



III Krajowa Konferencja Bezpieczeństwa Biznesu 2004

Bezpieczeństwo VoIP

Część I:

Podstawy VoIP oraz bezpieczeństwo protokołów sygnalizacyjnych

Wojciech Mazurczyk

Instytut Telekomunikacji, Politechnika Warszawska

E-mail: W.Mazurczyk@elka.pw.edu.pl

Miedzeszyn, 23 listopad 2004



Plan prezentacji części I

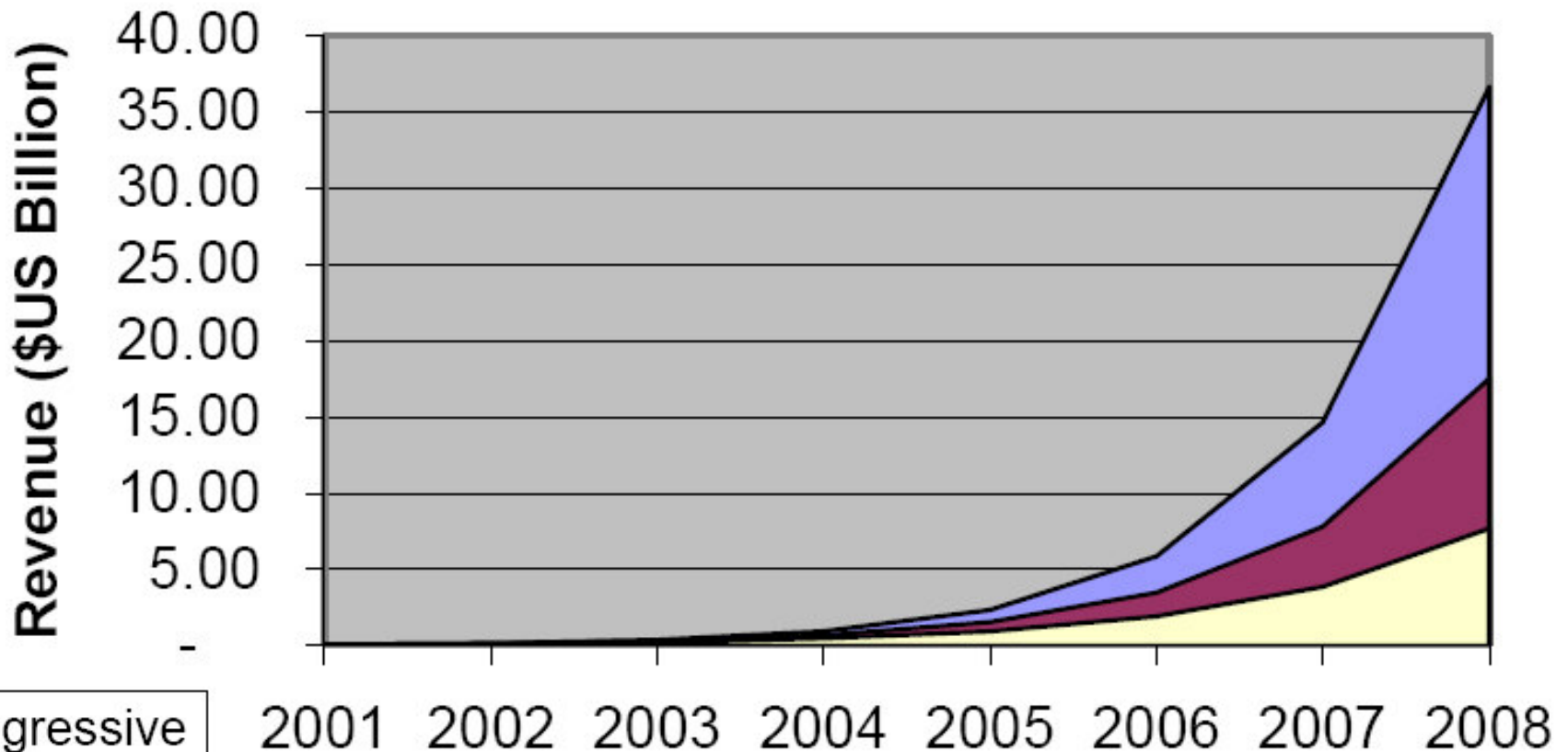
- Co to jest *Voice over Internet Protocol* ?
- Podstawowe pojęcia oraz ogólna idea działania
- Czynniki wpływające na jakość telefonii IP
- Dostępne protokoły sygnalizacyjne dla VoIP: SIP, H.323 oraz H.248/Megaco
- Problemy bezpieczeństwa VoIP
- Bezpieczeństwo protokołów sygnalizacyjnych

Co to jest VoIP?

- **VoIP** = usługa przesyłania głosu w czasie rzeczywistym z wykorzystaniem sieci IP
- Dotychczasowe sieci transmisji danych **nie** są wystarczające dla VoIP!
- Dlaczego usługa VoIP jest atrakcyjna?



Prognozy dla VoIP



- Aggressive
- Moderate
- Pessimistic

Źródło: ABI Research



Możliwości wdrożenia VoIP

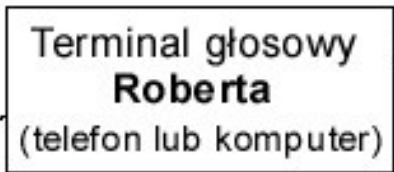
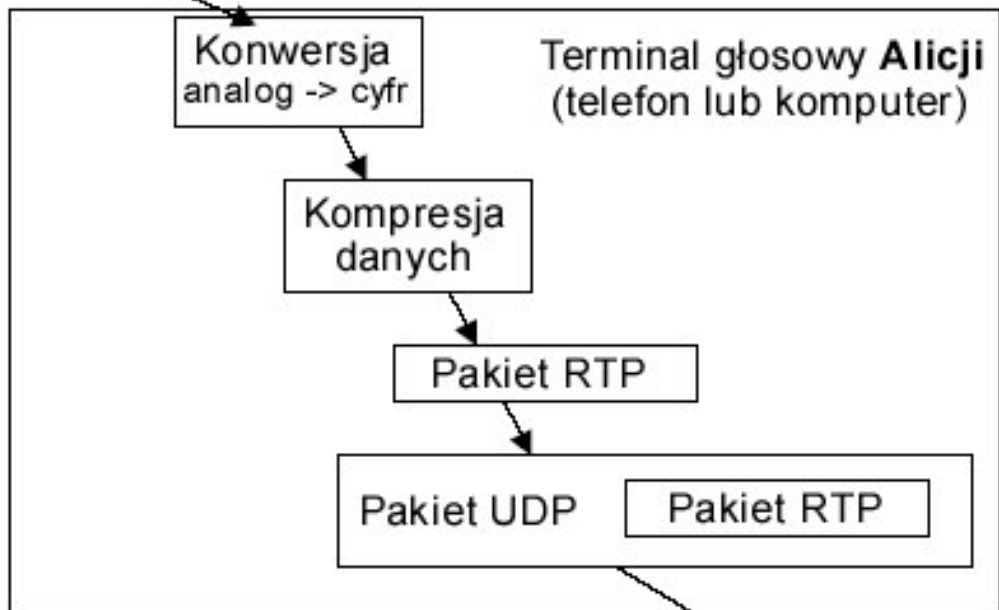
- Różne scenariusze dla różnych sytuacji początkowych:
 - **łączenie istniejących central telefonicznych poprzez sieć IP** (własną lub Internet)
 - **budowana jest nowa infrastruktura komunikacyjna**
 - **eksploatowana centrala zostaje zastąpiona** (np. ze względu na jej zużycie techniczne) lub uzupełniona systemem IP



Połączenie w telefonii IP

- Podział nawiązywania połączenia na dwie fazy:
 - **sygnalizacyjną** – kontrolującą sesję
 - **transportu strumienia danych**
- **Połączenie** = określony stan sygnalizacji pomiędzy urządzeniami końcowymi + przepływ głosu

Ogólny sposób transportu głosu w VoIP



Grupy protokołów dla VoIP

- Protokoły umożliwiające realizację telefonii IP (zespół protokołów):

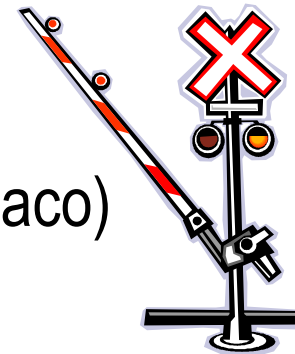
- Kodeki mowy (np. G.723.1)



- Protokoły transportowe (RTP, UDP, TCP)



- **Protokoły sygnalizacyjne**
(SIP, H.323, MGCP, H.248/Megaco)



- Protokoły uzupełniające (SDP, RTCP, RSVP)

Czynniki wpływające na QoS (1/2)

- Opóźnienie (*ang. Latency*)

Delay Source (G.729)	On-net Budget (ms)
Device Sample Capture	0.1
Encoding Delay (Algorithmic Delay + Processing Delay)	17.5
Packetization/ Depacketization Delay	20
Move to Output Queue/Queue Delay	0.5
Access (up) Link Transmission Delay	10
Backbone Network Transmission Delay	Dnw
Access (down) Link Transmission Delay	10
Input Queue to Application	0.5
Jitter Buffer	60
Decoder Processing Delay	2
Device Playout Delay	0.5
Total	121.1 + Dnw

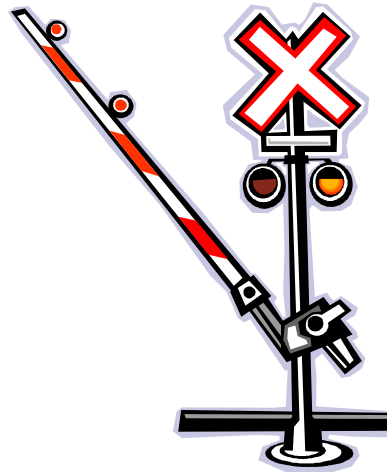


Czynniki wpływające na QoS (2/2)

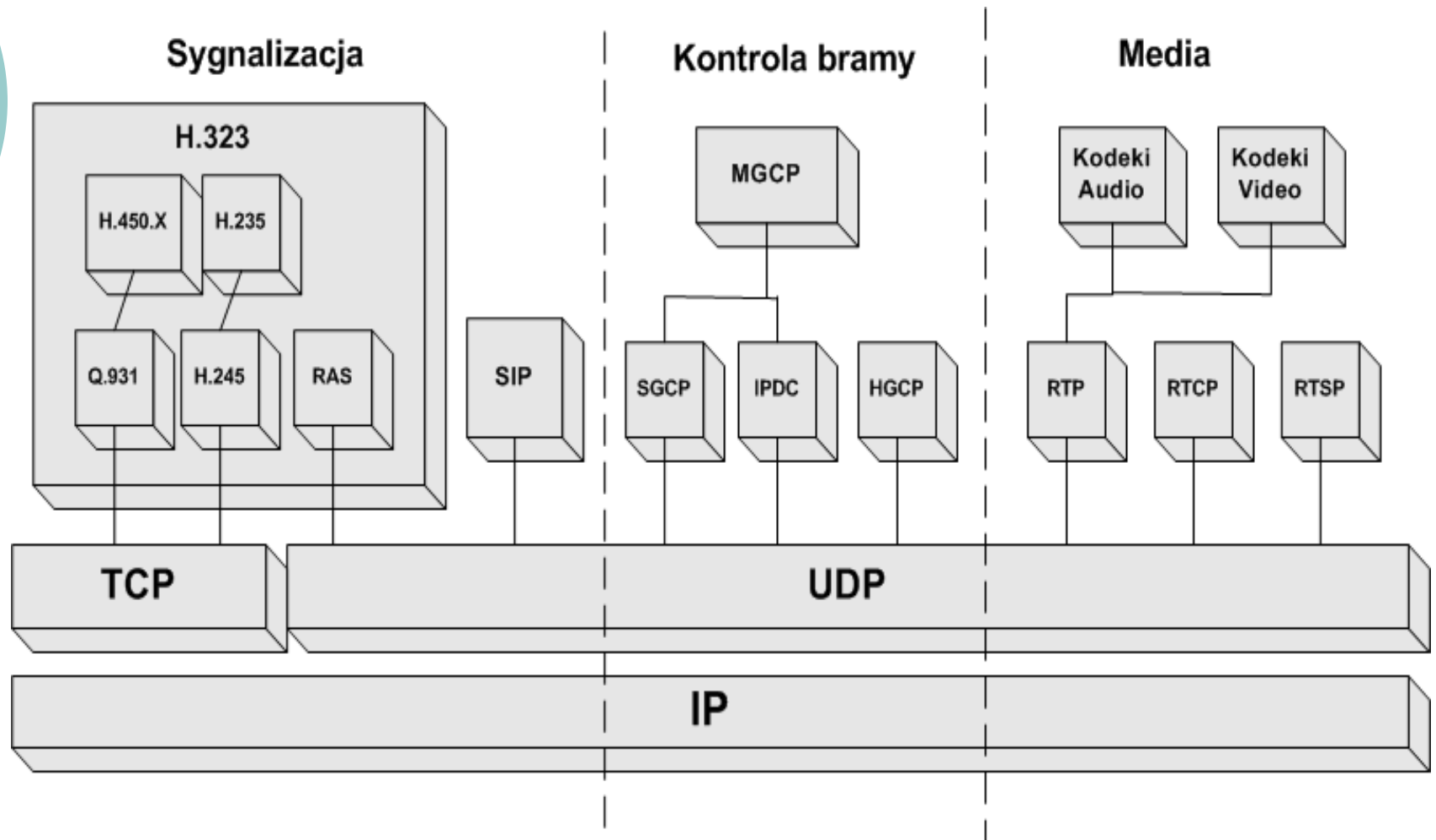
- **Jitter (wariancja opóźnienia)** – transport pakietów i ich przetwarzanie w nieodpowiedniej kolejności
- **Straty pakietów** (*ang. Packet Loss*) – max. 3%
Główne przyczyny:
 - Opóźnienia – grupa pakietów „z głosem” jest ważna tylko przez określony czas
 - Jitter – pakiet przychodzi po tym jak jego „współtowarzysze” zostali już dostarczeni
 - Cecha sieci pakietowych wykorzystujących UDP – najgorsze dla VoIP są straty grupy pakietów
- **Jak to się ma do bezpieczeństwa?**

PROTOKOŁY SYGNALIZACYJNE VOIP

SIP, H.323 oraz H.248/Megaco



Stos protokołów dla VoIP

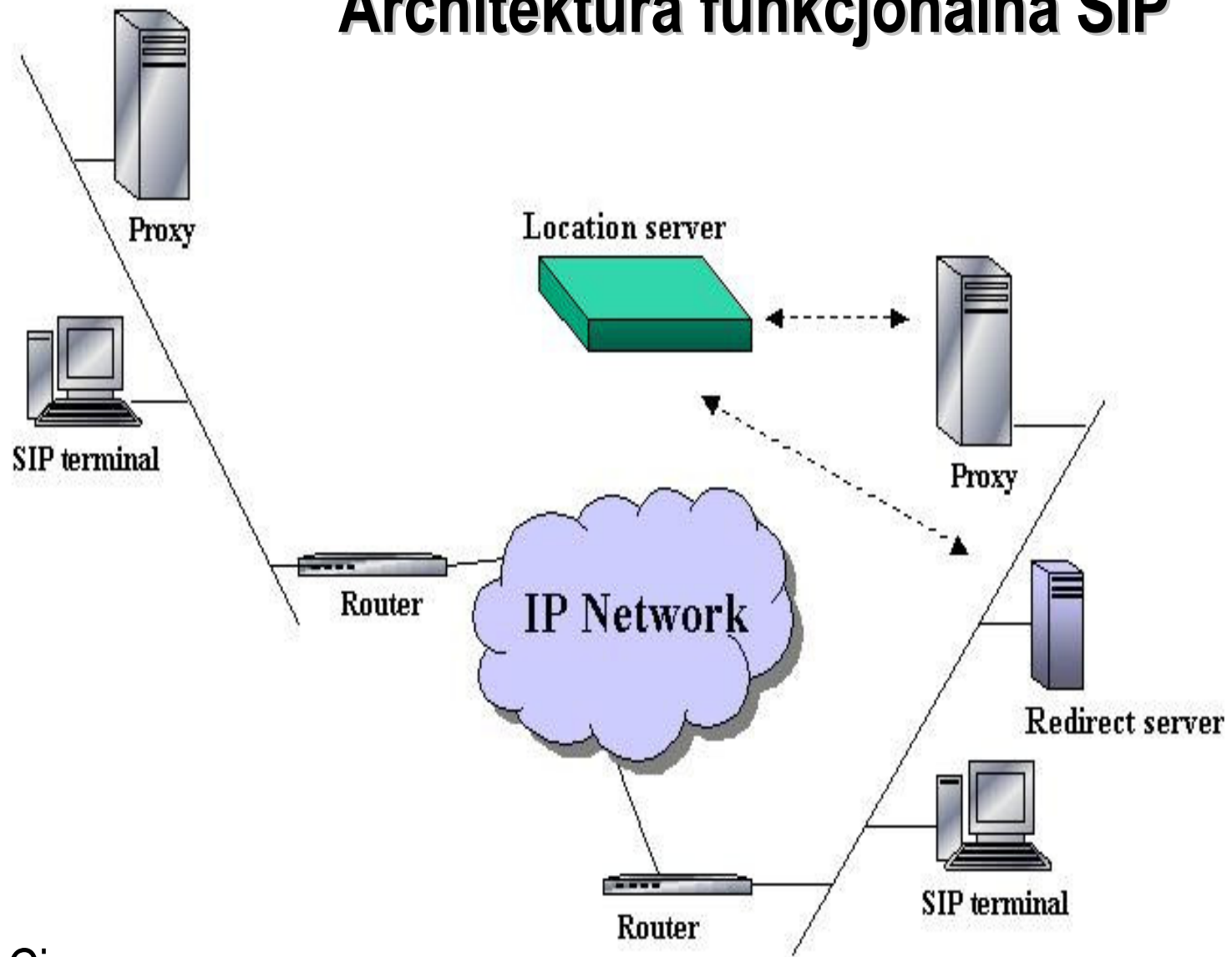




Protokół SIP

- Bieżąca wersja opisana w standardzie organizacji IETF: **RFC 3261**
- Architektura funkcjonalna:
 - **Agent Użytkownika** (ang. User Agent) – składa się z serwera (UAS) i klienta (UAC), system końcowy
 - **Serwery sieciowe** (ang. Network Servers) - dwa rodzaje:
 - Proxy** - odpowiedzialny jest za ustalenie adresu następnego serwera, do którego należy skierować wiadomość
 - Redirect**- wysyła do agenta użytkownika odpowiedź zawierającą adres następnego serwera

Architektura funkcjonalna SIP



Źródło: Cisco

Protokół H.323 (1/2)

- Zbiór standardów organizacji **ITU** pierwotnie do realizacji **usług multimedialnych**
- **Architektura funkcjonalna:**
 - Terminale abonenckie H.323
 - **Bramy (Gateways)** - służące łączeniu różnych typów sieci
 - **Strażnicy (Gatekeepers)** - inteligentne serwery sterujące, wokół których tworzone są tzw. strefy
 - **Jednostki MCU (Multipoint Control Unit)** – do tworzenia telekonferencji





Protokół H.323 (2/2)

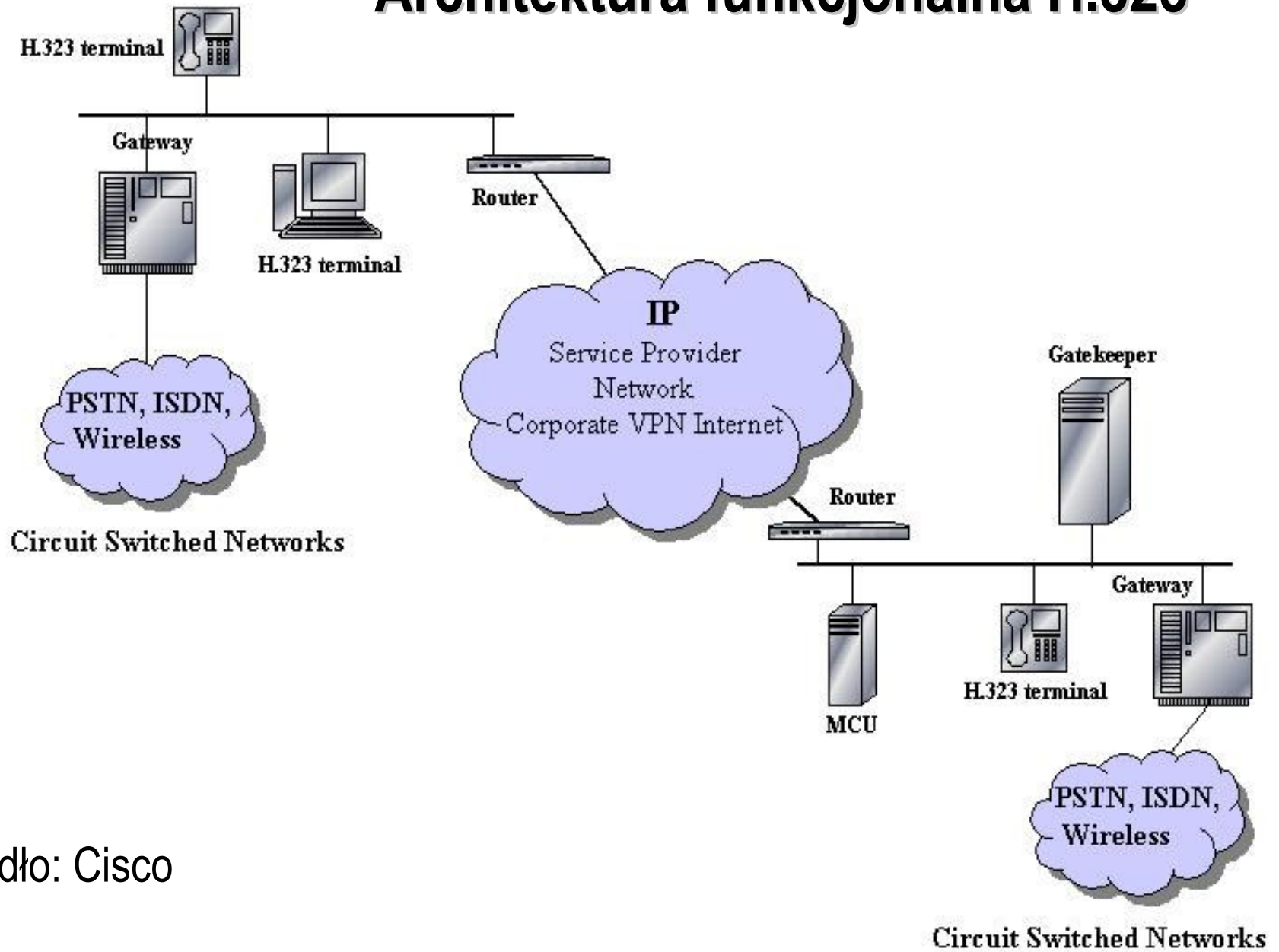
- Dostępne kanały sygnalizacyjne:

RAS (Registration, Admission & Status) – komunikacja: strażnik <-> inne elementy systemu. Zestawiany przed inicjacją innych kanałów.


Q.931 - procedury niezbędne do realizacji połączenia między stronami inicjującą i docelową

H.245 – do komunikacji między punktami końcowymi, wymiana właściwości obu terminali - negocjacja przesyłania danych w kanale logicznym

Architektura funkcjonalna H.323



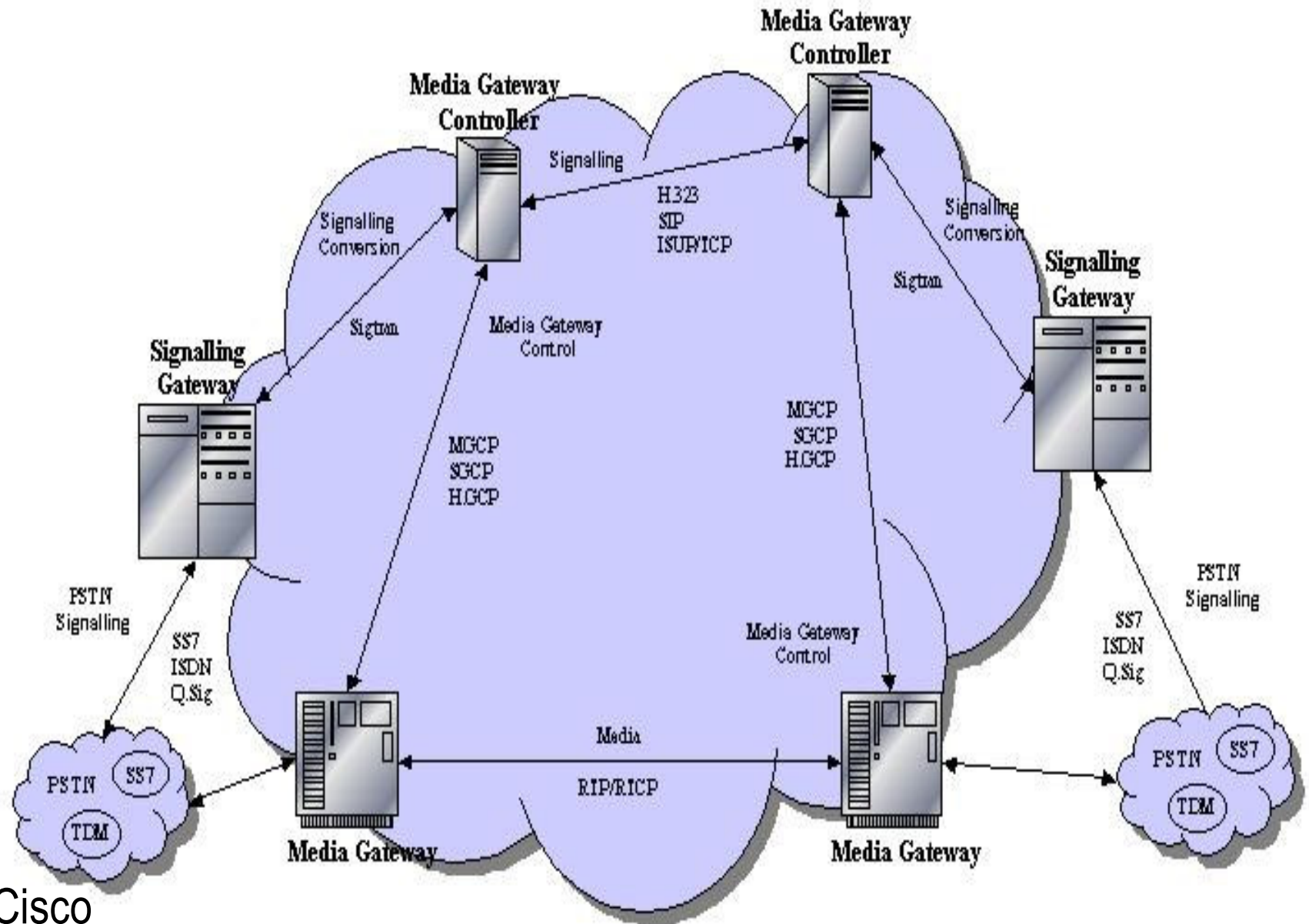
Źródło: Cisco



Protokół H.248/Megaco

- Stworzony z potrzeby współpracy z sieciami PSTN (sygnalizacja SS7)
- Dekompozycja **Strażnika** na **Sterownik Bramy Medialnej** (*ang. Media Gateway Controller*) oraz **Bramę Medialną** (*ang. Media Gateway*)
- Model '**master-slave**' – centralizacja inteligencji
- Wykorzystywanie:
 - **zakończeń** (porty w MG lub strumienie danych)
 - **kontekstu** (połączenie urządzeń na drodze między zakończeniami)

Architektura funkcjonalna H.248/Megaco/MGCP



Źródło: Cisco

BEZPIECZEŃSTWO PROTOKOŁÓW SYGNALIZACYJNYCH VOIP





Problemy bezpieczeństwa usługi VoIP

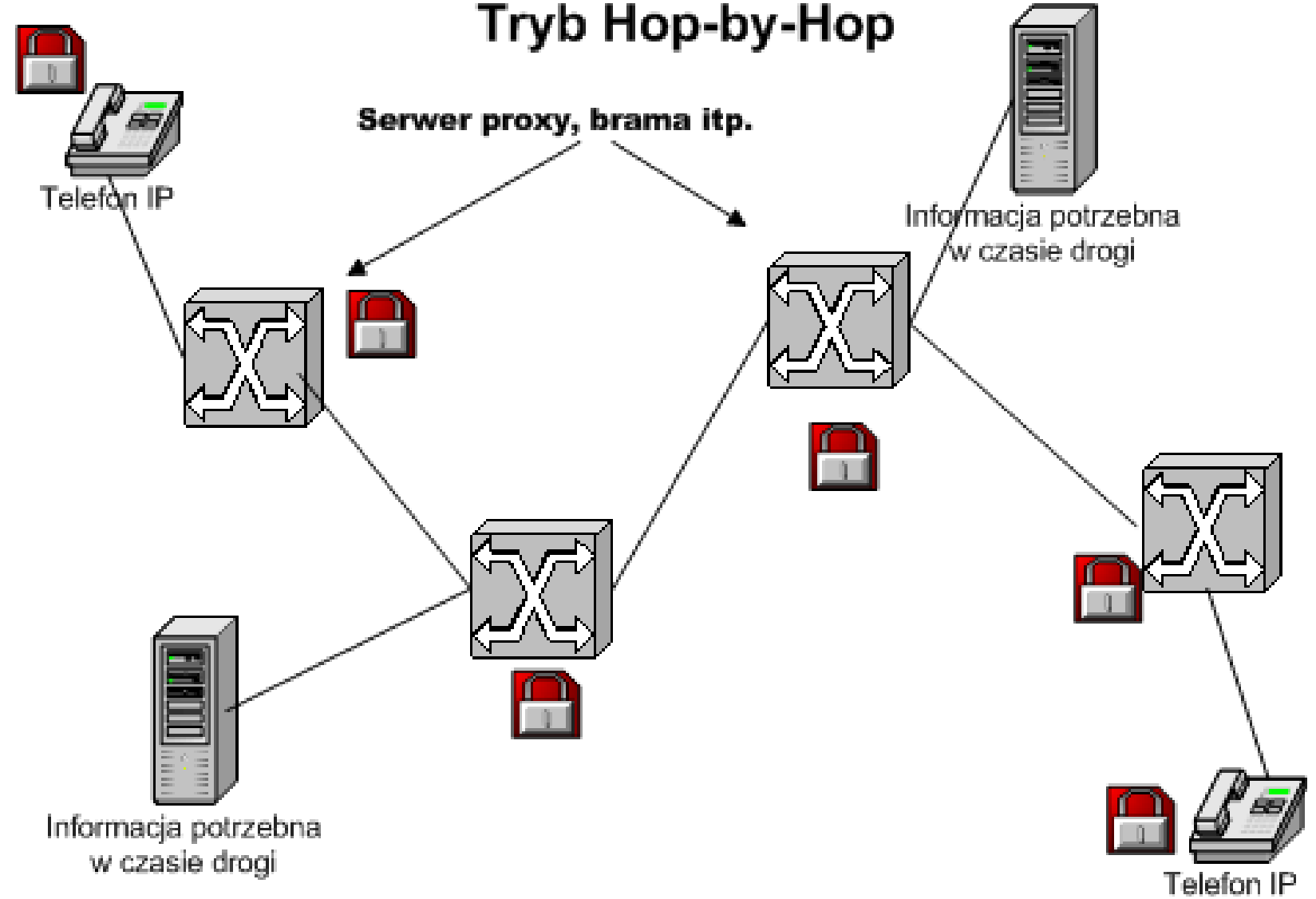
- Trzy grupy problemów bezpieczeństwa usługi VoIP:
 - Bezpieczeństwo sygnalizacji
 - Bezpieczeństwo pakietów RTP (z głosem)
 - Firewall oraz NAT
- **Phreakerzy + hackerzy = ?**

Zagrożenia i mechanizmy zabezpieczeń

- **Klasy ataków: aktywne i pasywne** - zagrożenia jak dla każdej w sieci IP
- Techniki ataków na sygnalizację VoIP:
 - **Podszywanie się** (*ang. Spoofing*)
 - **Podsluchiwanie** (*ang. Sniffing*)
 - **Odmowa usługi** (*ang. Denial Of Service*)
- Główne przyczyny **braku popularności** mechanizmów zabezpieczeń VoIP
- Tryby pracy mechanizmów zabezpieczeń:
HbH (Hop-by-Hop) oraz E2E (End-to-End)

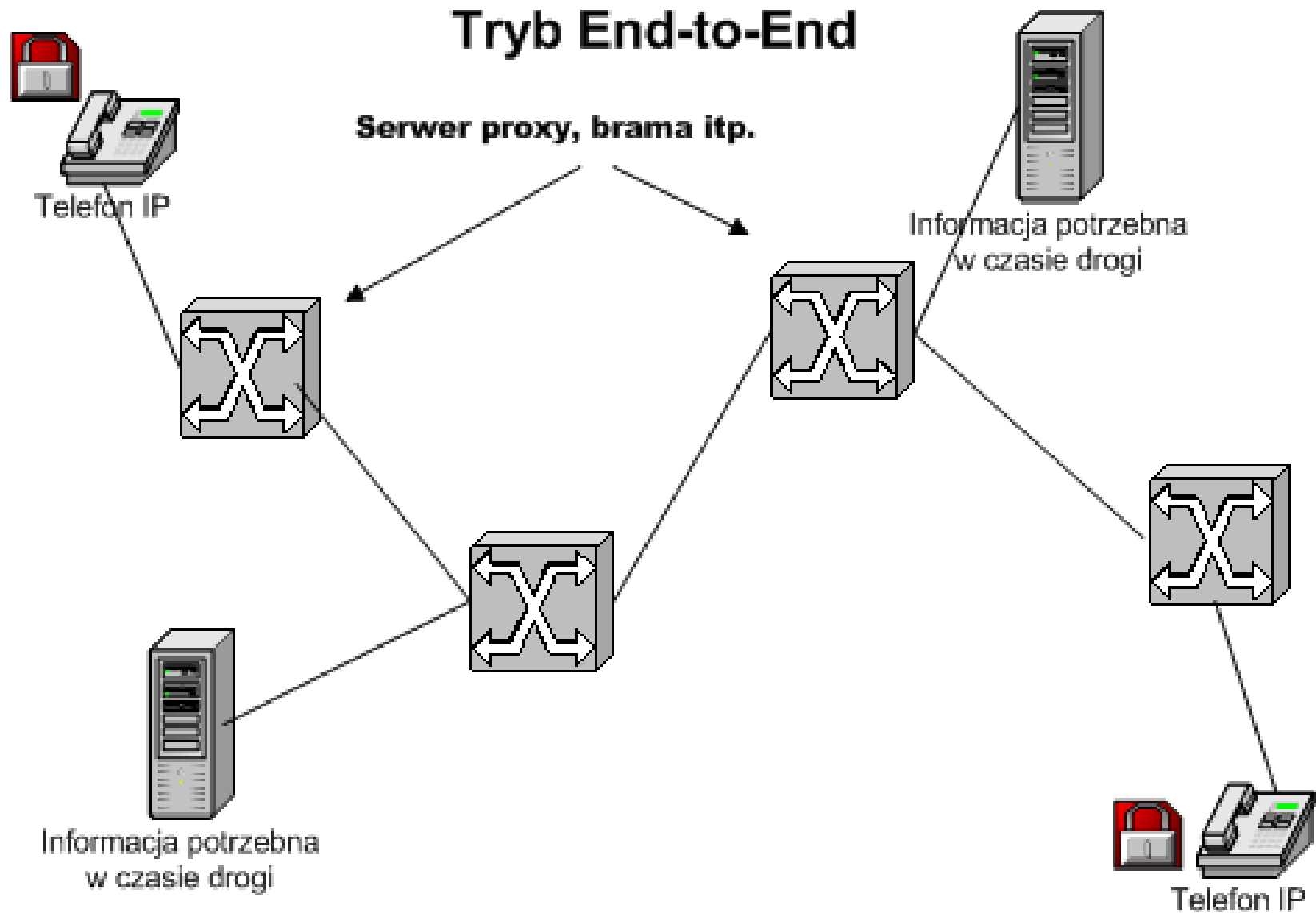


Tryb Hop-by-Hop



 - Szyfrowanie lub deszyfrowanie

Tryb End-to-End



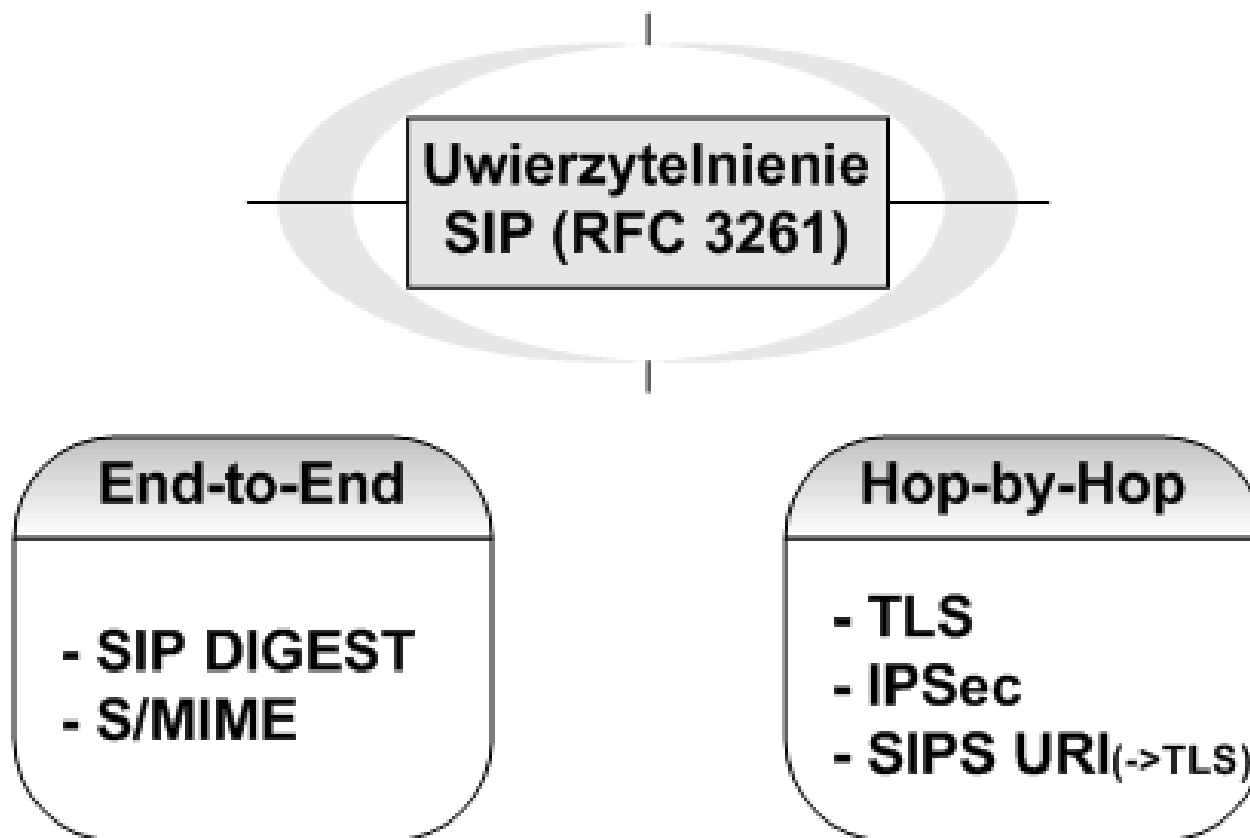
 - Szyfrowanie lub deszyfrowanie



Kryterium oceny mechanizmów zabezpieczeń dla VoIP

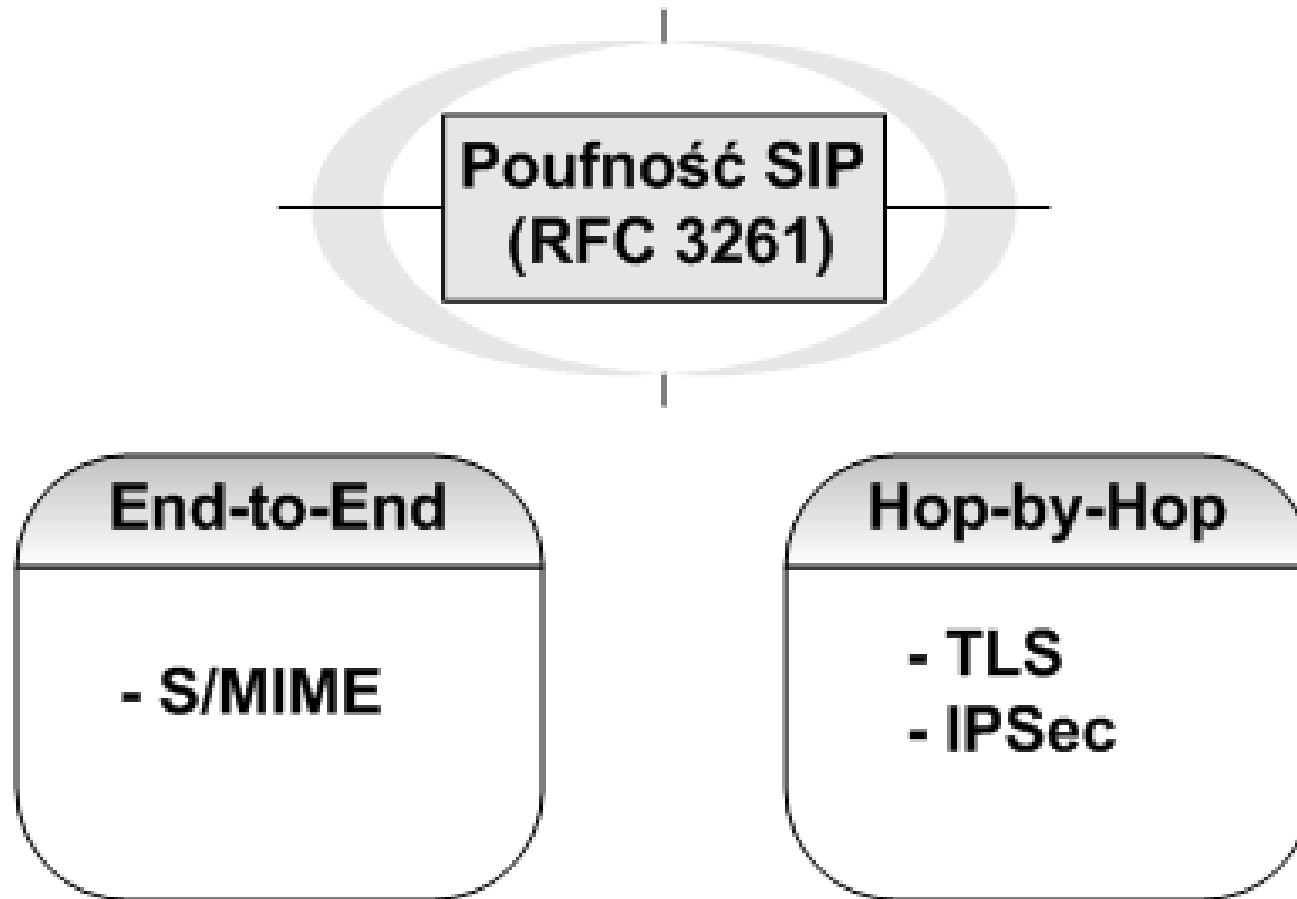
- Potrzeba istnienia kryterium oceny
- Modyfikacja kryterium z normy ISO 7498-2 (uwierzytelnienie, integralność, poufność, niezaprzeczalność i kontrola dostępu)
- **Uwierzytelnienie oraz poufność** - usługi ochrony informacji i komunikacji w sieci gwarantujące bezpieczeństwo protokołu sygnalizacyjnego VoIP

Analiza mechanizmów zabezpieczeń protokołu SIP (1/2)



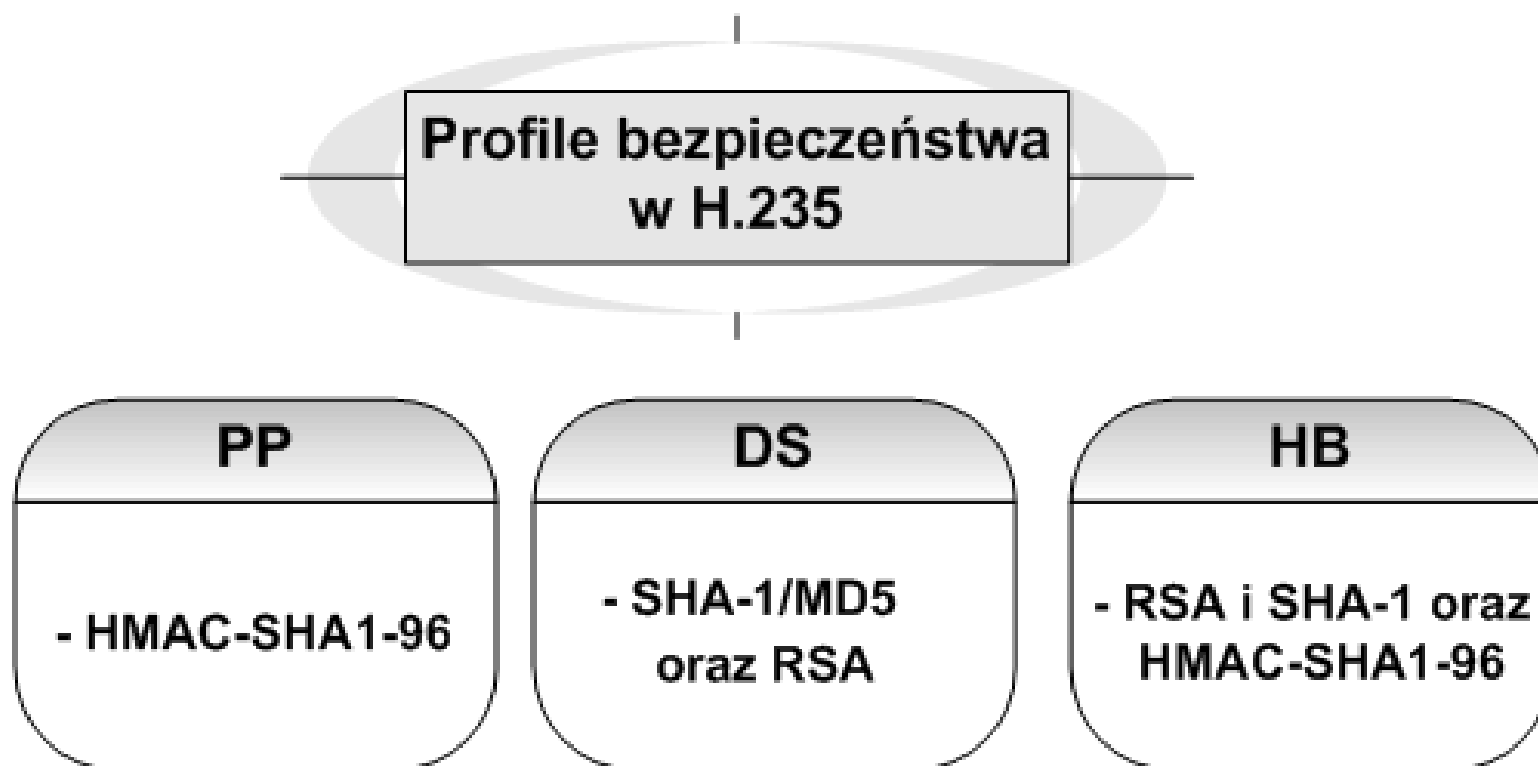
- Przystosowanie istniejących mechanizmów

Analiza mechanizmów zabezpieczeń protokołu SIP (2/2)



- Żaden z wykorzystanych mechanizmów nie jest bez wad

Analiza mechanizmów zabezpieczeń protokołu H.323 (1/3)



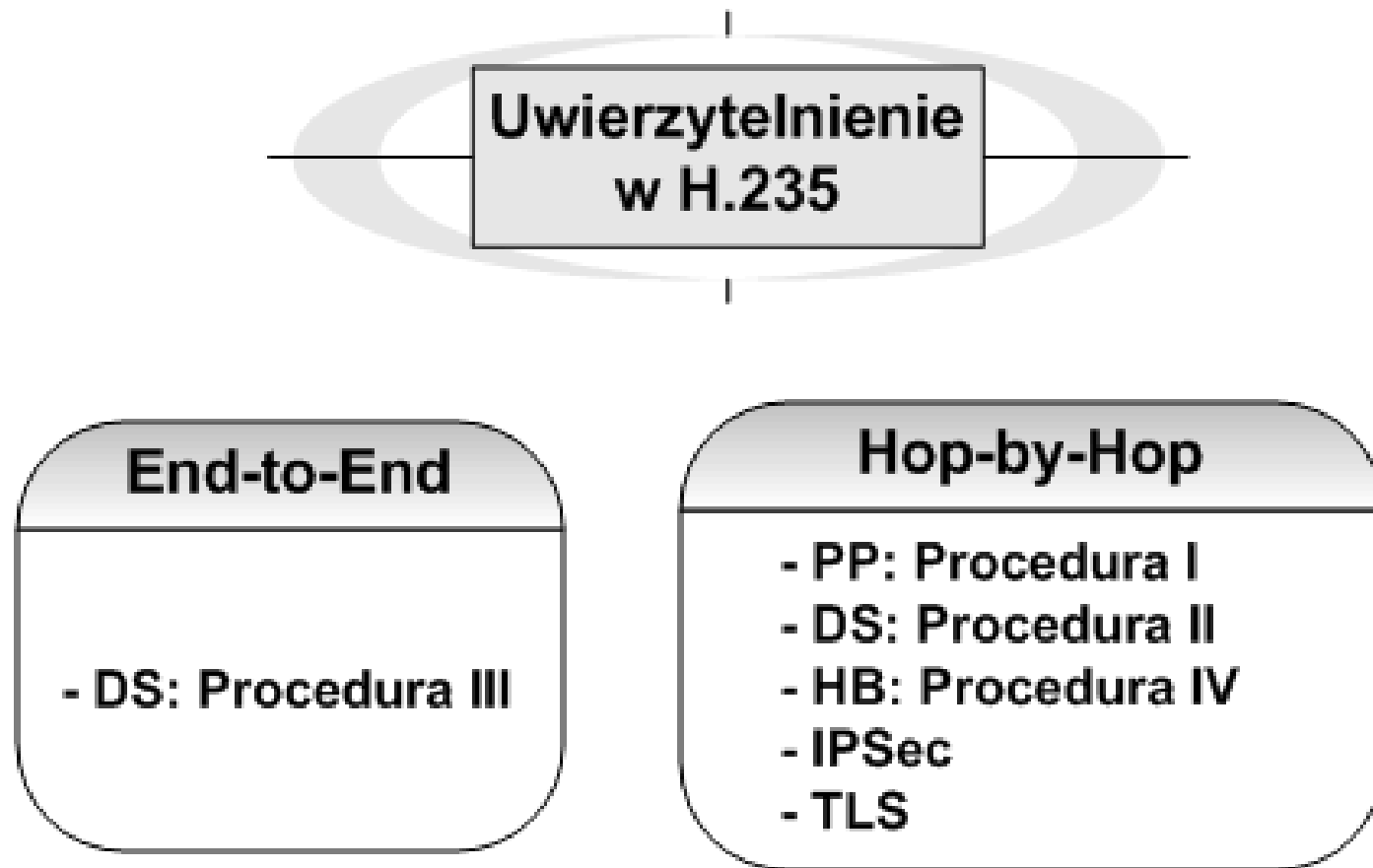
LEGENDA:

PP - Profil podstawowy

DS - Profil z wykorzystaniem podpisów cyfrowych

HB - Profil hybrydowy

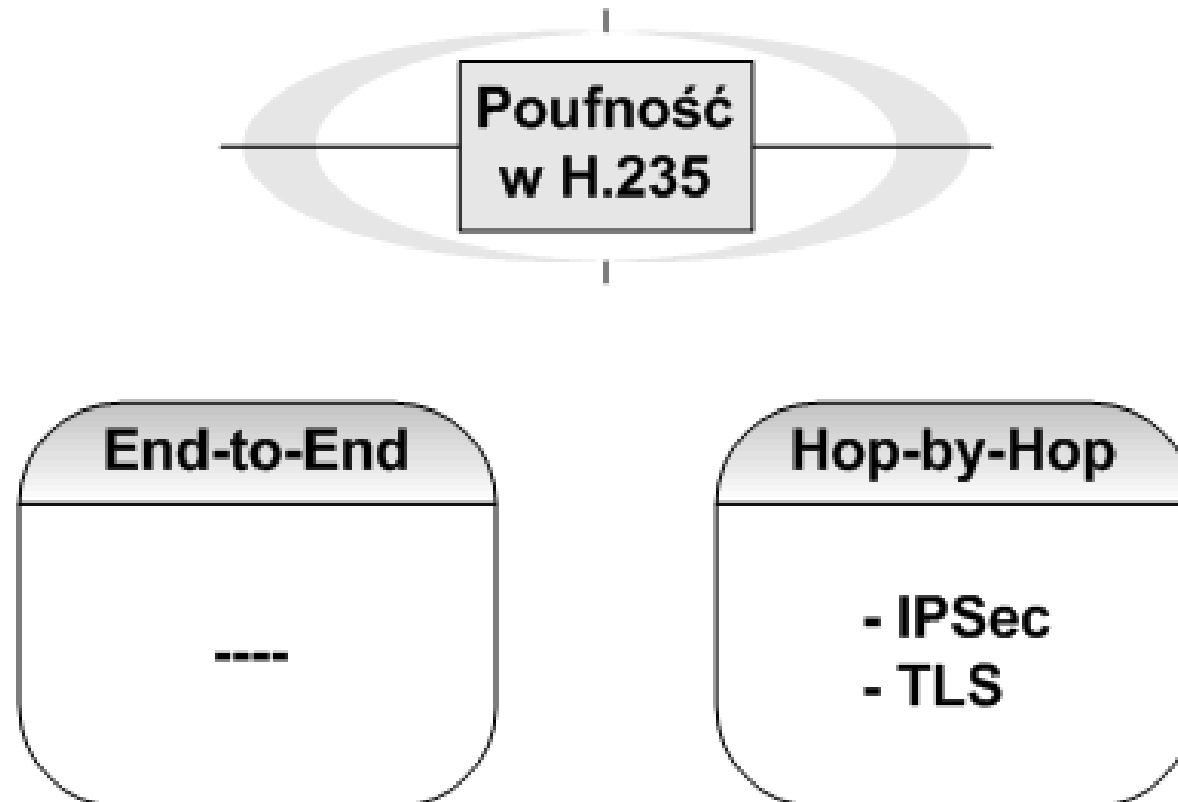
Analiza mechanizmów zabezpieczeń protokołu H.323 (2/3)



- Wykorzystanie opcjonalnej procedury *Fast Connect* oraz tunelowania H.245

Analiza mechanizmów zabezpieczeń protokołu H.323 (3/3)

- Realizacja każdego mechanizmu wymaga modelu sieci ze Strażnikiem (*GateKeeper*)





III Krajowa Konferencja Bezpieczeństwa Biznesu 2004

Bezpieczeństwo VoIP

Część II:

Współpraca protokołów sygnalizacyjnych VoIP oraz prognozy rozwoju

Wojciech Mazurczyk

Instytut Telekomunikacji, Politechnika Warszawska

E-mail: W.Mazurczyk@elka.pw.edu.pl

Miedzeszyn, 23 listopad 2004



Plan prezentacji części II

- Badania bezpieczeństwa **SIP UA**
- Potrzeba bezpiecznej współpracy protokołów sygnalizacyjnych VoIP oraz obecne rozwiązania (**IWF SIP-H.323**)
- Bezpieczne środowisko sieciowe dla VoIP
- Potencjalne zagrożenie przyszłości VoIP: **SKYPE?**
- Podsumowanie

BADANIE BEZPIECZEŃSTWA SIP UA





Przeprowadzone doświadczenia

- **Cel i przebieg badań praktycznych**
- Testowane aplikacje SIP UA
- Opis i konfiguracje przeprowadzonych doświadczeń
- Omówienie wykorzystanych testów



Testowane SIP UA

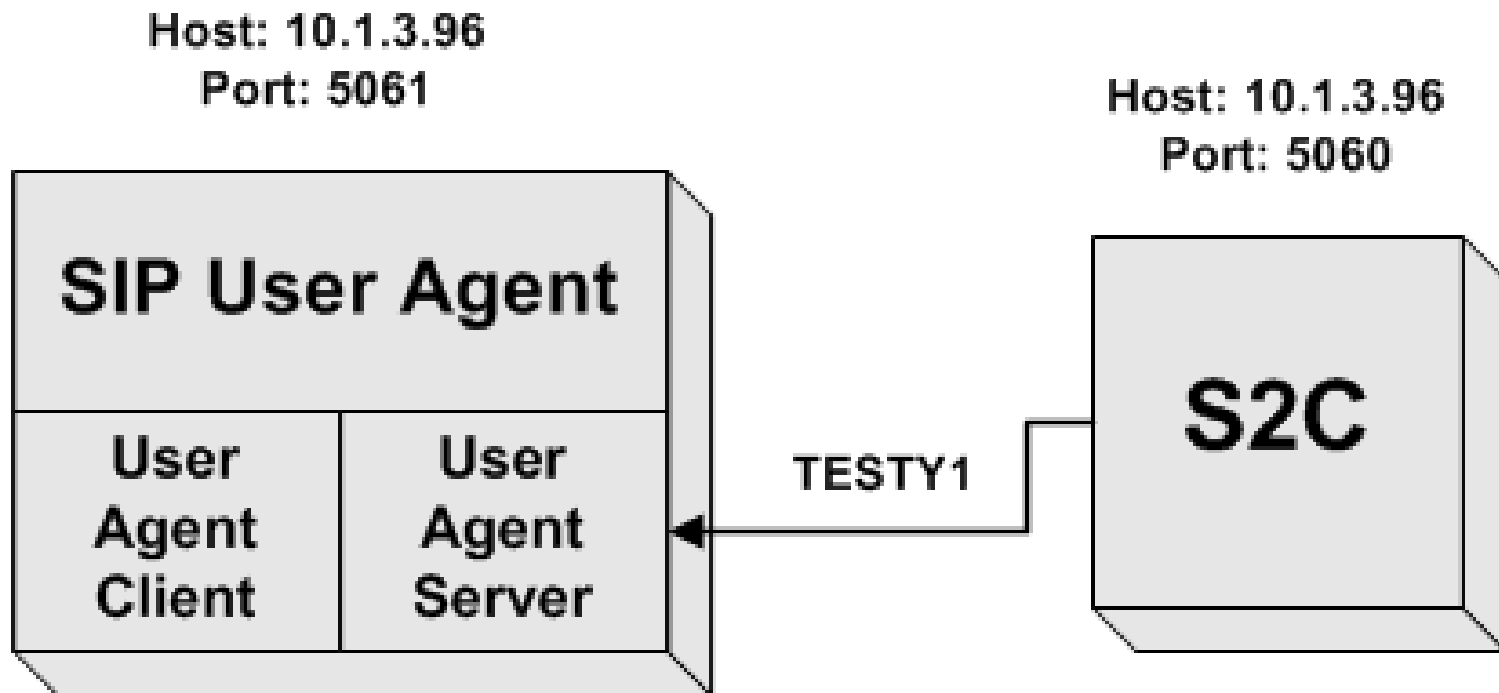
- Wybrane aplikacje:
 - **Helmsman User Agent 3.0.6** firmy Helmsman
 - **eStara SoftPHONE 3.0** firmy eStara
 - **Siemens Communication System Client v.1.0**
 - **Magellan 4.0** opracowany w IT PW
 - **Hughes SIP User Agent (E-Z Phone)** firmy Hughes Software Systems
 - **Vovida SIP UA 1.0.2** - Columbia University
- Kryterium wyboru - **powszechność**



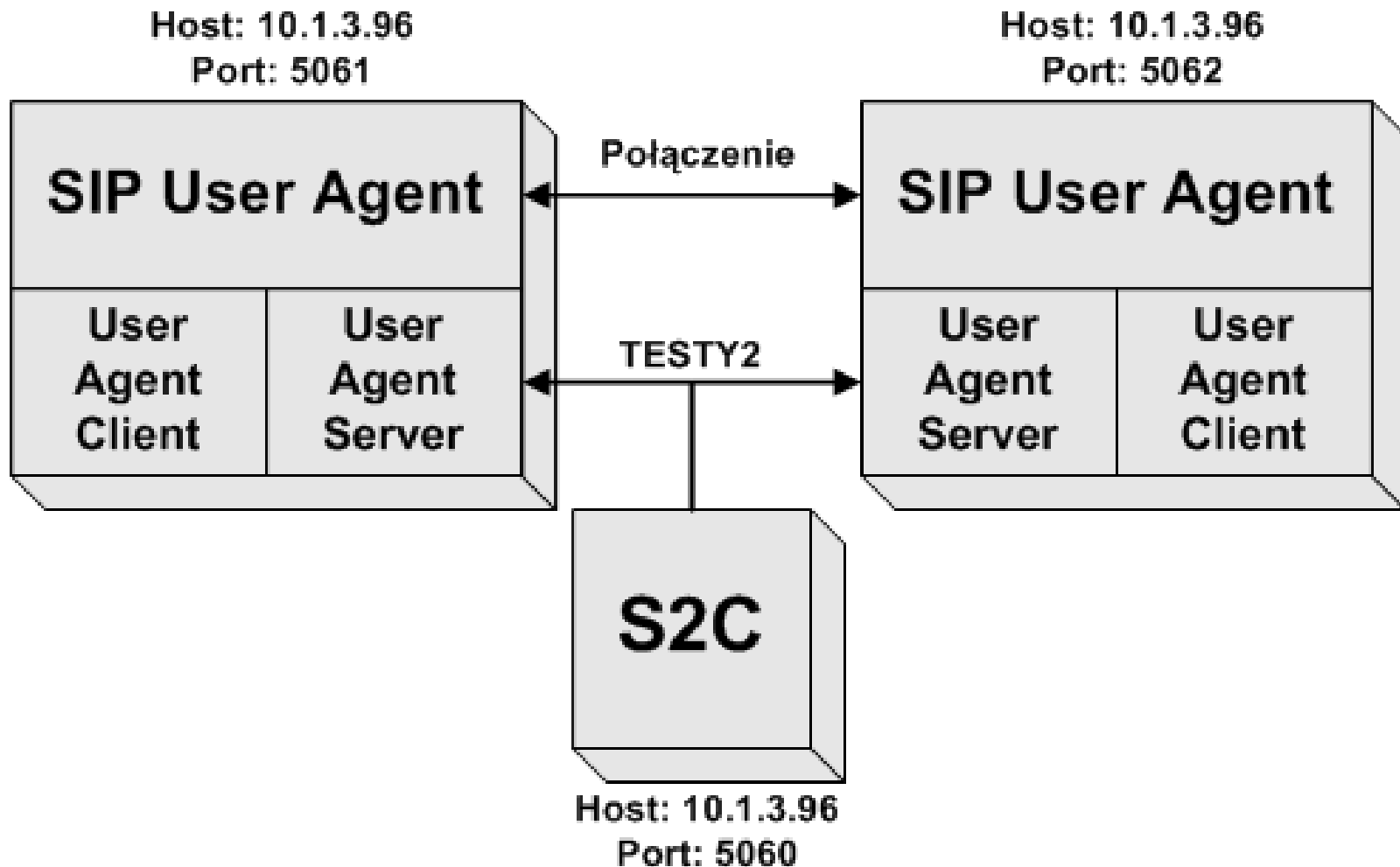
Przeprowadzone doświadczenia

- Cel i przebieg badań praktycznych
- Testowane aplikacje SIP UA
- **Opis i konfiguracje przeprowadzonych doświadczeń**
- Omówienie wykorzystanych testów

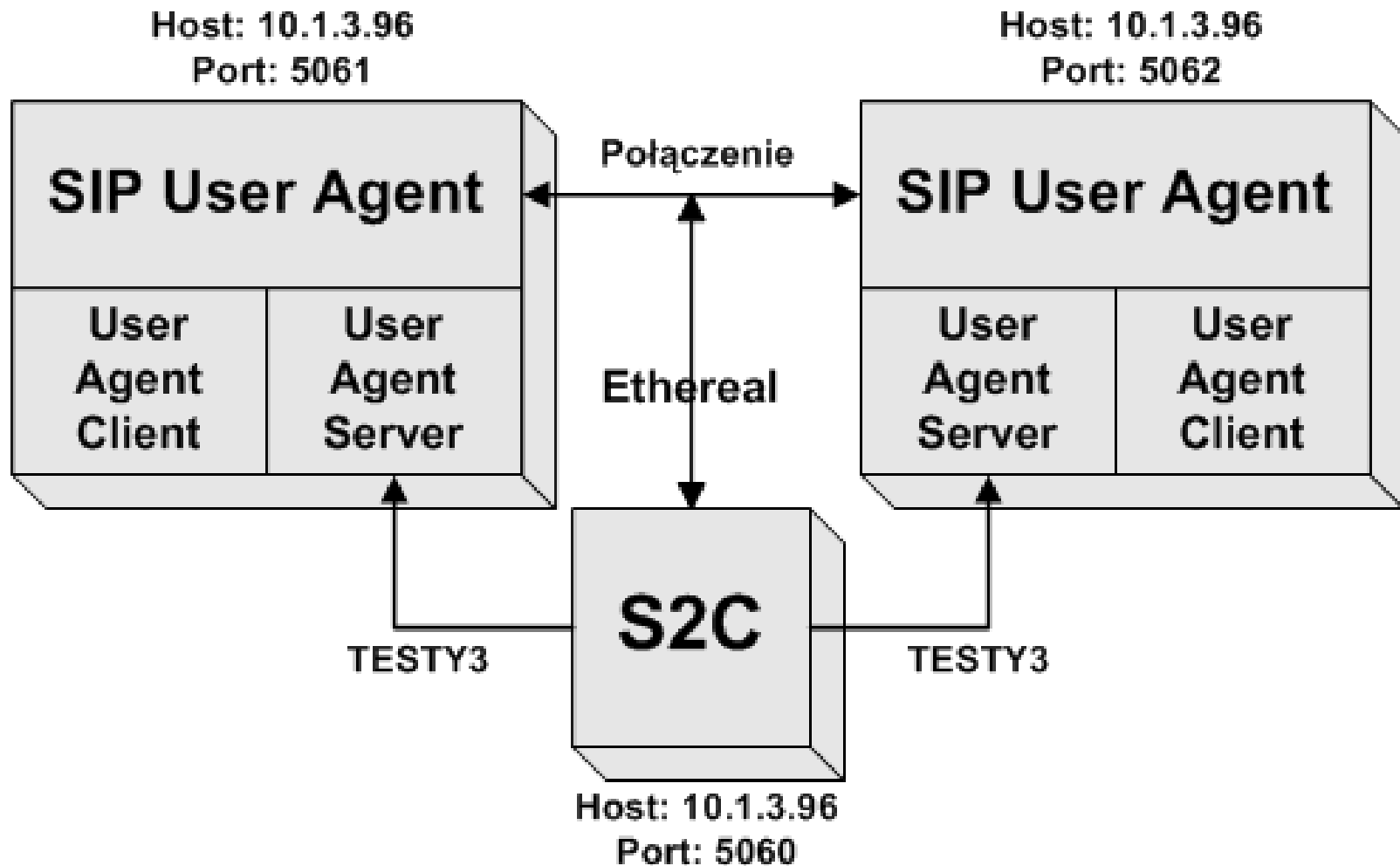
Konfiguracje testowe 1/3



Konfiguracje testowe 2/3



Konfiguracje testowe 3/3

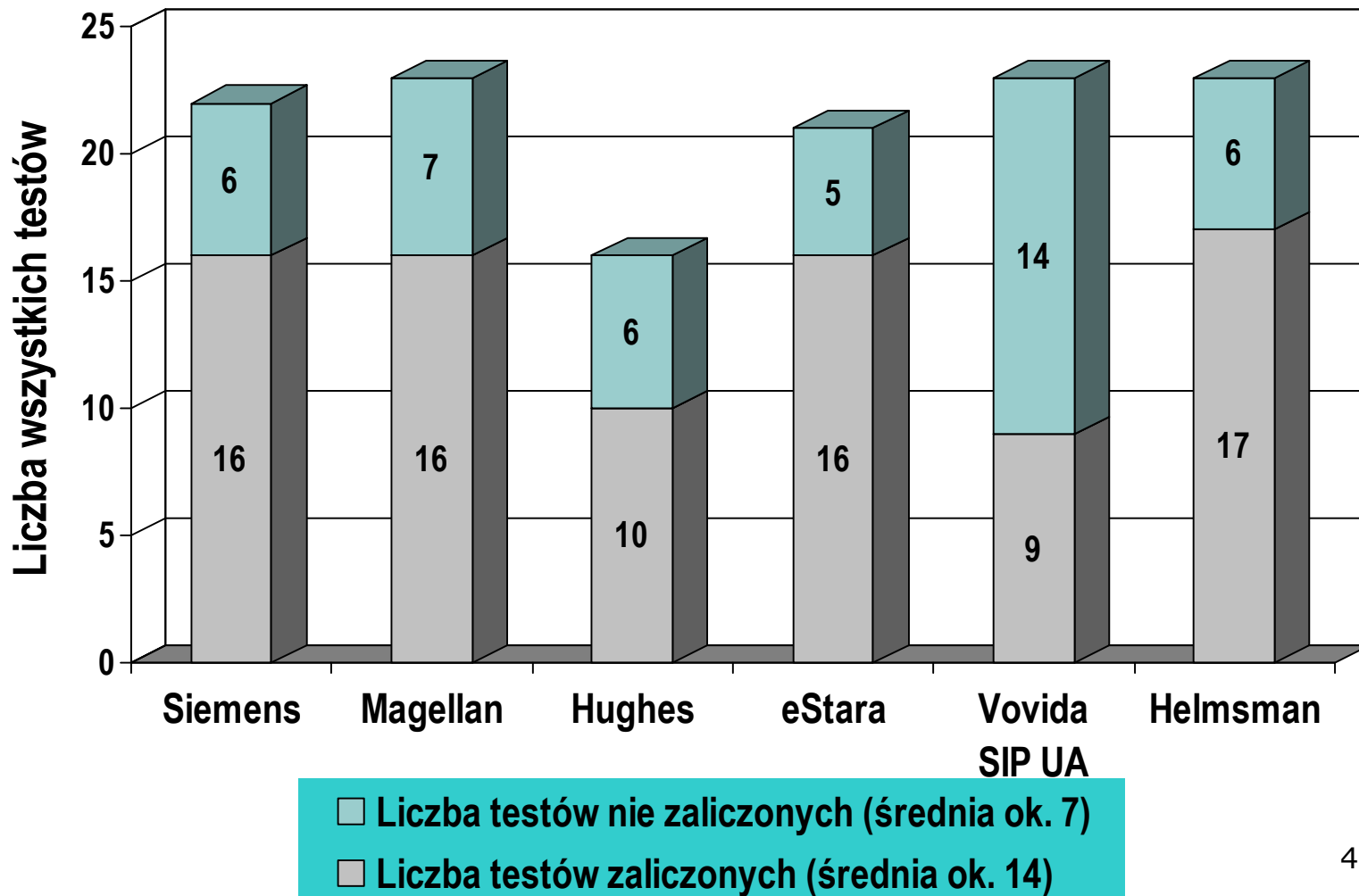




Przeprowadzone doświadczenia

- Cel i przebieg badań praktycznych
- Testowane aplikacje SIP UA
- Opis i konfiguracje przeprowadzonych doświadczeń
- **Omówienie wykorzystanych testów**

Wyniki doświadczeń badań SIP UA





Uzyskane wyniki - podsumowanie

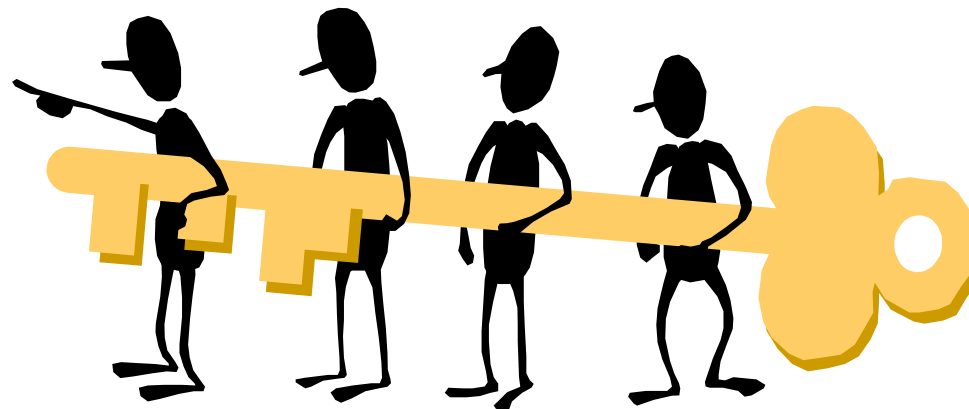
- Liczne błędy implementacyjne badanych SIP UA – większe możliwości ataku
- Wzrost bezpieczeństwa aplikacji w przypadku stosowania mechanizmów bezpieczeństwa (ale potrzebna większa moc obliczeniowa)
- Konieczność określenia w standardzie obowiązkowych mechanizmów zabezpieczeń



Wyniki testów organizacji CERT

- Przedstawienie opublikowanych badań
 - **SIP**: <http://www.cert.org/advisories/CA-2003-06.html>
 - **H.323**: <http://www.cert.org/advisories/CA-2004-01.html>
- Uzyskane wyniki – zgodność wniosków:
 - Potwierdzenie słuszności metod testowania Agentów Użytkownika SIP
 - Błędy implementacyjne w **komercyjnych** wersjach SIP UA

WSPÓŁPRACA SIP - H.323



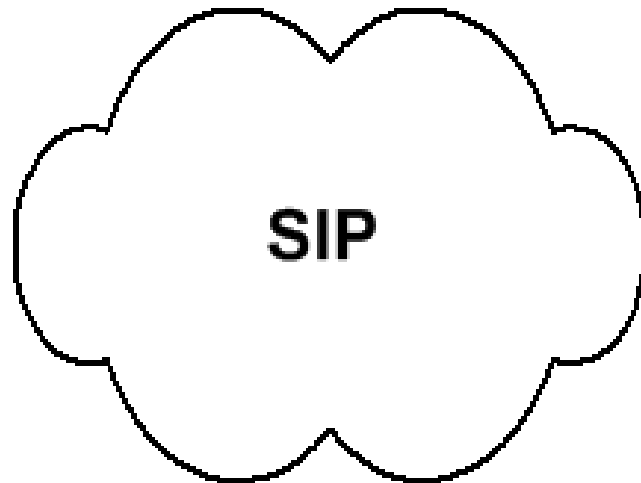


Współpraca protokołów sygnalizacyjnych VoIP

- Potrzeba zapewnienia współpracy protokołów sygnalizacyjnych SIP i H.323
- Koncepcja **IWF SIP-H.323**
 - Główny cel
 - Stan prac standaryzacyjnych
 - Dotychczas brak rozwiązań dla zapewnienia bezpieczeństwa sygnalizacji w połączonej sieci SIP-H.323

Po co bezpieczeństwo dla IWF? (1/3)

VoIP oparty na SIP



←→
Zakres działania protokołu SIP
oraz mechanizmów
zabezpieczeń

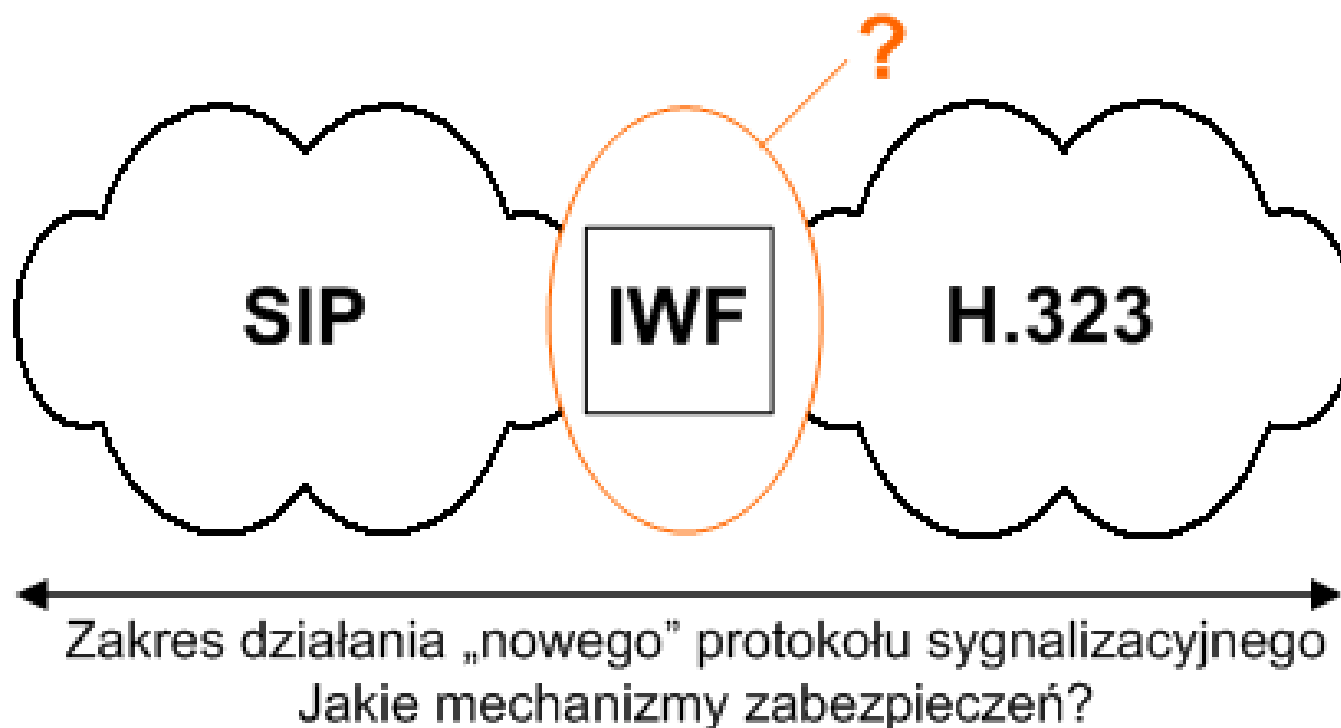
VoIP oparty na H.323



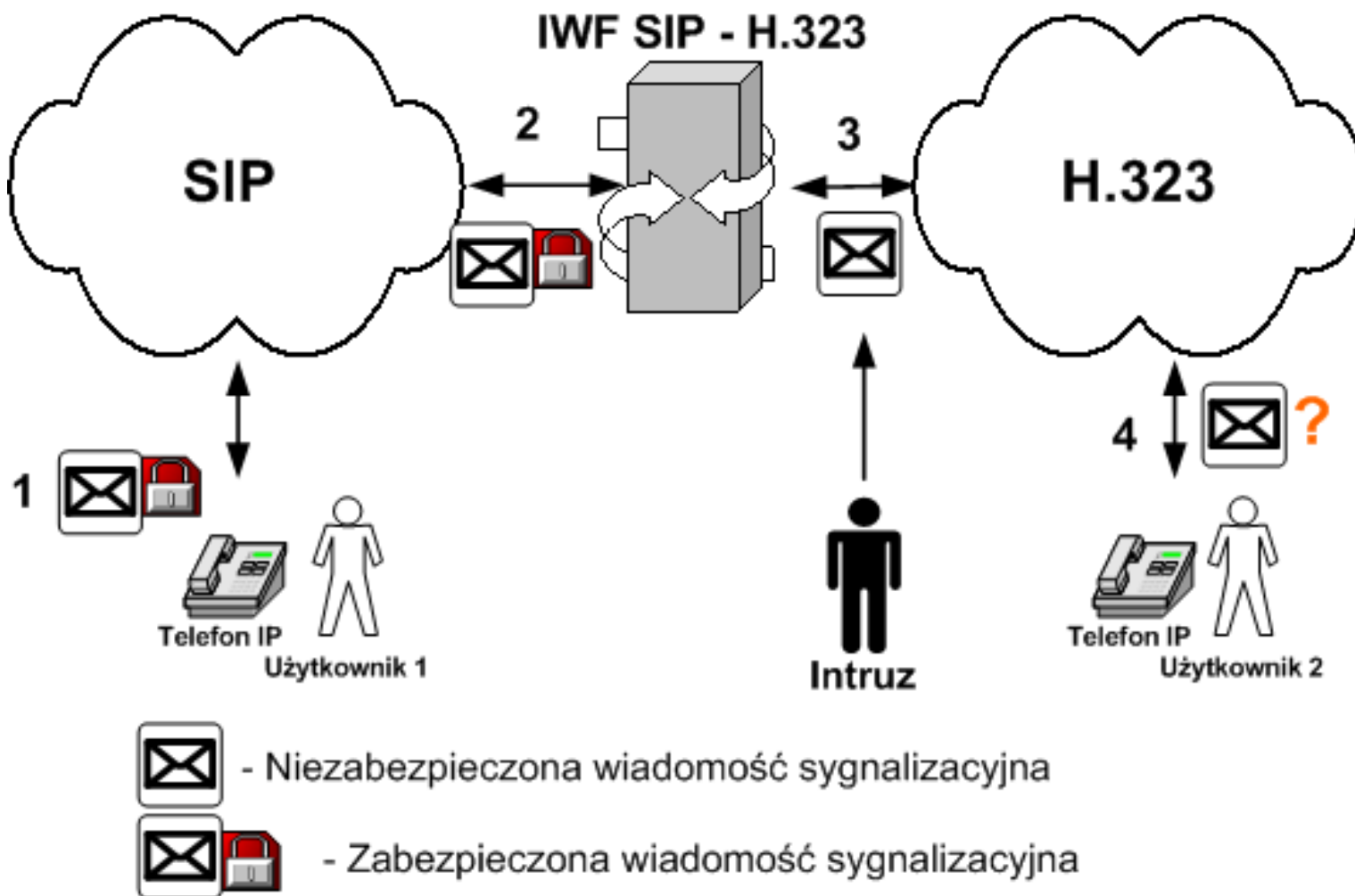
←→
Zakres działania protokołu H.323
oraz mechanizmów zabezpieczeń

Po co bezpieczeństwo dla IWF? (2/3)

Połączony system SIP - H.323



Po co bezpieczeństwo dla IWF? (3/3)





Cechy IWF SIP-H.323

- C1:** Nie musi wykorzystywać elementów opcjonalnych architektury funkcjonalnej protokołów SIP i H.323
- C2:** Może zostać zintegrowane ze Strażnikiem (*GateKeeper*) lub serwerami SIP (*proxy* lub *redirect*)
- C3:** Nie dokonuje konwersji strumieni mediów
- C4:** Powinno wspierać procedurę *Fast Connect* oraz tunelowanie H.245 (dla H.323)
- C5:** Powinno być przezroczyste dla punktów końcowych
- C6:** Translacja sygnalizacji nie może powodować zmian ani w protokole SIP ani w H.323

Źródło: H. Schulzrinne, C. Agboh, "SIP - H.323 Interworking Requirements", IETF Internet Draft, luty 2004



Założenia bezpieczeństwa IWF SIP-H.323

- S1:** IWF **powinien** wykorzystywać przypisane protokołom sygnalizacyjnym mechanizmy zabezpieczeń
- S2:** IWF musi posiadać procedury uniknięcia ataków typu Denial of Service (*DoS*)
- S3:** IWF musi być elementem zaufanym dla obu stron sieci
- S4:** IWF nie może ujawniać poziomu zaufania dla użytkownika po żadnej stronie sieci

Źródło: H. Schulzrinne, C. Agboh, "SIP - H.323 Interworking Requirements",
IETF Internet Draft, luty 2004



Wymagania bezpieczeństwa IWF SIP-H.323 (1/2)

- W1:** Nie spełnione kryterium bezpiecznego protokołu sygnalizacyjnego dla SIP-H.323 = **brak połączenia**
- W2:** Bezpieczeństwo połączonych sieci SIP-H.323 musi być takie, jak w ramach pojedynczej sieci
- W3:** Model sieci: H.323 ze Strażnikiem (*GateKeeper*); SIP z serwerami sieciowymi (*proxy* lub *redirect*)
- W4:** Dla protokołu H.323 niezbędne wsparcie procedury *Fast Connect* oraz tunelowania H.245



Wymagania bezpieczeństwa IWF SIP-H.323 (2/2)

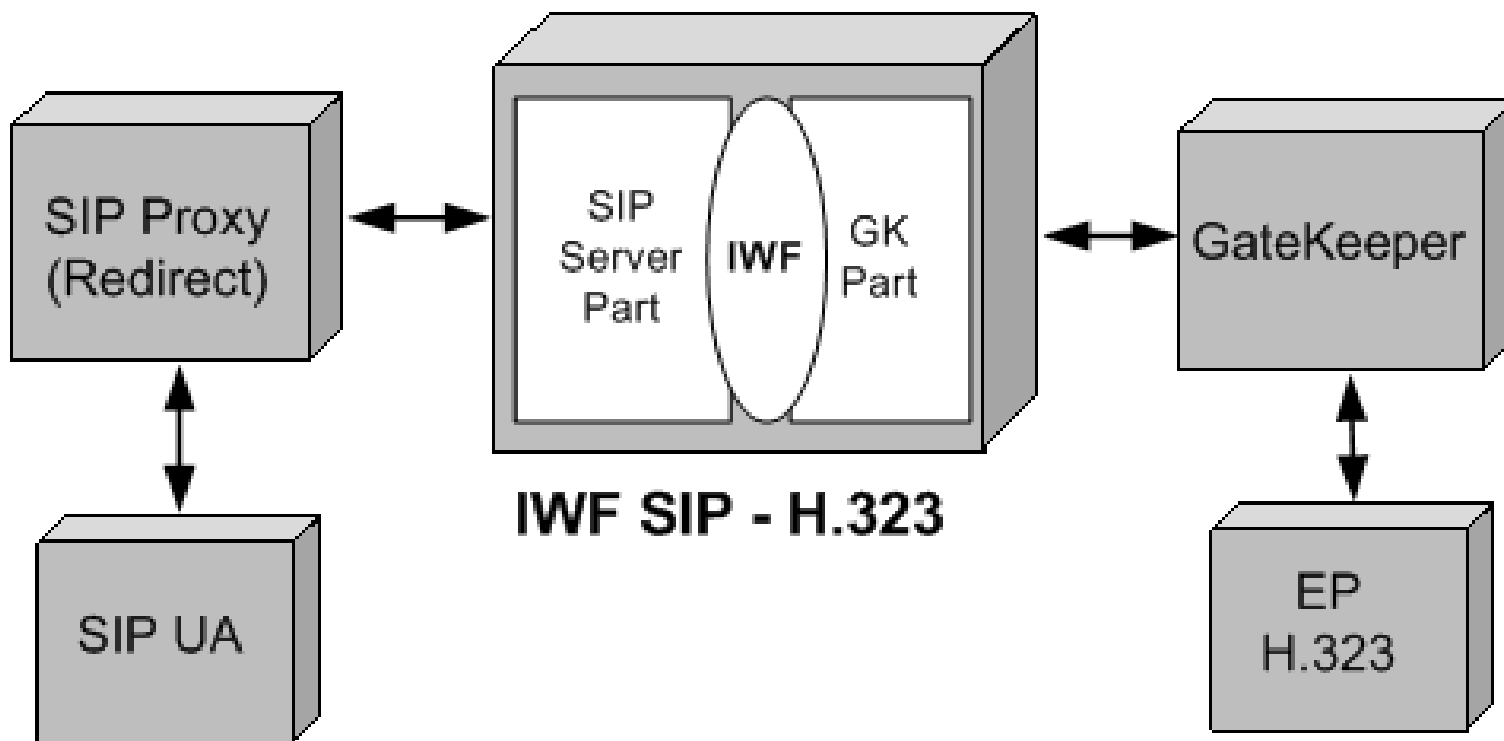
W5: Całkowita przezroczystość IWF SIP-H.323 dla wszystkich elementów architektury funkcjonalnej

W6: Musi być elementem zaufanym dla obu stron sieci

W7: Obowiązkowe obustronne uwierzytelnienie z wykorzystaniem TLS między IWF, a:

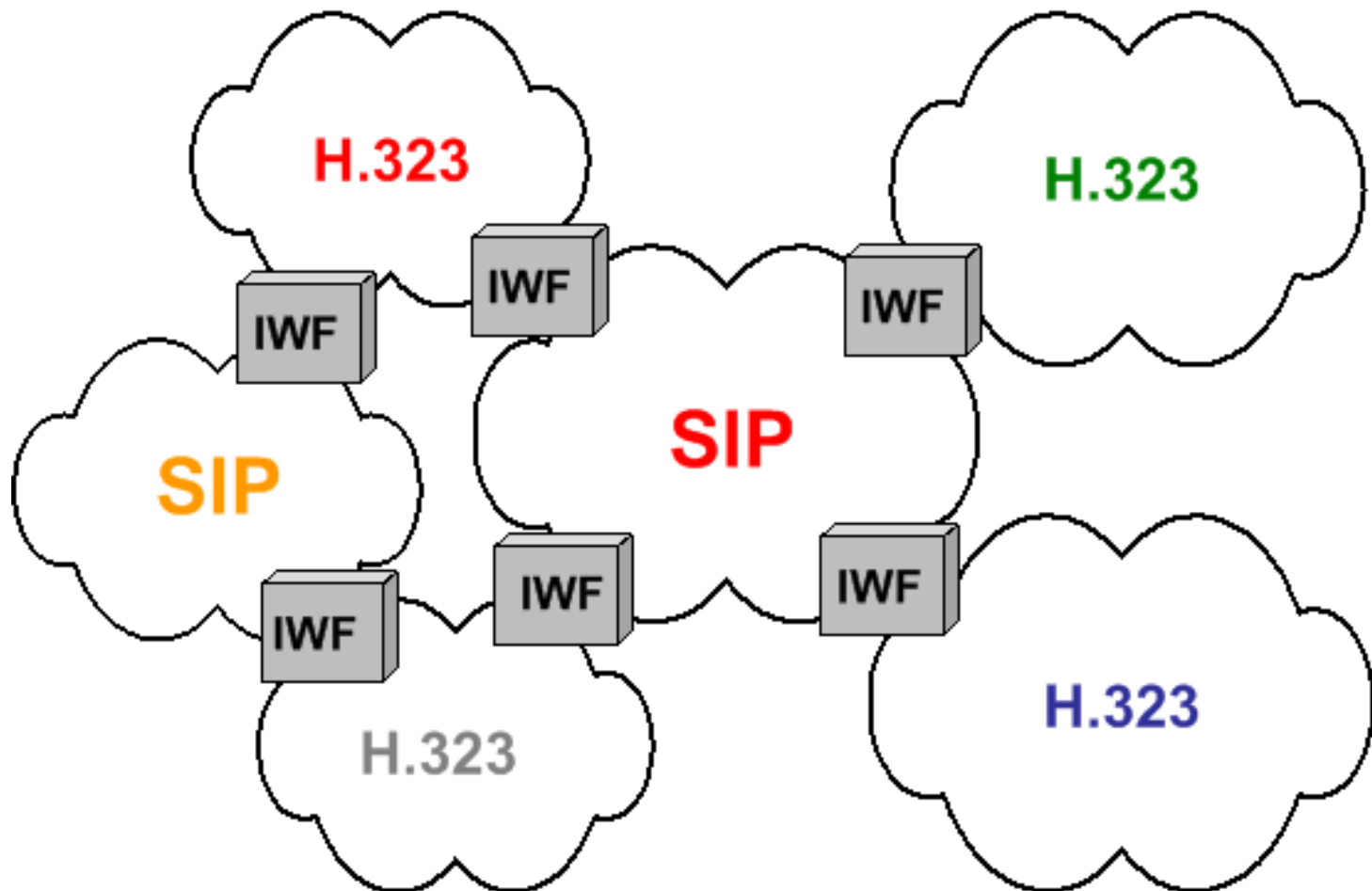
- serwerami proxy (redirect) dla SIP
- strażnikami dla części sieci z H.323

Dekompozycja funkcjonalna IWF SIP-H.323



- Główne zalety takiej dekompozycji

Wpływ IWF na bezpieczeństwo (1/3)

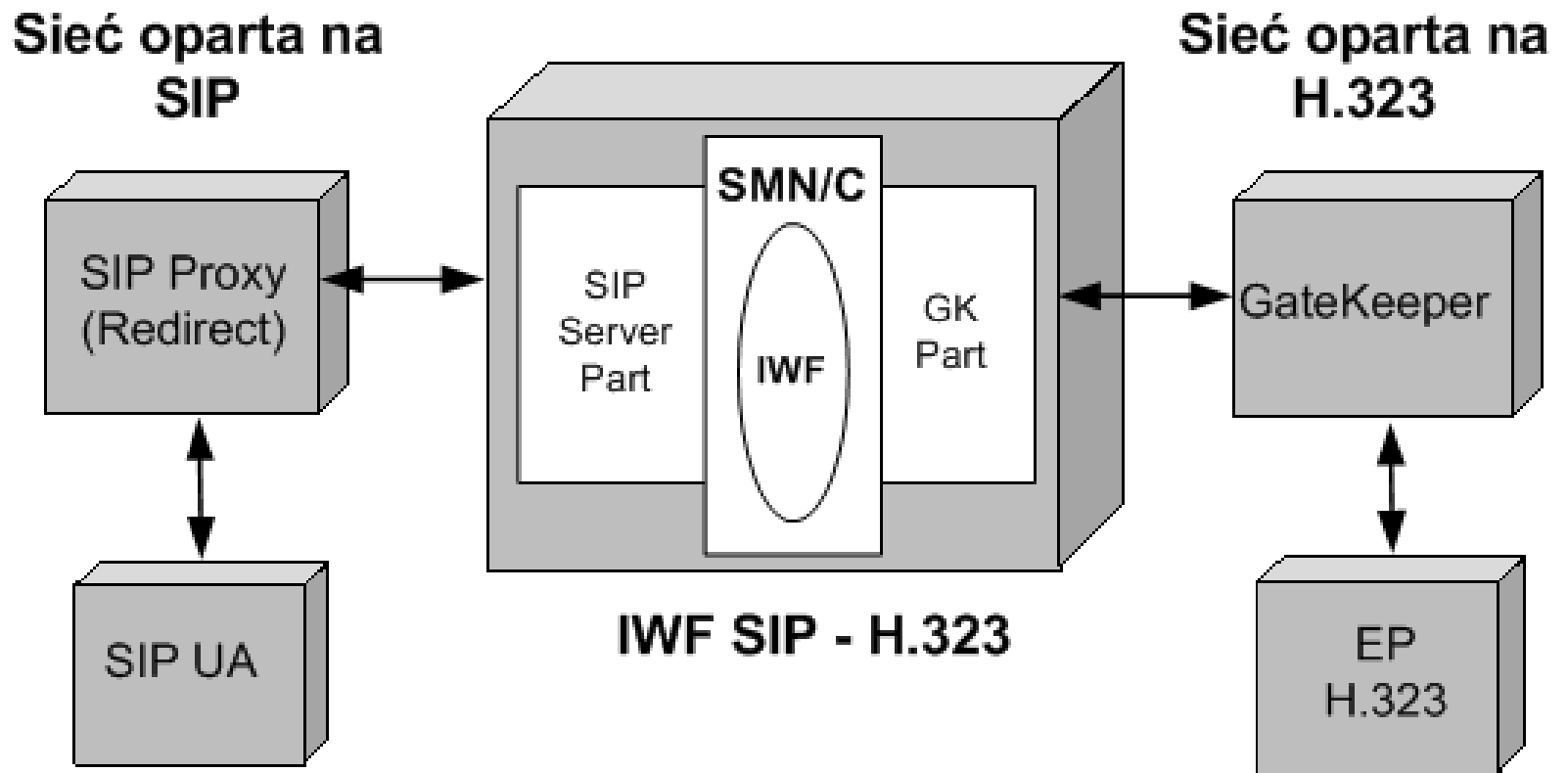




Wpływ IWF na bezpieczeństwo (2/3)

- **IWF** może wpływać na bezpieczeństwo:
 - **sprawdzać** oferowane mechanizmy zabezpieczeń
 - **negocjować** mechanizmy zabezpieczeń pomiędzy stroną inicjującą a docelową
 - zarówno **sprawdzać** jak i **negocjować**
 - **nie mieć wpływu** na wybór, czy sprawdzenie mechanizmów zabezpieczeń

Wpływ IWF na bezpieczeństwo (3/3)



SMN/C (*Security Mechanisms Negotiation/Control*)- służy do sprawdzenia bezpieczeństwa sygnalizacji lub/i odpowiada za negocjację zabezpieczeń

Bezpieczne środowisko dla VoIP (1/2)

- Generalne zasady projektowania sieci VoIP:
 - Logiczny podział sieci danych i telefonii (VLAN)
 - Nie stosowanie telefonów IP wykorzystujących stacje robocze
 - Kontrolowanie dostępu pomiędzy segmentami danych i telefonii



Źródło: Cisco



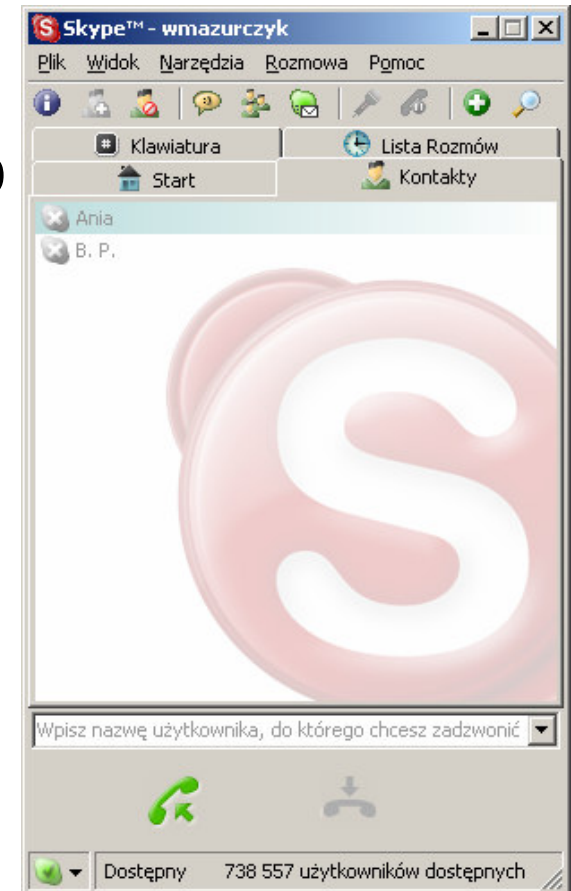
Bezpieczne środowisko dla VoIP (2/2)

- **Przeprowadzanie uwierzytelnienia** zarówno użytkowników jak i urządzeń
- **Uniemożliwienie włączenia do sieci potencjalnie groźnych urządzeń** poprzez:
 - 1) statyczne przypisywanie adresów IP do znanych adresów MAC. Konieczne wyłączenie DHCP!
 - 2) wyłączenie możliwości automatycznej rejestracji
 - 3) wykorzystywanie narzędzi do monitorowania adresów MAC (np. Arpwatch)
 - 4) filtrowanie wszystkich segmentów (blokowanie usługi)
- **Stosowanie narzędzi NIDS** (sieciowych systemów detekcji intruzów) w segmentach „głosowych”

SKYPE – zagrożenie dla VoIP?

■ Zalety:

- darmowy (!) i wykorzystuje technikę p2p
- do szyfrowania strumienia danych użyto 256 bitowy AES
- teoretycznie bardzo skalowalny
- brak problemów z Firewallami i NAT
- dobór kodeka do warunków w sieci i dostępnego łącza
- łatwa obsługa i konfiguracja
- rozproszona architektura i baza danych





SKYPE – zagrożenie dla VoIP?

- **Wady:**
 - brak informacji o protokole sygnalizacyjnym i jego bezpieczeństwie
 - niektóre firmy (np. CERN) **zabroniły użytkownikom instalacji Skype**
 - obserwacja adresu IP = zmiana miejsca przebywania użytkownika
 - problem tzw. **Supernodów** - anonimowa pomoc innym użytkownikom w połączeniu
 - pokusa użycia SN, **do celów komercyjnych**



Podsumowanie

- Wiele czynników wpływa na bezpieczeństwo VoIP
- Wystarczająca standaryzacja zabezpieczeń sygnalizacji VoIP – drobne słabości
- Główny problem: nie implementowanie zdefiniowanych mechanizmów zabezpieczeń
- Potrzeba bezpiecznej współpracy sieci opartych na różnych protokołach sygnalizacyjnych VoIP
- Środowisko sieciowe dla VoIP: rozdzielenie segmentów danych i głosu
- Przyszłość? Prognozy dobre, ale konkurencja potencjalnie mocna...



III Krajowa Konferencja Bezpieczeństwa Biznesu 2004

Bezpieczeństwo VoIP

Wojciech Mazurczyk

Instytut Telekomunikacji, Politechnika Warszawska

E-mail: W.Mazurczyk@elka.pw.edu.pl

Miedzeszyn, 23 listopad 2004