BSI 2003

Bezpieczeństwo Voice over IP bazującego na SIP

Wojciech Mazurczyk, Krzysztof Szczypiorski
Instytut Telekomunikacji, Politechnika Warszawska
E-mail: {W.Mazurczyk, K.Szczypiorski}@elka.pw.edu.pl
http://security.tele.pw.edu.pl

Układ prezentacji

- Usługa VoIP
- Omówienie podstaw protokołu SIP (zalecenia: RFC 2543 oraz RFC3261)
- Analiza bezpieczeństwa protokołu SIP
- Przeprowadzone doświadczenia praktyczne – uzyskane wyniki
- Podsumowanie

Usługa VoIP

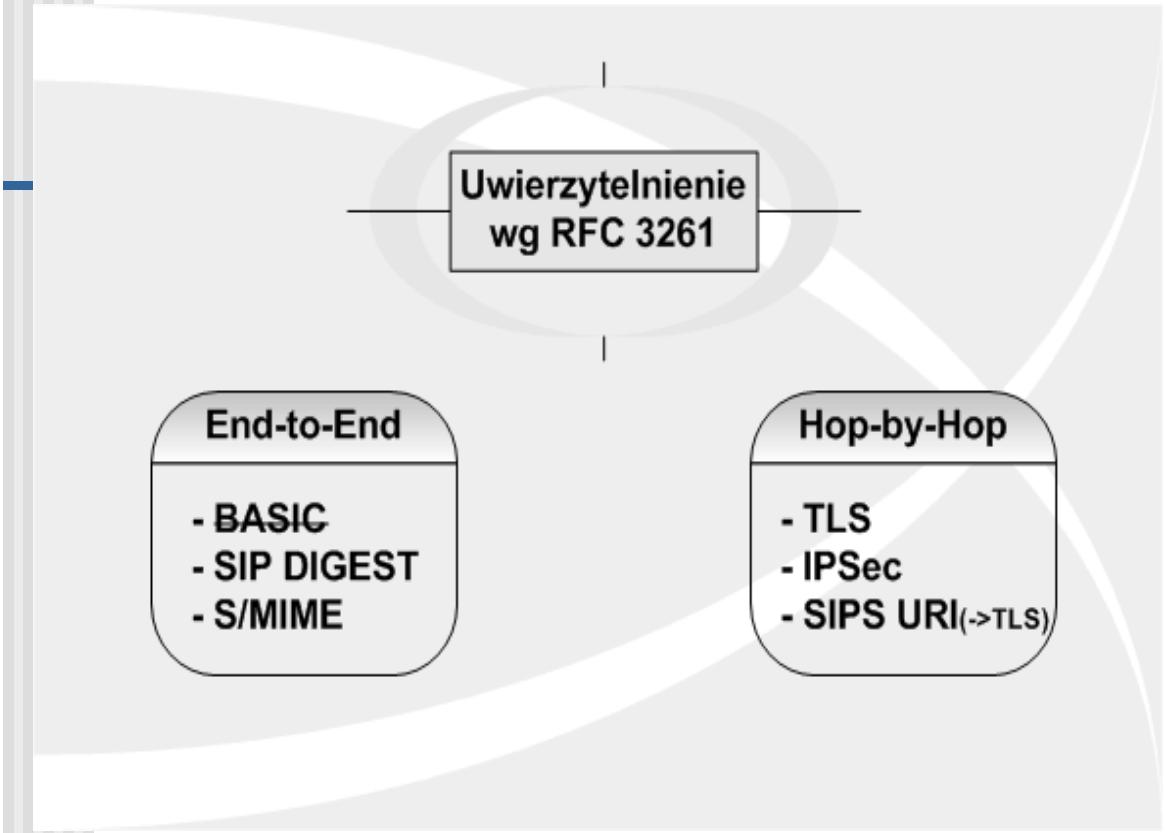
- Wprowadzenie do VoIP
- Protokoły umożliwiające realizację telefonii IP (zespół protokołów):
  - Kodeki mowy (np. G.723.1)
  - Protokoły transportowe (RTP, UDP, TCP)
  - **Protokoły sygnalizacyjne** (SIP, H.323, MGCP, H.248/Megaco)
  - Protokoły uzupełniające (SDP, RTCP, RSVP)

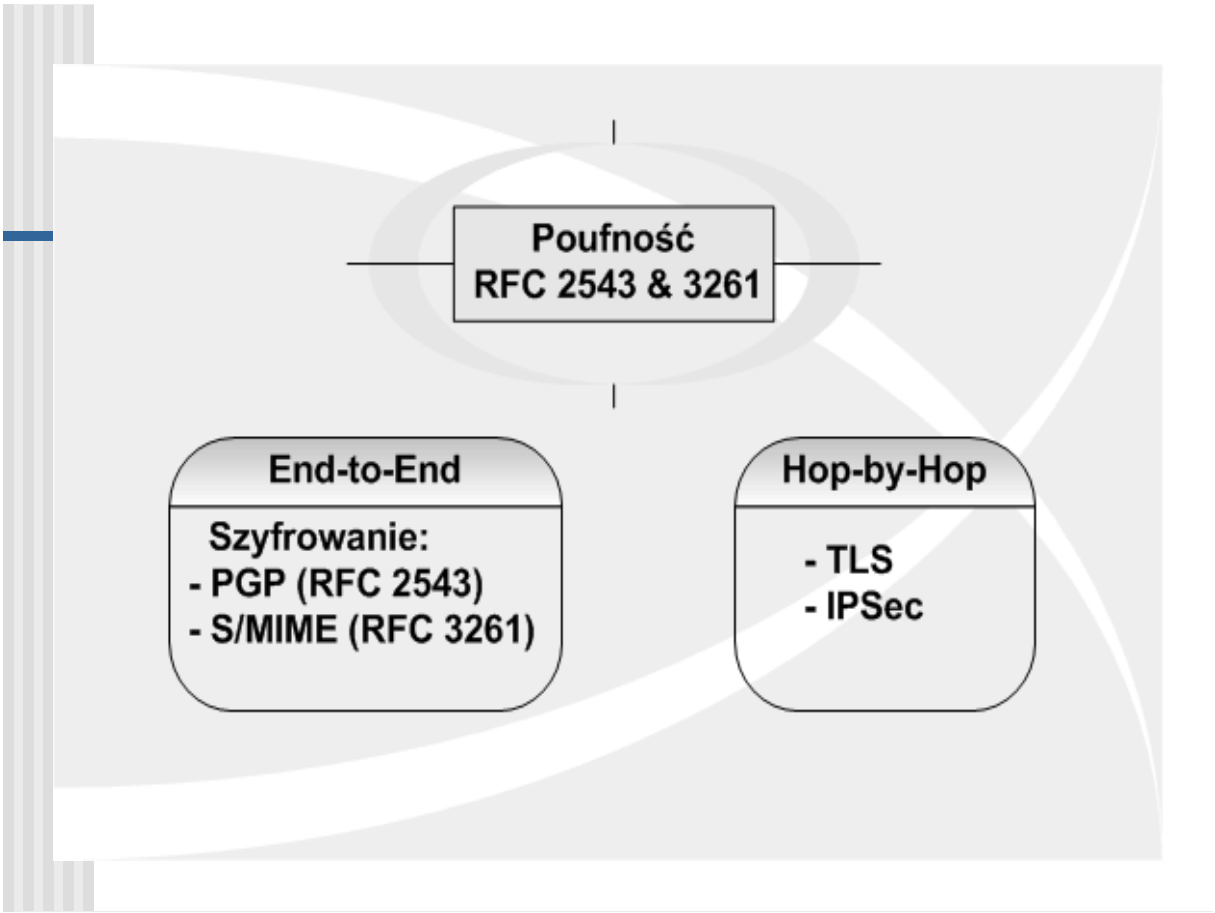
Protokół SIP

- Cechy i zalety SIP
  - Obsługa zmienności lokalizacji
  - Podobieństwo działania do HTTP
  - Wykorzystanie m.in. DNS, URI oraz MIME
  - Współpraca z protokołami transportowymi
  - Mała złożoność + duża rozszerzalność
- Podstawy Session Initiation Protocol
  - Adresowanie (sip://j.kowalski@tele.pw.edu.pl)
  - Architektura funkcjonalna
  - Metody i rodzaje odpowiedzi (INVITE, ACK, BYE, CANCEL, REGISTER, OPTIONS)

Bezpieczeństwo SIP 1/3

- Istota bezpieczeństwa usługi VoIP opartego na SIP
- Główne techniki ataków na wymianę wiadomości sygnalizacyjnych:
  - Podszycie się (Spoofing)
  - Podsłuchiwanie (Sniffing)
  - Blokowanie działania (Denial of Service)
- Dobór odpowiedniego kryterium oceny mechanizmów bezpieczeństwa SIP (modyfikacja normy ISO 7498-2)





Bezpieczeństwo SIP 3/3

- Wskazanie słabych punktów obu architektur bezpieczeństwa

RFC 2543

- Wiele luk bezpieczeństwa
- Mechanizmy SIP Digest, Basic
  - brak całkowitej integralności wiadomości
  - Basic - nieodporność na atak typu powtórka
- Szyfrowanie PGP
  - brak systemu certyfikacji

Bezpieczeństwo SIP 3/3

- Wskazanie słabych punktów obu architektur bezpieczeństwa

RFC 3261

- Poprawna architektura bezpieczeństwa
- Mankamenty SIP Digest
- Problemy S/MIME
  - brak systemu wymiany kluczy
  - ”duże” wiadomości sygnalizacyjne
  - problem rzadkich typów serwerów sieciowych

Przeprowadzone doświadczenia

- **Zakładany cel i przebieg badań praktycznych**
- Testowane aplikacje SIP UA
- Konieczność modyfikacji celu pierwotnego
- Opis i konfiguracje przeprowadzonych doświadczeń
- Omówienie wykorzystanych testów

Przeprowadzone doświadczenia

- Zakładany cel i przebieg badań praktycznych
- **Testowane aplikacje SIP UA**
- Konieczność modyfikacji celu pierwotnego
- 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** firmy Siemens
  - **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

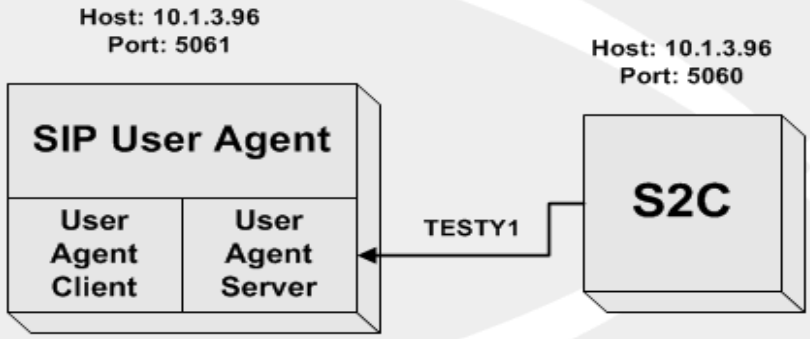
- Zakładany cel i przebieg badań praktycznych
- Testowane aplikacje SIP UA
- **Konieczność modyfikacji celu pierwotnego**
- Opis i konfiguracje przeprowadzonych doświadczeń
- Omówienie wykorzystanych testów

Przeprowadzone doświadczenia

- Zakładany cel i przebieg badań praktycznych
- Testowane aplikacje SIP UA
- Konieczność modyfikacji celu pierwotnego
- **Opis i konfiguracje przeprowadzonych doświadczeń**
- Omówienie wykorzystanych testów

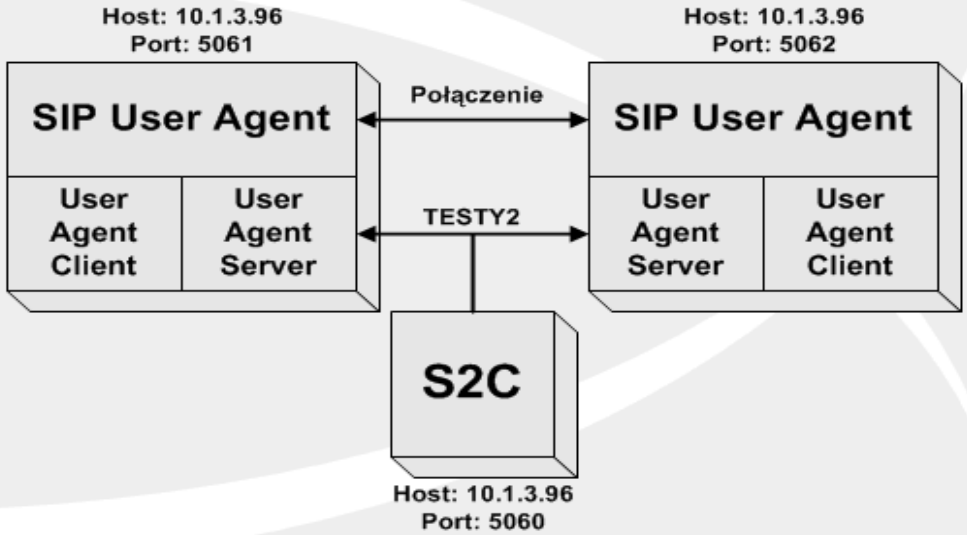
Konfiguracje testowe 1/3

Pierwsza konfiguracja testowa:

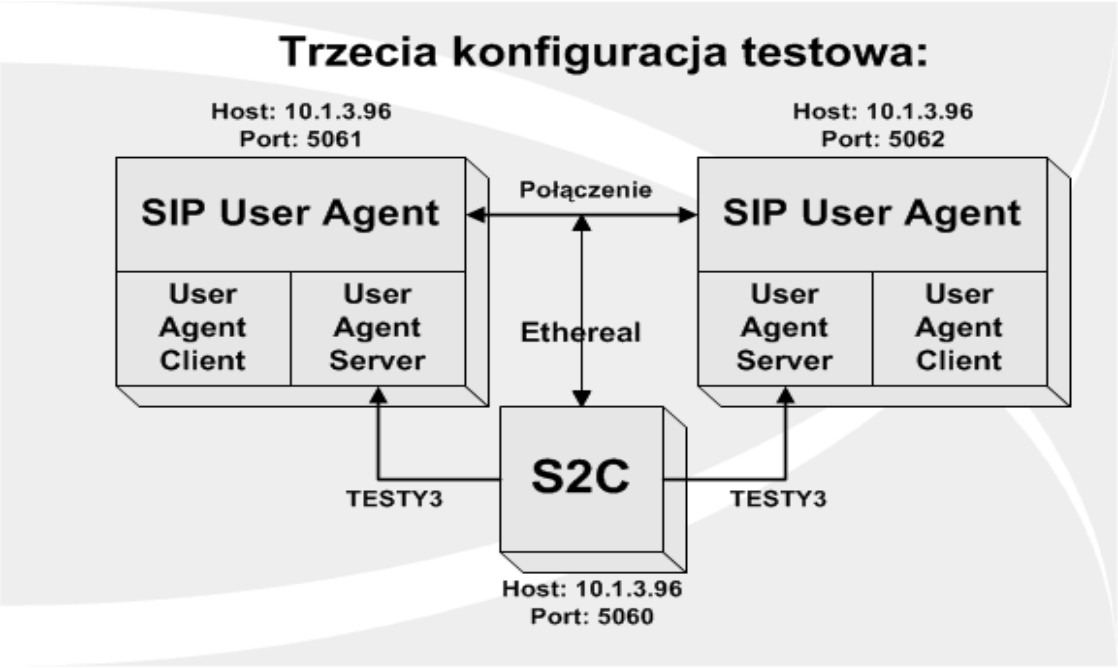


Konfiguracje testowe 2/3

Druga konfiguracja testowa:



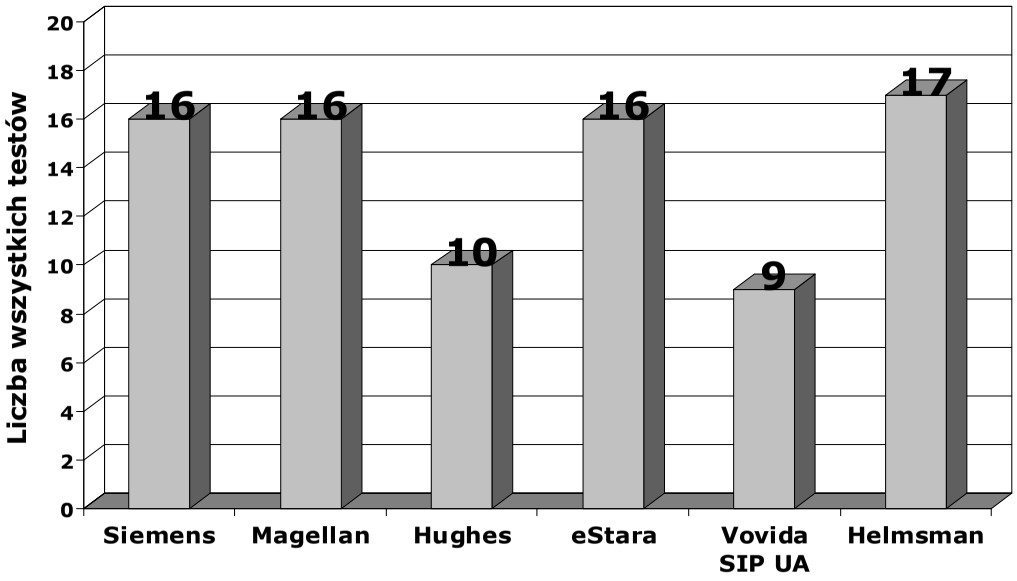
Konfiguracje testowe 3/3



Przeprowadzone doświadczenia

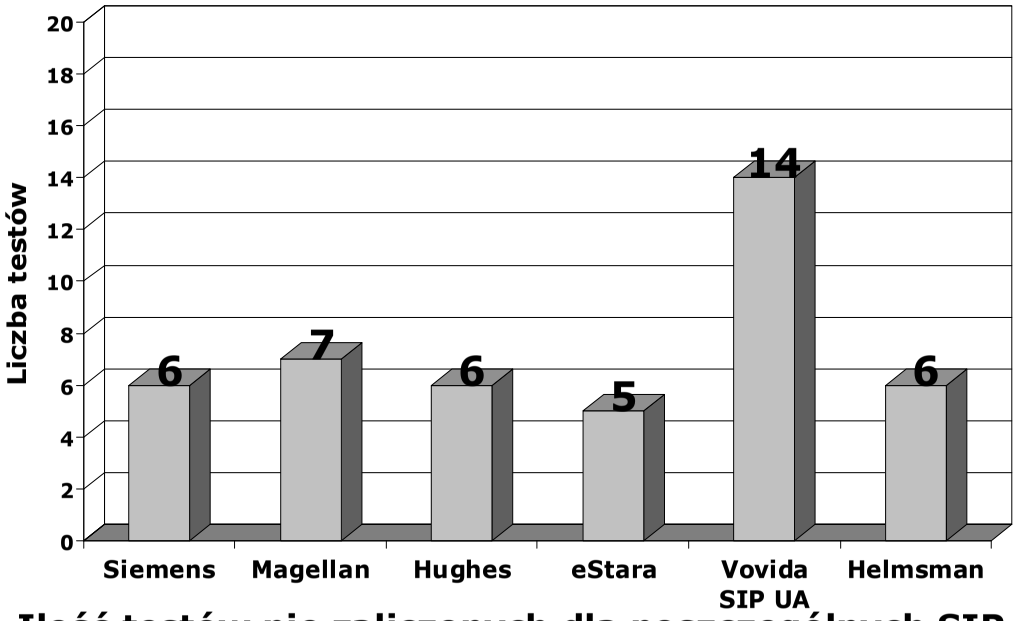
- Zakładany cel i przebieg badań praktycznych
- Testowane aplikacje SIP UA
- Konieczność modyfikacji celu pierwotnego
- Opis i konfiguracje przeprowadzonych doświadczeń
- **Omówienie wykorzystanych testów**

Wyniki doświadczeń 1/2



Ilość zaliczonych testów dla poszczególnych SIP UA

Wyniki doświadczeń 2/2



Ilość testów nie zaliczonych dla poszczególnych SIP UA

Uzyskane wyniki - wnioski

- Liczne błędy implementacyjne badanych SIP UA
- Potwierdzenie słuszności opracowania kolejnej wersji protokołu SIP
  (RFC 2543 → RFC 3261)
- Zalety stosowania mechanizmów bezpieczeństwa (testy SIP Digest)

Podsumowanie i wnioski

Zaprezentowano:

- Usługę VoIP
- Podstawy protokołu sygnalizacyjnego Session Initiation Protocol
- Mechanizmy bezpieczeństwa dla SIP w dwóch zaleceniach (RFC 2543 i RFC 3261)
- Metody testowania bezpieczeństwa aplikacji SIP UA

BSI 2003

Bezpieczeństwo Voice over IP bazującego na SIP

Wojciech Mazurczyk, Krzysztof Szczypiorski
Instytut Telekomunikacji, Politechnika Warszawska
E-mail: {W.Mazurczyk, K.Szczypiorski}@elka.pw.edu.pl
http://security.tele.pw.edu.pl