WOJCIECH MAZURCZYK
Instytut Telekomunikacji
Politechnika Warszawska, Warszawa
E-mail: W.Mazurczyk@elka.pw.edu.pl
http://security.tele.pw.edu.pl

Bezpieczeństwo SIP jako protokołu sygnalizacyjnego VoIP

STRESZCZENIE

W referacie przedstawiono zagadnienia związane z bezpieczeństwem protokołu SIP (Session Initiation Protocol) jako najbardziej obiecującego protokołu sygnalizacyjnego dla realizacji usługi VoIP (Voice over IP). Skupiono się przede wszystkim na zagadnieniach związanych z bezpieczeństwem wiadomości sygnalizacyjnych wymienianych pomiędzy stronami komunikującymi się. Szczególny nacisk położono na analizę mechanizmów bezpieczeństwa zastosowanych w dwóch zaleceniach organizacji IETF dla SIP: RFC 2543 (dot. pierwszej wersji SIP z 1999 r.) oraz RFC 3261 (dot. drugiej wersji SIP z 2002 r.).

Dodatkowo przedstawiono również wyniki przeprowadzonych badań praktycznych wybranych aplikacji, będących implementacjami Agenta Użytkownika SIP (będących interfejsem pomiędzy użytkownikiem a telefonią internetową).

1. Wstęp

Niniejszy artykuł poświęcony jest bezpieczeństwu usługi Voice over IP (VoIP) bazującej na protokole SIP (Session Initiation Protocol). Protokół SIP jest najbardziej obiecującym protokołem sygnalizacyjnym dla realizacji usługi VoIP w sieciach TCP/IP. W artykule przedstawiono zagadnienia związane z bezpieczeństwem wiadomości sygnalizacyjnych wymienianych pomiędzy komunikującymi się stronami, w szczególności przeanalizowane zostaną mechanizmy bezpieczeństwa zastosowane w dwóch zaleceniach organizacji IETF (The Internet Engineering Task Force) dla SIP: RFC 2543 (dot. pierwszej wersji SIP z 1999 r.) oraz RFC 3261 (dot. drugiej wersji SIP z 2002 r.).

2. Bezpieczeństwo połączeń VoIP

Usługa VoIP nazywana również „telefonią internetową" lub „telefonią IP" oznacza przesyłanie głosu w czasie rzeczywistym wykorzystując do tego celu pakietową sieć transmisji danych z protokołem IP.

Zagwarantowanie bezpiecznych połączeń dla tej usługi jest sprawą złożoną. Nie ogranicza się ono jedynie do zapewnienia bezpiecznego transportu strumieni danych zawierających głos, ważniejszą sprawą są warunki, w których następuje przesyłanie wiadomości protokołu sygnalizacyjnego, na którym bazuje VoIP.

Problemy bezpieczeństwa dla usługi telefonii IP w świetle powyższych stwierdzeń można podzielić na:

a. Bezpieczeństwo wiadomości sygnalizacyjnych wymienianych pomiędzy stronami komunikującymi się,
b. Bezpieczeństwo pakietów przenoszących głos (pakiety RTP),
c. Problemy związane z przesyłaniem pakietów przez ściany przeciwogniowe (Firewalls) oraz urządzenia NAT (Network Address Translators).

Niniejszy artykuł skupia się wyłącznie na tematyce zawartej w punkcie a.

3. Protokoły sygnalizacyjne dla usługi VoIP

Protokoły tej grupy nazywane są „sercem" telefonii internetowej, ponieważ od niej zależy zarówno architektura sieci, realizacja zaawansowanych usług jak i współdziałanie z tradycyjnymi sieciami telefonicznymi. Obecnie nie ma jednego standardu protokołu sygnalizacyjnego dla realizacji usługi VoIP obserwujemy współistnienie czterech protokoły tego rodzaju: SIP (Session Initiation Protocol), H.323, MGCP (Media Gateway Control Protocol) oraz H.248/Megaco.

Z wszystkich wymienionych powyżej protokołów sygnalizacyjnych dla telefonii IP to właśnie SIP jest najbardziej perspektywiczny i z nim wiąże się największe nadzieje.

4. Bezpieczeństwo SIP - techniki ataków

Dla usługi VoIP całość połączenia można podzielić na dwie podstawowe fazy: sygnalizacyjną (kontrolującą sesję) oraz transportującą strumień danych. W czasie fazy sygnalizacyjnej określone parametry sesji są wymieniane pomiędzy użytkownikami końcowymi w celu poprawnej realizacji żądanego połączenia. Mogą one zawierać informacje, które użytkownik wolałby pozostawić niedostępne dla osób trzecich (np. jego lokalizację, czy nazwisko). Ważne jest również, aby użytkownicy, którzy nie zostali uwierzytelnieni nie mieli możliwości zmiany, wstawiania oraz usuwania wiadomości wysyłanych w czasie fazy sygnalizacyjnej. Dlatego też najważniejszym celem przy zapewnianiu bezpieczeństwa usługi VoIP jest odpowiednie zabezpieczenie sygnalizacji protokołu SIP. Natomiast głównymi technikami ataków na wymianę wiadomości sygnalizacyjnych dla Session Initiation Protocol są:

- Podszycie się (Spoofing)
- Podsłuchiwanie (Sniffing)
- Blokowanie działania (Denial of Service)

Podane powyżej techniki mogą zostać wykorzystane do różnego rodzaju ataków. Dla przykładu technika podszycia może służyć do podszycia się pod czyjąś tożsamość lub do przekierowania połączenia; technika podsłuchiwania może zaowocować zarówno podsłuchiwaniem wiadomości sygnalizacyjnych jak również penetracją ciała wiadomości natomiast blokowanie działania opiera się głównie na wyłączeniu funkcjonalności serwerów sieciowych.

Istnienie wymienionych powyżej rodzajów technik i ataków powoduje konieczność istnienia określonych rodzajów mechanizmów bezpieczeństwa koniecznych, aby im przeciwdziałać.

5. Problem doboru kryterium oceny bezpieczeństwa dla SIP

Aby usystematyzować przegląd mechanizmów bezpieczeństwa protokołu SIP, jak i następnie być w stanie umiejętnie je oceniać należy ustalić kryterium, według którego nastąpi ich analiza. Przy jego wyborze należy kierować się zarówno specyfiką samego protokołu sygnalizacyjnego i opisywanej usługi jak i charakterem potencjalnych zagrożeń, technik oraz ataków.

W artykule zdecydowano się na wybór rozwiązania będącego modyfikacją podziału zawartego w normie ISO 7498-2, według którego bezpieczeństwo w systemach otwartych należy rozpatrywać w kontekście możliwości zapewnienia pięciu podstawowych **usług ochrony informacji**: (kontroli dostępu (access control), uwierzytelnienia (authentication), integralności danych (data integrity), poufności danych (confidentiality) oraz niezaprzeczalności (non-repudation).

Po uwzględnieniu zarówno specyfiki protokołu SIP jak i charakteru potencjalnych ataków przyjęte zostało kryterium oceny mechanizmów bezpieczeństwa zdefiniowane jako umiejętność zapewnienia dwóch głównych usług ochrony informacji oraz komunikacji w sieci tzn.:

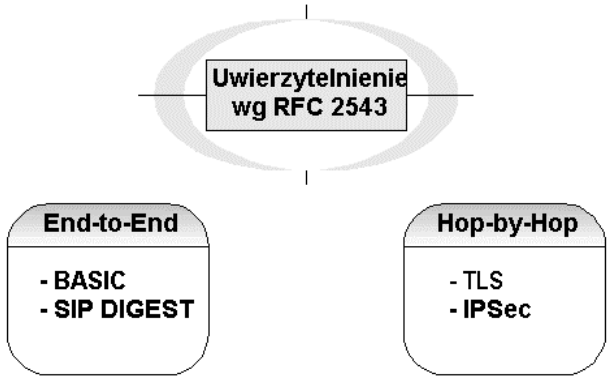
- **Poufności** – dającej ochronę przed atakami pasywnymi oraz zabezpieczającej wiadomości sygnalizacyjne, wymieniane pomiędzy komunikującymi się jednostkami, przed ich nieuprawnionym uzyskaniem przez strony do tego nieupoważnione;
- **Uwierzytelnienia (zawierającego integralność)** – gwarantującego ochronę przed atakami aktywnymi oraz kontrolę tożsamości stron i wiadomości sygnalizacyjnych wymienianych pomiędzy nimi.

Dlatego też przy omawianiu mechanizmów bezpieczeństwa protokołu SIP główny nacisk położono na sposób zapewnienia właśnie tych dwóch usług.

Mechanizmy bezpieczeństwa opisane w zaleceniach: RFC 2543 oraz RFC 3261 podzielono również w ramach każdej z usług ze względu na obszar realizacji omawianej usługi w odniesieniu do drogi komunikacyjnej na mechanizmy typu **End-to-End** (obsługa bezpośrednia źródło->cel) oraz **Hop-by-Hop** (obsługa tranzytowa – tylko pojedyncze połączenie, której z warstw niższych niż w. aplikacji). Z oboma rodzajami typów mechanizmów wiążą się pewne wątpliwości natury bezpieczeństwa. Hop-by-Hop wymaga zaufania użytkownika dla wszystkich elementów funkcjonalnych znajdujących się na drodze przesyłanej wiadomości. Natomiast End-to-End uniemożliwia zabezpieczenie całej wiadomości, gdyż część jej nagłówków jest niezbędna do poprawnego przesłania.

6. Realizacja usługi uwierzytelnienia wg RFC 2543

Wyszczególnienie konkretnych mechanizmów dla realizacji omawianej usługi dla SIP opisanego w zaleceniu RFC 2543 zostało umieszczone na rysunku numer 1:



Rys. 1. Realizacja usługi uwierzytelnienia w SIP wg RFC 2543

6.1. Uwierzytelnienie typu Hop-by-Hop

Mechanizmy tej grupy bazują na protokołach: TLS (Transport Layer Security) - operującym pomiędzy warstwą aplikacji i transportową oraz IPSec (Internet Protocol Security) działającym w warstwie sieciowej modelu odniesienia TCP/IP.

Mechanizmy te nie zostały obowiązkowo narzucone w RFC 2543 – zakłada się tam tylko, że jeśli trzeba będzie zapewniać uwierzytelnienie Hop-by-Hop to można użyć jednego z tych dwóch protokołów. Należy również wspomnieć, iż oba te mechanizmy realizują pełną usługę integralności wiadomości.

6.2. Uwierzytelnienie typu End-to-End

W protokole SIP realizacja usługi uwierzytelnienia typu End-to-End jest realizowana poprzez implementację dwóch mechanizmów: Basic i Digest. Oba zostały zaczerpnięte w prawie niezmienionej formie z protokołu HTTP i oba bazują na schemacie współdzielonego sekretu (shared secret) - użyty klucz w czasie procedury uwierzytelniającej jest znany przez obie strony, pomiędzy którymi zachodzi wymiana uwierzytelniająca (serwer i klient).

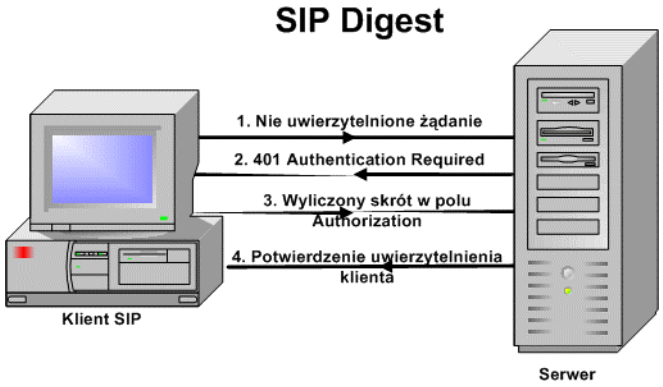
Mechanizm Basic

Jest to bardzo prymitywny mechanizm nie gwarantujący wystarczającego poziomu bezpieczeństwa, gdyż dane uwierzytelniające użytkownika są przesyłane jako tekst jawny, co czyni ten mechanizm całkowicie nieodpornym na atak typu powtórka.

Mechanizm SIP Digest

Jest on lepiej zabezpieczony od poprzednika (zapewnia ochronę przed defektami mechanizmu Basic), lecz nadal w konfrontacji z nowoczesnymi standardami kryptograficznymi jest stosunkowo słaby. Oprócz schematu współdzielonego sekretu wykorzystuje on dodatkowo metodę wyzwanie/odpowiedź (challenge / response) oraz funkcję skrótu (hash function) - MD5 (Message Digest 5).

Przebieg realizacji omawianej usługi dla mechanizmu SIP Digest został przedstawiony na rysunku numer 2:



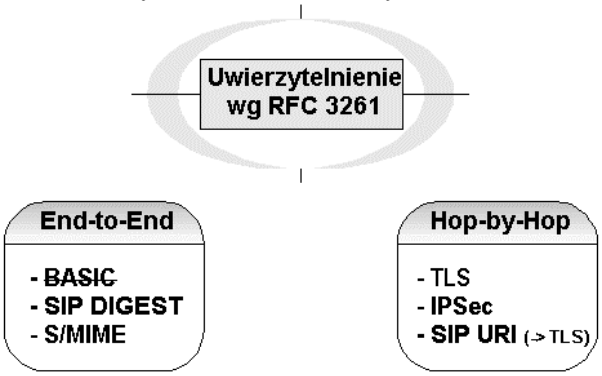
Rys. 2. Przebieg uwierzytelnienia mechanizmu SIP Digest

Gdy serwer, który wymaga uwierzytelnienia otrzyma od jednostki inicjującej żądanie (1), które nie jest uwierzytelnione, to zwracana jest odpowiedź *401 Authentication Required* (2), która zawiera w nagłówku wiadomości pole *WWW-Authenticate* parametry charakterystyczne zarówno dla samego serwera, ale i trwającej procedury uwierzytelnienia. Klient uzyskane w ten sposób parametry łączy ze swoimi danymi uwierzytelniającymi i wylicza skrót, który jest następnie umieszczany w nagłówku pola *Authorization* w ponownie wysyłanym do serwera żądaniu (3). Po swojej stronie serwer dokonuje wyliczenia skrótu na tej samej zasadzie. Uwierzytelnienie następuje po uzyskaniu zgodności obu skrótów (4).

SIP Digest oferuje również prymitywną formę wsparcia usługi integralności danych poprzez możliwość dodania do informacji poddanych obliczaniu skrótu, ciała wiadomości lub jej określonych nagłówków. Zapewniana jednak w ten sposób integralność wiadomości jest szczątkowa, ponieważ skrótowi nie mogą podlegać nagłówki, do których wymagany jest dostęp w czasie transportu wiadomości przez sieć.

7. Realizacja usługi uwierzytelnienia wg RFC 3261

Mechanizmy, które definiuje zalecenie RFC 3261 dla protokołu SIP w wersji drugiej przy realizacji usługi uwierzytelnienia, zostały zamieszczone na rysunku numer 3:



Rys. 3. Realizacja usługi uwierzytelnienia wg RFC 3261

7.1. Uwierzytelnienie typu Hop-by-Hop

W przypadku tego rodzaju mechanizmów pozostawiono sprawdzone z pierwszej wersji SIP rozwiązania wykorzystujące protokoły warstw niższych modelu TCP/IP: TLS oraz IPsec. Jedyną nowością dodaną w RFC 3261 jest mechanizm o nazwie SIPS URI.

Mechanizm SIPS URI

Jeśli zwykły adres URI (Uniform Resource Identifier) postaci np. **sip://JKowalski@pw.edu.pl** zamienimy na **sips://JKowalski@pw.edu.pl** będzie to oznaczać fakt, iż cel wyszczególniony w adresie ma zostać osiągnięty w sposób bezpieczny, co oznacza, każdy odcinek drogi komunikacyjnej powinien być zabezpieczony z wykorzystaniem mechanizmu TLS. Jeśli taki warunek nie może zostać spełniony - nie dochodzi do nawiązania połączenia. Innymi słowy, jeśli jako mechanizm gwarantujący uwierzytelnienie został wybrany SIPS URI oznacza to, że musi zostać zaimplementowany w całej sieci protokół TLS, gdyż jest on niezbędny do prawidłowego jego funkcjonowania.

7.2. Uwierzytelnienie typu End-to-End

W stosunku do poprzedniej wersji protokołu SIP w drugiej wersji całkowicie zrezygnowano ze stosowania mechanizmu Basic, natomiast obligatoryjne staje się implementowanie mechanizmu SIP Digest. Dodatkowo rozszerzono możliwość realizacji tej usługi z wykorzystaniem nowego rozwiązania nazwanego S/MIME (Secure / Multipurpose Internet Mail Extension).

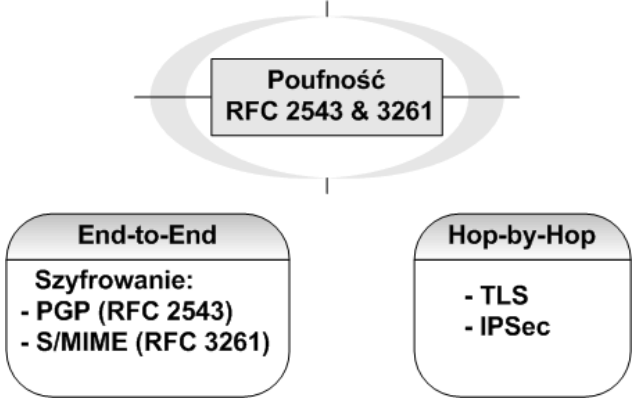
Mechanizm S/MIME

Usługa uwierzytelnienia realizowana za pomocą S/MIME wykorzystuje do tego celu tunelowanie oraz podpis cyfrowy. Mechanizm ten działa następująco: wykonywana jest pełna lub częściowa kopia nagłówków wiadomości SIP i umieszcza wraz z oryginalnym ciałem w jednostce MIME, która reprezentuje ciało nowej wiadomości. Następnie jest ona podpisywana cyfrowo z wykorzystaniem funkcji skrótu SHA-1. Dodatkowo wykorzystuje się algorytm klucza publicznego RSA do wymiany kluczy, a w konsekwencji do bezpiecznego przesłania obliczonego skrótu do właściwego odbiorcy.

Po osiągnięciu celu adresat wiadomości weryfikuje dostarczony podpis cyfrowy. Jeśli jest on prawidłowy to dodatkowo dokonuje się porównania tych nagłówków, które nie były wykorzystywane przez urządzenia znajdujące się na drodze komunikacyjnej w celu zapewnienia podstawowej integralności wiadomości.

8. Realizacja usługi poufności wg RFC 2543 oraz RFC 3261

Jeśli chodzi o realizację drugiej usługi zdefiniowanej w wybranym przez nas kryterium to osiąga się ją w SIP poprzez zastosowanie mechanizmu szyfrowania. Dla obu wersji protokołu SIP mechanizmy Hop-by-Hop oraz End-to-End są następujące:



Rys. 4. Realizacja usługi poufności wg RFC 2543 oraz RFC 3261

8.1. Poufność typu Hop-by-Hop

W tej grupie mechanizmów, zarówno dla protokołu SIP w wersji pierwszej jak i drugiej, szyfrowanie zapewniane jest z wykorzystaniem wspomnianych już mechanizmów realizacji usługi uwierzytelnienia tzn. IPSec lub TLS.

8.2. Poufność typu End-to-End

Szyfrowaniu w przypadku tego typu mechanizmów podlega całe ciało wiadomości oraz istotne z punktu widzenia bezpieczeństwa pola nagłówka. Żądania i odpowiedzi nie mogą być w ten sposób szyfrowane w całości, ponieważ wymagana jest dostępność niektórych pól po to, by zapewnić poprawne jej przesłanie.

RFC 2543 wyznacza dla realizacji mechanizmu szyfrowania wykorzystanie kryptosystemu PGP (Pretty Good Privacy), który jako szyfr symetryczny stosuje szyfr IDEA, natomiast jako algorytm klucza publicznego – RSA.

W przypadku drugiej wersji protokołu SIP nastąpiła całkowita rezygnacja z szyfrowania za pomocą PGP. Została ona zastąpiona opcjonalnym wykorzystaniem do tego celu mechnizmu S/MIME.

Mechanizm S/MIME

Realizacja usługi poufności przebiega podobnie jak w przypadku realizacji usługi uwierzytelnienia (również wykorzystywana jest enkapsulacja części wiadomości w jednostce MIME) z tą różnicą, że zamiast funkcji skrótu stosuje się szyfrowanie 3DES. Również algorytm klucza publicznego pozostał ten sam – RSA.

9. Słabe punkty w architekturze bezpieczeństwa SIP w zaleceniu RFC 2543

Jasną sprawą jest fakt, że skoro powstała druga wersja protokołu SIP to pierwsza nie spełniała oczekiwań twórców oraz użytkowników. Głównie chodziło tu właśnie o aspekty bezpieczeństwa (wykazano wiele słabych punktów i niedociągnięć SIP wg zalecenia RFC 2543).

Zastosowane tu mechanizmy wywodzące się z samego protokołu SIP (czyli bez grupy mechanizmów Hop-by-Hop) są niewystarczające, a zastosowane systemy kryptograficzne w dużej mierze przestarzałe w porównaniu z tymi uważanymi za należące do nowoczesnej kryptografii. Głównymi mankamentami architektury bezpieczeństwa zdefiniowanej w zaleceniu RFC 2543 jest:

- Zbyt duża opcjonalność w wyborze mechanizmów gwarantujących wymagane usługi oraz brak jasnego narzucenia i przypisania konkretnych mechanizmów bezpieczeństwa poszczególnym częściom drogi komunikacyjnej zawartej pomiędzy elementami funkcjonalnymi,
- Brak gwarancji całkowitej integralności wiadomości przy uwierzytelnieniu typu End-to-End (mechanizmy Basic oraz SIP Digest) oraz wykorzystywanie schematu współdzielonego sekretu,
- Zastosowanie do realizacji uwierzytelnienia mechanizmu Basic (całkowita nie odporność na atak typu powtórka),
- Dla realizacji usługi poufności wykorzystanie szyfrowania PGP. Obecnie nie zaleca się używania szyfrowania tym systemem kryptograficznym szczególnie w starszych wersjach głównie, dlatego iż brak mu dobrego systemu certyfikacji oraz gdyż używane długości kluczy kryptograficznych są zbyt krótkie.

10. Słabe punkty w architekturze bezpieczeństwa SIP w zaleceniu RFC 3261

Zalecenie RFC 3261 definiuje architekturę bezpieczeństwa, która jest poprawna i minimalizuje prawdopodobieństwo przeprowadzenia udanego ataku.

Przypomnijmy: w RFC 3261 nie ma uwierzytelnienia typu Basic, ale za to SIP Digest jest obowiązkowe. Dodatkowo opcjonalne jest wykorzystanie S/MIME do realizacji uwierzytelnienia wzajemnego.

W przypadku mechanizmów typu Hop-by-Hop protokół TLS musi być obowiązkowo implementowany (ale działa on niestety jedynie na TCP) lub IP Sec (wybór opcjonalny).

Pomimo, że architektura bezpieczeństwa zapewniana w SIP w omawianym zaleceniu redukuje ryzyko ataku posiada ona klika słabości. Są one następujące:

- **SIP Digest** – te same mankamenty jak w przypadku protokołu SIP w wersji pierwszej,
- **S/MIME** – główna słabość: brak infrastruktury wymiany kluczy publicznych - zdefiniowany w wersji drugiej SIP system wymiany kluczy jest nieodporny na atak typu *man-in-the-middle* (podobnie jak w innych systemach np. w SSH). W sytuacji, gdy atakujący przechwyci pierwszą wymianę kluczy pomiędzy komunikującymi się i będzie miał szansę przechwytywania całego dialogu między stronami komunikującymi się przeprowadzony atak można będzie uznać za udany. Druga sprawa – wykorzystanie S/MIME może owocować dużymi (w sensie objętości) wiadomościami.
  Ostatnim problemem jest fakt, iż jeśli na drodze wiadomości znajdzie się jakiś rzadki typ serwera sieciowego, którego prawidłowe działanie zależy od możliwości dostępu i modyfikowaniu ciała wiadomości SIP, to wtedy protokół S/MIME uniemożliwi prawidłowe funkcjonowanie takiego elementu sieciowego.

Dla obu wersji SIP typem ataku, przed którym nie ma całkowitej ochrony jest atak typu blokowanie działania (Denial of Service). Bez względu na rodzaj zaimplementowanych mechanizmów bezpieczeństwa zawsze możliwe jest „zalanie" serwera (głównie chodzi tu o serwery proxy) poprzez wysyłanie nadmiernej ilości zwykle niepoprawnych wiadomości, w ten sposób powodując odmowę świadczenia usług, dla których dana jednostka została stworzona.

Niestety tego typu ataku nie da się wyeliminować całkowicie, ponieważ wiązałoby się to z ograniczeniem podstawowych funkcji serwerów sieciowych. Jedynym rozwiązaniem, które może w sposób satysfakcjonujący ograniczyć prawdopodobieństwo wystąpienia takiego ataku jest przeprowadzanie wzajemnego uwierzytelnienie serwerów proxy z wykorzystaniem protokołu TLS.

11. Doświadczenia praktyczne

W ramach potwierdzenia wyników przeprowadzonej analizy mechanizmów bezpieczeństwa, dla protokołu SIP w obu wersjach, przeprowadzono badania praktyczne. Ich przebieg, wykorzystane aplikacje oraz testy zostaną zaprezentowane poniżej.

11.1. Przebieg badań

Całość przeprowadzonych działań praktycznych polegała na wykonaniu szeregu testów na aplikacjach będących implementacjami Agenta Użytkownika SIP. Pierwotnym celem takiego postępowania była próba zbadania praktycznej przydatności mechanizmów bezpieczeństwa zdefiniowanych w dwóch wersjach SIP. W zamierzeniu miała być to po prostu symulacja potencjalnych, celowych prób działań atakującego i na tej podstawie ocena umiejętności radzenia sobie w przypadku ich wystąpienia.

Ilość i różnorodność ataków na protokół SIP jest znaczna i testując samą aplikację Agenta Użytkownika SIP nie odda się całego spektrum potencjalnych zagrożeń dla systemu VIP bazującego na tym protokole. Jednakże uznając, że w praktyce użytkownik nie ma zbyt wielkiego wpływu na bezpieczeństwo innych komponentów architektury funkcjonalnej SIP innych niż SIP UA, właśnie na testowanie tego elementu funkcjonalnego położono nacisk.

11.2. Testowane aplikacje SIP UA

W Internecie dostępnych było około dziesięciu darmowych aplikacji będących implementacjami Agenta Użytkownika SIP. Przy doborze programów do testowania kierowano się głównie ich dostępnością oraz tym, by każdy z nich był firmowany przez innych twórców. Do celów badawczych wybrano następujące darmowe programy:

- **Helmsman User Agent 3.0.6** firmy Helmsman,
- **eStara SoftPHONE 3.0** – firmy eStara,
- **Siemens Communication System Client v.1.0** firmy Siemens,
- **Magellan 4.0** opracowany w IT PW,
- **Hughes SIP User Agent (E-Z Phone)** firmy Hughes Software Systems,
- **Vovida SIP UA 1.0.2 -** Columbia University.

11.3. Konieczność modyfikacji celu pierwotnego badań

Niestety po zapoznaniu się z aplikacjami będącymi implementacjami Agenta Użytkownika pierwotny cel testowania musiał zostać zmodyfikowany. Stało się tak z dwóch powodów:

- Żadna z testowanych aplikacji (prócz jednej) nie miała zaimplementowanego, choć najprostszego mechanizmu bezpieczeństwa.
- Wszystkie aplikacje bazowały wyłącznie na starym zaleceniu SIP (RFC 2543).

W związku z faktami, które przytoczono powyżej testowanie Agentów Użytkownika ograniczyło się do osiągnięcia dwóch celów:

- Zbadania zgodności implementacji wybranych aplikacji z zaleceniem, na którym bazuje (w przypadku testowanych aplikacji jest to RFC 2543),
- Wykazanie wyższości programu, w którym został zaimplementowany, choć prosty mechanizm bezpieczeństwa opisany w zaleceniu, nad aplikacją nie posiadającą żadnych wspomnianych mechanizmów.

11.4. Opis doświadczeń i wykorzystanych testów

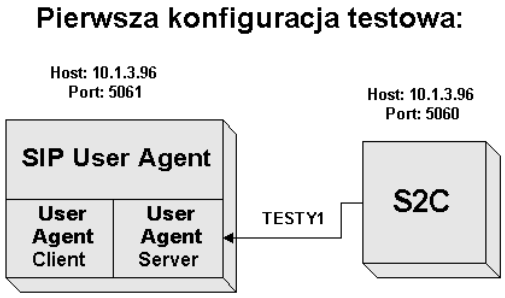
Do przeprowadzenia doświadczeń wykorzystana została autorska, pomocnicza aplikacja S2C (SIP Security Call Checker). Jej głównym zadaniem jest wysłanie określonego testu do wskazanego Agenta Użytkownika SIP, a następnie zbadanie jego reakcji w danym doświadczeniu.

Natomiast, jeśli chodzi o postać treści samych testów to składają się na nie wiadomości sygnalizacyjne protokołu SIP (zarówno żądania jak i odpowiedzi) skonstruowane tak (czasem niepoprawne), aby oddać spektrum możliwych zagrożeń i ataków na wymianę wiadomości sygnalizacyjnych pomiędzy Agentami Użytkownika SIP. Dodatkowo szczególny nacisk kładziono na ataki najłatwiejsze do wykonania, a tym samym najbardziej prawdopodobne.

Przy ich opracowaniu bazowano na testach, stworzonych przez twórców SIP'a: Neila Deasona, Andersa Kristensena, Jonathana Rosenberga oraz Henninga Schulzrinna. Całość testów była przeprowadzana w trzech konfiguracjach testowych, a na każdej z testowanej aplikacji przeprowadzono 25 różnych testów.

Konfiguracja1

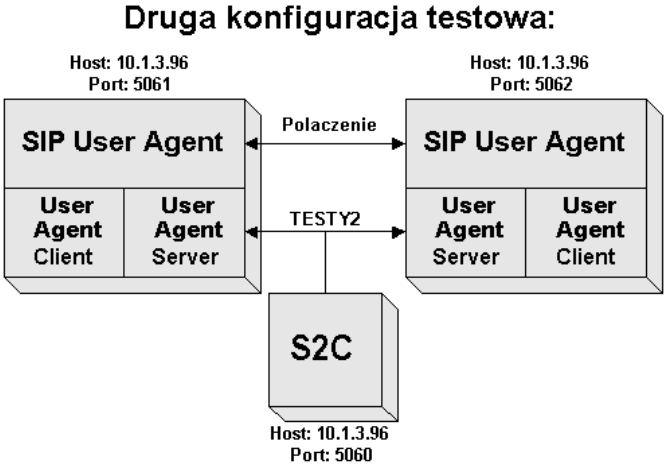
Konfiguracja ta ma na celu zarówno sprawdzenie zgodności zachowań testowanych aplikacji z zaleceniem RFC 2543 na którym bazują oraz symulację ataku, w którym intruz może się podszyć pod czyjąś tożsamość.



Rys. 5. Konfiguracja testowa pierwsza

Konfiguracja2

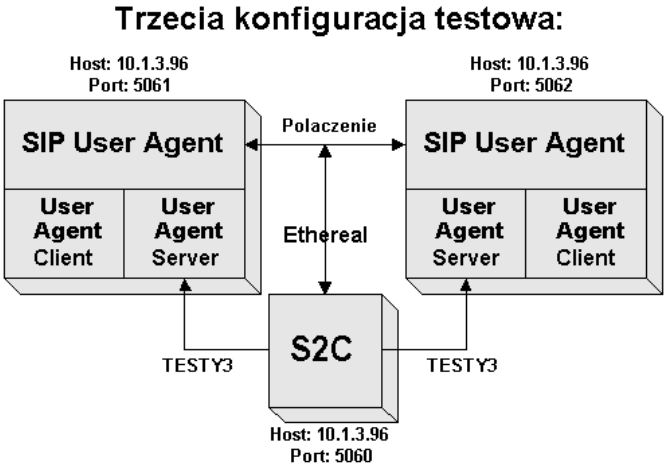
W tym przypadku nawiązywane było połączenie pomiędzy dwoma wybranymi aplikacjami Agenta Użytkownika SIP, a następnie za pomocą aplikacji S2C oraz poprzez określone testy próbowano wpłynąć w negatywny sposób na wymianę wiadomości sygnalizacyjnych/pakietów RTP (wiadomości-testy były raz wysyłane do jednej, raz do drugiej testowanej aplikacji). Była to próba symulacji ataku aktywnego, w którym intruz nie podsłuchuje komunikujących się między sobą agentów, jednak może wysyłać odpowiednio zaadresowane i sporządzone wiadomości w celu uniemożliwienia nawiązania lub przerwania trwającego połączenia.



Rys. 6. Konfiguracja testowa druga

Konfiguracja3

Sytuacja charakteryzowana w tej konfiguracji jest podobna do przypadku opisanego w poprzedniej. Badana była tu również odporność połączenia na przeprowadzane na nim prób ataków. Główną różnicą pomiędzy konfiguracjami drugą i trzecią było założenie, iż atakujący ma możliwość podsłuchiwania wiadomości sygnalizacyjnych (ja do tego celu wykorzystano popularną aplikację *Ethereal*) oraz odpowiednią ich modyfikację.



Rys. 7. Konfiguracja testowa trzecia

Testy mechanizmu SIP Digest

Do przeprowadzenia doświadczeń w tym punkcie wykorzystamy konfigurację trzecią (tam gdzie wykorzystuje się aplikację *Ethereal*) oraz odpowiednio ułożone testy, które będą odpowiadały sytuacji:

a) Podobnej jak w Konfiguracji2, gdy intruz przeprowadza ataki „na ślepo" – znając tylko adres SIP Agenta Użytkownika.

b) Podobnej jak w Konfiguracji3, gdy atakujący za pomocą aplikacji podsłuchującej pakiety jest wstanie odkryć zawartość przesyłanych wiadomości.

12. Analiza wyników przeprowadzonych testów

12.1. Wyniki testów aplikacji bez mechanizmów bezpieczeństwa

Na podstawie przeprowadzonych badań uzyskano następujące wyniki:

- Suma zaliczonych testów dla aplikacji, które wypadły najlepiej kształtuje się na poziomie 16 testów.
- Natomiast liczba testów nie zaliczonych średnio dla wszystkich aplikacji wyniosła ok. 6, czyli 25% prób ataków zakończyło się sukcesem. Jest to dość wysoki wskaźnik, bo oznacza, iż jeden na cztery ataki kończył się powodzeniem.

Żadna z aplikacji nie zaliczyła wszystkich testów, co dowodzi jak łatwo prostymi środkami osiągnąć udany atak na tego rodzaju program. Wielu Agentów Użytkownika w ogóle nie reagowało na wiadomość testującą, mimo tego, że działając zgodnie z zaleceniem, na którym bazują powinny zasygnalizować wystąpienie błędu, bądź zareagować określonym zachowaniem.

12.2. Wyniki i analiza testów mechanizmu SIP Digest

Poprzez analizę wyników doświadczeń przeprowadzonych na mechanizmie SIP Digest wykazano, iż jego zaimplementowanie w testowanej aplikacji w wydatny sposób poprawiło jej bezpieczeństwo. Okazało się, że z wykorzystaniem tych samych środków oraz narzędzi wykorzystanych we wcześniejszych doświadczeniach nie jest możliwe przeprowadzenie udanego ataku na takiego Agenta Użytkownika SIP.

13. Podsumowanie i wnioski

W niniejszym artykule zostały zebrane, przeanalizowane oraz ocenione mechanizmy bezpieczeństwa tworzące architekturę bezpieczeństwa SIP zdefiniowaną w dwóch zaleceniach: RFC 2543 oraz RFC 3261. Wykazano potencjalne zagrożenia, techniki oraz ataki, które mogą wystąpić dla obu tych architektur. Głównym wnioskiem z tej części jest możliwość utworzenia potencjalnie bezpiecznej architektury SIP – nowe zalecenie (RFC 3261) określa mechanizmy, które powinny umożliwić bezpieczną wymianę wiadomości sygnalizacyjnych. Wszystko pozostaje teraz w rękach implementujących, ponieważ nawet najlepsze plany są niczym w przypadku, gdy nie zostaną one poprawnie zrealizowane.

Sprawdzenie za pomocą odpowiednio dobranych testów-wiadomości sześciu dostępnych, darmowych Agentów Użytkownika SIP bazujących na RFC 2543 nie dostarczyło niestety optymistycznych wyników. Na cztery przeprowadzone ataki jeden był udany. Niestety z sześciu testowanych aplikacji tylko jedna miała zaimplementowany jakikolwiek mechanizm bezpieczeństwa (SIP Digest). To jednak wystarczyło, aby odpowiednio utrudnić „domowy" atak na sygnalizację SIP. Reszta aplikacji niestety nie została zabezpieczona w sposób należyty.

Część winy za taki stan rzeczy ponoszą sami twórcy zalecenia RFC 2543, gdyż mechanizmy bezpieczeństwa tam zdefiniowane są opcjonalne. Drugą przyczyną takiego stanu rzeczy jest fakt, iż większą część z tych aplikacji stanowią wersje testowe programów lub takie, które mają zachęcić do kupna jego pełnej wersji. Możliwe, że kupując pełną wersję produktu otrzymuje się program,

razem z zaimplementowanymi mechanizmami bezpieczeństwa należy, więc to bezwzględnie sprawdzić przed zakupem.

Z kolei, aby prawidłowo zabezpieczyć wymianę wiadomości sygnalizacyjnych z wykorzystaniem protokołu SIP należy umiejętnie dobierać dostępne mechanizmy bezpieczeństwa. A uściślając należy zdefiniować jak jednostki funkcjonalne tego protokołu mogą dokonywać wyboru pomiędzy odpowiednimi mechanizmami podczas komunikacji tak, aby być w stanie zagwarantować obie usługi ochrony informacji i komunikacji określone w przyjętym kryterium.

Podsumowując, jeśli usługa VoIP oparta na protokole sygnalizacyjnym SIP ma stać się powszechna i atrakcyjna dla „przeciętnego" użytkownika to musi oferować podobny poziom jakości usług jak w przypadku telefonii klasycznej, a dodatkowo jeszcze zachęcić użytkowników czymś więcej. Biorąc pod uwagę, że informacja, wymieniana w czasie rozmowy, a przede wszystkim podczas inicjacji połączenia w obecnych czasach staje się towarem i ma swoją cenę, więc zapewnienie jej bezpiecznego przesyłania wpływa bezpośrednio na wzrost atrakcyjności tej usługi.

Reasumując zapewnienie bezpieczeństwa wymiany wiadomości sygnalizacyjnych w SIP może być istotnym czynnikiem wpływającym zarówno na jego popularność jako protokołu sygnalizacyjnego dla realizacji VoIP jak i popularności samej usługi.

Literatura

1. M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg – „SIP: Session Initiation Protocol" – Request for Comments nr 3261 lipiec 2002
2. M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg – „SIP: Session Initiation Protocol" – Request for Comments nr 2543 marzec 1999
3. S. Salsano, L. Veltri, D. Papalilo – "SIP Security Issues: The SIP Authentication Procedure and its Processing Load" – IEEE Network, vol. 16, vol. 6, November 2002
4. W. Stallings - "Cryptography and Network Security : Principles and Practice, Second Edition". Prentice-Hall, June 1998.
5. J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart. "HTTP Authentication : Basic and Digest Access Authentication". Request For Comments 2617. Internet Engineering Task Force, June 1999.
6. T. Dierks, C. Allen. "The TLS protocol version 1.0". Request For Comments 2246. Internet Engineering Task Force, January 1999.
7. R. Rivest. "The MD5 Message-Digest Algorithm". Request For Comments 1321. Internet Engineering Task Force, April 1992.
8. T. Berners-Lee, R. Fielding, H. Frystyk. "Hypertext Transfer Protocol -- HTTP/1.0". Request For Comments 1945. Internet Engineering Task Force, May 1996.
9. N. Borenstein, N. Freed. "MIME (Multipurpose Internet Mail Extensions): Mechanisms for Specifying and Describing the Format of Internet Message Bodies ". Request For Comments 1341. Internet Engineering Task Force, June 1992.
10. B. Ramsdell. "S/MIME Version 3 Message Specification". Request For Comments 2633. Internet Engineering Task Force, June 1999.
11. J. Callas, L. Donnerhacke, H. Finney, R. Thayer, "Open PGP Message Format". Request For Comments 2440. Internet Engineering Task Force, November 1998.
12. P. Gajowniczek, M. Średniawa - „Voice over IP – Wykorzystanie techniki IP do przesyłania głosu" - CITCOM-PW październik 1999
13. H. Sinnreich, A. Johnston – „Internet Communications Using SIP" – Wiley Computer Publishing
14. W. Mazurczyk – „Bezpieczeństwo Voice over IP opartego na SIP " – VII Krajowa Konferencja Zastosowań Kryptografii Enigma'2003, Warszawa, maj 2003