jacek szleszyński

Uważaj na połączenia VoIP – można je łatwo podsłuchać

Rozmowa kontrolowana

Popularność systemów telefonicznych opartych na protokole IP jest ogromna. Można mówić nawet o swoistej modzie na pogaduchy przez Internet. Jednak usługi tego typu nie zawsze gwarantują poufność i bezpieczeństwo rozmów.

Wojciech Mazurczyk

Możliwość przesyłania głosu przez sieci transmisji danych rozpalała wyobraźnię naukowców już w latach siedemdziesiątych. Niestety, z uwagi na stan rozwoju technologicznego mało kto wtedy interesował się telefonią IP. Przez ponad dwadzieścia lat była to ciekawostka pozostająca w kręgu zainteresowań badaczy i niemająca perspektyw na komercyjne wykorzystanie.

Obecnie różnorodność usług i urządzeń przeznaczonych do Voice over IP jest ogromna, podobnie jak możliwości samej technologii. Za jej pomocą zbudujemy sieci VoIP o różnej skali, od małych firmowych po rozległe operatorskie. Rzeczywistość rozmów pakietowych nie wygląda jednak różowo. Ich główne wady to zmienna jakość połączenia (zależna np. od obciążenia łączy) oraz luki w bezpieczeństwie. Jednym z powodów takiego stanu rzeczy jest fakt, że usługi tego sektora rozwijają się dużo szybciej niż stosowane w nich mechanizmy ochronne.

Serce telefonii IP

Działanie systemów VoIP oparte jest na trzech grupach protokołów, odpowiedzialnych za: sygnalizację (H.323, SIP, H.248/Megaco), kodowanie mowy (np. G.711, G.729, G.723) i transport danych (RTP, UDP, TCP). Uzupełniają je dodatkowo takie protokoły jak: SDP, RTSP, RSVP. Najważniejszą rolę odgrywają protokoły sygnalizacyjne. To na nich są oparte systemy VoIP i to one decydują m.in. o architekturze oraz sposobie funkcjonowania tej sieci. Dlatego też często określa się je mianem serca telefonii IP.

Najpopularniejsze protokoły sygnalizacyjne to SIP (Session Initiation Protocol, patrz: ramka Protokół sygnalizacyjny SIP), H.323 (patrz: **CHIP 2/2005,** 24) oraz H.248/Megaco, a wykorzystujące je systemy telefoniczne nazywamy klasycznymi (generycznymi). Standardy te zostały opracowane przez takie organizacje, jak ITU i IETF, cieszące się prestiżem zarówno w środowisku naukowym, jak i wśród firm. W ostatnim czasie dynamicznie rozwijają się także inne metody przesyłania głosu przez sieci pakietowe (np. Tlenofon, Skype). Określamy je mianem telefonii internetowej, ponieważ wykorzystują inne protokoły niż generyczne systemy VoIP i działają w ramach sieci Internet (ale już nie np. w odseparowanych intranetach).

O autorze

Wojciech Mazurczyk jest doktorantem i członkiem Security Research Group na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej oraz autorem publikacji naukowych i popularnonaukowych z dziedziny bezpieczeństwa usług multimedialnych (w tym telefonii IP). Współtworzy i prowadzi „Warsztaty VoIP" w ITU Internet Training Centre na Politechnice Warszawskiej (**http://itu-itc.elka.pw.edu.pl**). Jest także prelegentem na licznych konferencjach poświęconych bezpieczeństwu z dziedziny telekomunikacji i ochrony informacji. Więcej informacji o autorze można znaleźć pod adresem: **http://mazurczyk.com**.

Niektórzy producenci sprzętu i oprogramowania dla telefonii IP forsują również własne protokoły. Przykładowo: firma Cisco wykorzystuje SCCP (Skinny Client Control Protocol). Kluczem do sukcesu w tego typu wypadkach jest przede wszystkim kompatybilność urządzeń ze standardami SIP, H.323 czy H.248/Megaco.

Geneza zagrożeń

W 2005 roku amerykański National Institute of Standards and Technology opublikował ciekawy raport pt. „Security Considerations for Voice Over IP Systems", w którym opisano ewidentne braki w zabezpieczeniach telefonii IP. Autorzy dokumentu podkreślają jednak, że nie ma uniwersalnych metod ochrony dla systemów telefonii pakietowej, które dałoby się z powodzeniem zastosować w każdej sieci VoIP. Dopiero po analizie konkretnych konfiguracji, architektury i specyfiki danej sieci można próbować łatać dziury i likwidować jej słabe punkty (najczęściej w tym celu wykorzystuje się mechanizmy stworzone do ochrony transmisji danych: firewalle, systemy IDS/IPS, VLAN oraz VPN itp).

Protokół sygnalizacyjny SIP

Session Initiation Protocol (SIP) jest tekstowym protokołem sygnalizacyjnym służącym do nawiązywania, zarządzania, kończenia i uzgadniania parametrów połączenia głosowego w sieci IP. Opracowała go organizacja IETF (Internet Engineering Task Force), korzystając z istniejących i sprawdzonych mechanizmów sieciowych (DNS, SDP, RSVP, RTP, RTSP). Protokół SIP jest podobny do HTTP, stąd też łatwo go integrować z WWW.

Architektura sieci VoIP opartej na protokole SIP składa się z kilku komponentów. Pierwszym jest Agent Użytkownika, stanowiący system końcowy (zazwyczaj jest to specjalne oprogramowanie). Działa on w imieniu uczestnika połączenia i składa się z dwóch części, funkcjonujących na zasadzie klient-serwer. Klient Agenta Użytkownika (User Agent Client) jest odpowiedzialny za wysyłanie żądań protokołu SIP (np. ustanowienia połączenia), natomiast Serwer Agenta Użytkownika (User Agent Server) odbiera żądania przesyłane do niego przez innych agentów oraz wysyła im odpowiedzi.

Drugą grupą elementów sieciowych omawianej architektury VoIP są serwery sieciowe, dokonujące translacji adresów oraz pośredniczące w procesie odnajdywania użytkownika (agenta) docelowego. W SIP wyróżnia się dwa rodzaje serwerów sieciowych: proxy (po otrzymaniu żądania ustalają adres następnego serwera, któremu mają przekazać dane) oraz redirect (odpowiedzialne za wysyłanie do agenta odpowiedzi zawierającej adres kolejnego serwera, z którym należy się skontaktować w poszukiwaniu właściwego serwera użytkownika końcowego).

Obecnie SIP staje się wiodącym protokołem dla usług VoIP, detronizując protokół H.323. Chętnie wykorzystują go najwięksi producenci sprzętu i oprogramowania (m.in. Cisco, Siemens, Alcatel). Jego głównymi zaletami są prostota działania oraz łatwość realizacji i implementacji zaawansowanych usług.

Informacje przesyłane za pomocą SIP składają się z pól nagłówka oraz ciała wiadomości. Rozróżniamy sześć rodzajów wiadomości protokołu SIP:

- **INVITE** – zaproszenie do udziału w połączeniu lub konferencji,
- **BYE** – zakończenie połączenia między dwoma uczestnikami połączenia/konferencji,
- **OPTIONS** – przekazanie informacji o funkcjonalności strony komunikującej się, np. kodeków mowy, które może obsługiwać,
- **STATUS** – informowanie drugiego serwera o postępie wywołanej metody,
- **ACK** – realizowanie niezawodnej wymiany wiadomości INVITE,
- **REGISTER** – przenoszenie informacji o lokalizacji użytkownika dla serwera SIP.

Wymienione wiadomości sygnalizacyjne zawierają m.in. pola: Call-ID (jednoznacznie identyfikujące rozmowę), From oraz To (określające nadawcę i odbiorcę) czy Via (pozwalające śledzić wiadomości INVITE, zapobiegające powstawaniu pętli). Za pomocą SIP przesyłane są także odpowiednie wartości wskazujące na postęp w przetwarzaniu informacji, oznaczające przekierowania, prawidłowe wykonanie operacji lub inne komunikaty (np. o błędach).

```
INVITE sip: bob@biloxi.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com:5060;
     branch=z9hG4bK74bf9
Max-Forwards: 80
From: Alice <sip:alice@atlanta.com>
      tag=9fxced76sl
To: Bob <sip:bob#biloxi.com>
Call-ID: 3848276298220188511@atlanta.com
CSeq: 31862 INVITE
Contact: <sip:alice@atlanta.com>
Content-Lenght: 151

v=0
o=alice 2890844526 2890844526
  IN IP4 atlanta.com
c=IN IP4 10.1.3.33
t=0 0
m=audio 49172 RTP/AVP 0 4 8
a=rtpmap:0 PCMU/8000
```

Informacja sygnalizacyjna (wiadomość SIP) składa się z nagłówka (fragment na szarym tle) i tzw. ciała wiadomości (na żółto).

Problemy z zabezpieczeniem telefonii IP wynikają przede wszystkim z różnorodności zagrożeń, na jakie jest ona narażona. Paradoksalnie główne źródło kłopotów leży w największej zalecie technologii VoIP – wykorzystaniu do przesyłania głosu tego samego medium, które stosuje się do transmisji danych. Po prostu „mieszanie się" pakietów zawierających głos z innymi informacjami pozwala intruzowi w prosty sposób na przechwycenie lub modyfikację rozmowy. Wystarczy zainstalować odpowiednie oprogramowanie i wyfiltrować określony ruch.

Podobnie jak w wypadku urządzeń i aplikacji przeznaczonych do transmisji danych, luki w systemach VoIP można podzielić na powstałe w oprogramowaniu oraz wynikające z błędów w ich konfiguracji (te ostatnie są najczęściej wykorzystywane przez atakujących).

Poważnym źródłem problemów telefonii IP jest również jej wrażliwość na opóźnienia. Graniczna wartość tego parametru, po której jakość rozmowy spada do nieakceptowalnego przez użytkowników poziomu, to 150 ms. Na opóźnienie składa się wiele czynników, m.in. czas potrzebny na „ucyfrowienie" głosu, podzielenie go na pakiety, a następnie zadbanie, aby w punkcie docelowym zostały one odpowiednio uszeregowane i odtworzone. Dodanie mechanizmów zabezpieczających wiąże się więc ze zwiększeniem wartości opóźnienia, co może niekorzystnie wpłynąć na jakość połączenia.

Rodzaje ataków

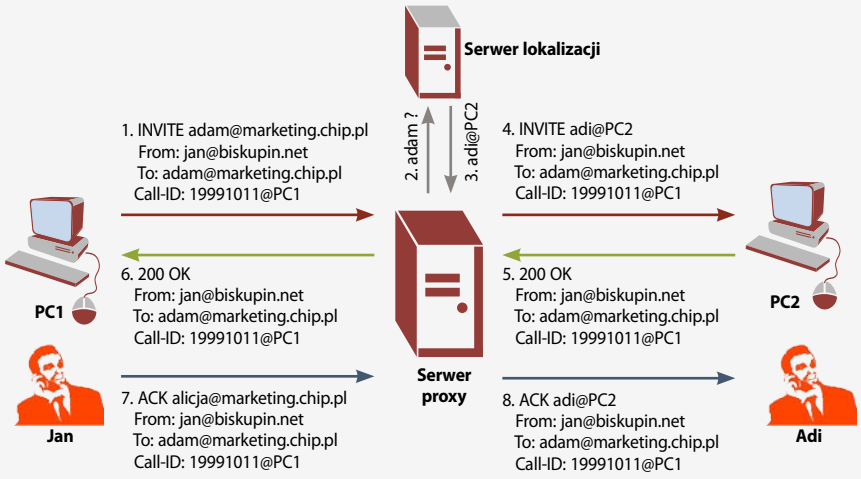
Zagrożenia wynikające z celowego działania intruza mogą mieć charakter pasywny (np. podsłuch) lub aktywny (ingerencja w przesyłane pakiety). Do wpływania na VoIP 40»

Nawiązywanie połączenia w sieci VoIP opartej na SIP

Faza sygnalizacji i transmisji rozmowy

Połączenie w telefonii IP składa się z fazy sygnalizacyjnej, w trakcie której wymieniane są odpowiednie wiadomości sygnalizacyjne i negocjowane parametry połączenia, oraz fazy przetworzenia i transmisji sygnału głosowego (rozmowy) poprzez sieć IP. Trzeba też pamiętać, że w odróżnieniu od tradycyjnej komunikacji głosowej (gdzie na czas rozmowy zestawiany jest fizyczny kanał transmisji danych) w telefonii IP za połączenie uznajemy jedynie określony stan sygnalizacji oraz transmisję strumienia z głosem pomiędzy dwoma punktami sieci IP.

Przebieg połączenia z wykorzystaniem protokołu SIP w trybie proxy:



1. Użytkownik wybiera osobę, z którą chce się skontaktować. Klient Agenta Użytkownika przesyła do serwera proxy wiadomość INVITE. Serwer akceptuje to żądanie.
2. Serwer proxy kontaktuje się z usługą katalogową, podając pełny adres osoby, do której dzwonimy.
3. Usługa katalogowa wysyła bardziej precyzyjną informację o lokalizacji osoby wybranej do połączenia.
4. Serwer proxy wysyła żądanie pod adres wskazany przez usługę katalogową. Serwer Agenta Użytkownika powiadamia użytkownika o połączeniu przychodzącym.
5. Serwer Agenta Użytkownika przekazuje do Proxy wiadomość o sukcesie przeprowadzonej operacji.
6. Serwer proxy przekazuje tę wiadomość do użytkownika wywołującego.
7. Odbiór wiadomości jest potwierdzany przez wywołującego za pomocą żądania ACK.
8. Żądanie ACK jest przekazywane do wywoływanego.
9. Po poprawnym wykonaniu kroków 1–8 następuje druga faza połączenia, czyli rozmowa (przepływ pakietów protokołu RTP).

Przebieg ataku Impersonating a Server

Gdy użytkownik wyśle wiadomości INVITE, intruz inicjuje przekierowanie połączenia (odpowiedź 301), co w rezultacie powoduje rozpoczęcie zestawiania połączenia z atakującym.

wykorzystuje się narzędzia oraz techniki znane z sieci pakietowych, takie jak spoofing (podszywanie się), sniffing (podsłuchiwanie) czy Denial of Service (odmowa usługi). Za ich pomocą przeprowadzone mogą być takie ataki, jak:

- utrata poufności danych – realizowana przy wykorzystaniu techniki podsłuchu. Ze względu na konieczność kompromisu między opóźnieniem a jakością przesyłane rozmowy zazwyczaj nie są szyfrowane. Brak tego zabezpieczenia umożliwia bardzo prosty w realizacji atak, w rezultacie którego mamy możliwość odsłuchiwania połączenia telefonicznego.
- odmowa usługi – polega na uniemożliwieniu prawowitym użytkownikom skorzystania z usługi telefonii. W wypadku sieci VoIP ataki tego typu dotyczą przede wszystkim terminali końcowych (telefonów IP lub tzw. softphone'ów), serwerów sygnalizacyjnych lub innych elementów infrastruktury sieciowej.
- kradzież usługi – zagrożenie tego typu oznacza najczęściej stratę finansową dla prawowitego użytkownika (na rachunek którego prowadzone są nielegalne rozmowy) lub samego operatora (phreaking).

Specyfika działania telefonii VoIP 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 spam, ale rodzi dużo poważniejsze problemy. Wyobraźmy sobie sytuację, w której korporacyjne telefony zostają sparaliżowane poprzez powtarzające się co kilka minut niechciane rozmowy, bo pracownik przed podniesieniem słuchawki nie jest w stanie określić, czy dzwoni ważny klient czy „reklama". SPIT może więc znacząco wpłynąć np. na wydajność pracy.

Bezpieczna sygnalizacja

Przy zabezpieczaniu telefonii IP należy działać dwutorowo. Po pierwsze, trzeba stosować takie same systemy ochrony jak w wypadku tradycyjnego sprzętu sieciowego. Urządzenia VoIP, a w szczególności serwery sygnalizacyjne powinny być zatem odpowiednio podpięte do sieci (fizyczna budowa sieci) i skonfigurowane (właściwe adresowanie IP, listy dostępu itp.). Po drugie, należy zdawać sobie sprawę ze specyfiki działania telefonii IP i w związku z tym ze szczególnych zagrożeń, które mogą z tego wynikać.

Z punktu widzenia użytkownika najważniejsze jest, by niepowołana osoba nie podsłuchała przeprowadzanej przez niego rozmowy. Reszta aspektów bezpieczeństwa (zwykle dla niego niewidoczna) jest mniej ważna. Stąd najbardziej eksponowaną zaletą systemów telefonicznych opartych na protokole IP jest szyfrowanie głosu.

Typowe ataki na SIP

- **Porwanie Rejestracji** (Registration Hijacking) polega na modyfikacji pola **From** w wiadomości **REGISTER** (przekierowaniu połączenia).
- **Porwanie Połączenia** – analogicznie do ataku powyżej, ale modyfikacji podlega pole **From** w wiadomości **INVITE**.
- **Atak Man in the Middle** – atakujący jest w stanie 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, a intruz podszywa się pod serwer.
- **Celowe zakańczanie** trwających połączeń poprzez wstawienie przez atakującego wiadomości **BYE** w czasie, gdy zachodzi komunikacja między użytkownikami.

Rzadko jednak wspomina się o ochronie serwerów i wiadomości sygnalizacyjnych przesyłanych między urządzeniami. A to one właśnie mają duży wpływ na zachowanie poufności konwersacji. Gdyby przesyłany w sieci IP głos porównać do jadącego pociągu, a semafory i zwrotnice do wiadomości sygnalizacyjnych, to brak ochrony tych ostatnich potencjalnie prowadziłby do utraty kontroli ruchu. Intruz mógłby dowolnie zmienić bieg pociągu i skierować go w innym, wyznaczonym przez siebie kierunku (przechwycenie, podsłuch) bądź spowodować katastrofę komunikacyjną (przerwanie połączenia).

Sposoby na bezpieczny VoIP

Najpopularniejsze obecnie sieci Voice over IP są oparte na protokole SIP. Dostępne dla niego zabezpieczenia możemy podzielić na trzy grupy:

- Wyspecjalizowane technologie informatyczne. Przykładowo: wirtualne sieci lokalne (VLAN) lub wirtualne sieci prywatne (VPN). Za pomocą pierwszej technologii możemy odseparować ruch telefonii IP od pozostałych danych. Jeśli natomiast w sieci nie da się uniknąć „wymieszania" obu rodzajów ruchu, to możemy wykorzystać VPN, czyli przesyłać ruch głosowy poprzez specjalne szyfrowane tunele.
- Algorytmy zabezpieczające transmisję głosu. Obecnie w sieciach IP mowa jest najczęściej przesyłana z wykorzystaniem protokołu RTP (Real-time Transport Protocol). Do zapewnienia jego ochrony został stworzony algorytm SRTP (Secure RTP). Dzięki niemu niemożliwe jest podsłuchanie przechwyconej rozmowy.
- Mechanizmy zabezpieczeń dla sygnalizacji: SIP Digest (zapożyczony z protokołu HTTP), S/MIME (stosowany do zabezpieczana poczty elektronicznej), TLS, IPSec.

W firmie bezpieczniej

W domowej telefonii IP mamy stosunkowo niewiele możliwości zabezpieczenia się przed atakami. Nasze działania ograniczają się raczej do

Bezpieczeństwo Skype'a

Darmowy komunikator Skype odniósł w minionym roku oszałamiający sukces. Oferuje bardzo dobrą jakość rozmowy, charakteryzuje się dużą prostotą interfejsu użytkownika i szczyci się tym, że przesyłany głos jest szyfrowany za pomocą mocnego algorytmu AES (Advanced Encryption Standard). W Skype'ie wykorzystano technologię P2P (twórcy komunikatora są też autorami programu Kazaa) oraz własne protokoły i mechanizmy. Wszystko wskazywałoby więc na to, że oto powstała usługa, która jest w stanie zagrozić dotychczasowym systemom VoIP.

Skazą na idealnym marketingowo wizerunku Skype'a jest ciągła odmowa udostępnienia środowisku teleinformatycznemu jakichkolwiek informacji dotyczących bezpieczeństwa transmisji i protokołu sygnalizacyjnego. Jest to nieco dziwne, szczególnie że najpowszechniejsze sieci VoIP bazują na ogólnie dostępnych standardach (np. opublikowanych w Internecie) po to, by użytkownicy mogli sami ocenić jakość protokołu i zastosowanych mechanizmów ochrony.

Historia teleinformatyki pokazuje, że czasami całe bezpieczeństwo systemu tkwi jedynie w jego tajności. Jako przykład może posłużyć sprawa szyfrów A5/1 i A5/2, używanych do kodowania transmisji głosu pomiędzy telefonem GSM a stacją bazową. Operatorzy GSM trzymali te algorytmy w sekrecie, ale w 1998 roku grupa Smartcard Developer Association zastosowała inżynierię wsteczną (ang. reverse engineering) i opublikowała ich kody źródłowe. W wyniku przeprowadzonej analizy tych algorytmów okazało się, że mają one wiele słabych punktów, pozwalających m.in. na klonowanie kart SIM. W tym czasie z telefonii GSM w Europie korzystało ponad 100 milionów osób!

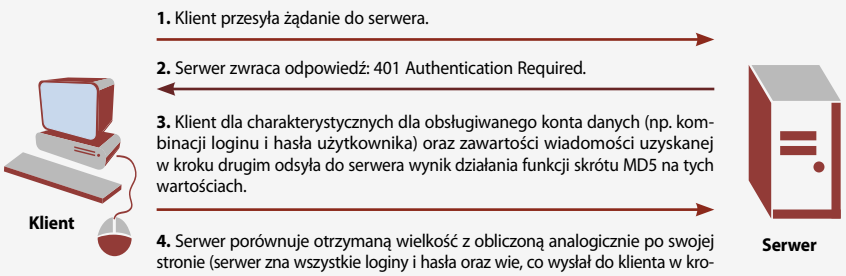
Właśnie z powodów niejasności dotyczących bezpieczeństwa niektóre firmy (np. CERN) czy instytucje (University of Cambridge) już wprowadziły zakaz korzystania ze Skype'a w swoich sieciach. Nie wiadomo też do końca, czy komunikator nie podzielił losu Kazy i nie zawiera spyware'u. Pojawia się także obawa, że każdy komputer z zainstalowanym Skype'em, który spełnia pewne warunki (szerokie łącze, publiczny adres IP, duża moc obliczeniowa), może stać się tzw. SuperNodem i w sposób anonimowy pośredniczyć w połączeniach. W takim wypadku trudno kontrolować ruch przepływający przez nasze urządzenia sieciowe.

Jak zapobiegać atakom

Rodzaj zagrożenia	Możliwe zabezpieczenia
Podsłuch	– szyfrowanie pakietów IP zawierających głos za pomocą sprawdzonych algorytmów – odseparowanie ruchu VoIP od reszty połączeń w celu uniemożliwienia podsłuchu (VLAN) – budowa szyfrowanych tuneli (VPN) pomiędzy segmentami sieci przeznaczonymi dla VoIP, jeśli ruch VoIP przechodzi przez segmenty danych
Atak odmowy usługi	– instalowanie systemów zabezpieczających przed atakami DoS (syn-flood, smurf itp.) – pozwolenie na dostęp do sieci VoIP jedynie dla autoryzowanych użytkowników (filtrowanie ruchu, uwierzytelnienie ruchu)
Kradzież usługi	– odseparowanie ruchu VoIP i danych (VLAN) – wyłączenie możliwości automatycznego rejestrowania się klientów VoIP na serwerach sygnalizacyjnych (dostęp do usługi tylko dla uwierzytelnionego sprzętu) – uniemożliwienie podpięcia się nieautoryzowanych urządzeń do sprzętu dostępowego (np. do przełączników)

Zabezpieczanie sygnalizacji za pomocą SIP Digest

SIP Digest jest popularnym mechanizmem służącym do zabezpieczania sygnalizacji dla systemów VoIP opartych na protokole SIP. Wykorzystuje współdzielone przez obie strony komunikacji tajne hasło oraz uwierzytelnienie metodą wyzwanie-odpowiedź (challenge-response). Dodatkowo korzysta się tutaj również z funkcji skrótu MD5.



kontroli zabezpieczeń stosowanych przez dostawcę usługi oraz wykorzystywanych przez niego urządzeń lub oprogramowania. Należy zatem upewnić się, czy i jak jest szyfrowany ruch oraz w jaki sposób chronione są wiadomości i serwery sygnalizacyjne. Dodatkowo warto zastosować osobistą zaporą ogniową.

Sytuacja administratorów sieci korporacyjnych jest inna. Infrastruktura sieciowa pozwala im bowiem na bardziej zaawansowane działania, zapewniające większe pole manewru. Ogólne zasady ochrony VoIP można zebrać w poniższych punktach:

- Należy zapewnić możliwie najpełniejsze odseparowanie ruchu sieci VoIP (sieci głosowej) od sieci, w której przesyłane są dane. Chodzi o izolację ruchu z wykorzystaniem odpowiednich technologii teleinformatycznych (np. VLAN, VPN), a nie rozdzielenie fizyczne obu infrastruktur.
- Jeśli możemy wyróżnić w sieci dwa logicznie odseparowane segmenty: głosowy i danych, to niezbędne jest monitorowanie tego pierwszego w celu wykrywania wszelkich anomalii. W tym celu możemy wykorzystać specjalnie opracowane dla systemów VoIP mechanizmy IDS i IPS (Intrusion Detection/Prevention System).
- Należy zadbać o bezpieczeństwo zarówno serwerów sygnalizacyjnych (samego urządzenia), jak i wymienianych wiadomości sygnalizacyjnych.
- Dobrze jest szyfrować przesyłane rozmowy, co uniemożliwi potencjalnemu atakującemu ich podsłuchiwanie. Warto jednak pamiętać o konieczność kompromisu pomiędzy stosowanym algorytmem szyfrowania a opóźnieniem przez nie wprowadzanym.
- Należy zadbać o wyłączenie wszelkich automatycznych procedur rejestracji sprzętu oraz niepotrzebnych usług, po to żeby nawet po wpięciu do segmentu głosowego sieci atakujący nie mógł w prosty sposób i nielegalnie skorzystać z usługi.
- Trzeba wykorzystywać dostępne narzędzia do testowania bezpieczeństwa zarówno oprogramowania, jak i sprzętu (dla testowania bezpieczeństwa produktów opartych na protokole SIP istnieją darmowe narzędzia, np.: Sivus, Protos czy SIP Forum Test Framework, patrz: ramka Więcej informacji).

Bezwzględnie należy korzystać z dostępnych mechanizmów ochrony. Nie powinno się spoczywać na laurach i wierzyć we wszystkie zapewnienia producenta o bezpieczeństwie dostarczonego przez niego sprzętu i oprogramowania. Poufność systemu telefonii IP zależy bowiem w dużej mierze od właściwej konfiguracji sieci IP oraz usług VoIP.

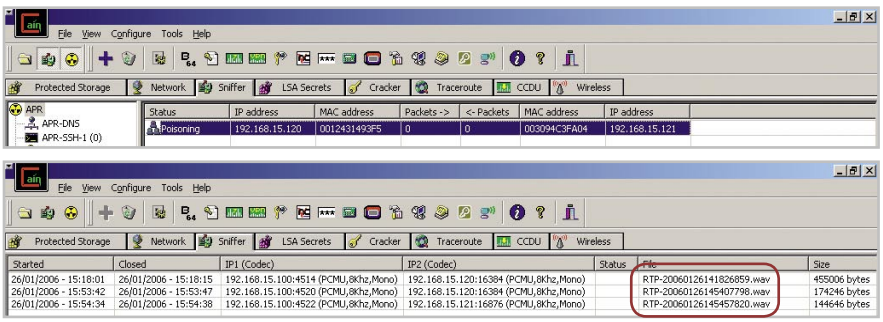
Warto rozmawiać

Problemy omówione w niniejszym artykule wskazują, że bezpieczeństwo telefonii IP nie jest do końca pewne. Jest ona bowiem podatna zarówno na ataki dotyczące transmisji danych (związane z protokołem IP), jak i na dodatkowe zagrożenia wynikające ze specyfiki VoIP. Z drugiej strony, nie można jednoznacznie powiedzieć, że telefonia internetowa zawiera same luki w bezpieczeństwie i nie nadaje się do wykorzystania.

Odpowiednio zaprojektowana i skonfigurowana sieć VoIP będzie bezpieczna, ale zastosowane w niej mechanizmy ochronne muszą bezwzględnie odpowiadać i być dostosowane do charakterystyki systemu. Dodatkowo trzeba mieć świadomość istnienia dwóch odrębnych rodzajów ruchu dla VoIP i zapewnić poufność transmisji zarówno dla wiadomości sygnalizacyjnych, jak i pakietów zawierających głos.

W sieciach korporacyjnych ze względów bezpieczeństwa nie powinno zezwalać się użytkownikom na instalowanie softphonów (komunikatorów telefonii IP) na stacjach roboczych, gdyż wtedy mamy do czynienia z „mieszaniem się" ruchu z obu segmentów sieci. W warunkach domowych kwestie ochrony możemy regulować poprzez wybór odpowiedniego dostawcy usługi.

Przyszłość usług Voice over IP wydaje się świetlana, ale warunkiem jej masowej akceptacji jest m.in. wypracowanie jednoznacznych i uniwersalnych metod ochrony dla każdego rodzaju i architektury sieci. ■



Hackowanie VoIP nie wymaga wiedzy tajemnej, wystarczy skorzystać z gotowej aplikacji, jak ta widoczna powyżej. Program Cain&Abel pozwala na wykonanie ataku MITM z wykorzystaniem techniki arp poisoning i zapisanie przeprowadzane w sieci LAN rozmów w postaci plików WAV.

Więcej informacji

Organizacje tworzące standardy VoIP
http://www.ietf.org/
http://www.itu.int/

Programy do testowania bezpieczeństwa SIP:
http://vopsecurity.org/html/tools.html
http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/
http://www.sipfoundry.org/sftf/index.html
http://www.codenomicon.com/products/telecommunications/sip/

Dodatkowe informacje o bezpieczeństwie VoIP:
http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf
http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf