T. Piotrowski, S. Wójcik, M. Wiśniewski, W. Mazurczyk
Instytut Telekomunikacji
Politechnika Warszawska
E-mail: s.m.wojcik@gmail.com, tpiotrowski1@gmail.com, wmiko@o2.pl, wmazurcz@elka.pw.edu.pl
Network Security Group
http://secgroup.pl

Bezpieczeństwo usługi VoIP opartej na systemie Asterisk

STRESZCZENIE

W artykule przeanalizowano bezpieczeństwo usługi VoIP (Voice over Internet Protocol) na podstawie jednego z najbardziej popularnych obecnie rozwiązań telefonii IP: darmowej, programowej centrali IP PBX: Asterisk [1]. Dla tego systemu scharakteryzowano potencjalne zagrożenia oraz ich źródła oraz wskazano jakie aspekty komunikacji powinny podlegać zabezpieczaniu dla usługi VoIP. Następnie wiedzę tę skonfrontowano ze stanem faktycznym centrali Asterisk. Przeprowadzone badania praktyczne wykazały niski stan zabezpieczeń w tym produkcie, co poddaje w wątpliwość jego szerokie zastosowanie w komercyjnych wdrożeniach telefonii IP, z jakimi mamy do czynienia obecnie.

1. Wstęp

VoIP (*Voice over Internet Protocol*) to usługa czasu rzeczywistego umożliwiająca prowadzenie połączeń głosowych z wykorzystaniem pakietowych sieci IP. Ze względu na zdobytą popularność, VoIP można nazwać jedną z najważniejszych usług teleinformatycznych ostatniej dekady. Mimo tego, iż systemów i produktów tego typu jest na rynku coraz więcej, szybkość rozwoju VoIP nie jest tak imponująca, jak pierwotnie prognozowano. Takiego stanu rzeczy należy upatrywać w nadal nierozwiązanych problemach wpływających negatywnie na rozwój VoIP tj. problemów z zagwarantowaniem odpowiedniej jakości usługi pomiędzy rozmawiającymi oraz niewystarczającego poziomu zabezpieczeń. Ten ostatni brak jest szczególnie wyraźny w zakresie bezpieczeństwa protokołu sygnalizacyjnego, na którym system telefonii IP bazuje [6, 8, 9].

Na tym tle Asterisk [1] to produkt stosunkowo młody, cieszący się, w świecie telefonii VoIP dość dużą popularnością. Jest to programowa centrala IP PBX oferująca wsparcie dla najpopularniejszych obecnie, zestandaryzowanych protokołów sygnalizacyjnych telefonii IP, tj. SIP (*Session Initiation Protocol*) [3], H.323 [4], MGCP (*Media Gateway Control Protocol*) [5] oraz producenckich: SCCP (*Skinny Call Control Protocol*, firmy Cisco), czy IAX2 (*InterAsterisk eXchange wersja 2,* firmy Digium). Jednak główną cechą, która przysparza Asteriskowi coraz większą rzeszę zwolenników jest to, że pomimo bogatych możliwości technicznych jest to oprogramowanie darmowe (na licencji GNU). W ten sposób każda osoba wykorzystująca to oprogramowanie jest w stanie zweryfikować poprawność implementacji poszczególnych elementów systemu oraz wprowadzać własne rozszerzenia, dodatkowe funkcjonalności czy usługi. Dzięki temu Asterisk oferuje szeroką gamę usług telekomunikacyjnych, złożoną obsługę połączeń oraz taryfikację. Dodatkowo pozwala na współpracę z wieloma typami aparatów VoIP i dedykowanymi kartami sprzętowymi do połączeń z sieciami PSTN, czy ISDN.

Przenoszenie miejsca świadczenia usług telefonicznych z tradycyjnej sieci telefonicznej PSTN (*Public Switched Telephone Network*) do sieci IP, które możemy śledzić od kilku lat, sprawia, że zagrożenia, kojarzące się dotychczas z bezpieczeństwem kabla telefonicznego (aspektu zupełnie fizycznego), zyskują zupełnie inny wymiar w sieciach telefonii pakietowej.

Chcąc podsłuchać rozmowę w VoIP nie musimy podłączać się do linii abonenckiej. Wystarczy, że będąc w tej samej sieci LAN wykorzystamy odpowiednie narzędzie (*sniffer*), a następnie posłużymy się nim do przechwytywania odpowiedniego protokołu telefonii IP (zupełnie tak jak podsłuchuje się istniejące usługi takie jak FTP, telnet, czy SMTP). Ponadto, aby przechwytywać rozmowy na masową skalę, nie trzeba podłączać się do każdej linii fizycznej z osobna, lecz wystarczy przejąć cały, obserwowany ruch w danej sieci lokalnej. Wskazane zagrożenia telefonii IP powodują, że kwestie bezpieczeństwa w systemach takich jak Asterisk należy traktować priorytetowo.

W artykule poddano szczegółowej analizie bezpieczeństwo systemu Asterisk, jako jednego z najpopularniejszych obecnie systemów VoIP. Spośród szerokiej gramy protokołów sygnalizacyjnych wspieranych przez Asterisk przeprowadzone doświadczenia skupiają się na analizie luk bezpieczeństwa protokołu sygnalizacyjnego SIP (ze względu na jego obecną popularność), protokołu sygnalizacyjnego IAX2 (rozwiązania producenckiego twórców systemu Asterisk, ze względu na obecnie największą liczbę mechanizmów zabezpieczeń) oraz standardu RTP (wykorzystywanego do transmisji głosu dla połączeń VoIP). Wspomniane protokoły, bez odpowiednich zabezpieczeń, mogą stanowić źródło zagrożeń, zwiększając tym samym podatność na ataki.

W kolejnych częściach niniejszego artykułu opisano system Asterisk oraz jego możliwości (punkt 2). Następnie w punkcie 3 wskazano jego miejsce wśród innych systemów telefonii IP. Punkt 4 charakteryzuje zagrożenia, ataki oraz wykorzystywane przez nie techniki. Kolejna część przedstawia analizę zabezpieczeń systemu Asterisk oraz przeprowadzone doświadczenia praktyczne badające jego bezpieczeństwo. Natomiast w ostatnim punkcie podsumowano całość poruszanych zagadnień.

2. Rozwój systemu Asterisk i jego możliwości

Historia oprogramowania Asterisk sięga 1999 roku, a jego twórcą jest Mark Spencer z firmy Digium [10]. Od czasu udostępnienia pierwszej wersji centrali jej kod został umieszczony w sieci Internet i odtąd jest intensywnie rozbudowywany przez wielu programistów na cały świecie. Właśnie dzięki tej dostępności i otwartości wspiera on obecnie najważniejsze protokoły sygnalizacyjne dla VoIP oraz umożliwia realizację wielu zaawansowanych usług. Asterisk wspiera takie funkcjonalności jak: pocztę głosową z książką telefoniczną, połączenia konferencyjne, system IVR (*Interactive Voice Response*), kolejkowanie połączeń, identyfikację numerów, czy ADSI (*Analog Display Services Interface*). Aby umożliwić pakietowe rozmowy telefoniczne Asterisk nie wymaga żadnego dodatkowego sprzętu fizycznego. Natomiast, jeśli niezbędne jest nawiązywanie połączeń pomiędzy telefonią cyfrową a analogową należy do tego celu wykorzystać specjalne karty (producentów takich jak m.in. Digium, Sangoma Technologies, Patton Electronics, Hitachi Cable, Policom, czy SUN Microsystems).

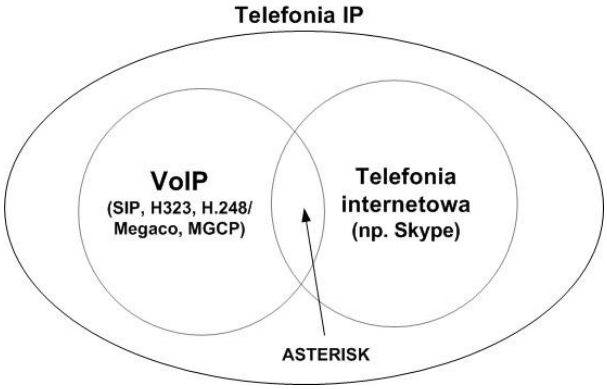
Obecnie wiele firm zajmuje się dystrybucją oprogramowania Asterisk oraz dedykowanego dla niego sprzętu. Wiodącym europejskim dystrybutorem sprzętu i oprogramowania stosowanego przy otwartych projektach głosowych związanych z Asterisk jest firma halo^2 - Halo Kwadrat, natomiast w Polsce takie firmy jak NETCOM, czy Virgo Kalisz. Zazwyczaj firmy tego typu zapewniają kompleksową obsługę teleinformatyczną przedsiębiorstw w ramach oferowanego produktu. Warto również wspomnieć, że popularny obecnie polski system VoIP – Tlenofon [2], który umożliwia wykonywanie tanich rozmów przez Internet również współpracuje ze środowiskiem Asterisk.

Wszystkie opisane powyżej cechy sprawiają, że system Asterisk jest coraz częściej stosowany we wdrożeniach różnej skali, a grupa odbiorcza takiego produktu jest praktycznie nieograniczona. Zazwyczaj, jednak firmy sięgają po tego typu rozwiązania, aby zastąpić konwencjonalne, analogowe centrale PBX dotychczas posiadane. Asterisk znajduje również

zastosowanie u operatorów np. francuski operator VoIP Wengo używa Asterisk do oferowania usługi poczty głosowej. Dodatkowo korzystać z tego rozwiązania mogą także administratorzy sieci osiedlowych, małe firmy oraz indywidualni użytkownicy.

3. Miejsce Asterisk w systemach telefonii IP

Na podstawie podziału systemów telefonii IP z [7], biorąc pod uwagę trzy aspekty rozwiązań głosowych tj. wykorzystywane protokoły sygnalizacyjne, zasięg wykorzystywanej sieci oraz zastosowany model architektury systemu, Asterisk należy umiejscowić w części wspólnej diagramu przedstawionego na rys. 1.



Rysunek 1. Umiejscowienie systemu Asterisk w klasyfikacji systemów telefonii IP

Zatem system Asterisk jest systemem telefonii IP, wykorzystującym generyczne protokoły sygnalizacyjne VoIP oraz rozwiązania producenckie w tym zakresie (SCCP, IAX2). Zasięgiem obejmuje sieci różnej wielkości (sieć Internet, intranet itp.) oraz bazuje na modelu klient serwer (w odróżnieniu od np. usługi Skype).

4. Rodzaje i techniki ataków na systemy VoIP

Zanim zostanie przedstawiona analiza zabezpieczeń systemu Asterisk niezbędne jest wprowadzenie odpowiedniej terminologii oraz wyjaśnienie technik ataków na telefonię IP. Pozwoli to uwypuklić problem niebezpieczeństw, którym może podlegać taki system teleinformatyczny.

Usługi ochrony informacji dla systemów VoIP należy rozważać według kryteriów, które dadzą nam możliwości zapewnienia, co najmniej, trzech z pięciu podstawowych usług ochrony informacji opisanych w normie ISO 7498-2 tj. uwierzytelnienia (*authentication*), integralności danych (*data integrity*) oraz poufności danych (*confidentiality*).

Przy dokonywaniu analizy bezpieczeństwa należy mieć również świadomość zagrożeń, na jakie może być narażony Asterisk. Akcje podejmowane przez intruzów można podzielić na dwie podstawowe grupy: ataki aktywne oraz pasywne. Te pierwsze polegają na celowej ingerencji w np. komunikację między stronami połączenie, natomiast drugie zawierają w sobie takie działania jak podsłuch czy monitorowanie wymienianego w sieci ruchu.

Do przeprowadzania ataków wykorzystywane są odpowiednie techniki. Podstawowe techniki ataków na systemy VoIP możemy podzielić na trzy kategorie: *Spoofing* (podszywanie się), *Sniffing* (podsłuchiwanie) oraz *Denial of Service* (odmowa usługi). Wymienione techniki można scharakteryzować następująco:

- **Spoofing** – polega na celowym podszywaniu się pod danego użytkownika (np. za pomocą jego adresu IP), dzięki czemu napastnik może mieć możliwość wysyłania sfałszowanych wiadomości,
- **Sniffing** – opiera się na szczegółowym obserwowaniu i analizowaniu pakietów wysyłanych przez sieć,

- **Denial of Service** – polega na zablokowaniu możliwości funkcjonowania danego elementu sieci, co może mu uniemożliwić świadczenie danej usługi prawowitym użytkownikom (np. poprzez zalanie danego elementu dużą ilością wiadomości).

Wykorzystanie każdej z wyżej przedstawionych technik może doprowadzić do różnego rodzajów ataków. Dla przykładu: za pomocą techniki podszycia możliwe jest odkrywanie treści wiadomości a następnie jej modyfikacja. Dzięki technice podsłuchania intruz potrafi w pasywny sposób zaglądać w przesyłane wiadomości, natomiast atak typu DoS stwarza ryzyko sparaliżowania działania platformy VoIP. Na wszystkie wymienione zagrożenia każdy system telefonii IP powinien być „przygotowany", by w sposób bezpieczny oferować użytkownikom swoje usługi.

Oprócz ataków charakterystycznych dla sieci IP, specyfika telefonii IP rodzi też nowe zagrożenia. Jednym z najpoważniejszych jest SPIT (*Spam over Internet Telephony*), który w ciągu kilku lat może stać się prawdziwą zmorą systemów telefonicznych opartych na protokole IP. Działa on na podobnej zasadzie co mailowy SPAM – niechciane rozmowy telefoniczne, ale rodzi dużo poważniejsze problemy, gdyż może znacząco wpłynąć np. na wydajność pracy lub prowadzić do ataków DoS.

5. Bezpieczeństwo systemu VoIP opartego na Asterisk

Rozważając potencjalne zagrożenia, na jakie może być narażony Asterisk należy brać pod uwagę bezpieczeństwo całej komunikacji, w której pośredniczy, jak również odporność na ataki maszyny, na której system ten się znajduje. Oznacza to w szczególności, iż trzeba zidentyfikować każdy rodzaj ruchu, który powinien podlegać zabezpieczaniu w telefonii IP oraz zadbać o fizyczne aspekty konfiguracji. Pierwsza z wymienionych kwestii dotyczy zapewnienia bezpieczeństwa protokołom komunikacyjnym wykorzystywanym w systemie Asterisk: przede wszystkim protokołom sygnalizacyjnym: SIP, H.323, MGCP, SCCP, IAX2 oraz transmisji głosu: RTP. W tym wypadku kluczowe jest to, czy komunikacja jest dostępna dla kogoś, kto nie powinien mieć do niej dostępu. Sytuacja taka będzie mieć miejsce zawsze wówczas, gdy można przechwytywać pakiety (np. w sieci LAN) oraz gdy ich zawartość nie jest zabezpieczana z wykorzystaniem kryptograficznych mechanizmów zabezpieczeń.

Drugim zagadnieniem, jak wspomniano, jest bezpieczeństwo maszyny, na której został zainstalowany i działa Asterisk. Duże znaczenie ma tu wybór systemu operacyjnego oraz jego bezpieczeństwo. Istotne jest także m.in. to, czy uruchamiamy równolegle na tej samej maszynie inne usługi i czy umożliwiamy użytkownikom zdalny dostęp (np. poprzez SSH).

W kolejnych podpunktach przedstawiono praktyczne doświadczenia, które przeprowadzono w celu zbadania obecnego poziomu bezpieczeństwa sygnalizacji oraz przesyłanego głosu w systemie Asterisk.

5.1 Bezpieczeństwo sygnalizacji i głosu

W przypadku zabezpieczania protokołu sygnalizacyjnego telefonii IP należy zagwarantować bezpieczeństwo wiadomościom tego protokołu, które są przesyłane pomiędzy stronami komunikującymi się. Z punktu widzenia usług bezpieczeństwa informacji oznacza to konieczność zapewnienia ich integralności, uwierzytelnienia oraz poufności. Typowe ataki na protokół sygnalizacyjny (tu na przykładzie protokołu SIP) scharakteryzowano poniżej:

- **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.

Dla analizowanego przez nas protokołu sygnalizacyjnego SIP, wśród zdefiniowanych w standardzie mechanizmów zabezpieczeń dostępne są algorytmy SIPS URI, S/MIME (*Secure MIME* [19]) oraz SIP Digest. Pierwszy z nich oparty jest na protokole TLS (*Transport Layer Security*). Niestety środowisko Asterisk, będąc w fazie ciągłego rozwoju, nie posiada, na chwilę obecną, zaimplementowanego tegoż mechanizmu. Podobnie jest z S/MIME. Jedynym wspieranym zabezpieczeniem jest SIP Digest, umożliwiający zapewnienie uwierzytelnienia i integralność przesyłanych danych (analogiczny w działaniu do HTTP Digest [18]). Mechanizm ten jednak nie spełnia do końca swojej roli, ponieważ wykorzystuje złamaną funkcję skrótu MD5 (*Message Digest 5*), a współdzielone hasło, jeśli jest zbyt krótkie, możliwe jest do uzyskania w rozsądnym czasie metodami słownikowymi bądź siłowymi (brute-force).

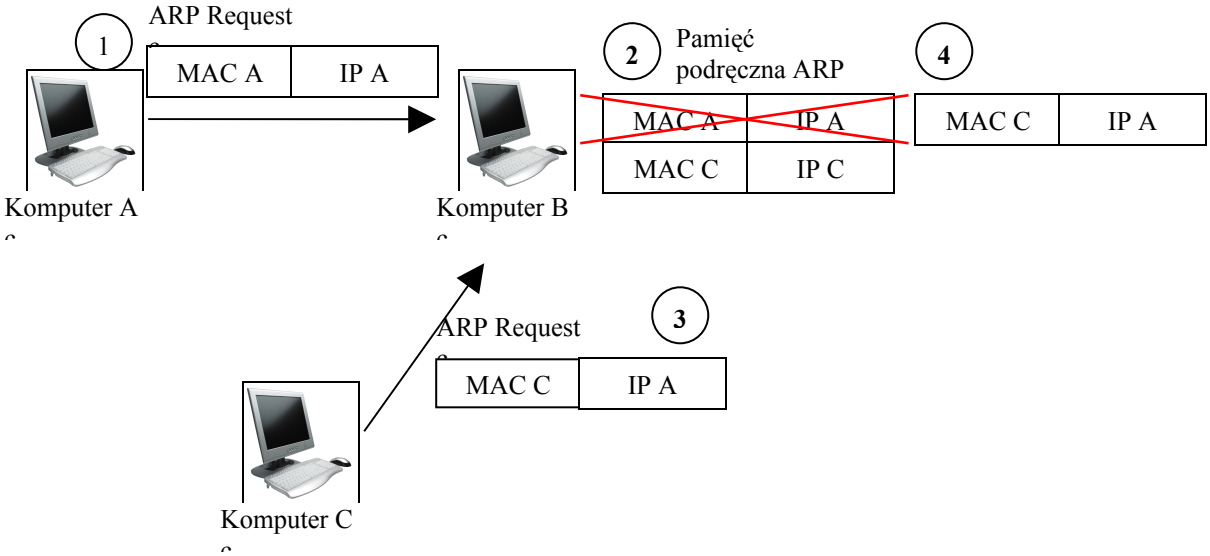
Przeglądając kierunki rozwoju firmy Asterisk znaleźć można plany wprowadzenia szyfrowania sygnalizacji i przesyłanego dźwięku. Należy jednak podkreślić, że na chwilę obecną opcja ta jest dopiero w fazie testów i wymaga pracy nad stabilnością.

5.2 Przeprowadzone doświadczenia: ataki na sygnalizację i głos

Wykonane przez nas doświadczenia były próbami ataków na protokół sygnalizacyjny oraz na przesyłany głos. Celem tych pierwszych było podsłuchiwanie wiadomości protokołu sygnalizacyjnego (ataki pasywny) oraz próba zmiany treści wiadomości (atak aktywny). Wykorzystano w tym celu atak Man-In-The-Middle (MITM) oraz technikę ARP Poisoning. Natomiast test bezpieczeństwa przesyłanego głosu koncentruje się na najczęściej wykorzystywanym w telefonii IP protokole transmisji mediów – protokole RTP (*Real-time Transport Protocol*). Jest on obsługiwany przez Asterisk, większość terminali oraz urządzeń typu ATA (tzw. bramka VoIP) dostępnych na rynku. Należy odnotować, że protokół RTP, jako taki, nie zapewnia jednak bezpieczeństwa transmisji, a tym samym pociąga za sobą ryzyko np. podsłuchania rozmowy. Nie zapewnia on także integralności, co z kolei powoduje podatność na ataki typu Man-In-The-Middle, które mogą polegać na modyfikacji transmitowanych pakietów. Rozwiązaniem tych problemów jest protokół SRTP (*Secure RTP*) jednakże nie jest on obecnie obsługiwany, ani przez stabilną wersję Asterisk (istnieje branch Asterisk SRTP), ani też przez większość wykorzystywanych terminali (bądź są one dużo droższe). Tym samym typowa konfiguracja z użyciem niezabezpieczonego protokołu RTP powoduje szereg zagrożeń związanych z brakiem zapewniania jakichkolwiek usług kryptograficznych.

Doświadczenie 1. Zatruwanie tablic ARP (ARP Poisoning)

Celem pierwszego doświadczenia jest wykonanie próby ataku ARP Poisoning, który może zostać dokonany np. przy użyciu narzędzia Ettercap [12], a polega na celowej modyfikacji pamięci podręcznej ARP biorących w komunikacji maszyn. Zasadę działania tego ataku przedstawiono na poniższym rysunku.



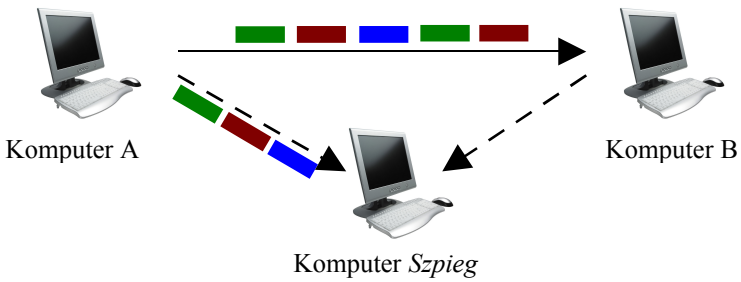
Rysunek 2. Schemat ataku ARP Poisoning

Komputer B otrzymując pakiet ARP Request spodziewa się połączenia z komputera A, więc żeby nie wysyłać zbędnych pakietów ARP, zapisuje parę MAC, IP z pakietu ARP Request w swojej pamięci podręcznej ARP. Taką sytuację można wykorzystać wysyłając wiele zapytań ARP Request ze swoim adresem MAC, ale zawierającym adres IP np. komputera A. Spowoduje to zmodyfikowanie pamięci podręcznych ARP wszystkich komputerów w sieci i pozwoli na przejmowanie tym samym komunikacji przeznaczonej dla tego komputera. Jest wiele gotowych narzędzi umożliwiających przeprowadzenie ataku ARP Spoofing/ARP Poisoning, w tym bardzo rozbudowane, użyte przez nas, sniffery, np. Ethereal [13] (w nowszej wersji WireShark), czy wspomniany Ettercap.

Wynik próby zakończył się pomyślnie. Prostym i skutecznym zabezpieczeniem przed takim atakiem jest ustawienie statycznych wpisów pamięci podręcznej ARP dla komputerów w naszej sieci ethernet.

Doświadczenie 2. Atak pasywny: analiza pakietów

Kolejnym przeprowadzonym doświadczeniem jest analiza pakietów, którą można wykonać przy użyciu oprogramowania Ethereal. Celem tej analizy jest uzyskanie niezbędnych do przeprowadzania ataku aktywnego informacji o połączeniu dla protokołu sygnalizacyjnego SIP są to m.in. adresy agentów użytkownika SIP (punktów końcowych), ich hasła czy identyfikatory połączeń (Call-ID). Schemat przeprowadzonego ataku przedstawiono na rys. 3.



Rysunek 3. Schemat sieci wykorzystywany do analizy pakietów.

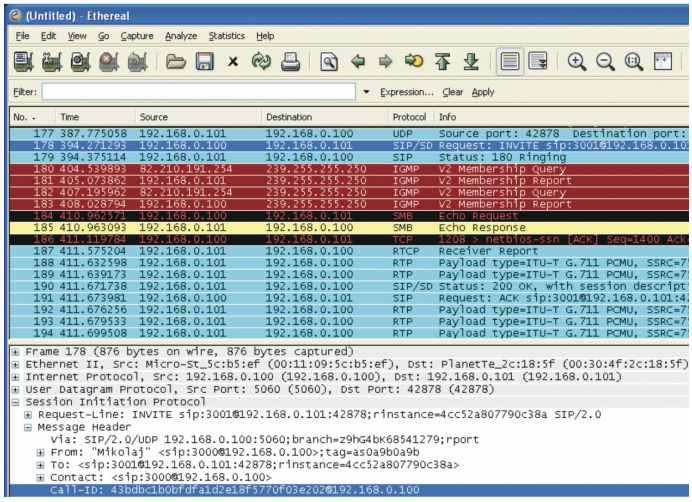
Komputer *Szpieg* przełącza kartę sieciową w tryb *promiscuous*, dzięki czemu urządzenie odbiera wszystkie pakiety z sieci, także te nie adresowane bezpośrednio do niego, w naszym

przypadku od komputera A. Narzędzie Ethereal, używane w doświadczeniu, może być uruchamiane na routerze, bądź serwerze sieciowym, który pośredniczy w wymianie wiadomości sygnalizacyjnych lub na komputerze będącym jedną ze stron komunikacji sieciowej - w takim przypadkach tryb *promiscuous* nie jest konieczny.

Jak wspomniano Asterisk oferuje dla protokołu SIP mechanizm uwierzytelnienia SIP Digest wykorzystujący funkcję skrótu MD5. Podsłuchując wymianę pakietów między agentami użytkowników możliwe jest wykonanie próby złamania zabezpieczonego hasła. Do przeprowadzania takiego ataku można użyć ogólnodostępnego narzędzia Cain & Abel [14], które umożliwia łamanie haseł metodami siłowymi (brute-force).

Przykładowe wyniki analizatora dla protokołu SIP przedstawia rys. 4. Prezentuje on osobie atakującej w sposób czytelny, niewymagający dalszej obróbki, wartości tj. adresy agentów użytkownika (pole From), rodzaj wiadomości (Request Line), identyfikator trwającego połączenia (Call-ID) i wiele innych wartości pól nagłówków protokołu SIP. Analogiczny atak pasywny może być przeprowadzony dla protokołu IAX2.

Próba złamania zabezpieczonego hasła za pomocą narzędzia Cain & Abel, dla mechanizmy SIP Digest zakończyła się pomyślnie. Złamanie hasła 4-znakowego zajmowało średnio 3 sekundy, natomiast hasła 6-znakowego średnio 40 minut.



Rysunek 4: Wynik pracy programu Ethereal dla protokołu SIP (podgląd wiadomości INVITE; wyróżniona linia zawierającą identyfikator połączenia Call-ID).

Doświadczenie 3. Atak aktywny

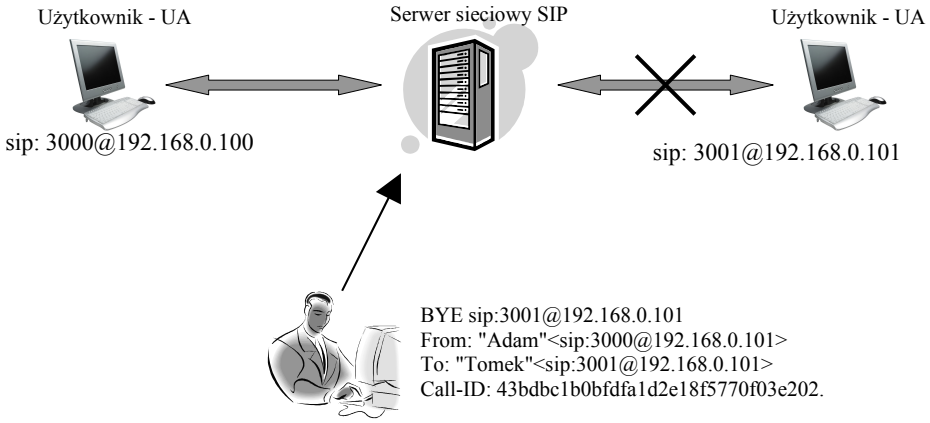
Po przeprowadzeniu udanych ataków pasywnych (zebraniu niezbędnych informacji) przechodzimy do wykonania ataków aktywnych. Ich zadaniem jest próba celowego zakańczania trwających połączeń, poprzez wysłanie przez intruza wiadomości BYE w czasie, gdy zachodzi komunikacja między użytkownikami. Doświadczenie to polega na utworzeniu i wysłaniu odpowiednio spreparowanego pakietu, który ma na celu zakończenie trwającego połączenia co przedstawiono na rys. 5.

Opisany atak wymaga również utworzenia i wysłania do centrali Asterisk odpowiednio spreparowanej wiadomości BYE protokołu SIP (służącej do zakańczania trwającego połączenia) dla przykładu:

```
BYE sip:3001@192.168.0.101:33924 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.100:5060;branch=z9hG4bK01f6f4fa;rport
From: "Adam"<sip:3000@192.168.0.101>;tag=as6486104f
To: "Tomek"<sip:3001@192.168.0.101>;tag=5c558618
Call-ID: 43bdbc1b0bfdfa1d2e18f5770f03e202.
CSeq: 102 BYE
```

```
User-Agent: Asterisk PBX
Max-Forwards: 70
Content-Length: 0
```

Pakiet ten powinien zawierać: adres SIP terminala i centrali oraz identyfikator trwającego połączenia Call-ID. Przygotowany pakiet należy umieścić w polu danych pakietu UDP i np. przy użyciu narzędzia Nemesis [15] wysłać do sieci lokalnej. Atak ten również został przeprowadzony pomyślnie.



Rysunek 5: Schemat układu ataku aktywnego – zakańczania trwającego połączenia

Innego rodzaju ataku aktywnego można dokonać za pomocą ogólnie dostępnego skanera luk sieci VoIP opartej na protokole SIP – SiVuS [16]. Składa się on z kilku modułów, które pozwalają przeprowadzać ataki oraz skanują odporność na błędy i stan bezpieczeństwa komunikatorów SIP, serwerów sieciowych SIP (Proxy, Redirect i Registrar). Narzędzie to umożliwia podszycie się pod innego użytkownika, przy jednoczesnym ukryciu tożsamości osoby atakującej. Po udanej operacji podszycia się możliwa jest ingerencja w aktywność sieciową zaatakowanego użytkownika np. zadzwonienie do jego znajomych lub wykorzystanie uprawnień przez niego posiadanych.

Opisany powyżej atak bazuje na luce w procesie rejestracji agentów użytkownika w serwerze Registrar. Każdy agent użytkownika jest zobligowany do rejestracji w tym serwerze, ponieważ rejestracja w sieci VoIP jest niezbędna do subskrybowania usługi. Żądanie rejestracji (wiadomość REGISTER) zawiera pole Contact, które zawiera adres IP urządzenia (niezależnie, czy to jest telefon IP, czy komunikator zainstalowany na PC). Osoba atakująca wysyła zmodyfikowaną wiadomość REGISTER, w której pole Contact zawiera adres IP osoby atakującej.

Powyższe przykłady doświadczeń są tylko wycinkiem z całej gamy dostępnych ataków. Dlatego też, należy wykorzystywać dostępne narzędzia do testowania bezpieczeństwa zarówno oprogramowania, jak i sprzętu tj. SiVuS, PROTOS czy SIP Forum Test Framework w celu przeprowadzania okresowego audytu we własnej sieci telefonii IP.

Doświadczenie 4. Przechwycenie strumienia RTP – nagrywanie rozmowy

Celem opisywanego ataku na strumień mediów jest przechwycenie komunikacji głosowej, która odbywa się pomiędzy użytkownikami. Z sieciowego punktu widzenia atak ten jest analogiczny do tego z doświadczenia nr 2 (analiza pakietów), gdyż sprowadza się do przechwytywania datagramów (schemat jak na rys. 3). Różnicą, w przypadku tego doświadczenia jest to, że analizowany jest ruch głosowy nie zaś sygnalizacyjny.

Dokonany przez nas atak na protokół RTP został zrealizowany przy pomocy tylko jednego programu. Użyte narzędzie to Cain & Abel. Aplikacja umożliwia przechwycenie i

nagranie strumienia RTP (w typowej sesji dwóch strumieni) mając zaszytą funkcjonalność ARP Poisoningu oraz rozpoznawania ruchu RTP. Wykonanie podsłuchu polega na włączeniu monitoringu wraz z atakiem ARP Poisoning, zaś program automatycznie po identyfikacji protokołu sygnalizacyjnego VoIP rozpoczyna zapis rozmowy do plików dźwiękowych WAV.

5.3 Analiza wyników doświadczeń oraz możliwe zabezpieczenia chroniące przed lukami

Powyżej, poprzez praktyczne doświadczenia, przedstawiono jak bardzo aspekty bezpieczeństwa protokołów sygnalizacyjnych zaimplementowanych w Asterisk są jeszcze niedopracowane. Obecnie to producencki protokół IAX2 oferuje najbardziej zaawansowane metody uwierzytelniania: z funkcją skrótu MD5 lub RSA pod warunkiem, że hasło będzie na tyle długie, że czas potrzebny na jego złamanie będzie dłuższy od ważności takiego hasła. Natomiast należy zdawać sobie sprawę, że protokół IAX2 jest protokołem producenckim. Jako taki, nie jest w stanie konkurować ze zestandaryzowanymi protokołami sygnalizacyjnymi SIP, H.323, czy H.248/Megaco np. pod względem ilości dostępnych produktów, czy usług.

Bezpieczeństwo głosu w Asterisk również stanowi potencjalne zagrożenie. Analizowany protokół RTP pozwolił na całkowite przechwycenie komunikacji głosowej w przypadku sieci pozwalającej na dostęp do pakietów danych jak w sieci lokalnej.

Zaprezentowane ataki aktywne udowodniły, że osoba niepowołana jest w stanie wpływać na przebieg sygnalizacji, a tym samym na trwające, czy zestawiane połączenie. Metodą na przeciwdziałanie tego typu atakom może być zabezpieczanie danych na poziomie warstwy aplikacji, transportowej bądź sieciowej. Jednakże Asterisk nie posiada na chwilę obecną wsparcia dla protokołu SIPS URI. Rozwiązaniem takiej sytuacji, zabezpieczeniem chroniącym przed lukami, mogą być wirtualne sieci prywatne VPN (Virtual Private Network). Jednak pomimo wielu zalet ma również wady. Przede wszystkim wprowadza dodatkowe opóźnienia przy jednoczesnym zwiększonym zużyciu dostępnego pasma, co może być kluczowym czynnikiem wpływającym na jakość przesyłanego głosu w VoIP. VPN zwiększa również zapotrzebowanie na moc obliczeniową urządzeń je obsługujących, co w konsekwencji prowadzi do poniesienia ich ceny (zwiększony koszt). Dodatkowo wirtualne sieci prywatne nastręczają czysto praktycznych trudności. VPN wymaga instalacji oprogramowania na stacji klienta, a co za tym idzie powstaje problem z obsługą wszystkich systemów operacyjnych. Dodatkowo mogą wystąpić problemy współdziałania pomiędzy klientami VPN różnych dostawców. Kolejnym problemem mogą być zapory sieciowe i inne urządzenia pomiędzy klientem i bramą VPN, które mogą niekorzystnie wpływać na możliwość zestawiania połączeń VPN. Wszystko to powoduje, że pomimo iż jest to rozwiązanie gwarantujące wysoki poziom bezpieczeństwa, w praktyce, raczej się go dla telefonii IP nie wykorzystuje.

Najlepszym rozwiązaniem dla zabezpieczenia głosu, byłoby wykorzystanie szyfrowania poprzez wykorzystanie protokołu SRTP, jednakże, jak wcześniej wspomniano, w systemie Asterisk te rozwiązania muszą zyskać jeszcze na stabilności. Ponadto istnieje możliwość transportu mediów przy użyciu protokołu IAX2. Jest to jednak rozwiązanie specyficzne dla Asterisk, a tym samym może być stosowane jedynie w wąskim gronie urządzeń, które je wspierają. Oprócz kilku softphone'ów (w tym Idefisk [17]) istnieją co najmniej dwa urządzenia ATA wspierające ten protokół. W podstawowej wersji IAX2 nie zapewnia szyfrowania. Istnieje, co prawda dokładnie nieudokumentowana możliwość szyfrowania 128-bitowym AES, jednak większość wdrożeń Asterisk nie wykorzystuje tego zabezpieczenia.

6. Podsumowanie

W każdym systemie telefonii IP skuteczna realizacja usług bezpieczeństwa informacyjnego jest podstawą do jego szerokiego zastosowania komercyjnego. Bez

zapewnienia minimalnych wymagań bezpieczeństwa w każdym z obszarów (sygnalizacja i media) oraz dla każdej z usług, nawiązywanych przez użytkowników połączeń nie można uznać za bezpieczne.

Analizowana platforma Asterisk ma wiele podatności, które zostały zilustrowane w przeprowadzonych doświadczeniach praktycznych. Spośród trzech, najważniejszych dla VoIP, usług bezpieczeństwa (tj. uwierzytelnienie, integralność, poufność) najlepiej zapewnia on pierwszą z nich. Głównie ze względu na mechanizm SIP Digest. Pozostałe dwie usługi nie są właściwie w żaden sposób wspierane, a jedynie za pomocą dodatkowych rozwiązań np. VPN. Poniższa tabela przedstawia zestawienie zapewnienia usług bezpieczeństwa dla obu omawianych protokołów sygnalizacyjnych:

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

Tabela 1. Realizacja usług bezpieczeństwa w systemie Asterisk (+) usługa wspierana, (-) usługa niewspierana

Literatura

[1] Asterisk: http://www.asterisk.org, AsteriskWin32 - http://www.asteriskwin32.com/
[2] Tlefon: http://www.tlenofon.pl
[3] M. Handley, H. Schulzrinne, J. Rosenberg, SIP: Session Initiation Protocol, IETF RFC 3261, czerwiec 2002
[4] H.323 - Packet-based multimedia communications systems, ITU-T
[5] F. Cuervo, N. Greene, A. Rayhan, C. Huitema, B. Rosen, J. Segers, Megaco Protocol Version 1.0, IETF RFC 3015, listopad 2000
[6] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries: Security Considerations for Voice Over IP Systems, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (2004).
[7] W. Mazurczyk - Aspekty bezpieczeństwa sieci P2P na przykładzie Skype - In Proceedings of XXII Krajowe Sympozjum Telekomunikacji i Teleinformatyki KSTiT 2006, Bydgoszcz, 13-15 wrzesień 2006
[8] W. Mazurczyk - Bezpieczeństwo SIP jako protokołu sygnalizacyjnego VoIP - XIX Krajowe Sympozjum Telekomunikacji KST 2003, Bydgoszcz, wrzesień 2003
[9] W. Mazurczyk - Bezpieczeństwo protokołów sygnalizacyjnych VoIP: koncepcja bezpiecznej współpracy protokołów SIP i H.323 - VIII Krajowa Konferencja Zastosowań Kryptografii Enigma 2004, Warszawa, maj 2004
[10] Digium – http://www.digium.com
[11] T. Piotrowski, S. Wójcik, M. Wiśniewski, W. Mazurczyk – Bezpieczeństwo Asterisk, czasopismo Hackin'9, październik 2007
[12] Ettercap – http://ettercap.sourceforge.net/
[13] Ethereal – http://www.ethereal.com/
[14] Cain & Abel – http://www.oxid.it/cain.html
[15] Nemesis – http://nemesis.sourceforge.net/index.html
[16] SiVuS – http://www.vopsecurity.org/index.php
[17] Idefisk – http://www.asteriskguru.com/idefisk/
[18] J. Franks (i in.), HTTP Authentication: Basic and Digest Access Authentication, IETF Request for Comments, RFC 2617, czerwiec 1999