcie zamkniętego pisma" , „podłączenie się do przewodu służącego do przekazywania informacji" oraz „przełamanie elektronicznych, magnetycznych albo innych szczególnych zabezpieczeń" nie stanowią już obiektywnych kryteriów naruszenia poufności informacji, lecz charakteryzują sposób uzyskania przez sprawcę informacji, do której nie jest on uprawniony. W konsekwencji, aby przypisać sprawcy winę nie wystarczy, tak jak poprzednio, udowodnić mu np., że bez zgody osoby uprawnionej otworzył on cudze pismo zamknięte, lecz że pismo to otworzył i przeczytał. Podobnie jest z karalnością *hackingu*. Ustawodawca zastosował w tym przypadku zasadę, że jeśli chcesz korzystać z prawnej ochrony poufności informacji, musisz ją najpierw zabezpieczyć. W tym samym kierunku idą zresztą przepisy wykonawcze do dwóch podstawowych w chwili obecnej ustaw chroniących informacje, a mianowicie Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych[1] i ustawy z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych[2]. I choć wydaje się, że ustawy te dotyczą dwóch bardzo różnych dziedzin życia, to jednak w dużym stopniu zakres ich obowiązywania będzie wspólny, a w szeregu przypadkach bardzo zbliżony. Jednocześnie, jako jedne z pierwszych obie ustawy dostrzegły problematykę systemów teleinformatycznych. Wydane do nich rozporządzenia wykonawcze jeszcze bardziej to uwidaczniają[3].

Przepisy kodeksu karnego nie nakładają na użytkowników i administratorów sieci komputerowych obowiązku stosowania zabezpieczeń. Nie przewidują w związku z tym sankcji za zaniechanie ich stosowania. Trzeba jednak pamiętać, że art. 51 i 52 UODO wprowadza odpowiedzialność karną nawet za nieumyślne spowodowanie uchybień w zabezpieczeniu.

Jednocześnie należy sobie zdać sprawę, iż w dobie gospodarki rynkowej, a więc gospodarki konkurencyjnej wzrasta zagrożenie walki o informacje wraz ze wszystkimi konsekwencjami tej walki. Rośnie znaczenie danych finansowych i personalnych we wszystkich instytucjach. Szpiegostwo i wywiad gospodarczy, w tym także między państwami będącymi – formalnie – sojusznikami, stanowi istotną – a niektórzy nawet twierdzą, że główną[4] – część działalności wywiadowczej, „zsyłając" na drugi plan wywiad polityczny i militarny. Należy także pamiętać, że szpiegostwo gospodarcze prowadzą nie tylko państwowe służby specjalne, ale także wywiadownie prywatne, w tym także działające metodami legalnymi. Niewiele osób w Polsce pamięta, że w interesach nie ma emocjonalnej przyjaźni, lecz bezwzględna walka, z której zwycięsko wychodzi ten, kto wyprzedzi lub wykorzysta informacje konkurenta. Przykłady takich zdarzeń w Polsce już mamy. Z jednej z dużych firm branży komputerowej pracownik zabrał pełną bazę danych klientów i w Internecie zaoferował jej sprzedaż.

Karalność nielegalnego podsłuchu i inwigilacji przy użyciu środków technicznych

Art. 267 § 2 k.k.

Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.

[1] Dz. U. 1997, nr 133, poz. 883 – zwana dalej UODO

[2] Dz. U. 1999, nr 11, poz. 95 – zwana dalej UOIN

[3] **Do UODO** – Rozporządzenie MSWiA z dn. 3.06.1998 r. w prawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 1998, Nr 80, poz. 521) - dalej zwane Rozp. UODO

Do UOIN – Rozporządzenie Rady Ministrów z dnia 25.02.1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. z 1999 r., Nr 18, poz. 162) - dalej zwane Rozp. UOIN

[4] Czachowski R., Sienkiewicz P.: Przestępcze oblicza komputerów, PWN Warszawa 1993, Szafrański B.: Omówienie obszarów zagrożenia, wspólna polityka ochrony danych. - Mat. III Forum Teleinformatyki, Legionowo 1997

Większość produktów służących do generowania certyfikatów realizuje przede wszystkim zadania tworzenia, publikacji i zarządzania samymi certyfikatami. Produkty, takie jak Netscape Certificate Server czy Microsoft Certificate Server posiadają narzędzia do publikowania listy wydanych i unieważnionych certyfikatów, jednak usługi realizowane przez te serwery nie spełniają oczekiwań instytucji zainteresowanych korzystaniem z bezpiecznych usług elektronicznych. Ten oczekiwany i niezbędny zakres usług może być realizowany w praktyce wyłącznie wspólnie lub przez Trzecią Zaufaną Stronę(TZS).

Poniższa lista zawiera przykłady usług realizowanych przez TZS :

- system wydawania certyfikatów,
- system publikacji,
- system unieważniania,
- automatyczny update klucza,
- baza danych kluczy,
- baza odzyskiwania i duplikaty kluczy,
- funkcja stemplowania czasem,
- procedury wspierające niezaprzeczalność,
- kros-certyfikacja.

Trzecia Zaufana Strona to instytucja ciesząca się zaufaniem publicznym, wskazana przez wielu użytkowników jako zaufana, ale - co najistotniejsze - nie będąca stroną ich transakcji elektronicznych. Poza zaufaniem i niezaangażowaniem w transakcje, TZS musi posiadać możliwości finansowe utworzenia niezbędnych struktur realizujących politykę certyfikacji. Zupełnie podstawową, z punktu widzenia każdego klienta TZS, jest również możliwość fizycznego zabezpieczenia procesów: obrotu kluczem i certyfikatem elektronicznym. W tym zakresie podstawą działania TZS jest prawidłowo przygotowana i realizowana polityka bezpieczeństwa.

Wybierając produkty pamiętajmy, że nie wszystkie zalecenia i rozwiązania wspaniale działające w innych miejscach, sprawdzą się w naszych warunkach. Dobry serwis, możliwość szkoleń i testowania rozwiązań, a także pewność, że znalezione błędy zostaną szybko poprawione, a uzupełnienia zostaną nam przesłane - to podstawowe elementy, na które musimy zwracać uwagę decydując się na współpracę z firmami.

Jest jeszcze jeden ogromnie ważny aspekt sprawy, o którym często zapominamy słuchając marketingowych wywodów przedstawicieli zagranicznych firm. Jeżeli chcemy „panować" nad bezpieczeństwem ochranianego przez nas systemu, musimy sami stworzyć klucz i zamek do „sejfu zawierającego informacje", który zbudowaliśmy wspólnie ze wszystkimi naszymi partnerami. Bez tego może się zdarzyć, że informacje drukowane przez nasze drukarki lub przesyłane w naszych sieciach z zachowaniem wszystkich zasad „sztuki zabezpieczeń", będą w tym samym momencie co u nas „wychodzić" z drukarek na innym kontynencie. Również w tym zakresie ścisła współpraca z TZS może zaoszczędzić wydatków i podnieść bezpieczeństwo zrealizowanego rozwiązania.

Namawiam więc do: kompleksowego oceny bezpieczeństwa systemów informacyjnych i stałego uzupełniania zabezpieczeń. Są to inwestycje, które oszczędzą rozczarowań i strat.

Pomimo wielu zastrzeżeń, namawiam do korzystania z doświadczeń i wiedzy polskich firm – szczególnie jeżeli budowane rozwiązania będą wymagały współpracy z TZS. Mam co najmniej dwa przemawiające za tym i trudne do obalenia argumenty. Budowanie bezpieczeństwa systemów informacyjnych przez firmy zagraniczne, których rzeczywistych powiązań i intencji nigdy nie będziemy w stanie skontrolować, jest jak wpuszczanie „wilka między owce". Po drugie, cena proponowanych przez nie kompleksowych rozwiązań jest z reguły przerażająca - stąd pogląd o ogromnych kosztach zabezpieczania systemów lub prowadzenia bezpiecznych transakcji. Ponadto, przyjmując zagraniczne rozwiązanie, którego prawdziwe funkcje zna tylko twórca, nigdy nie będą Państwo mieli pewności i pełnej kontroli zabezpieczenia swoich informacji.

Kompleks przepisów prawnych, tworzonych od pewnego czasu w Polsce, na który składa się poza wspomnianą, również ustawa o ochronie danych osobowych i nowy Kodeks karny oraz funkcjonujące przepisy branżowe, wskazują na przynajmniej częściowy sukces środowisk informatycznych, od prawie trzech lat promujących tę tematykę. Na jedno z wcześniej postawionych pytań już teraz możemy odpowiedzieć: faktem stało się prawne usankcjonowanie kompleksowego, globalnego spojrzenia na bezpieczeństwo systemów informacyjnych jako pierwszego z elementów prawidłowo rozpoczętej analizy zabezpieczenia każdego systemu.

Przygotowując analizę zabezpieczenia informacji i systemów informacyjnych, trzeba pamiętać, że - wbrew niektórym opiniom - w każdej instytucji, przedsiębiorstwie czy uczelni są informacje stanowiące tajemnice. Wynika z tego, że chronić należy nie tylko dane i systemy ale także ludzi, którzy mają bezpośredni dostęp do „wrażliwych informacji", a wszystko po to, aby ponoszone przez nas nakłady i wysiłki przynosiły oczekiwane efekty, a nie padały łatwym łupem elektronicznych włamywaczy.

Organizacje, które zawodowo zajmują się uzyskiwaniem informacji twierdzą, że rozprzestrzenianie się chronionej informacji postępuje według prostej zasady zwanej jedynkową - zapewne dla odróżnienia od systemu „dwójkowego". Jeżeli jedna osoba zna informację, informacja ta jest w pełni bezpieczna. Jeżeli do danej informacji mają dostęp dwie osoby, to zna ją już jedenaście osób, jeżeli trzy - to sto jedenaście itd.. Nie słyszałem o prowadzeniu badań nad tą prawidłowością, ale niestety sprawdza się ona w praktyce, a fakt ten dla bezpieczeństwa systemów informacyjnych ma zasadnicze znaczenie.

Natychmiast pojawia się kolejne pytanie: czy koniecznie wszystko musimy sami wymyślać i czy całość systemu i prac związanych z jego zabezpieczeniem musimy wykonać sami lub siłami własnego zespołu? Oczywiście, że nie! Jak jednak pogodzić dwa, wydaje się nie do pogodzenia, wymagania: bezpieczeństwo systemu i stały, często niemożliwy do pełnej kontroli, dostęp osób z zewnątrz. W polskich warunkach nie będzie to proste, ale planując działania związane z bezpieczeństwem naszych systemów, starajmy się nawiązywać współpracę z osobami i firmami, które spełniają dwa podstawowe warunki : są wiarygodne i gwarantują maksymalną poufność prowadzonych działań. Dlaczego te dwa czynniki są takie ważne? Otóż, nasz system będzie na tyle dobrze zabezpieczony, na ile wiedza o nim, o jego mechanizmach, funkcjach, wreszcie konkretnych programach i osobach, które go budowały i chronią, pozostanie w naszych rękach.

Okazuje się, że ochronę informacji można zrealizować wieloma sposobami. Jedną z metod zabezpieczania informacji stosowaną od najdawniejszych czasów, jest jej odpowiednie rozdrobnienie i ukrycie elementów istotnych wśród podobnych, ale nieistotnych. Tylko osoba posiadająca właściwy klucz może odczytać ukrytą treść. Taka zaufana osoba lub w przypadku dużych organizacji, zespół osób, powinien w każdej organizacji odpowiadać za kompleksowe bezpieczeństwo systemów. Należy tu podkreślić wspomnianą kompleksowość spojrzenia na bezpieczeństwo systemu rozumianego jako system informacyjny przedsiębiorstwa, a nie jego system informatyczny. Z tytułu ponoszonej odpowiedzialności i z uwagi na zakres działania, konieczne jest bezpośrednie podporządkowanie osób lub zespołu, odpowiedzialnego za bezpieczeństwo informacji, kierownictwu przedsiębiorstwa.

Przepisy i wytyczne w powyższym zakresie, w odniesieniu do informacji niejawnych, zawierają w szczególności rozdziały 10 i 11 ustawy o ochronie informacji niejawnych oraz rozporządzenie Prezesa Rady Ministrów z 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych.

Dlaczego dwa wcześniej wspomniane warunki wiarygodności i poufności partnerów są tak istotne i dlaczego wybór wykonawców nie będzie łatwy? Przede wszystkim, nadal brak w Polsce instytucji oraz mechanizmów licencjonowania i certyfikowania firm i osób zajmujących się zabezpieczaniem systemów informacyjnych. Koszt utworzenia i działania takich organizacji jest jednym z tych nakładów, które przynajmniej w części, musi ponieść państwo. Niestety, świat nie będzie chciał się z nami komunikować i wymieniać informacji, jeżeli instytucje i mechanizmy Trzeciej Zaufanej Strony nie zaczną w Polsce działać, i to jak najszybciej. Ponadto, tylko nadanie pewnego „statusu zaufania" w postaci elektronicznego certyfikatu, pozwoli każdemu z nas,

- ☞ Rozporządzenie w §10 określa SOP jako właściwe do potwierdzenia przydatności algorytmów i środków ochrony
- ☞Rozporządzenie w § 4 umożliwia uznanie przez SOP certyfikatów wydanych w innych państwach NATO

Problemy praktyczne. Wybór środków i metod zabezpieczeń.

❖ Wybór technicznych środków i metod zabezpieczeń - specjaliści (doświadczenie) + kierownik JO (możliwości finansowe) + zalecenia SOP

- ochrona kryptograficzna
- ochrona elektromagnetyczna
- mechanizmy ochrony fizycznej

❖ Zabezpieczenia administracyjne i fizyczne - najtańsze

❖ Można korzystać z wielu istniejących standardów GMITS, BS7799 ,ITBM, FIPS

Problemy praktyczne. Co szyfrować ?

❖ Przepisy nie nakazują kryptograficznej ochrony IN stanowiących tajemnice służbową przekazywanych w systemach i sieciach TI

A L E

☞ IN mogą być udostępnione wyłącznie osobom uprawnionym art. 20, ust 1

☞ IN muszą być .... przetwarzane... w warunkach uniemożliwiających ich nieuprawnione ujawnienie art. 20 ust 2

☞ Pełnomocnik ochrony zawiadamia SOP o przypadkach naruszenia przepisów ochrony IN o klauzuli poufne lub wyższej

---

Większość najbardziej znamiennych osiągnięć z dziedziny elektroniki oraz informatyki można porównać do broni obusiecznej. Z jednej strony otrzymujemy doskonałe narzędzia ułatwiające wyszukiwanie danych, ich gromadzenie, przetwarzanie oraz szybkie przesyłanie na dowolne odległości. Z drugiej zaś strony dowiadujemy się – zazwyczaj ze znacznym opóźnieniem – o różnych możliwościach kontroli, modernizacji lub niszczenia danych przetwarzanych w tychże systemach.

Minął już okres kiedy sprzęt i oprogramowanie były najcenniejszymi elementami systemu teleinformatycznego. Aktualnie najistotniejszym elementem systemu teleinformatycznego są zgromadzone, przetwarzane lub przesyłane informacje. Dlatego też dane – elementy składowe informacji - są jedynym bezpośrednim dobrem chronionym w systemie lub sieci teleinformatycznej. Hasła dostępu, łącza, algorytmy i klucze szyfrowe itp. to tylko pośrednie obiekty podlegające ochronie.

- Jeśli w systemie są tylko IN stanowiące tajemnicę służbowa to nie wniesienie przez SOP zastrzeżeń do SWBS w terminie 30 dni uprawnia do eksploatacji systemu TI - art. 61, ust. 3 (przejścia do następnego etapu tworzenia systemu)
  - ❖ Jeśli w systemie są IN stanowiące tajemnicę państwowa to SOP zatwierdza SWBS w terminie 30 dni - art. 61
  - ❖ Zatwierdzenie SWBS dla systemów w których znajduje się tajemnica państwowa jest podstawą wydania certyfikatu *akredytacji*, ale konieczna jest jeszcze:
    - ☞ ocena rzeczywistych zdolności systemu do ochrony IN - art. 62, ust. 2, p. 1 (audyt)
  - ❖ Możliwość odrzucenia SWBS (SWBS powinny być kompletnym i wyczerpującym opisem ich budowy, zasad działania.i eksploatacji... Art. 60, ust 3).
- Eksploatacja systemu TI
  - – administrator systemu art. 63, ust 1, p. 1
  - – pracownik pionu ochrony art. 63 ust 1 p. 2 - Inspektor bezpieczeństwa teleinformatycznego
- Konieczność uzyskania poświadczeń bezpieczeństwa w trybie art.18 ust. 5 (art. 64)
- Specjalistyczne szkolenie w SOP - art. 64

Stanowiska związane z systemem TI

- Kompatybilność z NATO i UZE wymaga określenia następujących stanowisk związanych z zapewnieniem bezpieczeństwa systemów TI
  - ☞ inspektor bezpieczeństwa teleinformatycznego (*centrala)*
  - ☞ lokalni inspektorzy bezpieczeństwa TI *(oddziały, filie, departamenty)*
  - ☞ inspektor ochrony elektomagnetycznej
  - ☞ administrator materiałów kryptograficznych
- Pewne stanowiska można łączyć
- Zalecenia SOP w zakresie ochrony kryptograficznej i elektromagnetycznej określą szczegółowo zadania

Tajemnica państwowa w systemach TI

- ❖ Załącznik do ustawy - wykaz rodzajów informacji niejawnych stanowiących tajemnicę państwową:
  - ☞ cz. II p. 10 (informacje dotyczące. ... systemów TI służących do przekazywania tajemnicy państwowej...)
  - ☞ cz. III p.6 (informacje o ...transportach wartości pieniężnych o wartości przekraczających ..500 tys. Euro)
  - ☞ cz. III p.16. (informacje dotyczące rozwiązań technicznych, technologicznych i organizacyjnych, których ujawnienie naraziłoby na szkodę ważny interes gospodarczy państwa)
- ❖ W wielu instytucjach IN stanowiących tajemnicę państwową jest mało bądź nie ma w ogóle !
- ❖ W każdej państwowej JO są IN, które powinny mieć klauzulę „poufne" bądź „zastrzeżone" !

Rozporządzenie Prezesa RM w sprawie określenia podstawowych wymagań bezpieczeństwa systemów i sieci TI 1/6

- Bezpieczeństwo teleinformatyczne:
  - ☞ ochrona fizyczna (strefy bezpieczeństwa, środki zabezpieczające pomieszczenia) - §5
  - ☞ ochrona elektromagnetyczna (strefy bezpieczeństwa lub urządzenia o obniżonej emisji lub ekranowanie) - §7

USTAWA O OCHRONIE INFORMACJI I JEJ KONSEKWENCJE W SIECIACH KOMPUTEROWYCH

Brunon Czabok – Zastępca Dyrektora

Biuro Bezpieczeństwa Łączności i Informatyki

Ustawa z 22 stycznia 1999 r. nie wyróżnia sieci telekomunikacyjnych, informatycznych, czy komputerów indywidualnych. Określenie „sieci telekomunikacyjne" występuje tylko w załączniku nr 1 zawierającym wykaz rodzajów informacji niejawnych stanowiących tajemnicę państwową, w którym jako informacje niejawne oznaczone klauzulą tajne ze względu na obronność i bezpieczeństwo państwa oraz porządek publiczny możemy znaleźć :

II. [...]

9. *Organizacja kompleksowego przygotowania jednolitej* ***sieci telekomunikacyjnej*** *państwa dla potrzeb obronnych.*
10. *Informacje dotyczące przygotowania, budowy, zarządzania oraz funkcjonowania systemów i 10.* ***sieci telekomunikacyjnych****, teleinformatycznych i pocztowych służących do przekazywania informacji niejawnych stanowiących tajemnicę państwową, wykorzystywanych dla potrzeb Sił Zbrojnych, służb ochrony państwa lub administracji publicznej w zakresie niezbędnym do zabezpieczenia tych systemów i sieci.*

W pozostałych przypadkach ustawodawca używa określeń o znacznie szerszym zakresie znaczeniowym, a mianowicie :

- ***system teleinformatyczny*** *- który tworzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji,*
- ***sieć teleinformatyczna*** *- organizacyjne i techniczne połączenie systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi.*

Z powyższych definicji wynika, że tytułową sieć telekomunikacyjną należy traktować jako sieć teleinformatyczną. W przypadku gdy sieć służy do przekazywania informacji niejawnych musi ona spełniać wymogi bezpieczeństwa. Zasady tworzenia polityki bezpieczeństwa oraz konkluzje prawne wynikające z Ustawy o ochronie informacji niejawnych oraz wydanego na jej podstawie Rozporządzenia Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych pokrótce obrazuje poniższa prezentacja.

Polityka bezpieczeństwa i system zabezpieczeń

❖ Polityka bezpieczeństwa - zestaw praw, reguł i praktycznych zasad określających, jak informacje oraz pozostałe aktywa są zarządzane, chronione oraz udostępniane

❖ System zabezpieczeń - administracyjne, fizyczne i techniczne środki i metody zapewniające poufność, integralność, dostępność danych, rozliczalność, audyt oraz ochronę innych aktywów systemu - sprzętu, kadr i dokumentów

Megatrend wyzwań intelektualnych

Wreszcie za trzeci megatrend zasadniczy można uznać wielkie wyzwania co do sposobu pojmowania świata, niesione przez cywilizację informacyjną. *Mechaniczny sposób pojmowania świata* - jako wielkiej maszyny, kręcącej się z nieuchronnością koła zamachowego - *zastąpiony będzie sposobem nowym, systemowo-chaotycznym*, traktującym świat jako wielki a złożony system dynamiczny, w którym można zaobserować pewne prawidłowości, ale bardzo prawdopodobne jest również zachowania chaotyczne, w którym wszystko może się wydarzyć. To, co wydawało się naturalne przy starym sposobie pojmowania świata, może być łatwo zakwestionowane w cywilizacji informacyjnej. Dotyczy to przy tym zagadnień całkiem podstawowych - pojmowania rynku, demokracji, praw człowieka itp.

Trzeba przy tym pamiętać, że podstawą cywilizacji informacyjnej jest dobrze działający, rozwinięty rynek. Na przykład, zmiany strukturalne wywołane postępem cywilizacji informacyjnej wymagają elastyczności i innowacyjności, a więc także intensywnej konkurencji rynkowej. Dlatego też rozwój cywilizacji informacyjnej odbywa się często na drodze liberalizacji rynków - np. telekomunikacyjnych. Zbyt silne działanie opiekuńcze państwa może być niesprzyjające innowacyjności. Nie oznacza to jednak, że wszystko można załatwić poprzez liberalny lesseferyzm; jak wykażemy niżej, zbyt słabe działanie regulacyjne państwa na rynkach nowych technologii może z kolei doprowadzić do poważnego kryzysu samych podstaw gospodarki rynkowej.

Popularna jest w Polsce - szczególnie dzisiaj - zasada *wolności rynku, nieinterwencjonizmu,* czyli liberalne przeświadczenie o tym, że rynek działa najlepiej, jeśli się go zostawi samemu sobie. Stosując metody teorii gier do teorii rynku można wykazać, że przeświadczenie to jest wprawdzie uzasadnione, ale przy dwóch bardzo poważnych założeniach. Pierwsze z tych założeń dotyczy liczby producentów, która powinna być dostatecznie duża; rynek nie poradzi sobie sam z monopolistami, którzy go zdominują, potrzebna jest regulacja antymonopolistyczna. Drugie założenie dotyczy stabilności równowagi rynkowej: po niewielkich odchyleniach od równowagi, mechanizm rynkowy powinien sam do niej powracać, nie może w sobie zawierać elementów wywołujących destabilizację równowagi.

Źródłem poważnych zagrożeń dla gospodarki rynkowej w początkach cywilizacji informacyjnej może stać się fakt, że wymienione powyżej dwa założenia sprawnego działania rynku nie muszą być automatycznie spełnione na rynkach związanych z nową technologią, zwłaszcza z technikami informacyjnymi. Jest wiele znanych przykładów[2] wykorzystywania nowych technologii dla monopolizacji rynku, a także aktualnych przykładów samorzutnego powstawania monopolu na światowych rynkach oprogramowania. Mniej oczywisty jest fakt, że rynki z udziałem nowych technologii mogą być wewnętrznie niestabilne.

Przytoczymy tu więc przykład największego dziś na świecie rynku - operacji i spekulacji finansowych. Rynek ten rozwinął się znacznie w ostatnim dziesięcioleciu właśnie dzięki sieciom komputerowym i systemom wspomagania decyzji, możliwości bardzo szybkiego przekazywania i przetwarzania dużej liczby informacji finansowych. Operacje finansowe spekulacyjne przekraczają już ponad stukrotnie swym wolumenem operacje finansowe rzeczowe, czyli związane z handlem międzynarodowym. Jednocześnie, szybkie przekazywanie dużych zbiorów danych i szybkie ich przetwarzanie, a zwłaszcza konstrukcja dedykowanych systemów wspomagania decyzji są kosztowne; najwięksi gracze na tym rynku inwestują duże sumy w te narzędzia. Inwestycje te pozwalają największym graczom mieć szybszą informację, a więc sporo zyskać na operacjach finansowych, ale pod jednym warunkiem: jeśli na rynku wystąpią znaczne zmiany lub niestabilności. Można tu więc zadać

[2] Łącznie z najbardziej aktualnymi, jak metody zabezpieczania pozycji rynkowej dla oprogramowania wytwarzanego przez największych producentów.

zmian w kierunku cywilizacji informacyjnej i określające pewne trendy pochodne - które jednak same mają też charakter megatrendów, t.j. mają duże znaczenie społeczne i będą obserwowane jeszcze prawdopodobnie przez dziesięciolecia:

a) Ponieważ *adaptacyjność ludzka jest ograniczona,* kształtowanie się nowych zawodów i zmiany systemów edukacyjnych niezbędne dla wprowadzania tych nowych zawodów są najważniejszym czynnikiem społecznym ograniczającym szybkość rozwoju społeczeństwa czy cywilizacji informacyjnej.

b) Ponieważ gospodarka rynkowa opiera się na dostatecznie dużej liczbie dość dobrze zarabiających konsumentów, którzy decydują o popycie rynkowym, nie sposób jest ograniczyć społeczeństwo informacyjne tylko do tej (z natury niewielkiej) części populacji, która jest dostatecznie adaptacyjna i umie się szybko nauczyć nowych technik informacyjnych. Warunkiem powodzenia cywilizacji informacyjnej jest więc *innowacyjność ludzka w wynajdywaniu nowych zawodów,* które pozwolą na zatrudnienie większości, a nie tylko małej części populacji w gospodarce wiedzą.

c) Ponieważ czekające nas zmiany zawodów będą bardzo głębokie, można przewidywać *kilka dziesięcioleci wzrastającego popytu na edukację* - wszystkich szczebli, ale w szczególności edukację wyższą i *podyplomową edukację ustawiczną.* Razem z innymi, dyskutowanymi niżej megatrendami technicznymi, wyrażać się to będzie w *megatrendzie multimedialnej edukacji zdalnej i ustawicznej.*

Megatrend integracji technicznej

Druga z tendencji zasadniczych to ***megatrend zbieżności (convergence) lub integracji technicznej*** - dotyczący mediów, sposobów i systemów przekazu i przetwarzania informacji. Zawiera on w sobie powszechną *cyfryzację* tych sposobów przekazu lub przetwarzania, tendencje do wykorzystania *komunikacji multimedialnej,* tendencje do zapewnienia *telekomunikacji mobilnej* (których tylko jednym z przejawów jest popularność telefonii komórkowej), tendencje do *szybkiego zwiększania przepływności* czyli szybkości transmisji w sieciach telekomunikacyjnych, tendencje do *integracji nowych usług telematycznych* w złożone systemy usługowe, itd. Omówimy tu tylko kilka tendencji pochodnych lub szczegółowych związanych z tym wielkim megatrendem.

a) Należy przewidywać - prawdopodobnie już w ciągu najbliższego dziesięciolecia lub dwóch - nie tylko powstanie (początki istnieją już dzisiaj) ale rozpowszechnienie *globalnego, zintegrowanego systemu mobilnej łączności cyfrowej,* łączącego w sobie elementy telekomunikacji kablowej i radiowej, tradycyjne usługi telefoniczne i nowoczesne usługi sieci komputerowej, multimedialne usługi telekomunikacyjne i funkcje rozsiewcze (radiowe, telewizyjne). Pełne rozpowszechnienie i wykorzystanie takiego systemu w skali całej kuli ziemskiej może być przy tym dodatkowo opóźnione poprzez czynniki ekonomiczne i społeczno-kulturowe (a nawet - w niektórych krajach - polityczne). Jeśli nawet w Polsce trudno spodziewać się aktywnych prac badawczo-rozwojowych nad techniką takiego systemu a zwłaszcza ich wdrożeń, to jednak musimy zainwestować w badania w tej dziedzinie chociażby po to, by nie stracić własnych źródeł ekspertyzy, niezbędnych na rynkach o szybko zmieniających się technologiach.

b) Należy przewidywać - w związku z wykorzystaniem technik łączności światłowodowej dla zwiększenia przepływności i ograniczeniami szybkości przetwarzania w urządzeniach elektronicznych - pełniejszą *integrację fotoniczną urządzeń i systemów przekazu i przetwarzania informacji.* Oznacza to w szczególności konieczność intensyfikacji prac badawczych i badawczo-rozwojowych w zakresie fotoniki oraz wykorzystania współpracy