Bezpieczeństwo sesji - protokół IPSec

Wojciech Dworakowski
ABA sp.z.o.o.

Abstrakt. Wykład będzie miał na celu przedstawienie technik służących do zabezpieczania transmisji danych w sieciach publicznych. Zostaną omówione najpopularniejsze techniki ataków na sesje sieciową a także metody ochrony przed nimi, ze szczególnym uwzględnieniem protokołu IPSec.
IPSec to bezpieczna odmiana protokołu IP mogąca zapewnić znaczny stopień bezpieczeństwa pracy zarówno sieci rozległych jak i lokalnych. Omówione zostaną zasady pracy IPSec (tryby pracy protokołu, proces uwierzytelniania oraz szyfrowania przesyłanych danych). Zostaną również przedstawione dostępne implementacje IPSec.

Jakie niebezpieczeństwa wiążą się z przesyłaniem danych przez sieci publiczne?

Niestety z reguły nie mamy żadnej kontroli nad naszymi danymi, które przepływają przez sieci publiczne. Nasze wiadomości mogą być narażone na całą gamę ataków. Najpopularniejsze to:

- pasywny podsłuch transmisji (sniffing)
- podszywanie się pod inny host (spoofing)
- przechwytywanie sesji
- powtarzanie fragmentów sesji

Sniffing to po prostu podsłuch przesyłanych danych. Technika ta jest stosunkowo prosta, jednak wymaga dostępu do medium transmisyjnego, po którym płyną dane. Dane powinny płynąć przez ten sam segment sieciowy, w którym działa podsłuchujący. Intruz może to osiągnąć na kilka sposobów. Najłatwiej oczywiście podsłuchać dane na drodze którą one normalnie podróżują, a więc w sieci LAN nadawcy, w sieciach operatorów WAN lub w sieci LAN odbiorcy. Można też sobie wyobrazić takie zmienienie tablic routingu, aby pakiety przechodziły przez miejsce, gdzie intruz może mieć do nich fizyczny dostęp.

Sniffing jest metodą pasywną, czyli nie modyfikującą żadnych danych (można by rzec „read-only"), lecz najczęściej stanowi wstęp do ataków aktywnych, takich jak np. Spoofing.

Spoofing, to szereg technik zmierzających do podszycia się pod kogoś innego w sieci. Komputery w sieciach identyfikują się po adresie IP lub/i po adresie MAC. Zauważmy że adres IP jest jedyną metodą autoryzacji. O uwierzytelnienie dbają z reguły protokoły wyższych warstw. Uwierzytelnienie klienta (np. poprzez podanie hasła) następuje na początku sesji. Później aplikacje ufają, że rozmawiają ciągle z tym samym klientem. Jeżeli potencjalny intruz zdoła wysyłać pakiety w imieniu autoryzowanego wcześniej klienta, to może on np. zerwać połączenie, zmodyfikować sesje (np. zmieniając kwotę 10zł na 10000zł) lub też doprowadzić do przejęcia całości sesji.
Zauważmy że na spoofing nie są również odporne zaawansowane technologie uwierzytelniania takie jak np. S/Key czy SecureID. Dzieje się tak ze względu na to, że atak następuje na już nawiązaną sesję a nie na algorytm uwierzytelniania.
Inne wykorzystanie techniki spoofingu to stworzenie nowej sesji w imieniu zaufanego klienta. Jest to z reguły stosowane przeciwko wszelkim usługom bazującym na autoryzacji poprzez adres IP, np. rlogin, rsh, rcmd ale również do obchodzenia firewalli bazujących na prostym filtrowaniu pakietów.

Generalnie - Jeśli przesyłamy dane przez sieć publiczną to nigdy nie możemy być pewni czy dotrą na miejsce nie zmodyfikowane.

Metody ochrony przed opisanymi technikami

Pierwsza – najprostsza, ale I najmniej skuteczna, to zastosowanie firewalla wykrywającego spoofing. Firewall taki potrafi skojarzyć adresy IP przychodzących pakietów z konkretnym swoim interfejsem fizycznym. Gdy przez interfejs podpięty do sieci WAN przyjdzie pakiet z adresem źródła z sieci wewnętrznej, to firewall powinien taki pakiet odrzucić. Oczywiście zabezpiecza on tyko przed wąską klasą ataków na sesje.

Pełną ochronę daje dopiero szyfrowanie transmisji.

Szyfrowanie transmisji

Dane możemy szyfrować praktycznie na każdej warstwie protokołów sieciowych.

Szyfrowanie na bardzo niskich warstwach (np. na drugiej – szyfrowany Ethernet, ATM, FrameRelay) daje nam dużą niezależność od wykorzystywanych protokółów wyższych warstw, ponieważ szyfrowanie transmisji jest dla nich przeźroczyste. Niestety to rozwiązanie wymaga stosowania specjalizowanego sprzętu (przełączniki, karty sieciowe, FRAD-y). Poza tym nie ma ogólnie przyjętego standardu szyfrowania na warstwie sieci, a więc jest to praktycznie nie do zrealizowania w sieciach publicznych.

Z drugiej strony mamy dostępne rozwiązania szyfrujące na wysokich warstwach. Takim rozwiązaniem jest np. protokół TLS (SSL). Jest to zabezpieczenie transmisji dla protokołów używających mechanizmu „gniazd" TCP. Zapewnia silne uwierzytelnianie i szyfrowanie danych. Nie jest to metoda uniwersalna i „przeźroczysta" – wymaga specjalnie przystosowanego oprogramowania serwerowego i klienckiego (np. serwera www i przeglądarki). Poza tym każda nawiązana sesja SSL w dosyć znaczny sposób pochłania zasoby obliczeniowe serwera.

Kompromisowym rozwiązaniem wydaje się być zabezpieczanie danych na trzeciej warstwie – warstwie IP. Funkcjonalność tą realizuje protokół IPSec.

IPSec

IPSec jest to bezpieczny protokół IP. W czwartej (obecnie obowiązującej) wersji IP jest to opcjonalne rozszerzenie, natomiast w IPv6 będzie on obowiązkowy.

Protokół IPSec jest implementowany w stosie protokołu IP, a więc nie wymaga specjalizowanego hardware. Jest on także całkowicie przeźroczysty dla wszelkiego rodzaju aplikacji sieciowych, ponieważ działa na niższych warstwach.

Protokół IPSec zapewnia:

- *Poufność* - zabezpieczenie przed podsłuchem pasywnym, czyli celowym lub przypadkowym dostaniem się informacji w niepowołane ręce
- *Integralność* - zabezpieczenie przed podsłuchem aktywnym (fałszowanie i wstawianie danych), przejmowaniem sesji, błędy transmisji
- *Autentyczność* - pewność, że druga strona jest tym za kogo się podaje; uwierzytelnienie drugiej strony

IPSec może być używany w różnych zastosowaniach dlatego też istnieją dwa tryby pracy tego protokołu (*transport mode* i *tunneling mode*), oraz dwa niezależne podprotokoły (AH i ESP).

Protokół AH (*Authentication Header*), jak sama nazwa wskazuje zapewnia usługi związane z uwierzytelnieniem pakietu. Robi to za pomocą algorytmów typu MAC (*Message Authentication Code*). Dodatkowo zapewnia to również integralność przesyłanych danych.

Protokół ESP (*Encapsulation Security Payload*) zapewnia poufność danych plus funkcjonalność protokołu AH. Oprócz mechanizmów MAC stosuje on algorytmy szyfrujące dane.

Oprócz tych dwóch głównych podprotokołów istnieje jeszcze protokół IPCOMP zapewniający kompresje danych. Wszystkie te protokoły działają niezależnie i można je stosować na raz.

Ponadto IPSec współpracuje z protokołami dodatkowymi służącymi do uzgadniania parametrów IPSEC pomiędzy stronami połączenia (ISAKMP, Photuris). Dbają one o negocjację parametrów szyfrowania oraz zarządzanie kluczami.

Dwa tryby pracy IPSec

Tryb transportowy – w tym trybie nagłówki związane z IPSec (AH/ESP) są dodawane po nagłówku IP, a więc nagłówek IP nie jest ukrywany. Z tego powodu można go stosować tylko do transmisji w sieciach LAN (w WAN – problemy z fragmentacją i routingiem). Tryb transportowy stosuje się do komunikacji między komputerami, oraz komunikacji komputerów z gatewayami IPSec.

Tryb tunelowy powoduje dodanie nowego nagłówka IP wraz z nagłówkami IPSec i w rezultacie ukrycie całego pakietu, łącznie z nagłówkami. Stosuje się go głównie do komunikacji gateway-gateway. Umożliwia on budowę sieci VPN (wirtualnych sieci LAN) przy użyciu Internetu.

Gateway'e IPSec to specjalne urządzenia które pracują na styku LAN i WAN. Pracują one w trybie tunelowym i przesyłają dane w sposób bezpieczny poprzez sieci niebezpieczne (publiczne). Zwykły ruch IP z sieci LAN zostaje zaszyfrowany i przesłany przez sieć publiczną (np. Internet). Zastosowanie gateway'a IPSec jest całkowicie przeźroczyste dla użytkownika końcowego. W ten sposób urządzenia te umożliwiają budowę bezpiecznych sieci rozległych, przy małych kosztach wdrożenia.

Security Association

Z każdym połączeniem IPSec (sesją) związanych jest wiele parametrów:

- algorytm szyfrowania
- algorytm uwierzytelniania
- metoda wymiany klucza
- klucze sesji
- czas ważności kluczy
- kolejność protokołów
- …

Wszystkie te parametry razem tworzą strukturę opisującą dane połączenie - Security Association (SA).

SA mogą być konfigurowane ręcznie przez administratora dla każdego połączenia, lub tworzone automatycznie na podstawie polityki zapisanej w bazie polityki bezpieczeństwa - Security Policy Database. Jeśli przystępujemy do budowy infrastruktury IPSec, to musimy wybrać jeden z tych sposobów.

Protokoły negocjacji parametrów transmisji

Ręczne definiowanie kanałów SA i ustawianie kluczy staje się nieefektywne przy sieciach z dużą (powyżej kilku) ilością węzłów, w związku z tym pojawiła się konieczność stosowania mechanizmów dynamicznej negocjacji kanałów SA. Protokoły te przy zwiększeniu funkcjonalności IPSec nie powinny narażać danych i kluczy na niebezpieczeństwa w związku z tym muszą spełniać określone wymagania:

- Uwierzytelnienie stron nawiązujących połączenie IPSec, dokonywane jest na podstawie współdzielonego sekretu (shared secret), certyfikatów X.509, klucza PGP lub informacji z DNSSEC
- Negocjacja takich parametrów kanałów SA, które będą spełniać wymagania polityki bezpieczeństwa obu stron
- Renegocjacja parametrów kanałów w określonych odstępach czasu
- Obecnie dostępnych jest kilka protokołów negocjacji parametrów:
- ISAKMP (Internet Security Association and Key Management Protocol) - opracowany przez NSA, najbardziej rozbudowany
- Oakley - protokół negocjacji parametrów kluczy oparty o algorytm Diffiego-Hellmana
- IKE (Internet Key Exchange) - połączenie ISAKMP oraz Oakley na potrzeby IPSEC
- Inne: Photuris (OpenBSD), SKIP (Sun)

Wszystkie te protokoły posiadają możliwość narzucenia administracyjnie wymogów co do bezpieczeństwa komunikacji w określonych relacjach. W związku z czym są dobrymi narzędziami do realizacji polityki bezpieczeństwa transmisji.

Jakie mechanizmy kryptograficzne są używane przez IPSec?

Kryptograficzne funkcje skrótu

- Skrót wiadomości jest dodatkowo zabezpieczony kluczem, dzięki temu jest zapewniona ochrona integralności i uwierzytelnienie nadawcy.
- Obowiązkowo muszą być zaimplementowane algorytmy HMAC/MD5 i HMAC/SHA1, firmy implementujące IPSec mogą też stosować swoje własne algorytmy.

Algorytmy szyfrowania

- DES CBC (obowiązkowo)
- 3DES, Blowfish, IDEA, CAST-128, inne
- Uwaga: duża liczba implementacji komercyjnych używa tylko DESa z krótkim (40 bit) kluczem.
- Algorytmy używane zawsze w trybie CBC (Cipher Block Chaining) - utrudnia to ataki przez powtórzenie bloku i ataki ze znanym tekstem jawnym
- Dołączony wektor inicjujący umożliwia synchronizację sesji w razie zgubienia pakietów

IPSec – Implementacje - gateway

W tej chwili wsparcie dla IPSec oferują w swych routerach wszyscy więksi producenci (najdłużej BorderGuard, Cisco, Shiva). Implementacja protokołu odbywa się w systemie operacyjnym routera i z reguły bazuje na Net/OpenBSD lub oprogramowaniu firmy SSH Communications.

Router – routerowi nie równy, modele z „dolnej półki” zapewniają bardzo niską wydajność. (Np. Cisco: seria 1000 - 64kbps, 2600 - 500kbps, 7206 - 5Mbps). W wysokowydajnych rozwiązaniach, stosowane jest hardware’owe wspomaganie szyfrowania, lub silne procesory routera.

IPSec – Implementacje - software

W zaawansowanych systemach operacyjnych również istnieją moduły do obsługi IPSec. Za implementację wzorcową uważa się KAME – projekt rozwijany przez grupę firm japońskich. Jest to implementacja dla rodziny xBSD.

Microsoft w Windows 2000 również zaimplementował IPSec.
Istnieje też kilka implementacji dla systemów otwartych (Linux, BSD) – tu należy wymienić FreeS/WAN, NIST-Cerberus i PGPnet. Ostatnia z tych implementacji działa również w Windows.
Niestety ze względu na dużą złożoność protokołu, część implementacji nie jest kompatybilna z innymi. Rozbieżności pojawiają się z reguły w protokołach zarządzania kluczami.

Dla hostów stosujących protokół IPSec dostępne są Karty sieciowe z IPSec. Odciażają one procesor z operacji obliczania sum kontrolnych i szyfrowania. Potrafią zredukować obciążenie procecora nawet o 80%. Produkty takie posiada m.in. Intel. Karty te współpracuja tylko z implementacja Microsoft.

UWAGA: Karty obsługują tylko transport mode, a więc nie mogą komunikować się przez WAN

ABA Cryptonite

Istnieje również polskie rozwiązanie oparte o protokół IPSec. Firma którą reprezentuje – ABA opracowała urządzenie Cryptonite.

Cryptonite jest gateway'em IPSec pracującym w trybie tunelowym. Jako hardware zastosowano jednostkę Intel ISP1100 wyposażoną w procesor Pentium III 650. Urządzenie nadaje się do instalacji w standardowym racku 19" i zajmuje zaledwie 1U wysokości.

Firmware urządzenia znajduje na pamięci flash, system urządzenia działa z pamięci RAM. Jako implementacje IPSec zastosowaliśmy KAME. Urządzenie obsługuje protokół dynamicznej negocjacji SA: IKE.

W Cryptonite zastosowano silne algorytmy szyfrujące. Ze względu na to że urządzenie powstało w Polsce nie stosują się do niego ograniczenia eksportowe USA dotyczące technologii kryptograficznych.

Przeprowadzone testy wykazały że urządzenie szyfruje dane najsilniejszym z dostepnych algorytmów (3DES-CBC-168bit) w tępie 6,5Mbit/s

Dodatkowe informacje na temat IPSec:

www.ipsec.pl

- informacje o protokole IPSec
- prezentacje z konferencji
- zbiór linków do innych stron
- bieżące informacje dotyczące bezpieczeństwa informacji i kryptografii