Enigma 2004

Bezpieczeństwo protokołów sygnalizacyjnych VoIP:
Koncepcja bezpiecznej współpracy protokołów SIP i H.323

Wojciech Mazurczyk
Instytut Telekomunikacji
Politechnika Warszawska
W.Mazurczyk@elka.pw.edu.pl
http://security.tele.pw.edu.pl

Układ prezentacji

- Cele referatu
- Problemy bezpieczeństwa usługi VoIP
- Zagrożenia i mechanizmy zabezpieczeń
- Kryterium oceny mechanizmów zabezpieczeń
- Analiza bezpieczeństwa protokołów sygnalizacyjnych VoIP: SIP i H.323
- Współpraca protokołów sygnalizacyjnych VoIP
- Podsumowanie

Cele referatu

- Przedstawienie stanu zabezpieczeń protokołów sygnalizacyjnych VoIP: SIP oraz H.323
- Prezentacja koncepcji, cech oraz własności IWF SIP-H.323
- Wymagania na bezpieczną współpracę protokołów sygnalizacyjnych VoIP

Problemy bezpieczeństwa usługi VoIP

- Trzy grupy problemów bezpieczeństwa usługi VoIP:

  - Bezpieczeństwo sygnalizacji
  - Bezpieczeństwo pakietów RTP
  - Firewall oraz NAT

- Protokoły sygnalizacyjne dla usługi VoIP (SIP, H.323 oraz H.248/Megaco)

Zagrożenia i mechanizmy zabezpieczeń

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

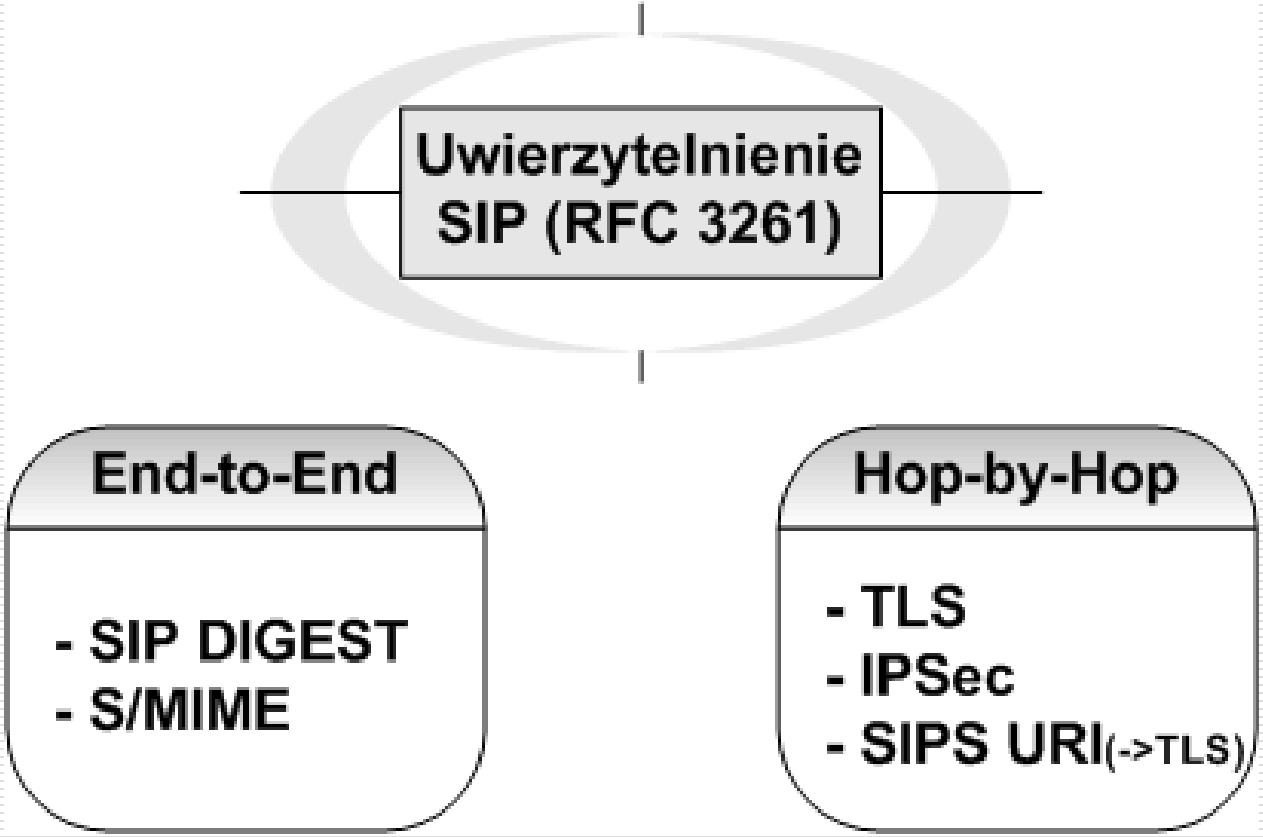
Kryterium oceny mechanizmów zabezpieczeń

- Potrzeba istnienia kryterium oceny
- Modyfikacja kryterium z normy ISO 7498-2

(uwierzytelnienie, integralność, poufność, niezaprzeczalność i kontrola dostępu)

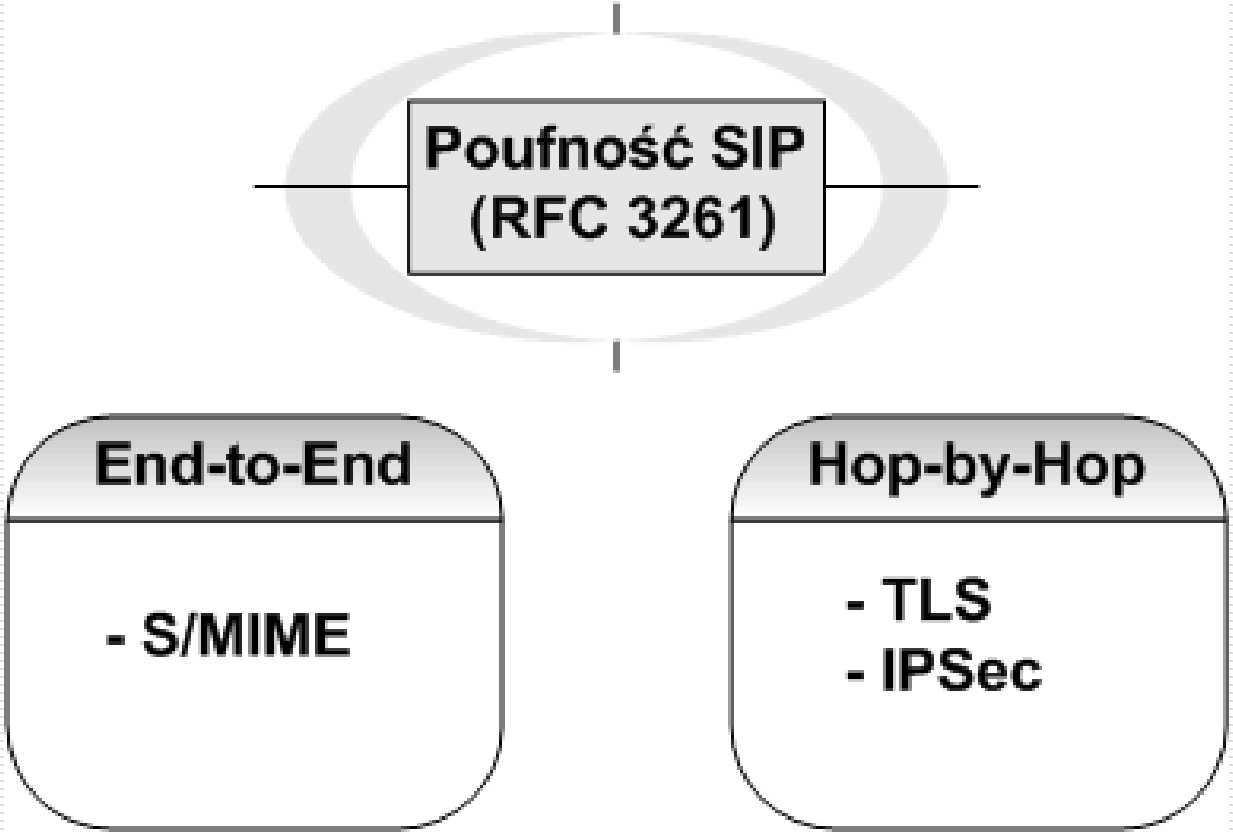
- Uwierzytelnienie oraz poufność - usługi ochrony informacji i komunikacji w sieci gwarantujące bezpieczeństwo protokołu sygnalizacyjnego VoIP

Analiza mechanizmów zabezpieczeń protokołu SIP (1/2)



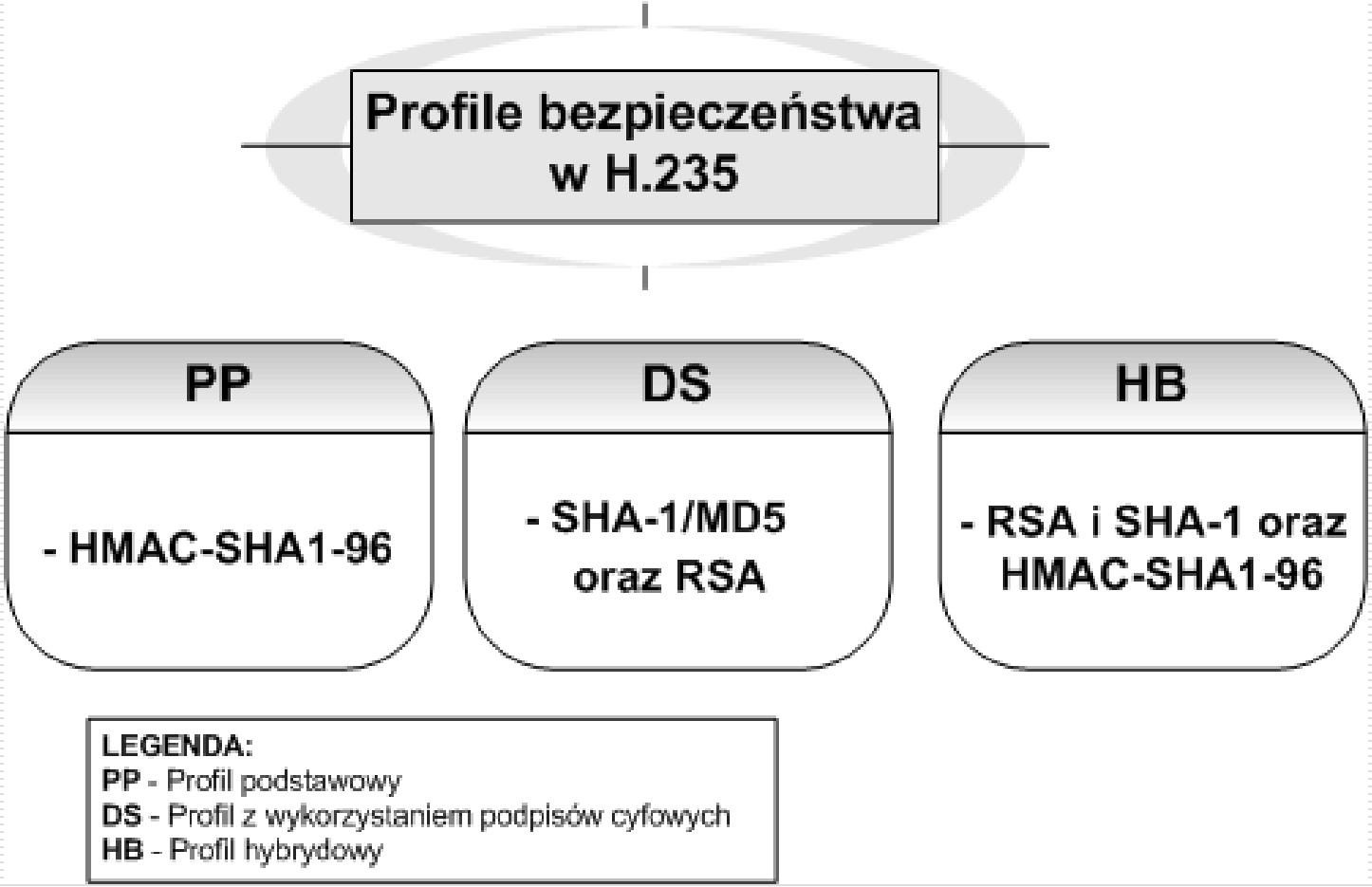
- Przystosowanie istniejących mechanizmów

Analiza mechanizmów zabezpieczeń protokołu SIP (2/2)

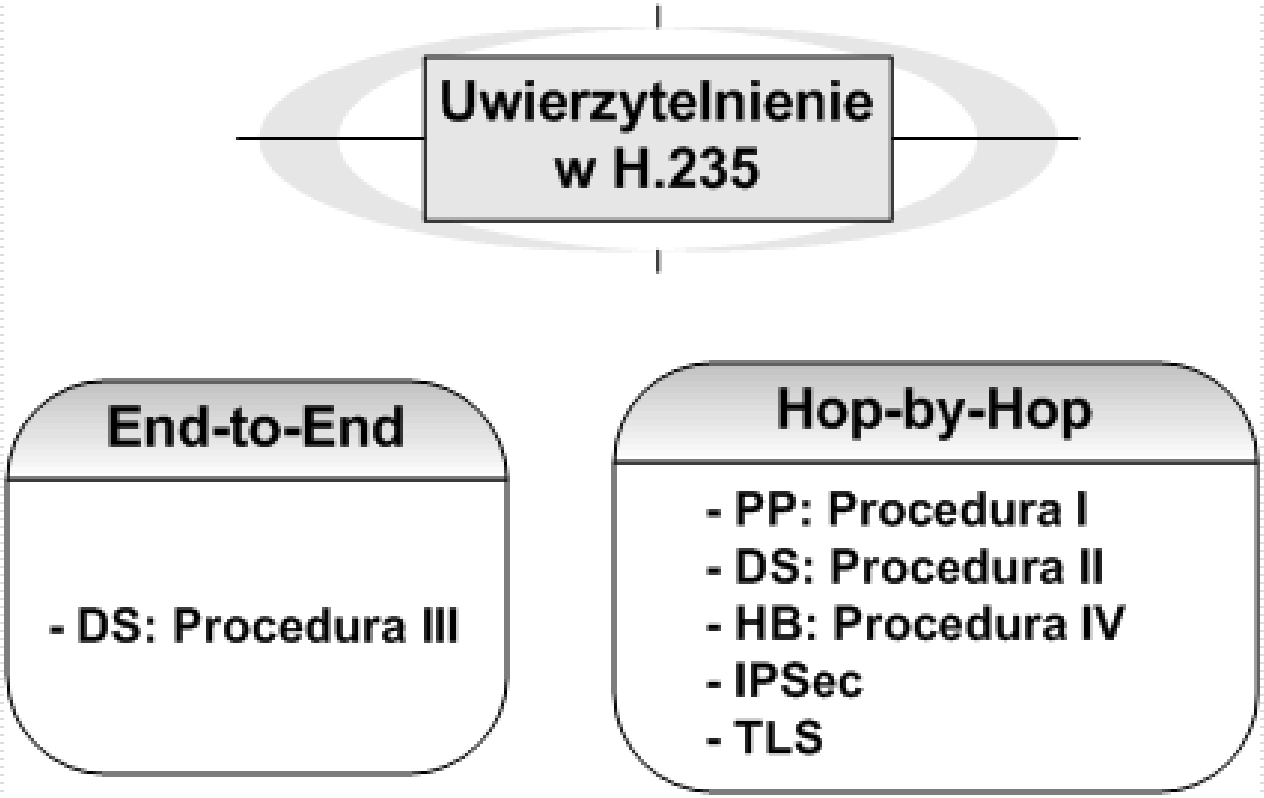


- Żaden z mechanizmów nie jest bez wad

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



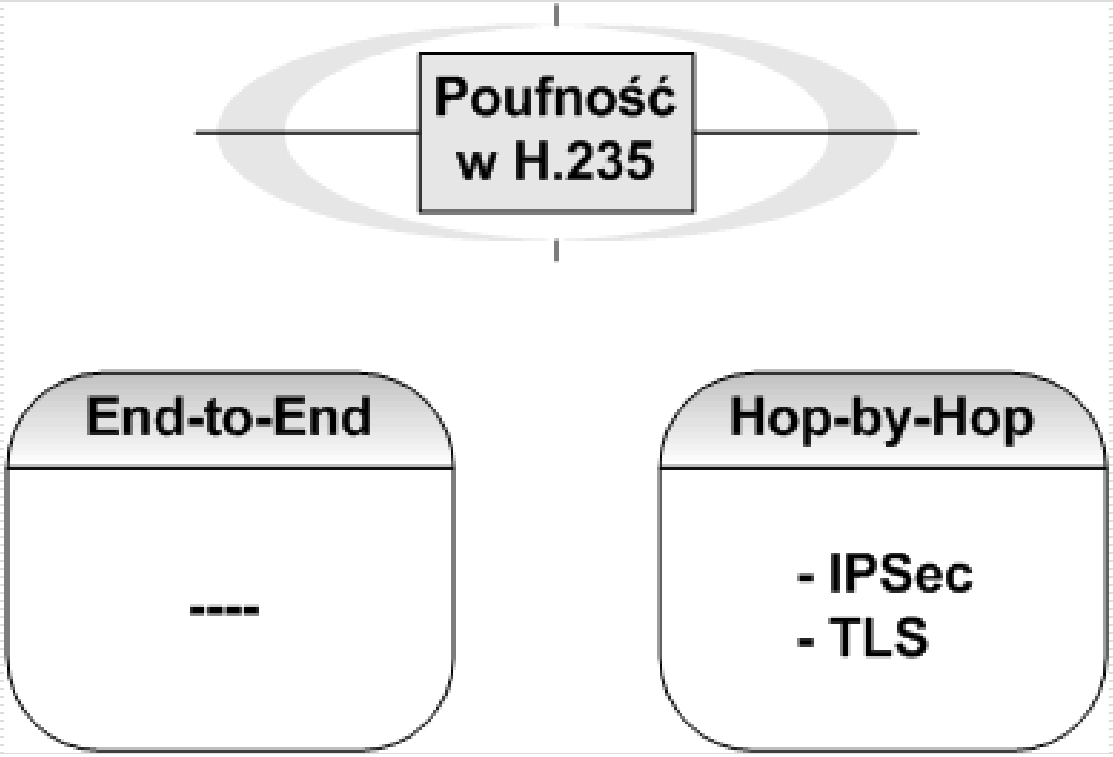
Analiza mechanizmów zabezpieczeń protokołu H.323 (2/3)



- 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*)



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

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

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

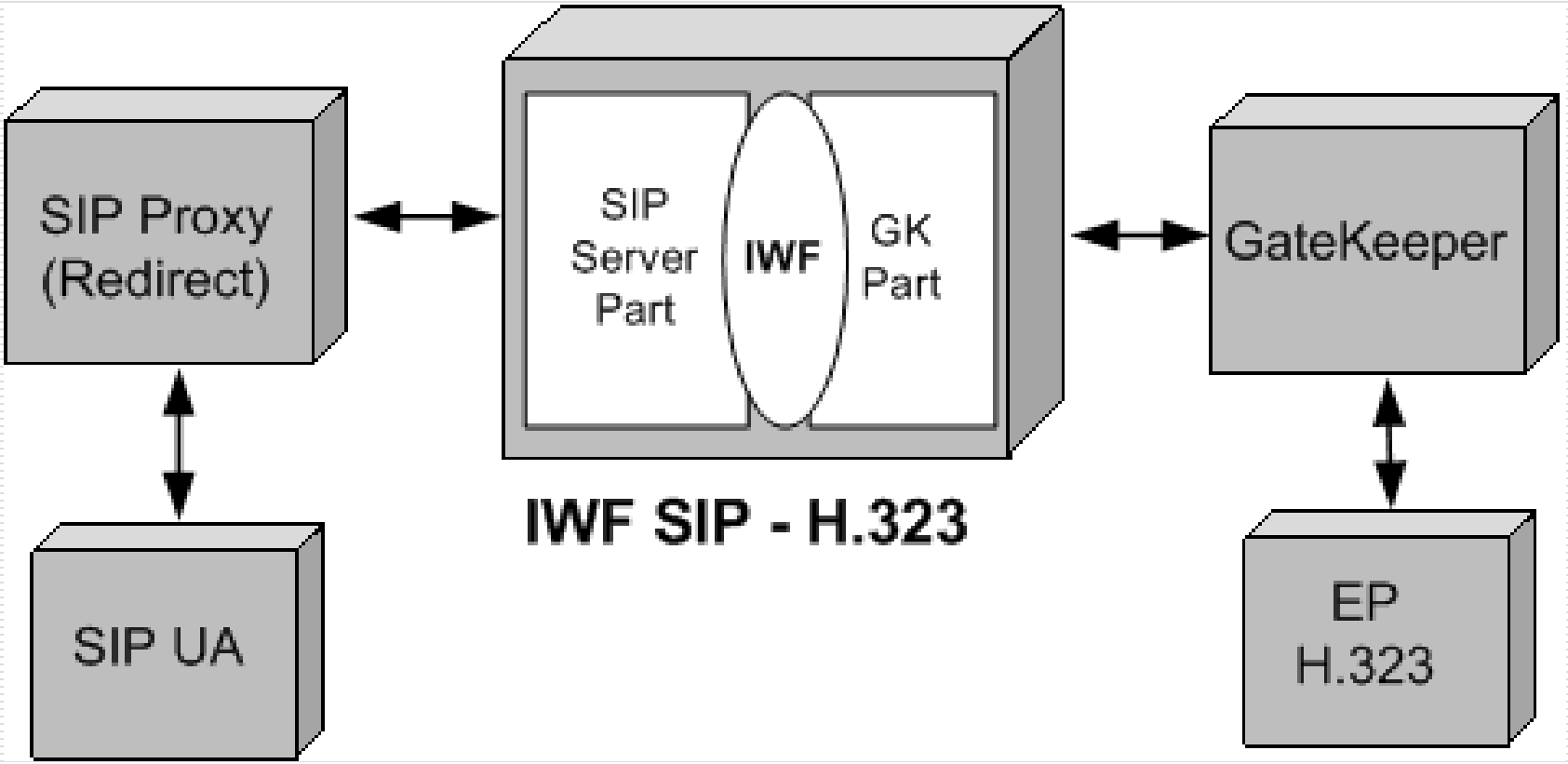
Wymagania bezpieczeństwa IWF SIP-H.323 (2/2)

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

Podsumowanie

- Wystarczający stan zabezpieczeń sygnalizacji VoIP – drobne słabości
- Główny problem: nie implementowanie zdefiniowanych mechanizmów zabezpieczeń
- Konieczność zapewnienia bezpieczeństwa również przy współpracy sieci opartych na różnych protokołach sygnalizacyjnych VoIP

Enigma 2004

Bezpieczeństwo protokołów sygnalizacyjnych VoIP:
Koncepcja bezpiecznej współpracy protokołów SIP i H.323

Wojciech Mazurczyk
Instytut Telekomunikacji
Politechnika Warszawska
W.Mazurczyk@elka.pw.edu.pl
http://security.tele.pw.edu.pl