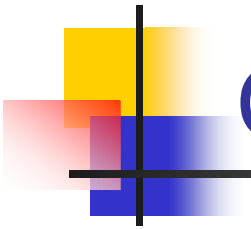
Politechnika Warszawska
Wydział Elektroniki i Technik Informacyjnych

Bezpieczny system telefonii VoIP opartej na protokole SIP

Leszek Tomaszewski

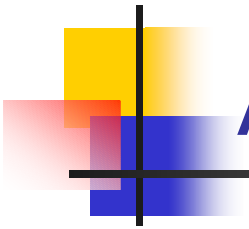


Cel

- Stworzenie bezpiecznej i przyjaznej dla użytkownika architektury sieci SIP zapewniającej:
  - Szyfrowane sygnalizacji
  - Szyfrowanie mediów

Przyczyny zagrożeń

- Otwarta infrastruktura sieciowa
  - Internet
- Niezależność dostawcy usługi i sieci
- Nieznana droga transmisji danych (wielu pośredników)

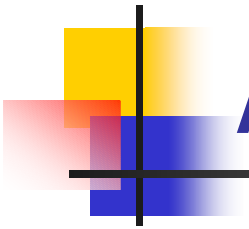


Ataki na sygnalizację

- Podsłuchanie wiadomości
  - analiza przesyłu
  - odkrycie treści (URI użytkownika)
- Podszycie
  - Modyfikacja wiadomości
    - nagłówka *Connect* w metodzie REGISTER (Registration Hijacking)
    - nagłówka From w metodzie INVITE
    - Inne ....
  - Podrobienie
    - wysłanie spreparowanej wiadomości BYE (Tearing Down Session)

Ataki na media

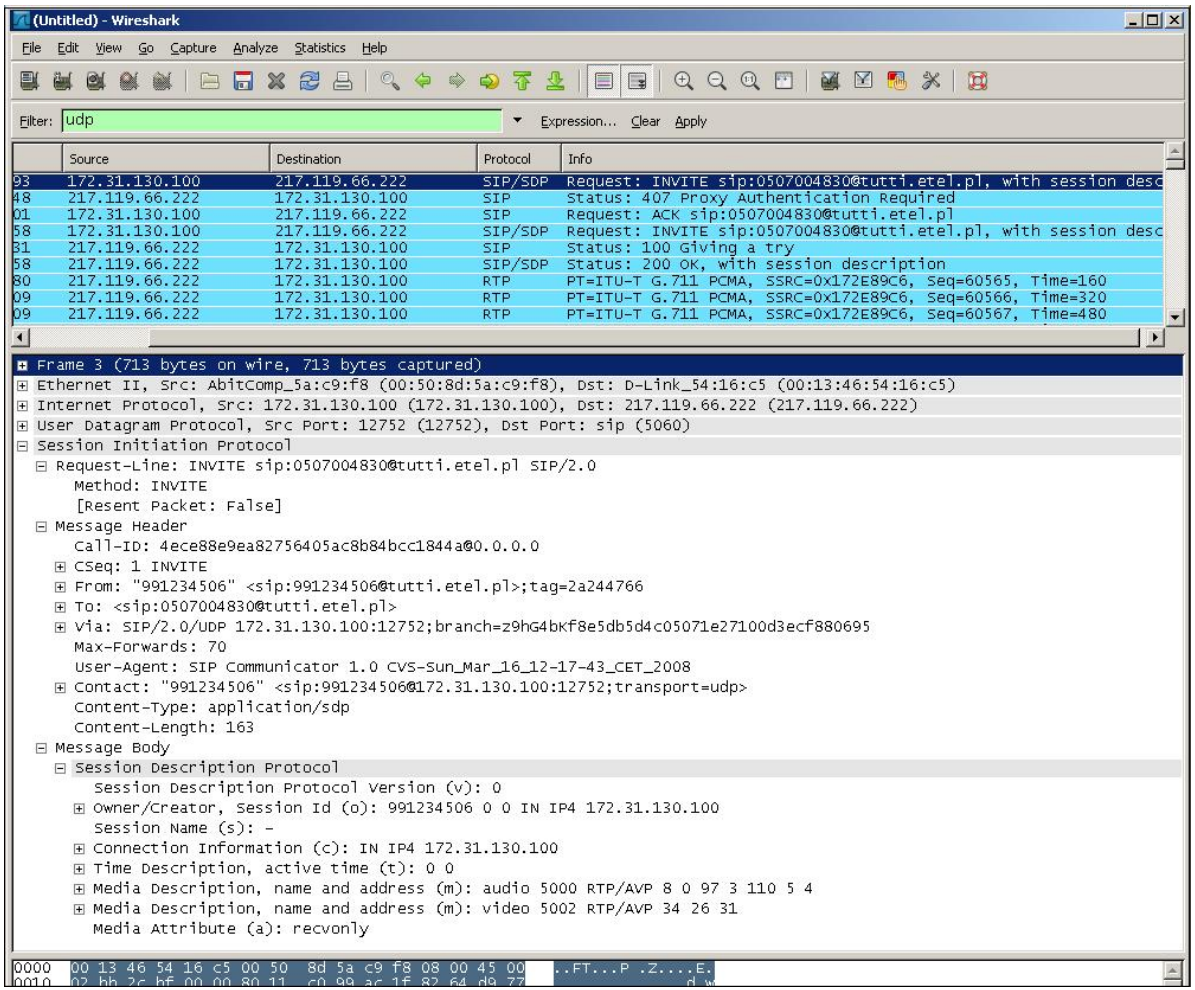
- Podsłuchanie wiadomości
  - analiza przesyłu
  - odkrycie treści



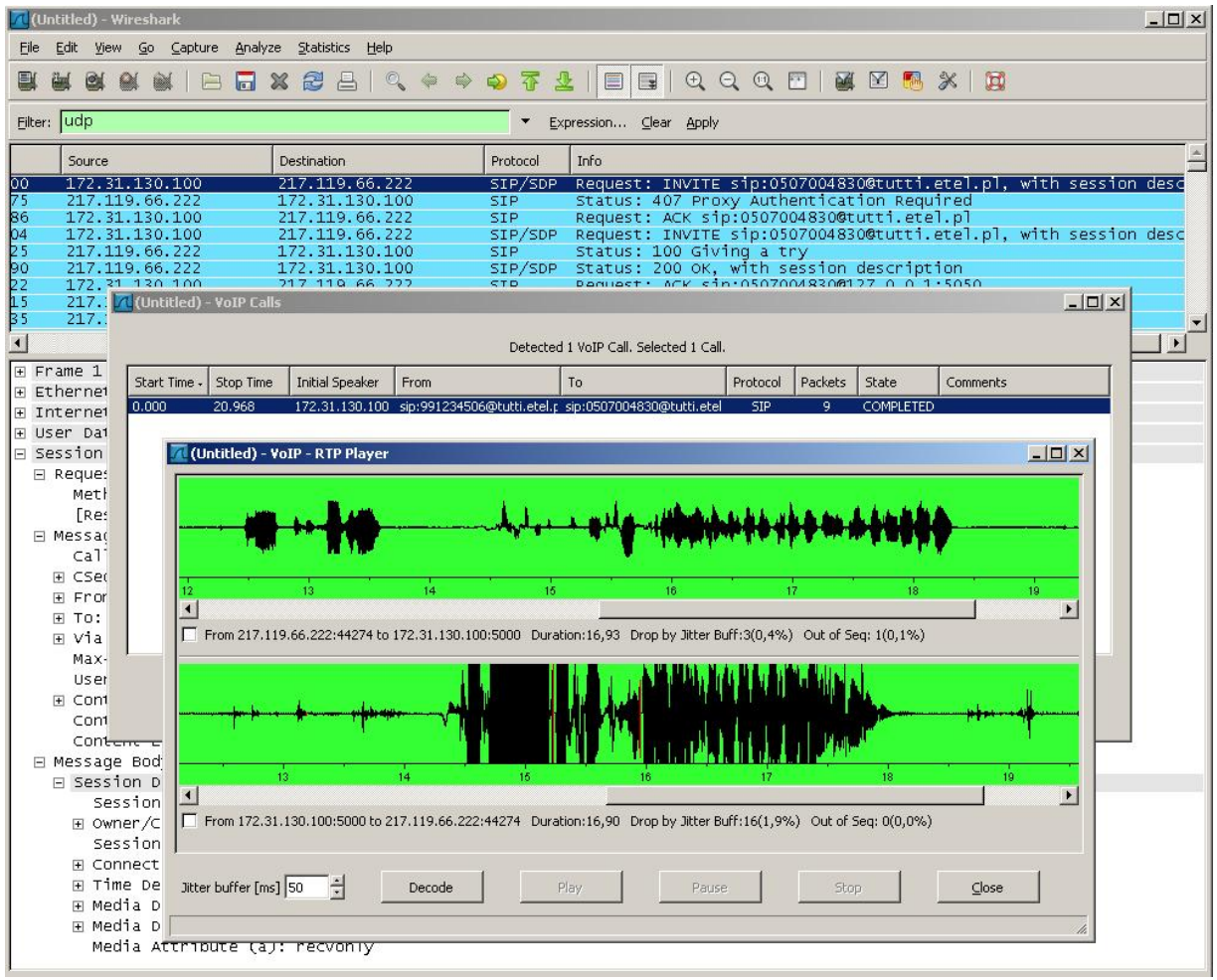
Ataki typu DoS

- Zalanie serwera wiadomościami sygnalizacyjnymi
- Zalanie serwera pakietami RTP

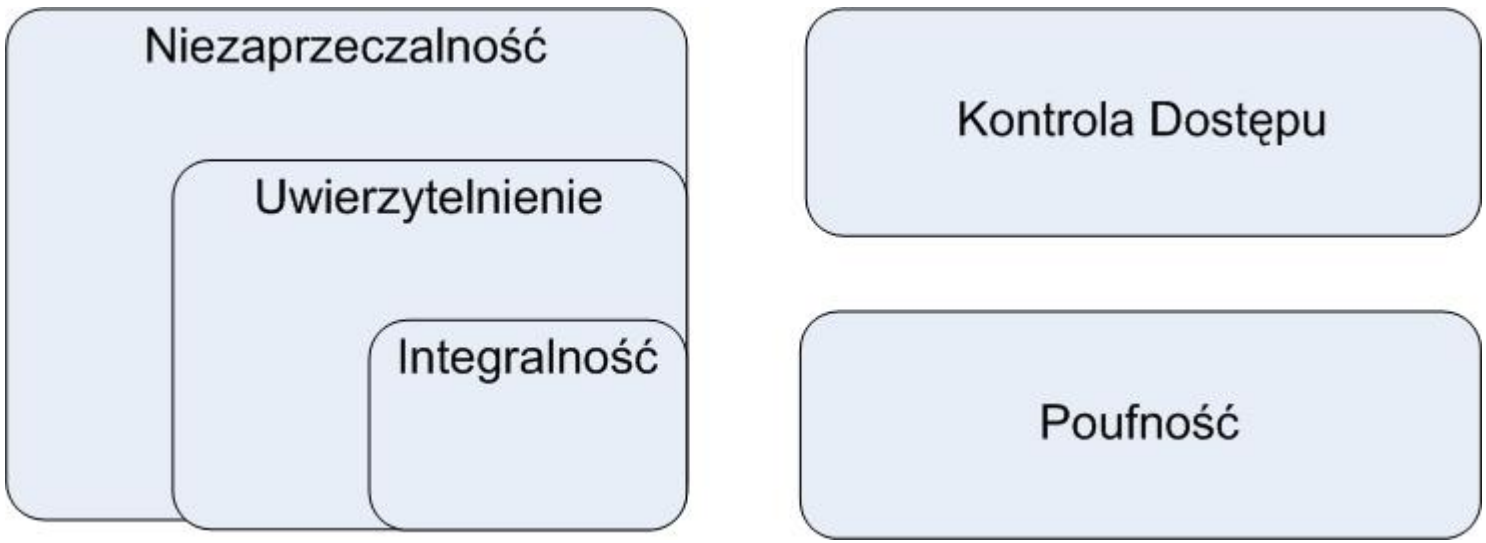
Przykład ataku podsłuchu



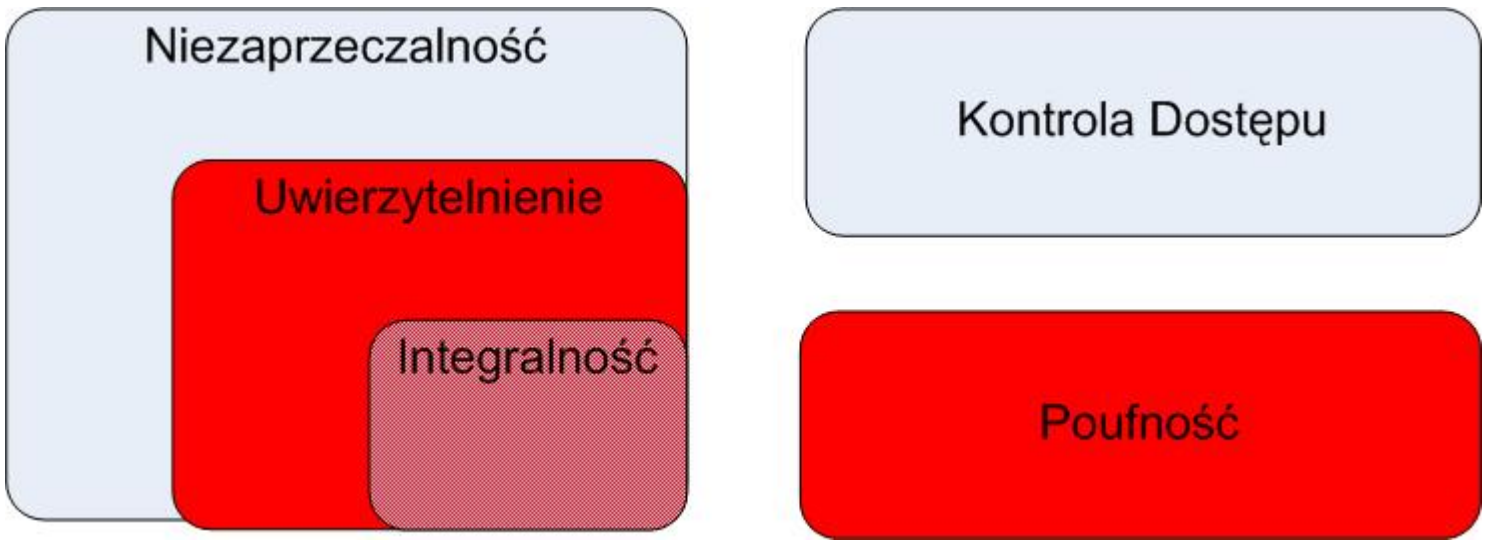
Przykład ataku podsłuchu



Usługi ochrony informacji



Usługi ochrony informacji



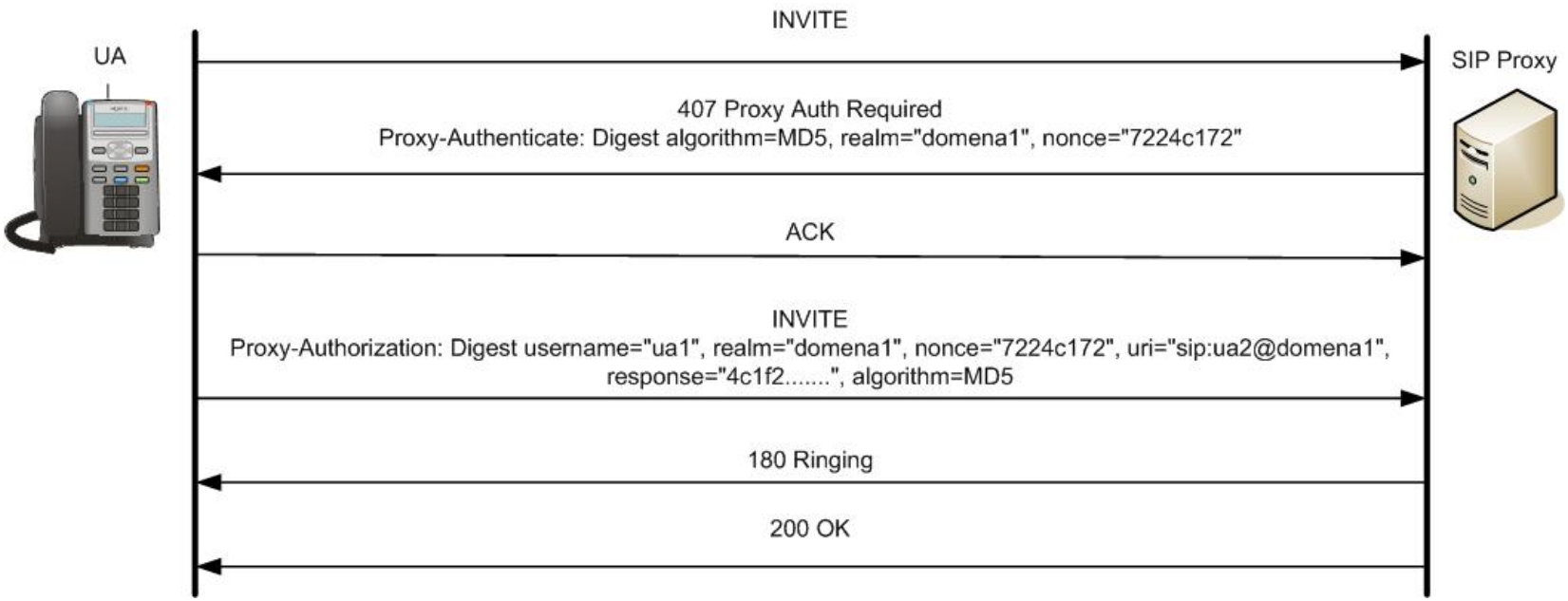
SIP – wymagania bezpieczeństwa (RFC 3261)

- Uwierzytelnienie
  - Tryb end-to-end
    - SIP DIGEST (obowiązkowy)
    - S/MIME
  - Tryb hop-by-hop
    - TLS
    - IPSec
    - SIPS URI

SIP – wymagania bezpieczeństwa(RFC 3261)

- Poufność
  - Tryb end-to-end
    - S/MIME
  - Tryb hop-by-hop
    - TLS
    - IPSec

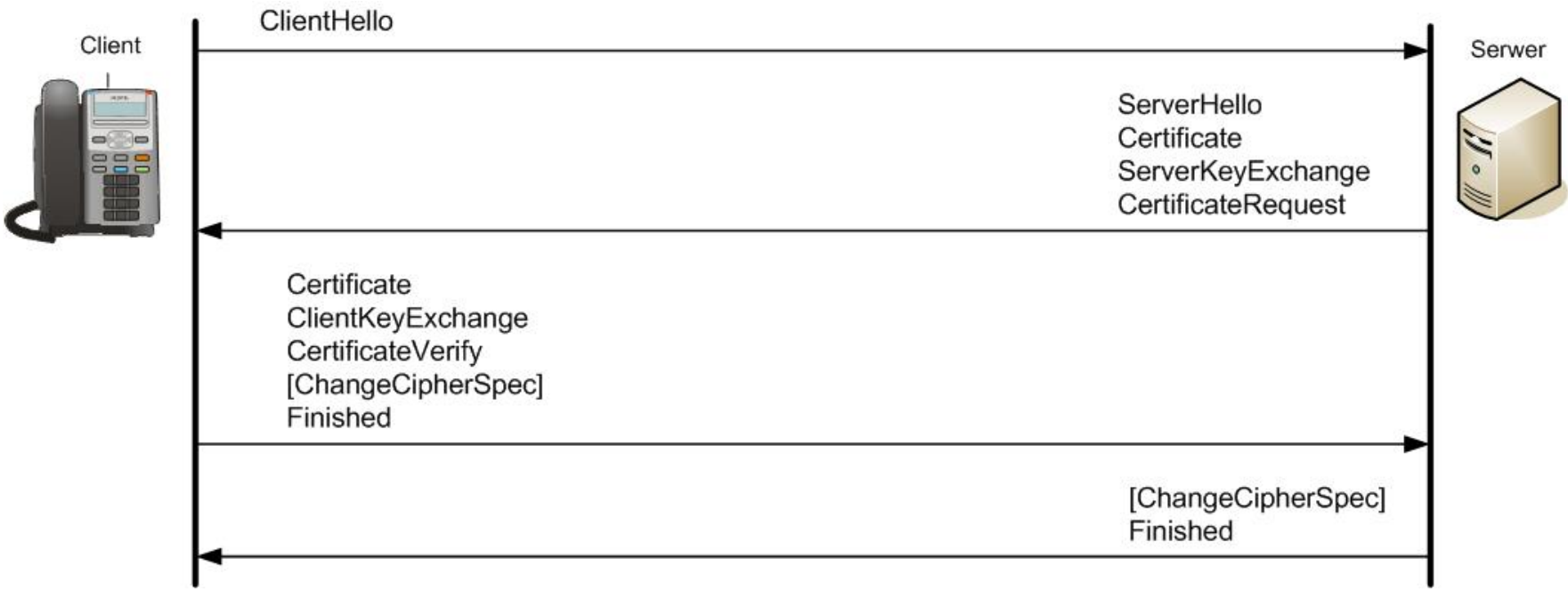
SIP DIGEST


UA
SIP Proxy
INVITE
407 Proxy Auth Required
Proxy-Authenticate: Digest algorithm=MD5, realm="domena1", nonce="7224c172"
ACK
INVITE
Proxy-Authorization: Digest username="ua1", realm="domena1", nonce="7224c172", uri="sip:ua2@domena1",
response="4c1f2.....", algorithm=MD5
180 Ringing
200 OK

S/MIME

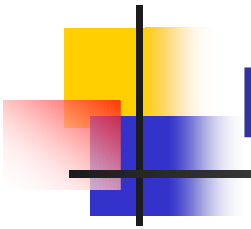
```
INVITE sip:bob@biloxi.com SIP/2.0
Contact: <sip:alice@10.1.3.3>
Content-Type: application/sdp
Content-Length: 147
v=0
o=UserA 2890844526 2890844526 IN IP4 here.com
s=Session SDP
c=IN IP4 100.101.102.103
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s
ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756
--boundary42-
```

TLS


Client
Serwer
ClientHello
ServerHello
Certificate
ServerKeyExchange
CertificateRequest
Certificate
ClientKeyExchange
CertificateVerify
[ChangeCipherSpec]
Finished
[ChangeCipherSpec]
Finished

Bezpieczeństwo SIP - podsumowanie

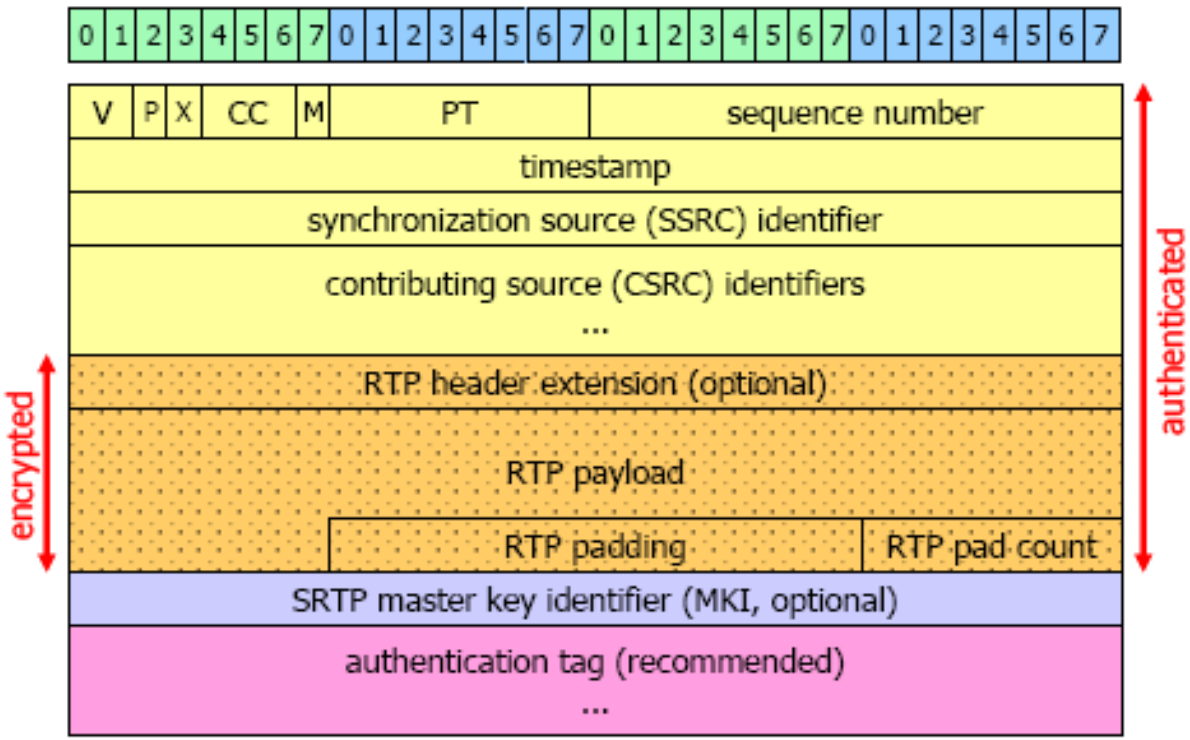
	Uwierzytelnienie	Poufność	Brak wymogów na dystrybucję kluczy lub certyfikatów	Obowiązkowość
Digest	**+**	**-**	**+**	**+**
S/MIME	+	+/-	-	-
TLS (DTLS)	**+**	**+**	**+/-**	-
IPSec	+	+	-	-



Bezpieczeństwo mediów

- **SRTP**
- IPSec
- TLS (DTLS)

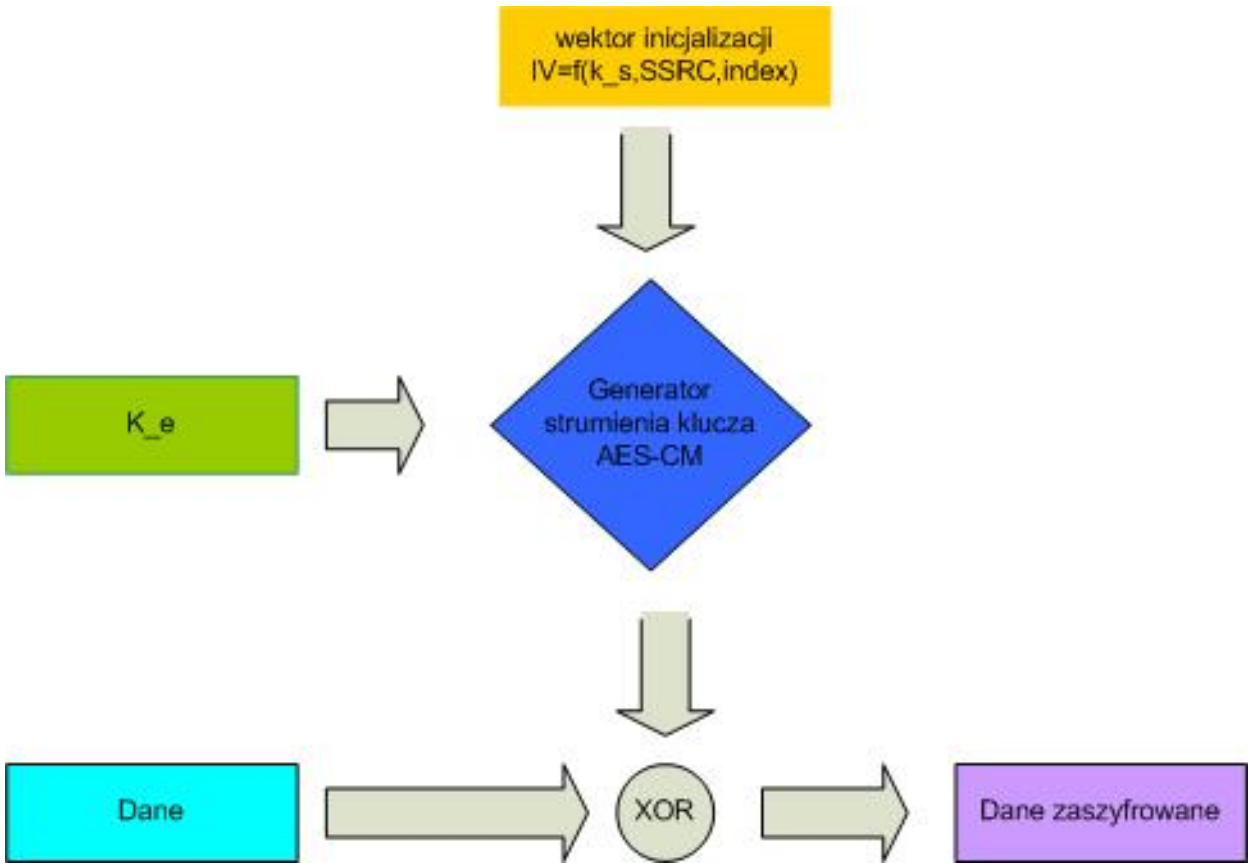
SRTP


0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
V
P
X
CC
M
PT
sequence number
timestamp
synchronization source (SSRC) identifier
contributing source (CSRC) identifiers
...
RTP header extension (optional)
RTP payload
RTP padding
RTP pad count
SRTP master key identifier (MKI, optional)
authentication tag (recommended)
...
encrypted
authenticated

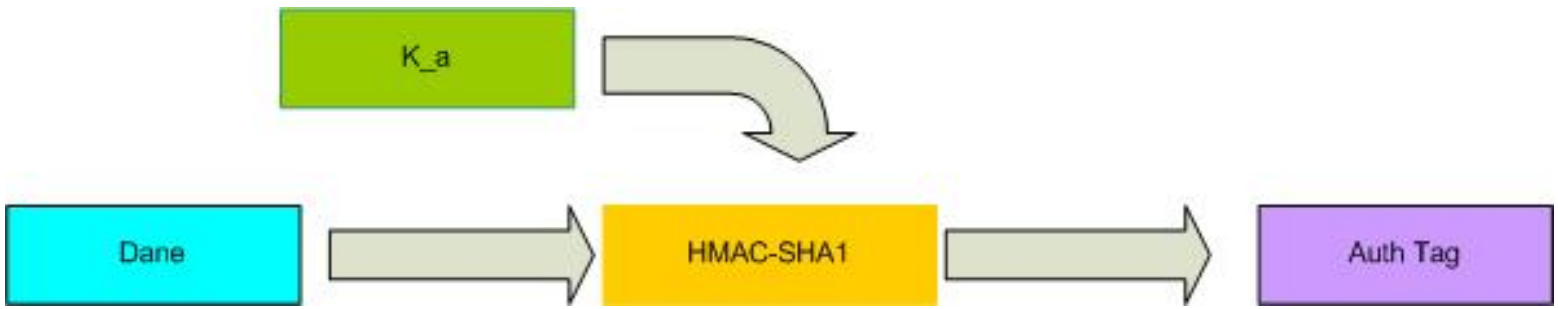
SRTP - algorytmy

- Szyfrowanie
  - AES-CM (domyślny, obowiązkowy)
  - AES-f8 (opcjonalny)
- Funkcja skrótu
  - HMAC-SHA1 (domyślna, obowiązkowa)

SRTP proces szyfrowania



SRTP podpis danych



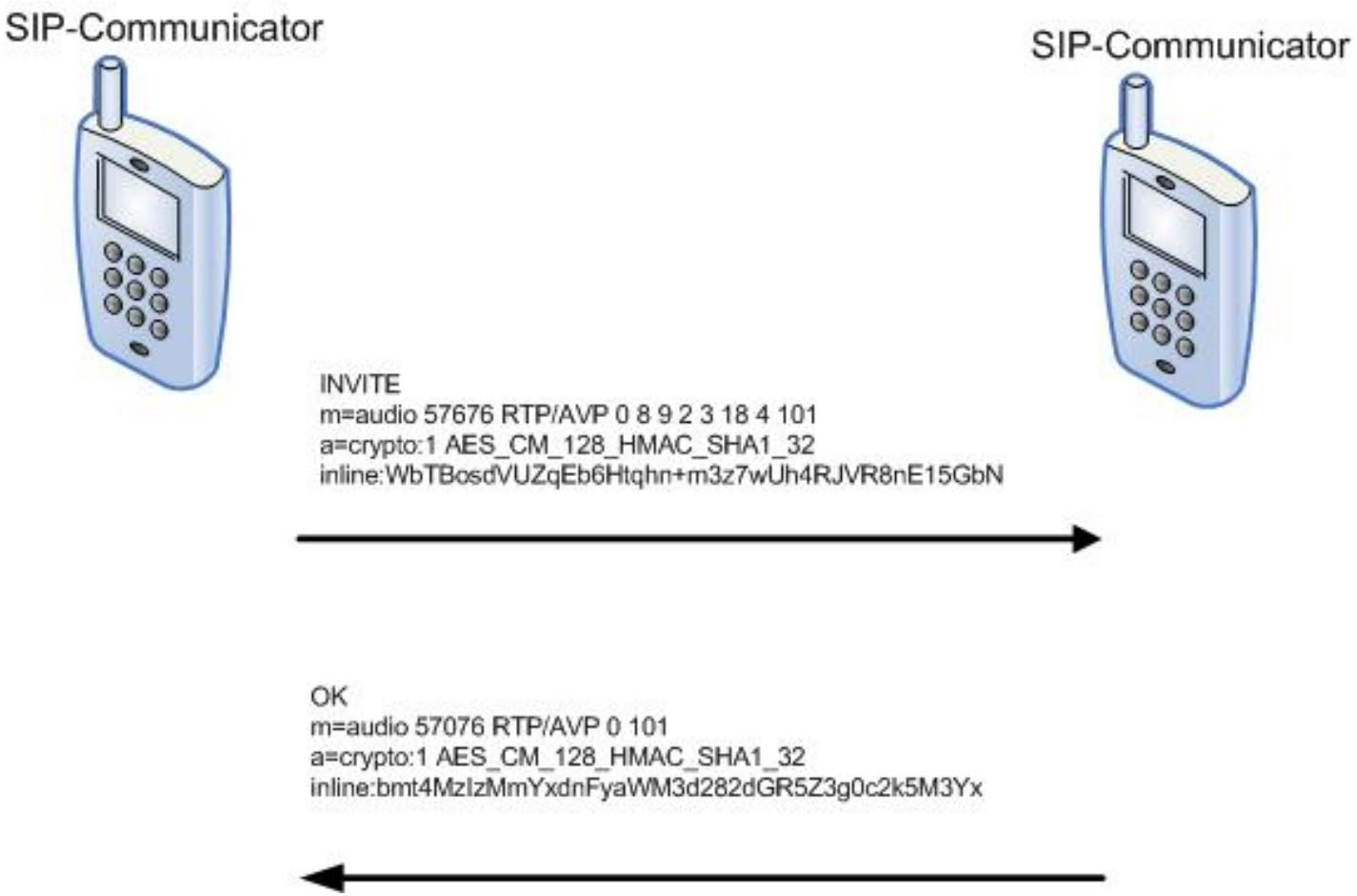
SRTP – dystrybucja klucza głównego

- SDES (RFC 4568)
  - Nie wymaga współdzielonego sekretu
  - Nie wymaga Infrastruktury Klucza Publicznego (PKI)
  - Wymaga bezpiecznego kanału transmisji
- MIKEY
  - Nie wymaga bezpiecznego kanału transmisji
  - Wymaga współdzielonego sekretu lub (PKI)

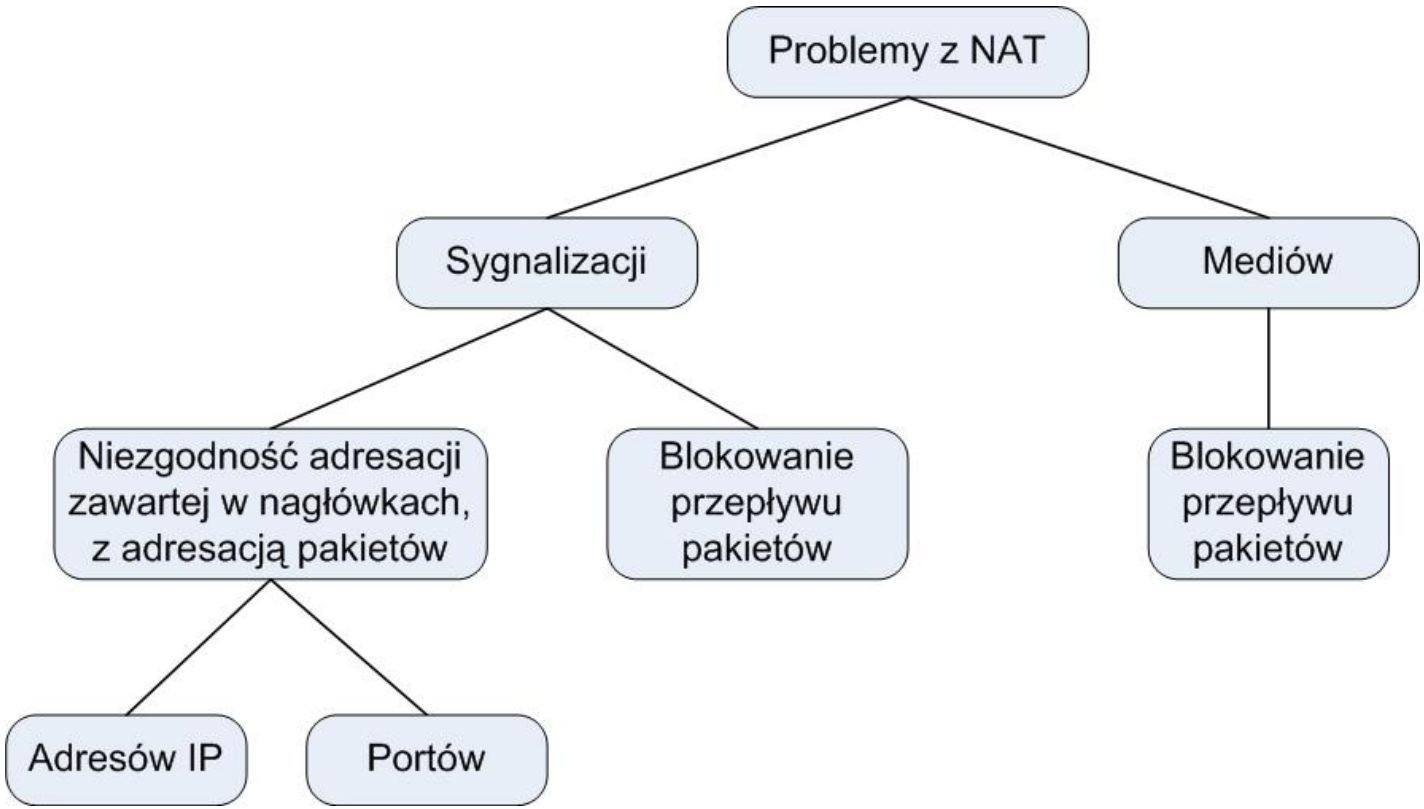
SRTP – dystrybucja klucza głównego

- ZRTP
  - Niezależny od sygnalizacji
  - Wymiana klucza algorytmem D-H
  - Uwierzytelnienie oraz integralność gwarantowana za pomocą parametru SAS (Short Autentication String)

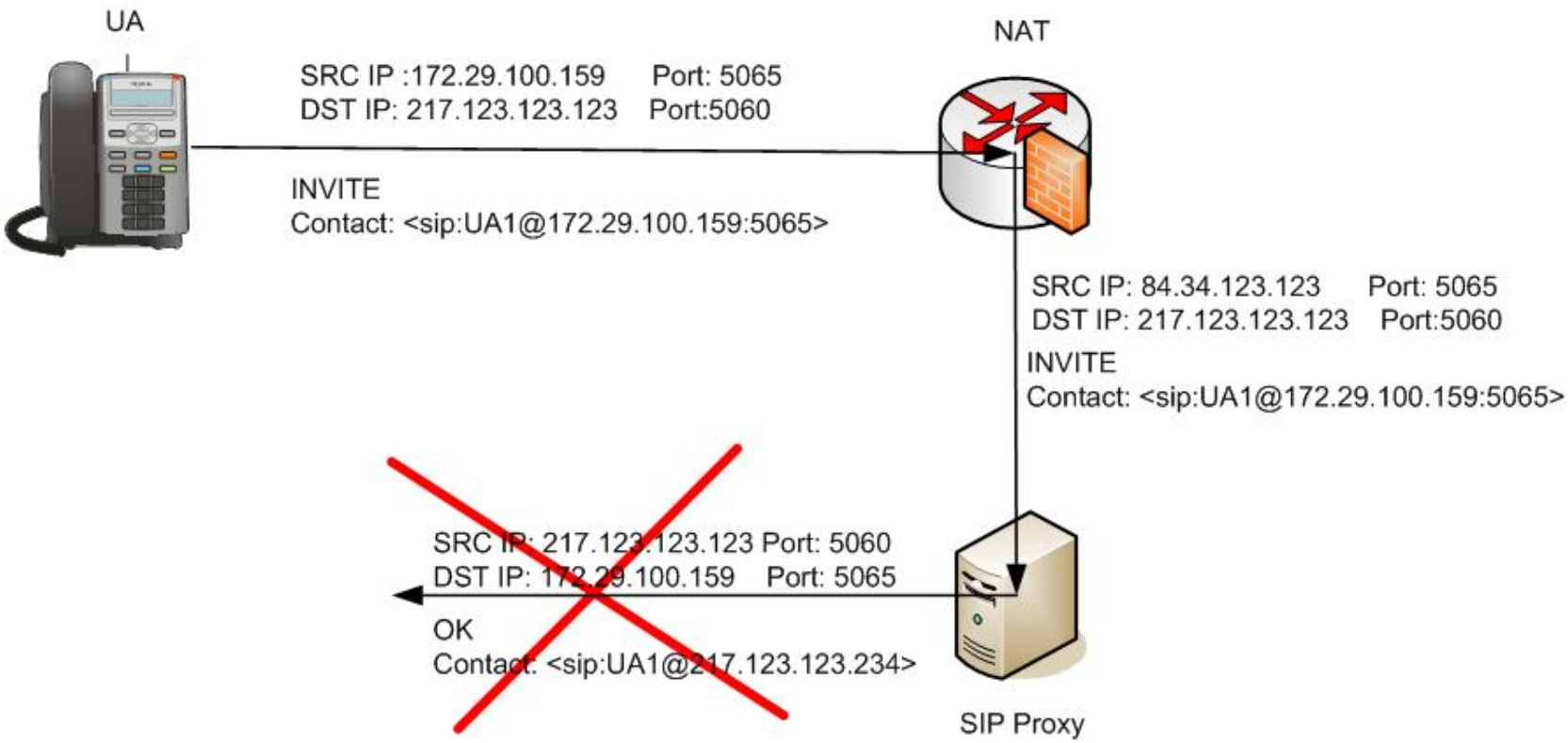
SDES - dystrybucja klucza głównego



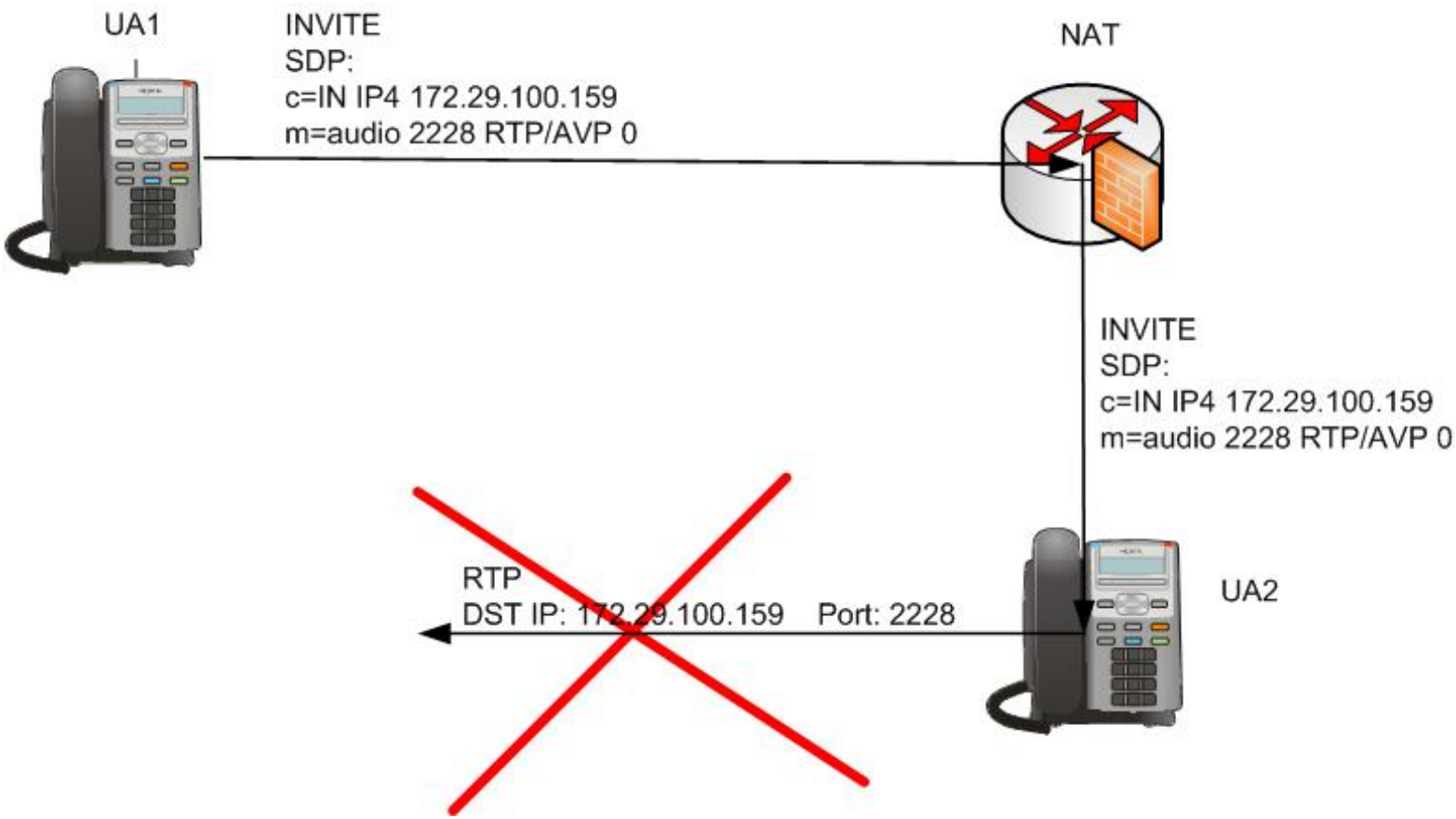
Problemy z NAT



Problemy z NAT – blokowanie sygnalizacji



Problemy z NAT – blokowanie mediów

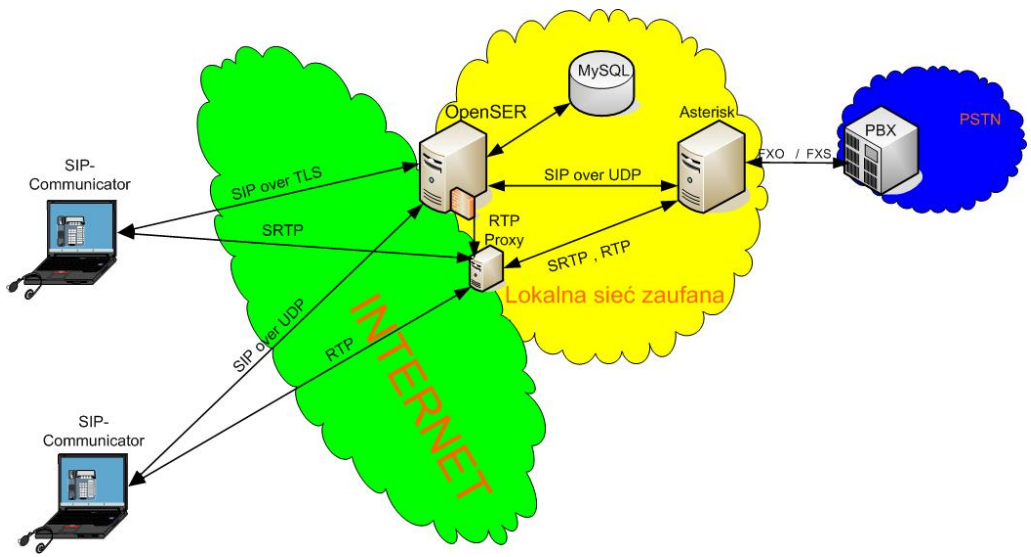


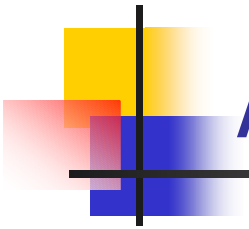
Rozwiązania problemów z NAT

- **Routing symetryczny**
- **Keep-alive**
- STUN (Simple Traversal of UDP Through NAT)
- TURN (Traversal Using Relay NAT)
- **RTP-proxy**
- IGD (Internet Gateway Device)

Komponenty + Architektura systemu

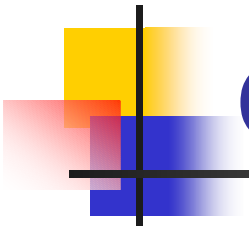
- Serwer
  - OpenSER
  - RTP Proxy
  - Asterisk
  - MySQL
- Klient
  - SIP-Communicator





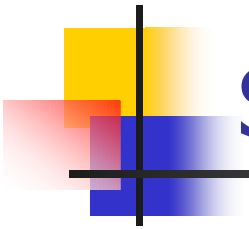
Astersk - cechy

- Otwarty software-owy PBX integrujący usługi VoIP i PSTN
- Obsługa protokołów **SIP**, H323, IAX2
- Możliwość wyposażenia w karty ISDN, FXO(modem)
- Bezpieczeństwo SIP – uwierzytelnienie Digest
- SRTP – moduł testowy opary na libSRTP
- W pracy wykorzystany jako brama medialna pomiędzy siecią SIP a PSTN



OpenSER

- Funkcje serwera Registrar i Proxy
- Skalowalność i elastyczność konfiguracji
- Współpraca z bazami danych (MySQL)
- Obsługa TLS
- Wsparcie dla NAT
  - RTP-proxy



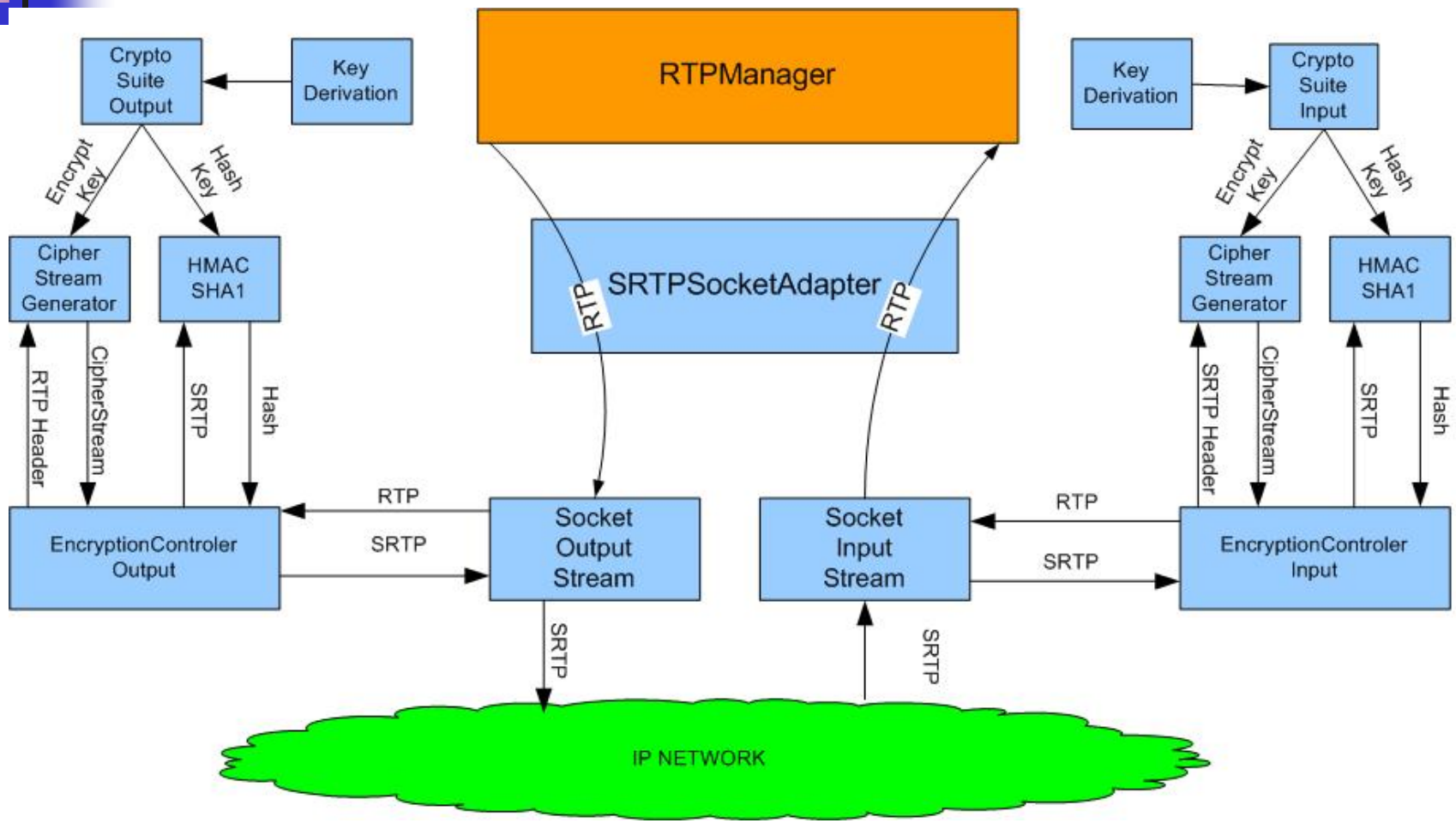
SIP-Communicator

- Internetowy telefon oparty na interfejsie JAIN-SIP
- Obsługa protokołów UDP/TCP/TLS
- **Brak** obsługi SRTP
- **Brak** obsługi SDES

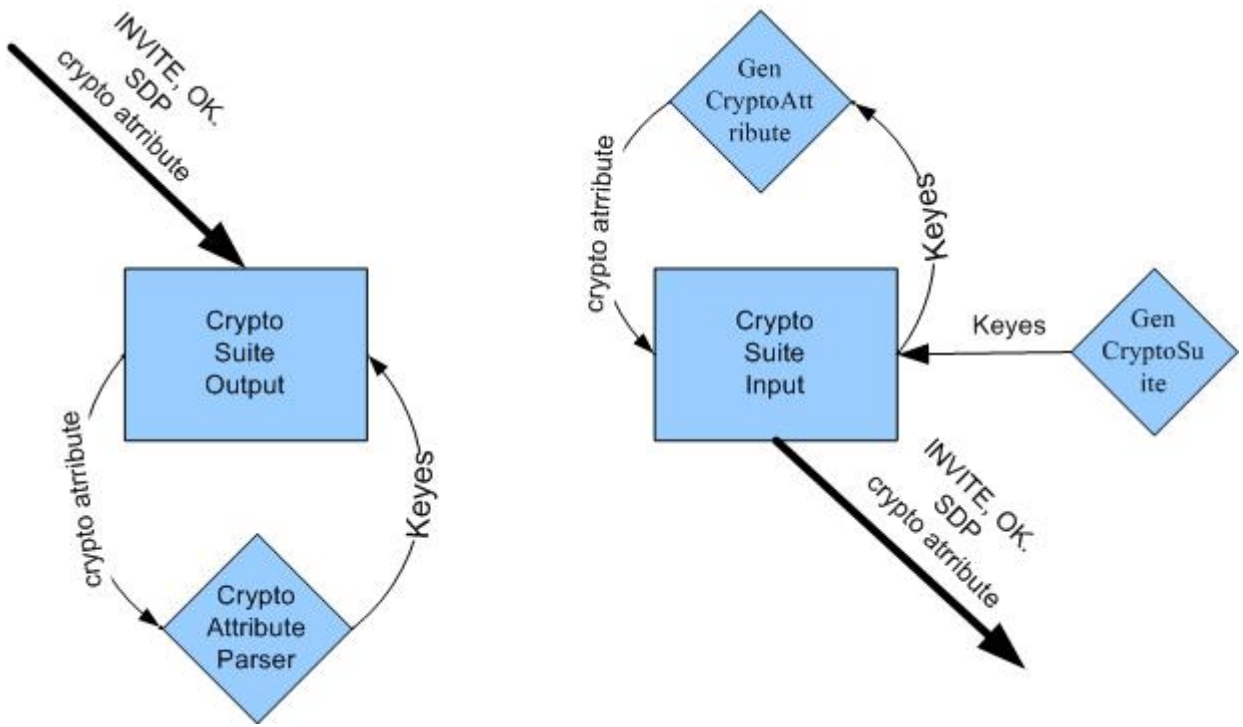
Zakres wykonanej pracy, napotkane problemy

- Implementacja obsługi protokołu SRTP w aplikacji SIP-Communicator (wykorzystanie biblioteki JCE oraz SunJCE)
- Implementacja obsługi wymiany klucza szyfrującego protokołem SDES
- Zarządzanie obsługą schematu URI typu SIPS po stronie klienta
- Kierowanie połączeń oraz obsługa schematu URI typu SIPS po stronie serwera (bloki routingowe)
- Mechanizmy powiadamiania użytkownika o niespełnionych wymaganiach bezpieczeństwa
  - 406 SIPS Not Acceptable
  - 416 SIPS Required
  - 480 SIPS Unavailable
- Powiadamiania użytkownika o zagrożeniach bezpieczeństwa
- Obsługa NAT (RTP Proxy)

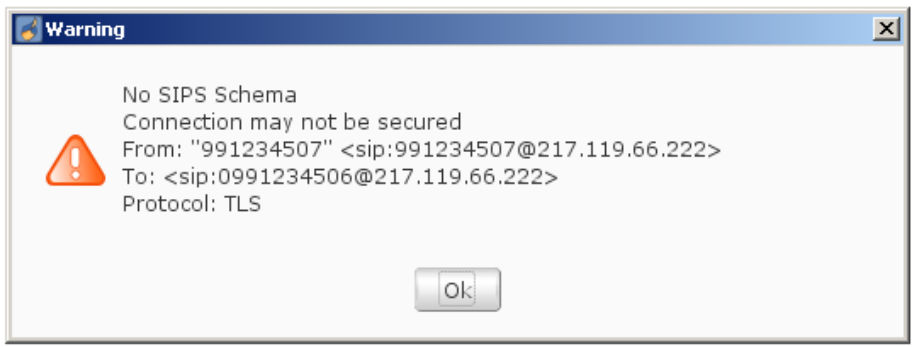
Implementacja SRTP

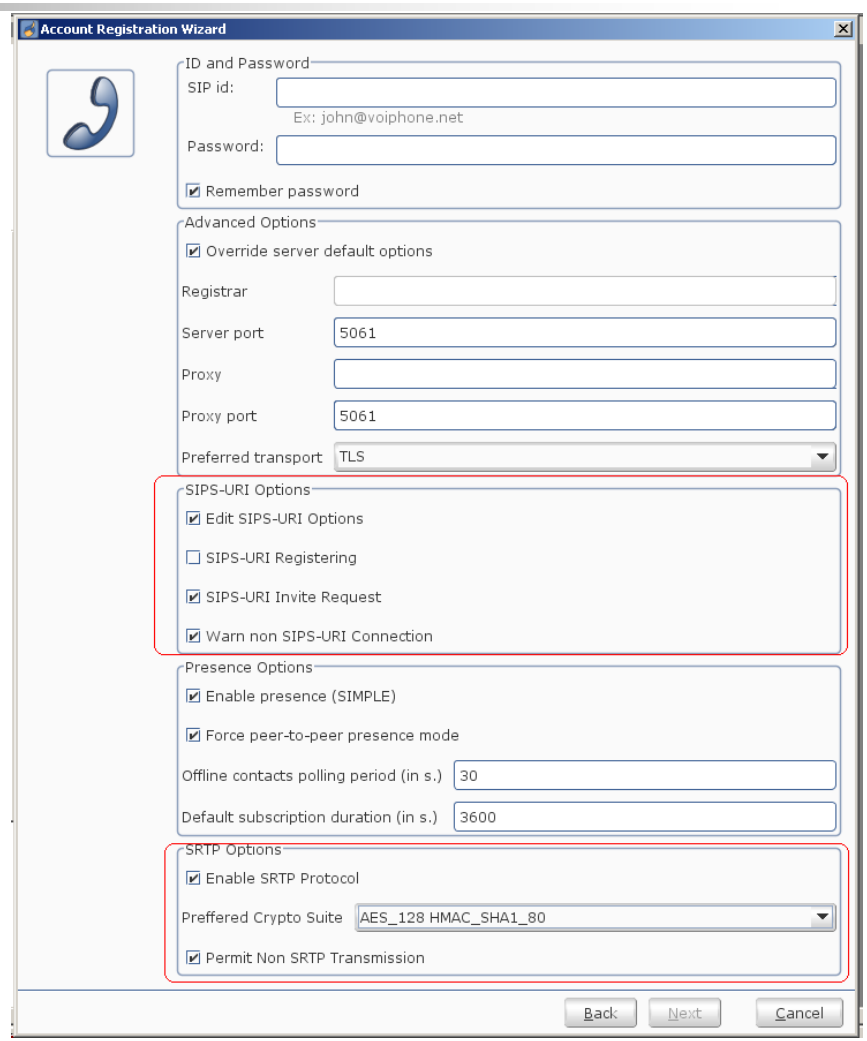


Implementacja SDES

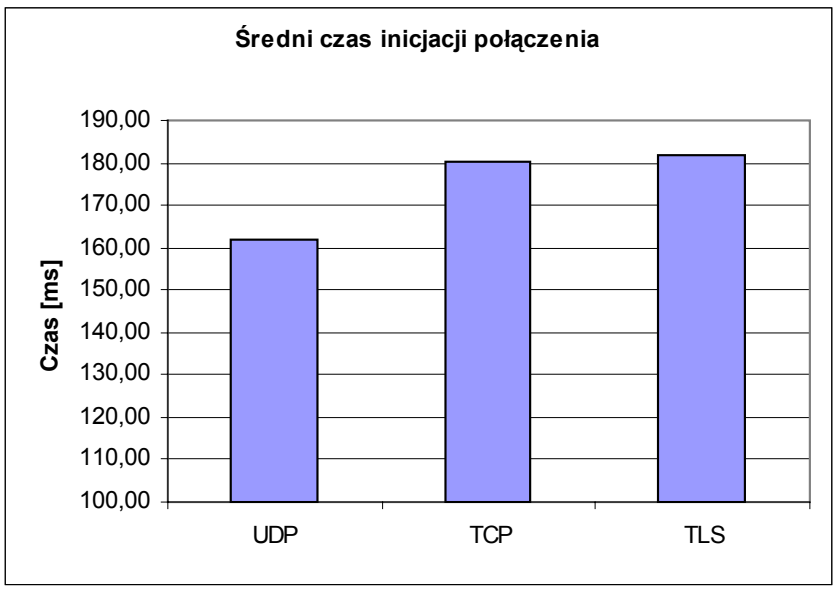


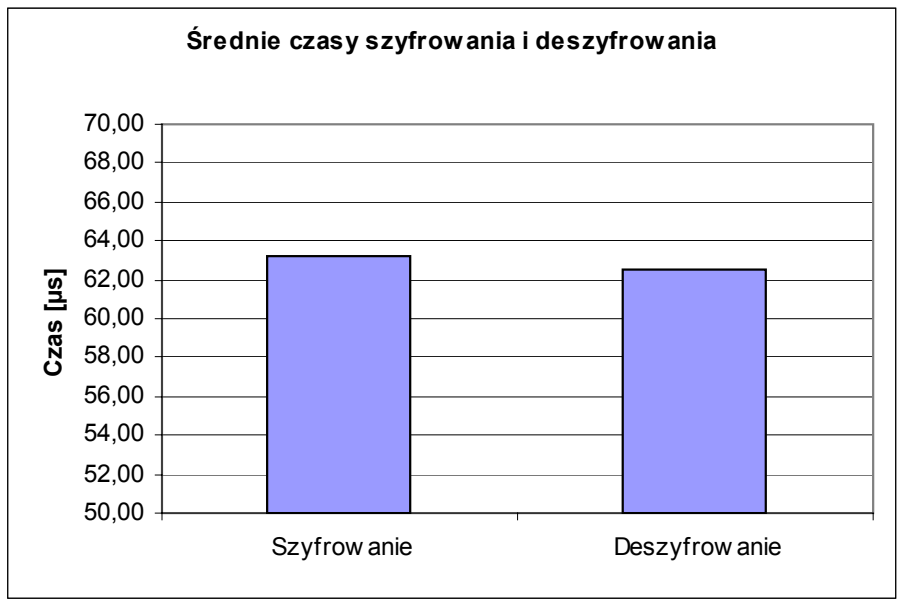
Okno dialogowe + panel konfiguracyjny



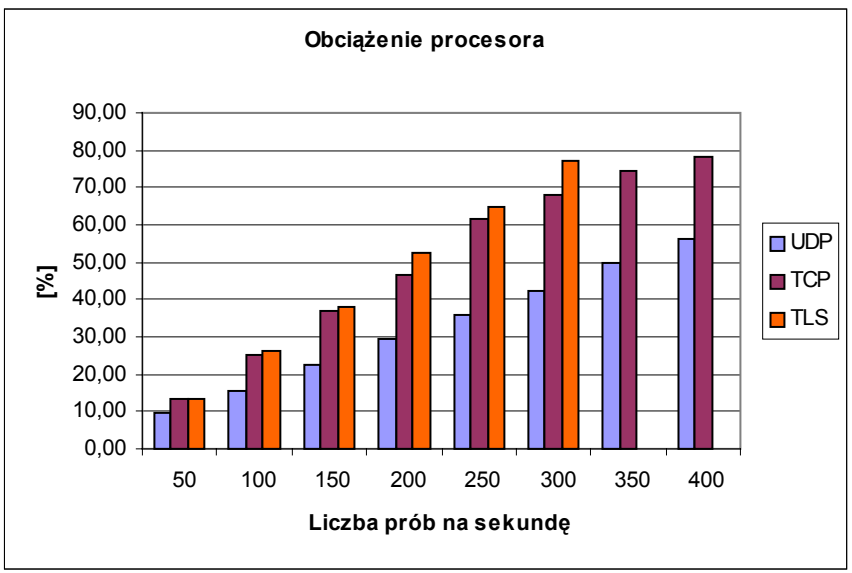


Test wydajności aplikacji

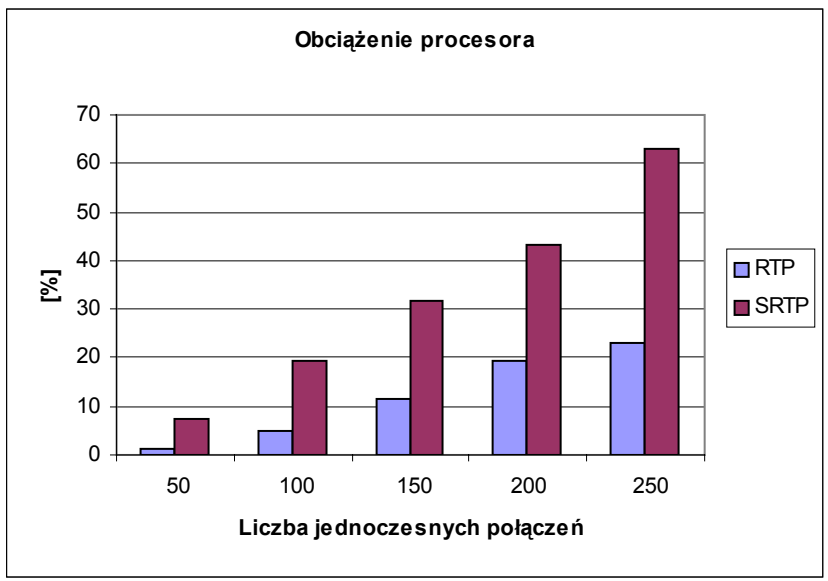




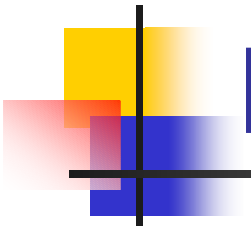
Testy wydajności serwera



Obciążenie procesora w zależności od liczby prób inicjacji sesji



Obciążenie procesora w zależności od liczby jednoczesnych połączeń



Dziękuję