Ochrona informacji i sieci telekomunikacyjne - symbioza z konieczności

mgr inż. Krzysztof Szczypiorski
e-mail: K.Szczypiorski@tele.pw.edu.pl
Instytut Telekomunikacji Politechniki Warszawskiej

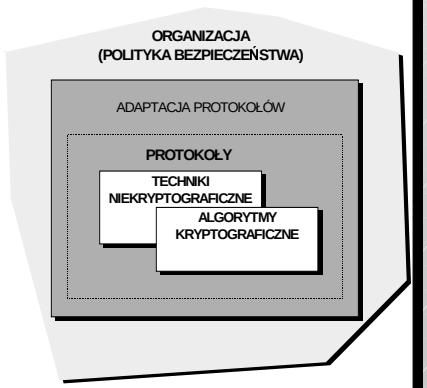
ENIGMA'98 - II Krajowa Konferencja Zastosowań Kryptografii
Warszawa, 26-28 maja 1998 r.

Plan prezentacji

- podstawowe problemy
- budowa sieci telekomunikacyjnej i jej model; modele komunikacji
- klasyfikacja zagrożeń
- zarządzanie ochroną informacji w sieciach telekomunikacyjnych
- rola Internetu w kształtowaniu kierunków zabezpieczeń sieci telekomunikacyjnych
- algorytmy kryptograficzne i protokoły - wyzwania
- przyszłość

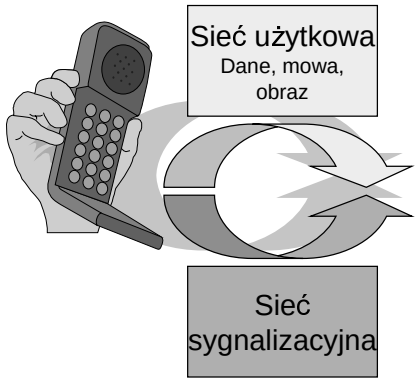
Podstawowe problemy

- sieci telekomunikacyjne + systemy informatyczne = **systemy informacyjne**
- jak spoglądać na ochronę informacji z punktu widzenia telekomunikacji?
- „światy” w telekomunikacji



• podejście geograficzne
• zbiorowość Internetu a reszta świata (stosunek do normalizacji)

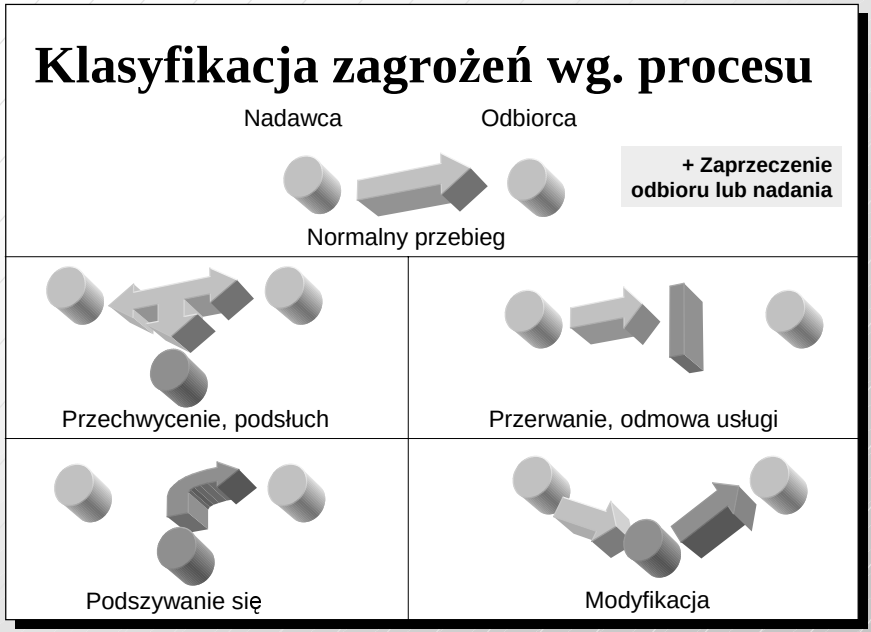
Budowa sieci telekomunikacyjnej



- różnorodna architektura
- wiele standardów
- wiele usług
- różnorodność abonentów
- różne wymagania na szybkość, jakość
- wielu operatorów

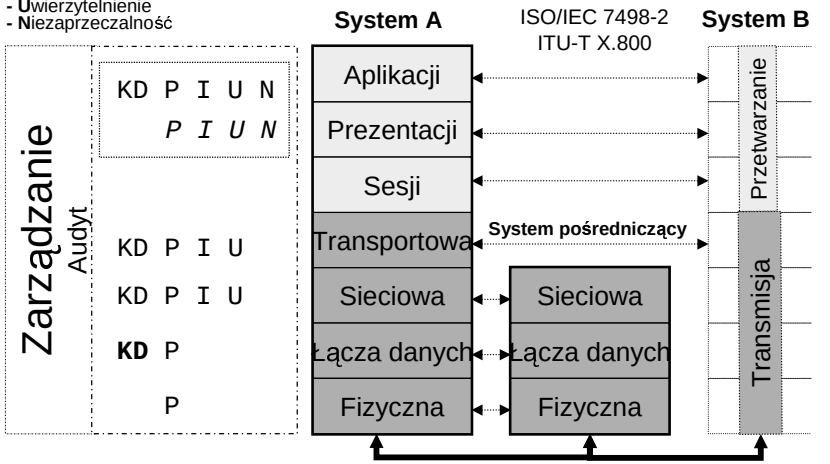
- wyzwania dot. algorytmów, protokołów i zarządzania

Klasyfikacja zagrożeń wg. procesu



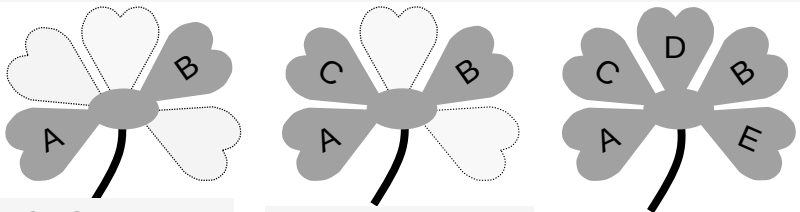
Model sieci a usługi ochrony informacji

Podstawowe usługi:
- **K**ontrola **D**ostępu
- **P**oufność
- **I**ntegralność danych
- **U**wierzytelnienie
- **N**iezaprzeczalność



Modele komunikacji - realizacja usług ochrony informacji

Problemy: z poufnością, integralnością z użyciem funkcji kluczowanych, uwierzytelnieniem względem grupy (ogólnie z zarządzaniem kluczami)



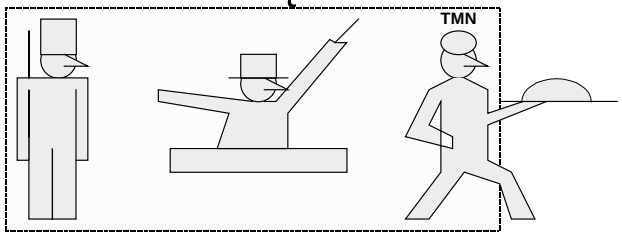
UNICAST
- dwa obiekty
- podejście klasyczne (system asymetryczny)
- rozmowa telefoniczna, praca w sieci (klient - serwer)

MULTICAST
- grupa
- dynamiczne dołączanie/odłączanie
- obliczenia równoległe, sieci ruchome, kablowe

BROADCAST
- „wszyscy”
- trywialne po rozstrzygnięciu ochrony multicastu

Zarządzanie ochroną informacji w sieciach telekomunikacyjnych

Zarządzanie

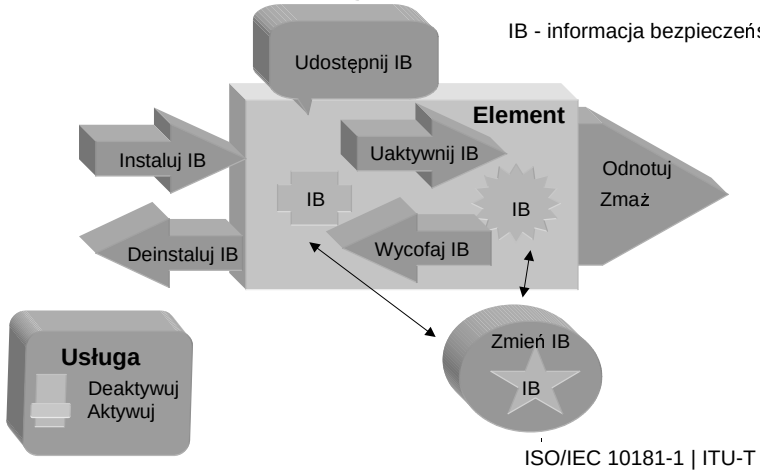


Bezpieczeństwo zarządzania | **Zarządzanie bezpieczeństwem** | **Świadczenie usług bezpieczeństwa**

Bezpieczeństwo

Zarządzanie usługami, kluczami i polityką bezpieczeństwa

Zarządzanie generyczną usługą ochrony informacji



ISO/IEC 10181-1 | ITU-T X.810

Rola Internetu

- zbiorowość Internetu - największy wpływ na rozwój i kształtowanie trendów w dziedzinie bezpieczeństwa sieci
- powody:
  - brak standaryzacji
  - otwarte grupy dyskusyjne
  - szybkie wdrażanie i ocena
  - łatwa i tania dystrybucja oprogramowania oraz dokumentacji
- The Internet Engineering Task Force (IETF) - WG - Security Area
  - An Open Specification for Pretty Good Privacy (openpgp)
  - Authenticated Firewall Traversal (aft)
  - Common Authentication Technology (cat)
  - Domain Name System Security (dnssec)
  - IP Security Protocol (ipsec)
  - One Time Password Authentication (otp)
  - Public-Key Infrastructure (X.509) (pkix)
  - S/MIME Mail Security (smime)
  - Secure Shell (secsh)
  - Simple Public Key Infrastructure (spki)
  - Transport Layer Security (tls)
  - Web Transaction Security (wts)

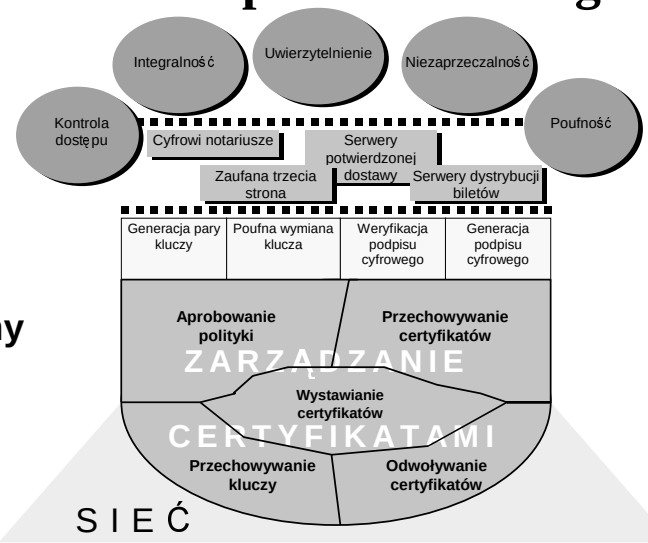
Algorytmy kryptograficzne i protokoły

- algorytmy (szyfry i funkcje skrótu) wraz z innymi mechanizmami niekryptograficznymi tworzą protokoły, które z kolei realizują wybrane usługi
- szybkość sieci (kbit/s - Mbit/s - Gbit/s)
- nowe algorytmy? nowe technologie? układy równoległe?
- problemy synchronizacji (High Speed Data Networks, sieci ruchome)
- dystrybucja klucza:
  - system hybrydowy
  - „podwójny” system hybrydowy (Master Key + Secret Key)
- problemy prawne

Przyszłość

- jaka będzie przyszłość zarządzania kluczami - czy PKI zjednoczy usługi ochrony informacji w sieciach?
- czy więcej protokołów sieciowych będzie zintegrowanych z ochroną informacji?
- czy więcej produktów będzie miało kryptograficzne wsparcie (rozwiązania producentów, CAPI)?
- czy tzw. produkty pierwszej generacji zabezpieczeń - firewalls znikną po wprowadzeniu nowych protokołów sieciowych wyposażonych w mechanizmy kryptograficzne?
- czy Internet nadal będzie wyznaczał kierunki zabezpieczeń?
- czy rynek sieci ruchomych wpłynie na rynek sieci stałych?

Globalna PKI - platforma usług



Problemy

Podsumowanie

- integracja protokołów sieciowych z ochroną informacji jest naturalnym, chociaż powolnym procesem (Internet, GSM/DCS)
- należy tworzyć (kupować) systemy / produkty „zarządzalne”
- ograniczenia dotyczące szybkości algorytmów i efektywności protokołów
- świadomość rozwoju ataków, starzenia się rozwiązań, dojrzewania cyber-młodzieży
- wpływ środowiska Internetu
- prywatność - potrzeba abonentów - sensowny katalizator zmian?

KONIEC

Czy mają Państwo pytania?