Bezpieczeństwo usługi VoIP opartej na systemie Asterisk

Krajowe Sympozjum Telekomunikacji i Teleinformatyki

KSTiT 2007

Autorzy:

- Tomasz Piotrowski
- Szczepan Wójcik
- Mikołaj Wiśniewski
- Wojciech Mazurczyk

Bydgoszcz, 14 września 2007

Agenda

- Usługa VoIP
- Programowa centrala Asterisk
- Geneza zagrożeń
- Analiza bezpieczeństwa sygnalizacji i głosu
- Doświadczenia
- Analiza uzyskanych wyników

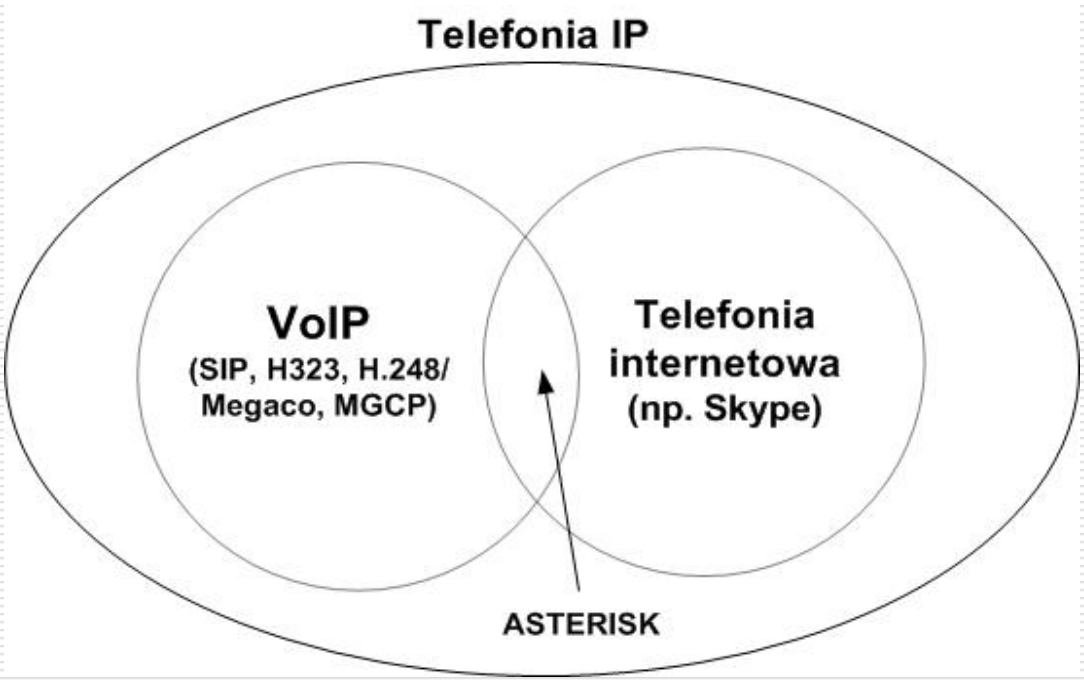
VoIP
(*Voice over Internet Protocol*)

- Usługa czasu rzeczywistego
- Transport pakietowy
- Oparta o trzy grupy protokołów:
  - sygnalizacji (SIP, H.323, Megaco, ...)
  - kodowania głosu (G.711, G.729, ...)
  - transportowych (RTP, UDP, TCP, ...)

Rozwój systemu Asterisk i jego możliwości

- Programowa centrala IP PBX
- Twórca: Mark Spencer (Digium)
- Wspierany przez GNU
- Wspiera obecnie najważniejsze protokoły sygnalizacyjne dla VoIP (SIP, H.323, MGCP, IAX2, SCCP,...)
- Nie wymaga dodatkowego sprzętu fizycznego

Miejsce Asterisk w systemach telefonii IP



Geneza zagrożeń

- Brak uniwersalnych metod ochrony dla systemów telefonii pakietowej
- Wykorzystanie do przesyłania głosu tego samego medium, które stosuje się do transmisji danych (największa wada i zaleta jednocześnie)
- Błędy w oprogramowaniu, konfiguracji
- Wrażliwość na opóźnienia

Rodzaje i techniki ataków na systemy VoIP

- Kryteria: uwierzytelnianie, integralność, poufność
- Klasy ataków: aktywne i pasywne
- Techniki ataków:
  - Spoofing (podszywanie)
  - Sniffing (podsłuchiwanie)
  - Denial of Service (odmowa usługi)
- Inne zagrożenia: SPIT

Bezpieczeństwo systemu VoIP opartego o Asterisk

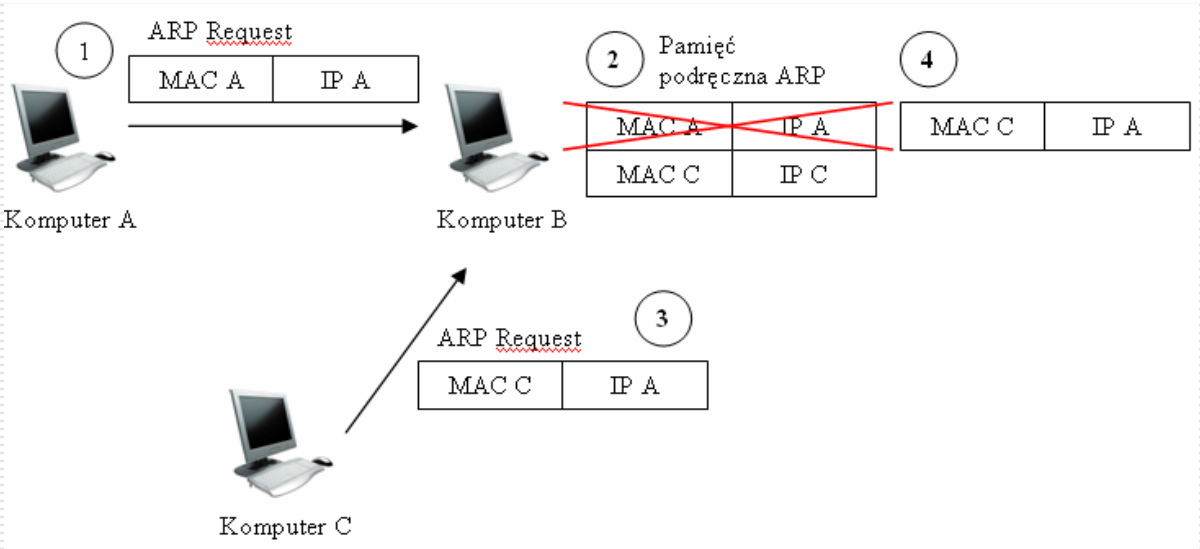
- Bezpieczeństwo protokołów sygnalizacyjnych
- Bezpieczeństwo przesyłanych danych
- Bezpieczeństwo maszyny

Bezpieczeństwo sygnalizacji i głosu

- **Porwanie Rejestracji** (*Registration Hijacking*) polega na modyfikacji pola From (identyfikującego nadawcę) w wiadomości REGISTER (przekierowanie połączenia),
- **Porwanie Połączenia** (*Connection Hijacking*) - analogicznie do ataku powyżej, ale modyfikacji podlega pole From w wiadomości INVITE,
- **Atak Man in the Middle (**MITM**)** – pozwala atakującemu przechwycić komunikację z/do serwerów sieciowych i w ten sposób wpływać na kluczowe informacje w wiadomościach sygnalizacyjnych,
- **Atak Podszycia się pod serwer** (*Impersonating a Server*) - klient Agenta Użytkownika kontaktuje się z serwerem sieciowym w celu dostarczenia żądania, natomiast intruz podszywa się pod serwer,
- **Celowe zakańczanie trwających połączeń** poprzez wysłanie przez atakującego wiadomości BYE w czasie, gdy zachodzi komunikacja między użytkownikami.

Doświadczenie 1: Zatruwanie tablic ARP (ARP Poisoning)

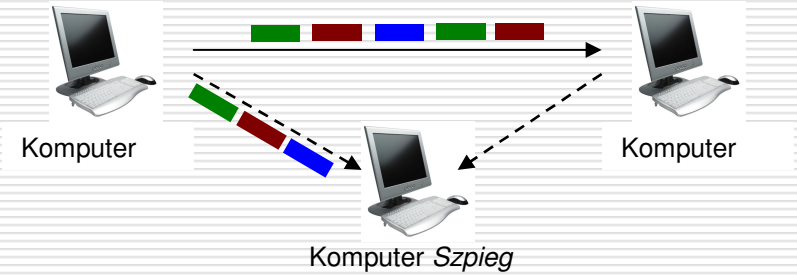
- Atak polegający na celowej modyfikacji pamięci podręcznej ARP



- Atak udany

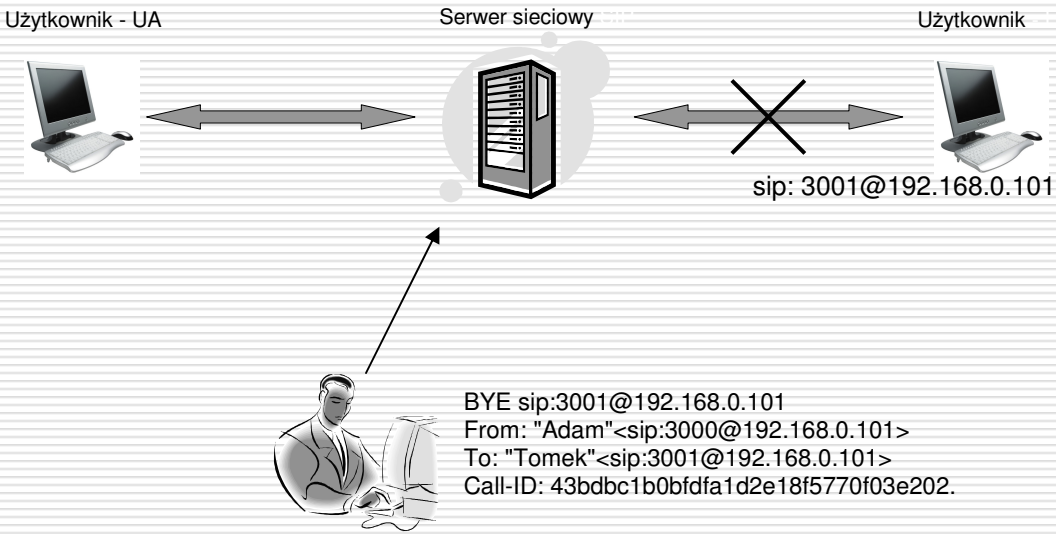
Doświadczenie 2: Atak pasywny: analiza pakietów

- Analiza pakietów przy użyciu odpowiedniego oprogramowania (np.. Ethereal, WireShark, ….)
- Cel – uzyskanie informacji potrzebnych ataku aktywnego (np. call-ID, hasła, adresy agentów itp.)



Doświadczenie 3: Atak aktywny

- Próba celowego zakańczania trwających połączeń, poprzez wysłanie przez intruza wiadomości BYE



Doświadczenie 4: nagrywanie rozmowy

- Przechwycenie strumienia RTP
- Atak analogiczny do doświadczenia nr.2 (analiza przesyłanych pakietów)
- Wykonanie podsłuchu polega na włączeniu monitoringu wraz z atakiem ARP Poisoning
- Aplikacja (np. Cain&Abel) nagrywa przechwycone dane do formatu .wav

Analiza wyników doświadczeń oraz możliwe zabezpieczenia chroniące przed lukami

- Protokół IAX2 oferuje najbardziej zaawansowane metody uwierzytelniania: z funkcją skrótu MD5 lub RSA
- Analizowany protokół RTP pozwolił na całkowite przechwycenie komunikacji głosowej (nagranie rozmowy)
- Asterisk nie posiada na chwilę obecną wsparcia dla protokołu SIPS URI (TLS)
- Najlepszym rozwiązaniem dla zabezpieczenia głosu: wykorzystanie szyfrowania (protokół SRTP)

Podsumowanie - Asterisk

Rodzaj protokołu	Rodzaj ruchu VoIP	Uwierzytelnienie	Integralność	Poufność
SIP / RTP	Sygnalizacja	+	-	-
	Media	+	-	-
IAX2	Sygnalizacja	+	-	-
	Media	+	-	+/-

Bezpieczeństwo usługi VoIP opartej na systemie Asterisk

Krajowe Sympozjum Telekomunikacji i Teleinformatyki
KSTiT 2007

Dziękuję za uwagę !

Autorzy:
- Tomasz Piotrowski
- Szczepan Wójcik
- Mikołaj Wiśniewski
- Wojciech Mazurczyk

Bydgoszcz, 14 września 2007