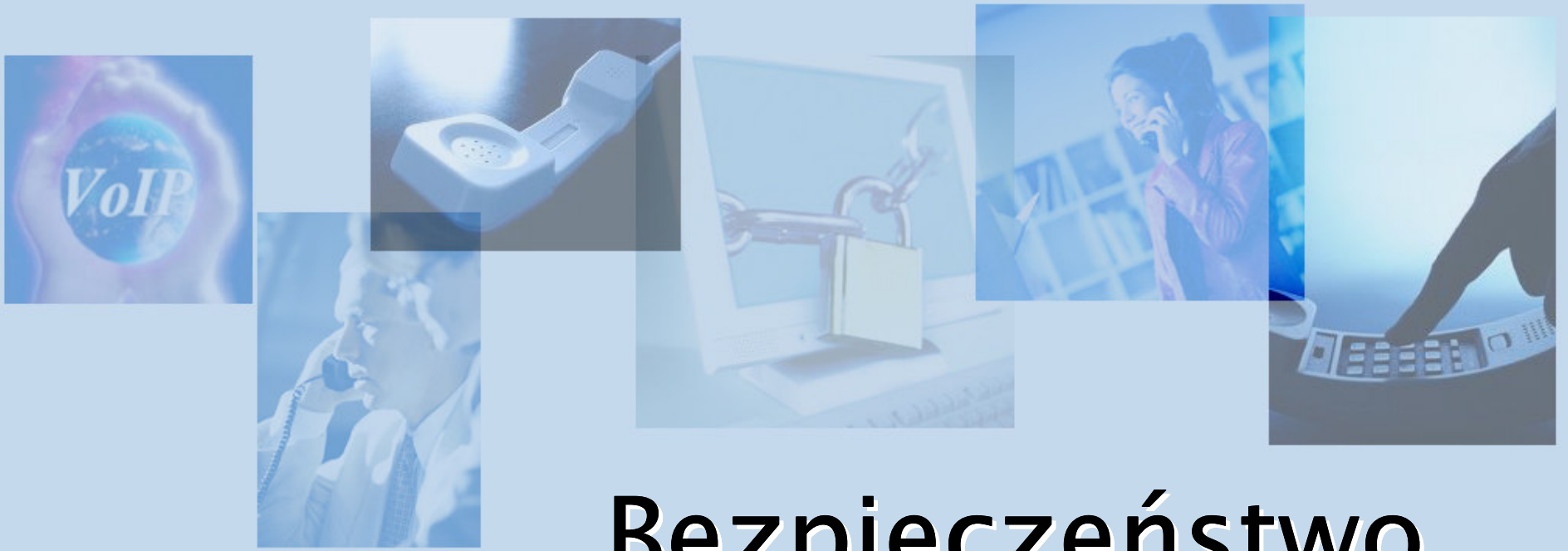


Bezpieczeństwo VoIP

Wojciech Mazurczyk

Instytut Telekomunikacji
Politechnika Warszawska
wmazurczyk@tele.pw.edu.pl
http://mazurczyk.com

Plan wykładu

Część I - Teoretyczna

- Wstęp, czyli przypomnienie
- Źródła problemów bezpieczeństwa VoIP
- Najpoważniejsze zagrożenia
- Podstawowe zasady bezpieczeństwa
- Korzystać, czy nie?

Część II - Praktyczna

- **Praktyczna** prezentacja najprostszych ataków na VoIP, jako podkreślenie konieczności stosowania mechanizmów i systemów bezpieczeństwa

Wstęp

- **VoIP (Voice over IP)** = Możliwość wykonywania połączeń telefonicznych z wykorzystaniem istniejącej infrastruktury teleinformatycznej
- **Na sieć VoIP składają się:**
  - **Terminale** – urządzenia/oprogramowanie pełniące funkcje telefonu (telefon IP, softphone, telefon analogowy)
  - **Serwery** odpowiedzialne za działanie całej sieci, łączenie z siecią PSTN, itp. (SIP: serwery proxy, redirect; H.323: gatekeeper ...)
- **Telefonia IP to dwa rodzaje ruchu:**
  - sygnalizacyjny – tworzący i kontrolujący połączenie
  - transportujący głos

Zalety VoIP a jej bezpieczeństwo

- **Największa zaleta VoIP to możliwość wykorzystania tej samej infrastruktury do przesyłania danych i głosu**
- **Jest to jednocześnie jej największa wada!**
- **Problem:** możliwość dostępu do segmentu głosowego z segmentu danych (łatwość instalacji niebezpiecznego oprogramowania)
- **Bezpieczne rozwiązanie oznaczają m.in.:**
  - Rezygnację z rozwiązań typu softphone (oprogramowania)
  - W przypadku konieczności zastosowania telefonu i komputera na jednym przewodzie wykorzystać wirtualne sieci lokalne (VLAN)

Źródła problemów bezpieczeństwa VoIP

- **Systemy VoIP są narażone na wszystkie znane zagrożenia, które dotyczą obecnych sieci, sprzętu i oprogramowana sieciowego**
- **Dodatkowo spotyka się dwa rodzaje luk:**
  - **błędy w oprogramowaniu** czy wykorzystywanym sprzęcie (potrzebna reakcja producenta)
  - **błędy w konfiguracji urządzeń** (najczęściej wykorzystywane przez atakujących)
- **Usługa VoIP jest wrażliwa na opóźnienia!**

Podwójna ostrożność

- **Podejście identyczne jak w zabezpieczeniu tradycyjnego sprzętu sieciowego** tzn. sprzęt VoIP w szczególności serwery trzeba zabezpieczać jak każdy inny sprzęt teleinformatyczny
  - Ataki mogą być identyczne jak w przypadku „zwykłych” serwerów
  - Analogicznie trzeba zabezpieczyć wykorzystywane urządzenia sieciowe
- **Podejście specyficzne dla VoIP** oznacza budowanie i konfigurację sieci w taki sposób, aby zabezpieczyć się przed atakami wykorzystującymi specyficzne cechy systemów VoIP

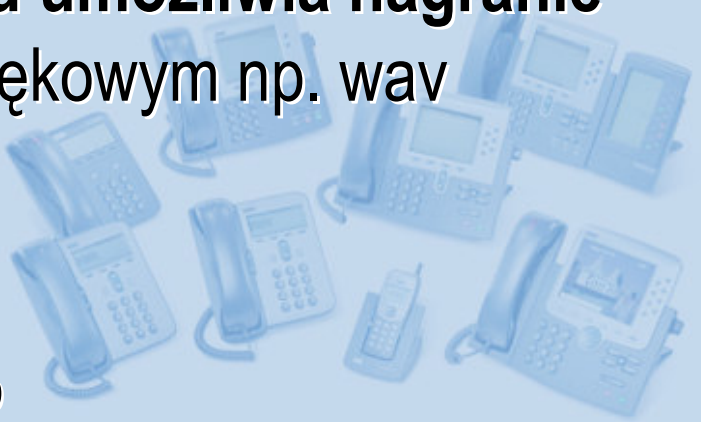
Zagrożenia dla sieci VoIP

- **Najważniejsze zagrożenia dla systemów VoIP**
  - **Utrata poufności danych -** podsłuch (sniffing)
  - **Ataki odmowy usługi** (Denial of Service, DoS)
  - **Kradzież usługi** (defraudacja)

- Specyfika działania telefonii VoIP rodzi również **nowe zagrożenia**
  - **SPIT** (Spam over Internet Telephony) – niechciane rozmowy mające na celu zachęcić nas do zakupów, usług itp.

Zagrożenie: Podsłuch

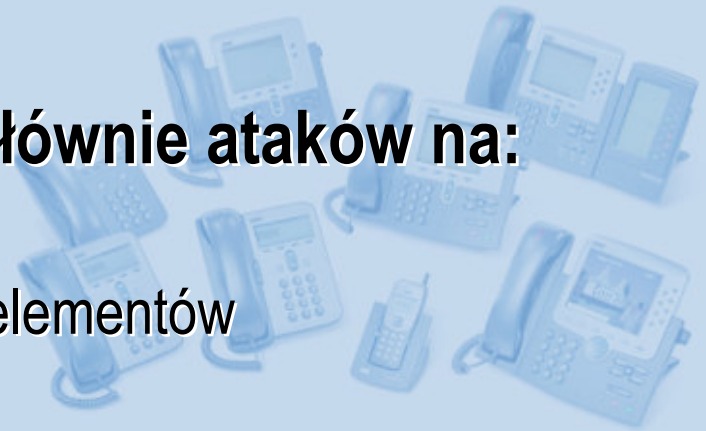
- **Głos bardzo często jest przesyłany bez szyfrowania**
- **Podsłuch danych z głosem ruchu umożliwia nagranie rozmowy** do pliku w formacie dźwiękowym np. wav



- **Możliwe rozwiązania:**
  - Szyfrowanie całego ruchu głosowego
  - Odseparowanie ruchu VoIP od reszty ruchu w celu uniemożliwienia podsłuchu
  - Budowa szyfrowanych tuneli (VPN) pomiędzy segmentami sieci dla ruchu VoIP, jeśli ruch ten przechodzi przez segmenty danych

Zagrożenie: Ataki odmowy usługi

- **Ataki odmowy usługi polegają na uniemożliwieniu prawowitym użytkownikom skorzystania z usługi telefonii (brak dostępności)**
- **W wypadku sieci VoIP dotyczą głównie ataków na:**
  - Terminali końcowych
  - Serwerów sygnalizacyjnych, innych elementów
- **Możliwe rozwiązania:**
  - Instalowania systemów zabezpieczających przez atakami (D)DoS (typu syn-flood,smurf itp.)
  - Dostęp do sieci VoIP jedynie autoryzowanych użytkowników (filtrowanie ruchu, uwierzytelnienie ruchu)



Zagrożenie: Kradzież usługi

- **Możliwość wykonywania połączeń na czyjś koszt, bądź wykonywania połączeń bez płacenia za nie**
- Łatwość podpięcia się do istniejącej sieci VoIP

- **Możliwe rozwiązania:**
  - Odseparowania ruchu VoIP i danych
  - Wyłączenie automatycznego rejestrowania klientów VoIP w serwerach sygnalizacyjnych
  - Zabezpieczenia na sprzęcie dostępowym uniemożliwiające podpięcie dodatkowych, nieautoryzowanych urządzeń

Podstawowe zasady bezpieczeństwa VoIP

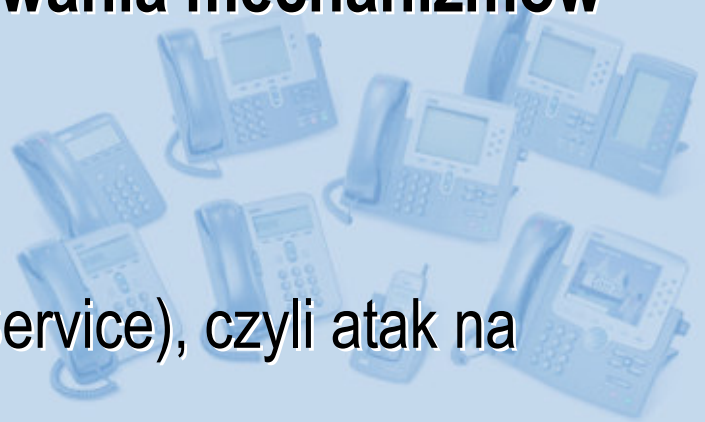
- Możliwie najpełniejsze **odseparowanie sieci VoIP** (sieci głosowej) **od sieci gdzie są przesyłane dane**
- Zadbać o **bezpieczeństwo serwerów sygnalizacyjnych i wymienianych wiadomości sygnalizacyjnych**
- **Szyfrować przesyłane rozmowy**
- **Monitorować segment głosowy** (rozwiązania typu IDS/IPS)
- **Wyłączyć** wszelkie automatyczne **procedury rejestracji** sprzętu i niepotrzebne usługi
- **Korzystać z dostępnych mechanizmów bezpieczeństwa!**

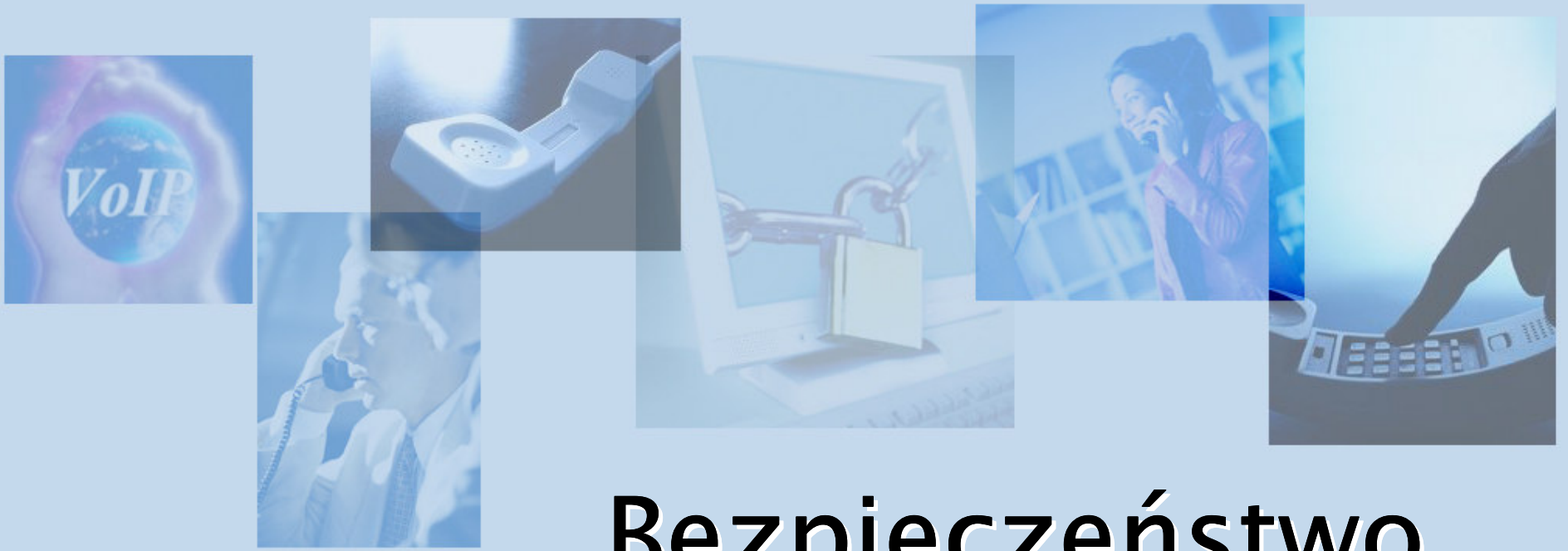
Bezpieczeństwo

- **Dużo zalet (m.in. darmowy, szyfrowanie głosu), ale:**
  - **brak informacji o protokole sygnalizacyjnym i jego bezpieczeństwie**
  - **ciągła odmowa odkrycia jakiegokolwiek aspektu bezpieczeństwa transmisji**
  - niektóre firmy (np. CERN), czy instytucje (University of Cambridge) już **zabroniły użytkownikom instalacji Skype** w swoich sieciach ze względów bezpieczeństwa
  - problem tzw. **SuperNodów** - anonimowa pomoc innym użytkownikom w połączeniu
  - pokusa użycia SN, **do celów komercyjnych**

Część II

- **Praktyczna prezentacja prostych ataków na VoIP, jako podkreślenie konieczności stosowania mechanizmów bezpieczeństwa**
  - Podsłuch (Sniffing)
  - Odmowa usługi - DoS (Denial Of Service), czyli atak na dostępność
  - „Psucie” jakości trwającego połączenia





Bezpieczeństwo VoIP

Wojciech Mazurczyk

Instytut Telekomunikacji
Politechnika Warszawska
wmazurczyk@tele.pw.edu.pl
http://mazurczyk.com