Krajowe Sympozjum Telekomunikacji 2003

Bezpieczeństwo SIP jako protokołu sygnalizacyjnego VoIP

inż. Wojciech Mazurczyk
Instytut Telekomunikacji, Politechnika Warszawska
E-mail: W.Mazurczyk@elka.pw.edu.pl

Bydgoszcz, 10 – 12 września 2003

Plan prezentacji

- Usługa VoIP
- Bezpieczeństwo SIP
- Przeprowadzone doświadczenia praktyczne: idea, przebieg i wyniki
- Wyniki testów organizacji CERT
- 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)

Bezpieczeństwo SIP

- Istota bezpieczeństwa usługi VoIP opartej na SIP
- Główne techniki ataków na wymianę wiadomości sygnalizacyjnych:
  - Podszycie (Spoofing)
  - Podsłuchiwanie (Sniffing)
  - Blokowanie działania (Denial of Service)
- Mechanizmy bezpieczeństwa SIP
  - Zewnętrzne (TLS, IPSec)
  - Wewnętrzne (np. SIP Digest)

Przeprowadzone doświadczenia

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

Testowane SIP UA

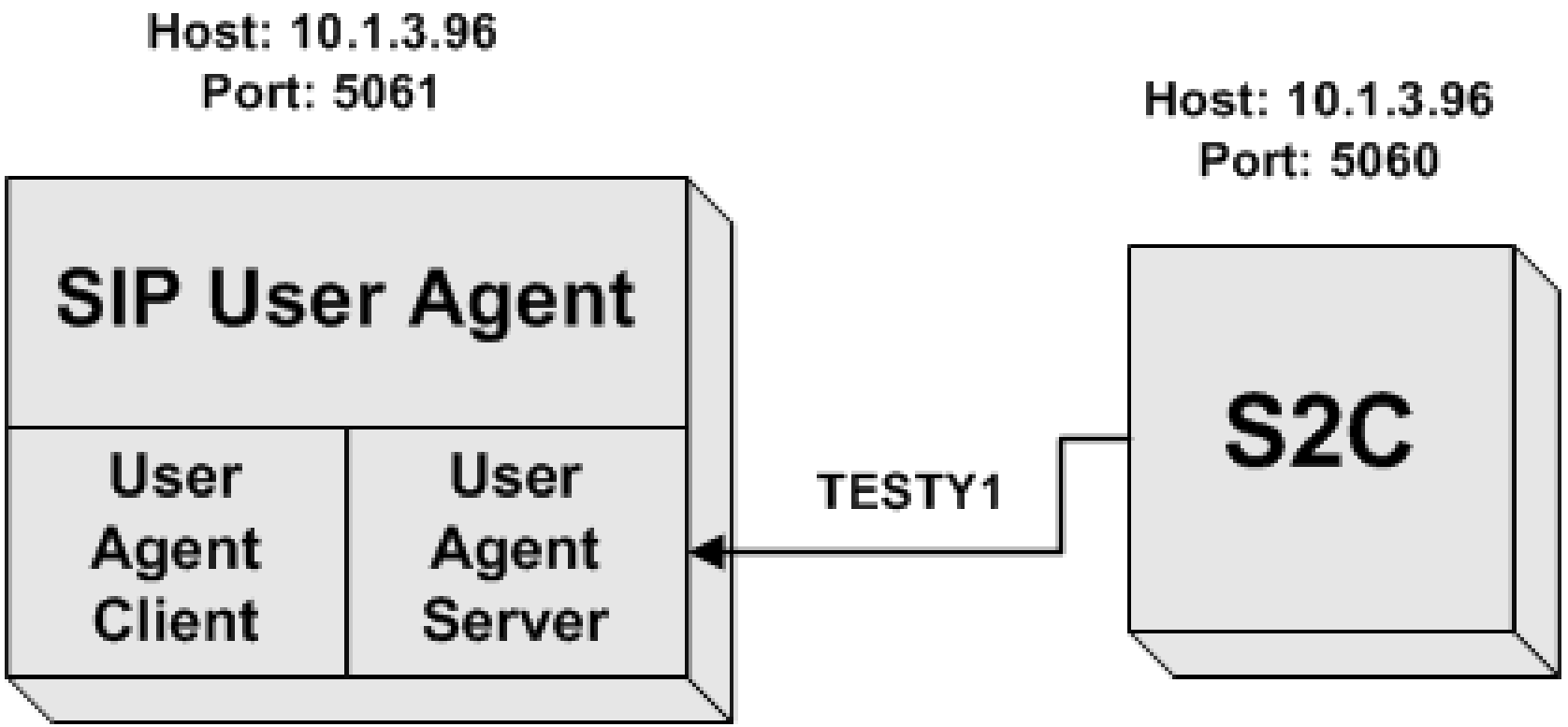
- Wybrane aplikacje:
  - **Helmsman User Agent 3.0.6** firmy Helmsman
  - **eStara SoftPHONE 3.0** firmy eStara
  - **Siemens Communication System Client v.1.0**
  - **Magellan 4.0** opracowany w IT PW
  - **Hughes SIP User Agent (E-Z Phone)** firmy Hughes Software Systems
  - **Vovida SIP UA 1.0.2 -**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

- Kryterium wyboru **- powszechność**

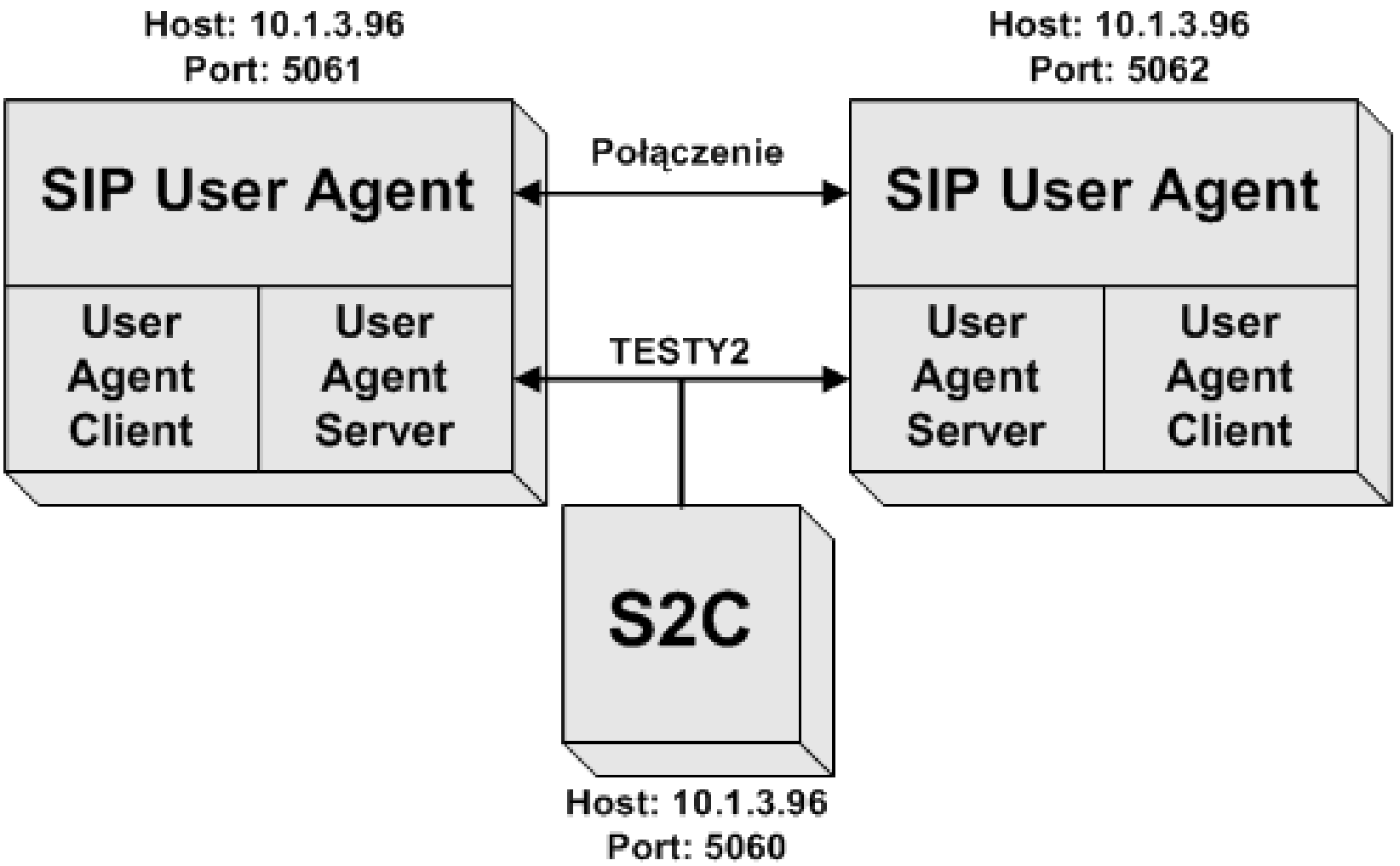
Przeprowadzone doświadczenia

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

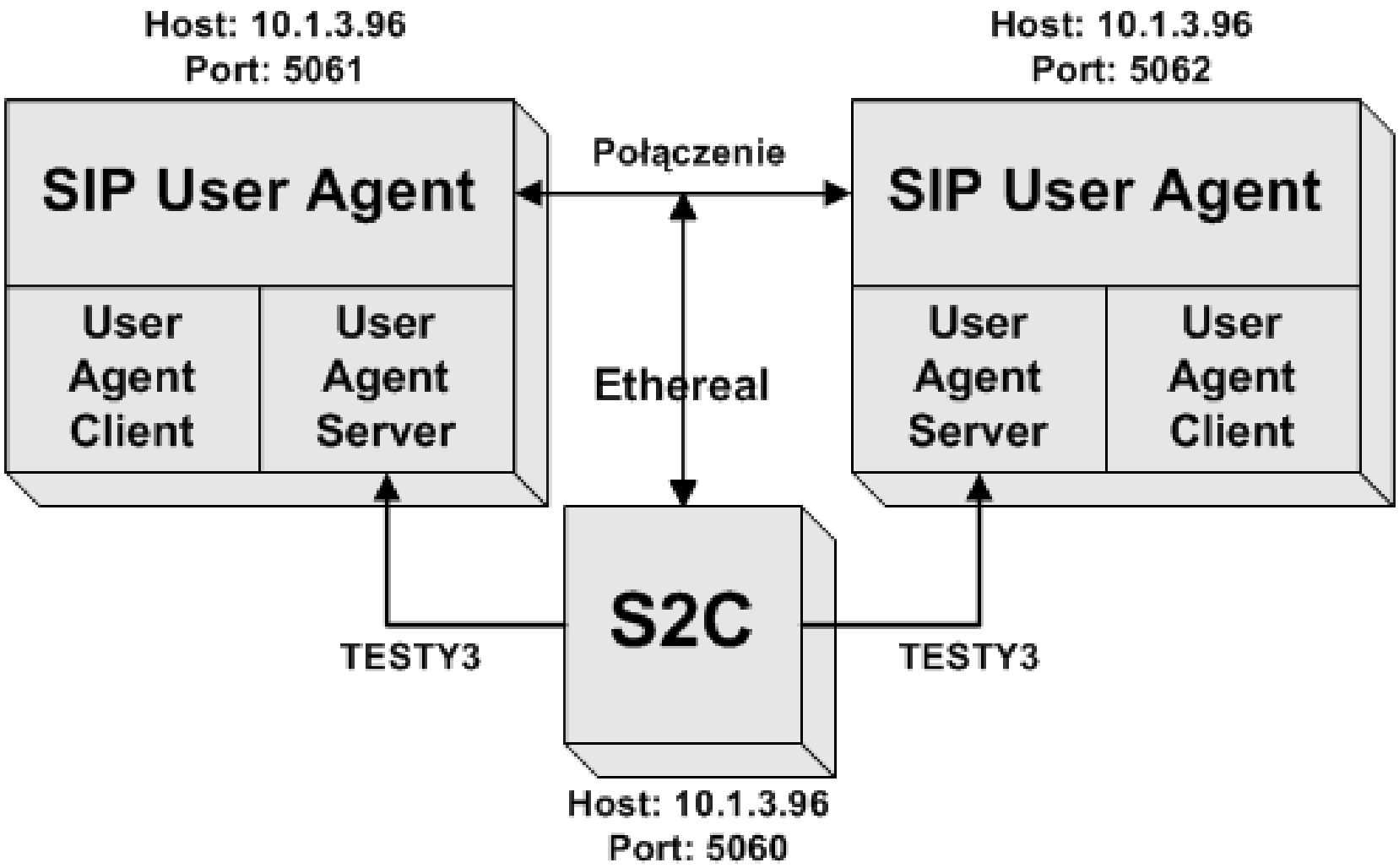
Konfiguracje testowe 1/3



Konfiguracje testowe 2/3



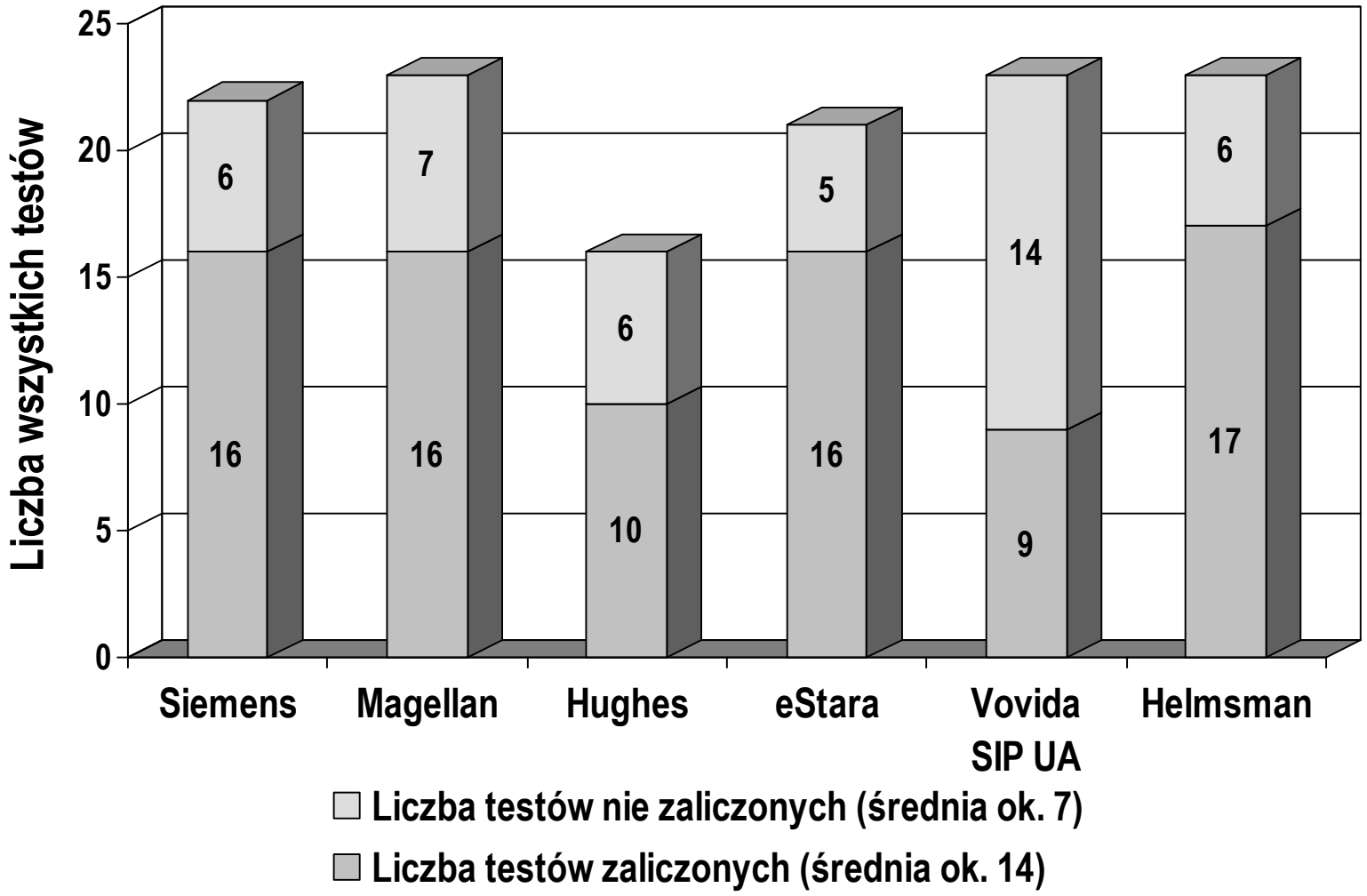
Konfiguracje testowe 3/3



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
- Potwierdzenie konieczności opracowania kolejnej wersji protokołu SIP (RFC 2543 → RFC 3261)
- Wzrost bezpieczeństwa aplikacji w przypadku stosowania mechanizmów bezpieczeństwa (ale potrzebna większa moc obliczeniowa)

Wyniki testów organizacji CERT

- Przedstawienie opublikowanych badań
- Metoda testowania (zestaw PROTOS)
- Uzyskane wyniki – zgodność wniosków:
  - Potwierdzenie słuszności metod testowania Agentów Użytkownika SIP
  - Błędy implementacyjne w **komercyjnych** wersjach SIP UA
- Podsumowanie