BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 20, 2004

Mechanizmy zabezpieczeń transmisji w środowisku IPSec

Janusz FURTAK

Instytut Teleinformatyki i Automatyki WAT
ul. Kaliskiego 2, 00-908 Warszawa

STRESZCZENIE: W artykule opisane zostały mechanizmy zabezpieczeń udostępniane w środowisku IPSec. Przedstawiono właściwości, strukturę nagłówków i tryby pracy protokołów w architekturze IPSec. Opisano podstawowe komponenty środowiska IPSec: relacje zabezpieczeń, bazy danych zabezpieczeń oraz sposoby zarządzania kluczami kryptograficznymi na potrzeby IPSec przy wykorzystaniu publicznej sieci Internet.

1. Zagrożenia bezpieczeństwa transmisji danych w sieci Internet

W pierwszych dwudziestu latach rozwoju sieci Internet wszystkie wprowadzane technologie koncentrowały się na tym, aby przesyłanie danych było efektywne i dostępne dla możliwie szerokiego grona użytkowników. W małym stopniu zastanawiano się nad tym, że przesyłane dane mogą być przechwycone, zniekształcone lub wykorzystane w inny niezamierzony sposób przez niepowołanych użytkowników. Na sieć Internet czyhają różne zagrożenia. Należą do nich:

- brak poufności;
- utrata integralności danych;
- podszywanie się pod legalnych użytkowników;
- uszkodzenie systemu realizacji usług.

Brak poufności występuje wtedy, gdy nieuprawniony użytkownik może przechwycić dane w trakcie ich przesyłania, wykorzystując właściwości stosowanej techniki transmisji danych (np. według standardu Ethernet). Ten fakt

jest największym niedostatkiem sieci Internet hamującym powszechne wykorzystanie go w prowadzeniu interesów.

Utrata integralności przesyłanych danych ma miejsce w sytuacji, kiedy niepowołany użytkownik przechwyci oryginalne dane, zmieni ich zawartość i przekaże do adresata tak zmienione dane. Adresat przejmie zniekształcone dane traktując je jak dane prawdziwe. Na przykład w transakcjach bankowych bardzo istotną daną jest wartość transakcji. Łatwo sobie wyobrazić skutki utraty integralności takich danych.

Podszywanie się pod legalnych użytkowników (*ang. identity spoofing*) polega na tym, że legalny użytkownik otwiera sesję podając wymagane dane do autoryzacji, a napastnik przejmuje jego sesję i w imieniu legalnego użytkownika wykonuje wszelkiego rodzaju czynności.

Jeżeli przechwycenie danych lub podszywanie się nie jest możliwe lub bardzo utrudnione, napastnik może podjąć próbę uszkodzenia systemu realizacji usług sieciowych (*ang. Denial-of-service*). W tym przypadku wykorzystywane są własności bardzo powszechnych w sieci Internet protokołów z rodziny TCP/IP. Operacje dostępne w tych protokołach wykonywane w specjalny sposób mogą spowodować przepełnienie kolejek pakietów w urządzeniach sieciowych, przeciążenie łączy sieciowych lub procesorów. W rezultacie usługa oferowana w sieci staje się niedostępna.

Podejmowano próby rozwiązania zasygnalizowanych problemów poprzez opracowanie procedur, które zwykle były lokowane w warstwie transportowej w modelu sieci ISO/OSI. Na przykład pakiet SSL (*ang. Secure Socket Leyer*), który umożliwia zabezpieczanie transmisji dla takich aplikacji, jak usługa WWW, czy FTP. Istotnym niedostatkiem tych rozwiązań było to, że były one dedykowane dla wybranych aplikacji. Przeniesienie mechanizmów zabezpieczeń z warstwy transportowej do warstwy sieciowej stworzyłoby bezpieczną i uniwersalną platformę dla wszystkich aplikacji korzystających z sieci Internet. Takim rozwiązaniem jest architektura IPSec.

2. Architektura IPSec

Architektura IPSec udostępnia różne usługi zabezpieczające transferowane dane w warstwie sieciowej przez niezabezpieczone łącza. Może być wykorzystywana w środowisku wykorzystującym protokół IP w wersji 4 i w wersji 6. Daje systemowi możliwość wyboru odpowiedniego protokołu i algorytmów do zabezpieczenia transmisji przy wykorzystaniu kluczy kryptograficznych. Architektura IPSec może być wykorzystywana

do zabezpieczania jednej lub wielu ścieżek pomiędzy hostami, pomiędzy bramami bezpieczeństwa[1] albo pomiędzy hostem, a taką bramą.

IPSec jest zbiorem otwartych standardów zapewniających bezpieczną prywatną komunikację w sieciach IP (opis zagadnień związanych z protokołem IPSec jest dostępny w dokumentach RFC 2401-2411, 2451 i 3168). IPSec umożliwia realizację następujących operacji:

- weryfikowanie źródła pochodzenia datagramu protokołu IP (eliminacja możliwości zamiany adresu źródłowego pakietu);
- bezpołączeniowe weryfikowanie integralności datagramu IP (zabezpieczenie przed modyfikacją zawartości pakietu);
- zabezpieczenie zawartości pakietu przed odczytaniem (stosowanie różnych metod kryptograficznych);
- zapobieganie wielokrotnego wysyłania do odbiorcy poprawnego takiego samego pakietu, który wcześniej został przechwycony (unikanie zablokowania działania usług).

Z tego względu, że IPSec funkcjonuje w warstwie sieciowej, mechanizmy IPSec mogą być wykorzystane do zabezpieczania wszystkich pakietów protokołów wyższych warstw, np. TCP, UDP, ICMP, BGP, itd.

IPSec stanowi połączenie kilku różnych technologii zabezpieczeń, dzięki czemu tworzy pełny system chroniący dane. W szczególności IPSec używa:

- algorytmu wymiany kluczy Diffie'go-Hellmana;
- infrastruktury klucza publicznego do negocjacji klucza sesji;
- algorytmów szyfrowania danych typu DES;
- algorytmów generowania skrótów typu MD5 i SHA;
- cyfrowych certyfikatów.

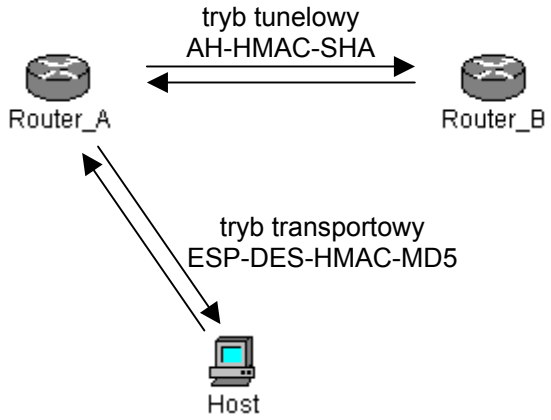
Na pełen zestaw zabezpieczeń oferowanych w środowisku IPSec składają się dwa komponenty:

- definicja danych dodawanych do standardowego pakietu IP w celu zapewnienia poufności, integralności, autentyczności pakietu (nagłówki AH i ESP) i definicja sposobu kodowania zawartości pakietu;
- mechanizm wymiany kluczy przez łącza publiczne IKE (*ang. Internet Key Exchange*) niezbędnych do negocjacji parametrów bezpiecznego połączenia pomiędzy dwoma węzłami sieci i wymiany kluczy sesji.

[1] Brama bezpieczeństwa (ang. *security gateway*) – system pośredniczący w wymianie danych (np. router lub firewall), który implementuje usługę związaną z IPSec.

3. Relacja zabezpieczeń (*SA - Security Association*)

Relacja zabezpieczeń SA określa zależności bezpieczeństwa pomiędzy dwoma lub więcej jednostkami. Wyjaśnia, w jaki sposób jednostki używać będą systemów zabezpieczeń do bezpiecznej komunikacji. Relacja zabezpieczeń jest jednokierunkowa. Zatem dla każdej pary komunikujących się urządzeń zdefiniować należy przynajmniej dwa bezpieczne połączenia - z A do B i z B do A. Relacja zabezpieczeń jest jednoznacznie definiowana przez losowo wybrany jednoznaczny numer tzw. *Security Parameters Index* (SPI), docelowy adres IP odbiorcy oraz identyfikator protokołu zabezpieczeń (AH lub ESP). Kiedy system wysyła pakiet, który wymaga ochrony IPSec, przegląda relacje zabezpieczeń w swojej bazie i następnie umieszcza SPI w nagłówku IPSec. Parametry relacji zabezpieczeń są negocjowane w trakcie zestawiania bezpiecznego połączenia i obowiązują przez cały czas funkcjonowania tej relacji (Rys.1).

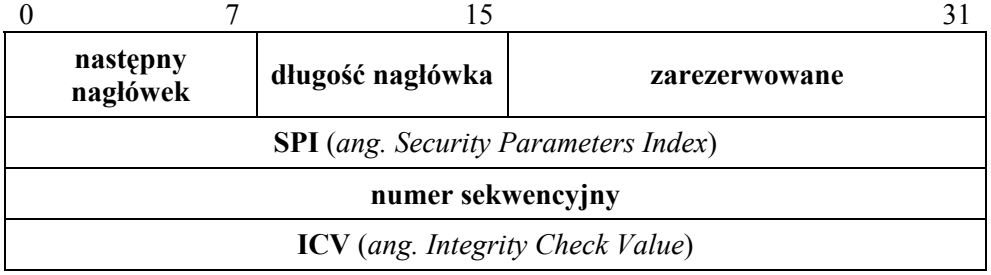


Rys.1. Przykład relacji zabezpieczeń

4. Nagłówek AH (*Authentication Header*)

Nagłówek AH zapewnia bezpołączeniową integralność datagramu (*ang. connectionless integrity*), wiarygodność źródła danych (*ang. data origin authentication*) oraz zabezpiecza łącze przed wielokrotnym przesyłaniem tych samych datagramów IP (*ang. anti-replay service*). Uwiarygodnianiu podlega całe pole danych pakietu i te pola nagłówka, które są niezmienne w trakcie transferu pakietu przez sieć oraz te zmienne pola nagłówka, których wartości są przewidywalne przez nadawcę.

Nagłówek AH może być stosowany samodzielnie, w kombinacji z nagłówkiem ESP (*ang. Encapsulating Security Payload*) albo może być zagnieżdżony w przypadku wykorzystywania trybu tunelowego. Może być wykorzystywany do zabezpieczania łącza pomiędzy hostami, pomiędzy bramami bezpieczeństwa albo pomiędzy hostem a bramą bezpieczeństwa. Struktura nagłówka AH jest przedstawiona na rysunku 2.



Rys.2. Struktura nagłówka AH

Znaczenie pól nagłówka AH:

- **następny nagłówek** – numer protokołu[2], którego pakiet jest umieszczony za nagłówkiem AH (np. dla protokołu TCP jest to liczba 6);
- **długość nagłówka** – liczba 32-bitowych słów nagłówka pomniejszona o 2;
- **zarezerwowane** – wypełnione zerami, uwzględniane przy wyznaczaniu wartości pola ICV;
- **SPI** – wynegocjowana 32-bitowa liczba identyfikująca relację zabezpieczeń[3] dla pakietu (liczby 1-255 są zarezerwowane; 0 występuje w tym polu w trakcie negocjowania parametrów połączenia);
- **numer sekwencyjny** – liczba zwiększająca się w każdym pakiecie; po zestawieniu połączenia ma wartość 0; gdy osiągnie wartość 2^{32} relacja zabezpieczeń musi być ponownie zestawiona;
- **ICV** – suma kontrolna o długości będącej wielokrotnością 32 bitów (zwykle 96 bitów) wyliczana na podstawie wybranych pól nagłówka IP, pól nagłówka AH i danych pakietu.

Nagłówek IP bezpośrednio poprzedzający nagłówek AH w polu określającym protokół zawiera wartość 51. Wszystkie pola nagłówka AH są obowiązkowe i brane pod uwagę przy obliczaniu pola ICV.

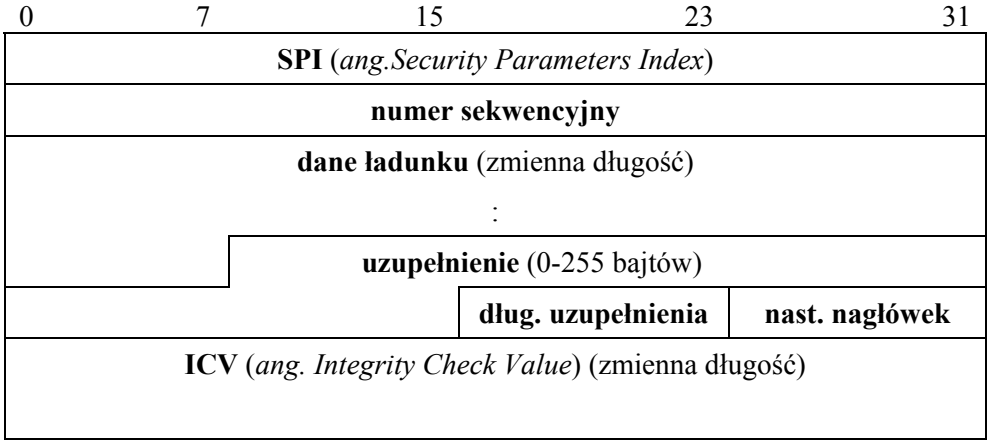
[2] Lista wykorzystywanych numerów jest podana w RFC 1700.

[3] Relacja zabezpieczeń – logiczne połączenie pomiędzy dwoma węzłami pracującymi w protokole IPSec – kojarzy adresy węzłów i używany protokół bezpieczeństwa.

5. Nagłówek ESP (*Encapsulating Security Payload*)

Nagłówek ESP może być stosowany samodzielnie, w kombinacji z nagłówkiem AH albo może być zagnieżdżony w przypadku wykorzystywania trybu tunelowego. Może być wykorzystywany do zabezpieczania łącza pomiędzy hostami, pomiędzy bramami bezpieczeństwa albo pomiędzy hostem a bramą bezpieczeństwa.

Nagłówek ESP zapewnia poufność przesyłanych danych (*ang. confidentionality*), bezpołączeniową integralność datagramu (*ang. connectionless integrity*), wiarygodność źródła danych (*ang. data origin authentication*), zabezpiecza łącze przed wielokrotnym przesyłaniem tych samych datagramów IP (*ang. anti-replay service*) oraz ograniczoną poufność strumienia ruchu pakietów (*ang. limited traffic flow confidentionality*). Zestaw stosowanych usług w danym połączeniu jest konfigurowalny spośród wyżej wymienionych. Usługi integralności datagramu i wiarygodności źródła danych są usługami występującymi zawsze wspólnie i mogą występować równocześnie z usługą poufności. Usługa *anti-replay* może być wybierana pod warunkiem stosowania usługi wiarygodności źródła danych. Usługa poufności ruchu pakietów wymaga wyboru trybu tunelowego i działa najefektywniej, gdy jest zaimplementowana na bramie bezpieczeństwa – dane docelowego węzła są ukryte. Struktura nagłówka ESP jest przedstawiona na rysunku 3.



Rys.3. Struktura nagłówka ESP

Wśród pól nagłówka ESP można wyróżnić pola obowiązkowe i opcjonalne. Pole opcjonalne występuje, jeżeli została wybrana usługa, dla której dane pole jest niezbędne. Jeżeli pole opcjonalne nie występuje, to nie jest uwzględniane przy obliczaniu wartości pola ICV. O tym, czy dane pole będzie

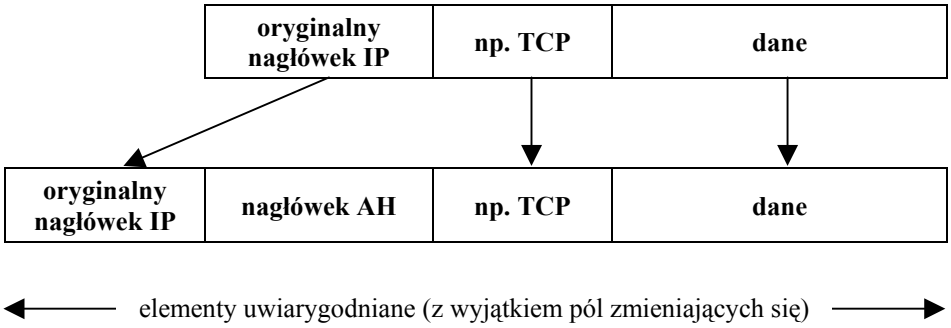
wykorzystywane czy nie, decyduje procedura zestawiania relacji zabezpieczeń. Po wynegocjowaniu parametrów relacji zabezpieczeń struktura pakietu jest ustalona. Znaczenie pól nagłówka ESP:

- **SPI** – wynegocjowana 32-bitowa liczba identyfikująca relację zabezpieczeń dla pakietu (liczby 1-255 są zarezerwowane; 0 występuje w tym polu w trakcie negocjowania parametrów połączenia) (pole obowiązkowe);
- **numer sekwencyjny** – liczba zwiększająca się w każdym pakiecie; po zestawieniu połączenia ma wartość 0; gdy osiągnie wartość 2^{32} relacja zabezpieczeń musi być ponownie zestawiona (pole obowiązkowe);
- **dane ładunku** – pakiet danych protokołu opisanego w polu **następny nagłówek**, może to być np. datagram TCP, oryginalny pakiet IP w trybie tunelowym itp.; pole może być szyfrowane lub nie (pole obowiązkowe);
- **uzupełnienie** – stosowane, gdy algorytmy szyfrowania wymagają odpowiedniej długości danych przeznaczonych do zakodowania oraz aby spełnić wymaganie mówiące, że pola: **długość wypełnienia** i **następny nagłówek** muszą być umieszczone na ostatnich dwóch bajtach 4-bajtowego słowa (pole opcjonalne);
- **długość uzupełnienia** – liczba bajtów pola **uzupełnienie** (pole obowiązkowe);
- **następny nagłówek** – numer protokołu, którego pakiet jest umieszczony w polu **dane ładunku** (pole obowiązkowe);
- **ICV** – suma kontrolna o długości będącej wielokrotnością 32 bitów; długość pola wyznacza wybrana funkcja autentykacji dla danej relacji zabezpieczeń określona przez pole SPI (pole opcjonalne).

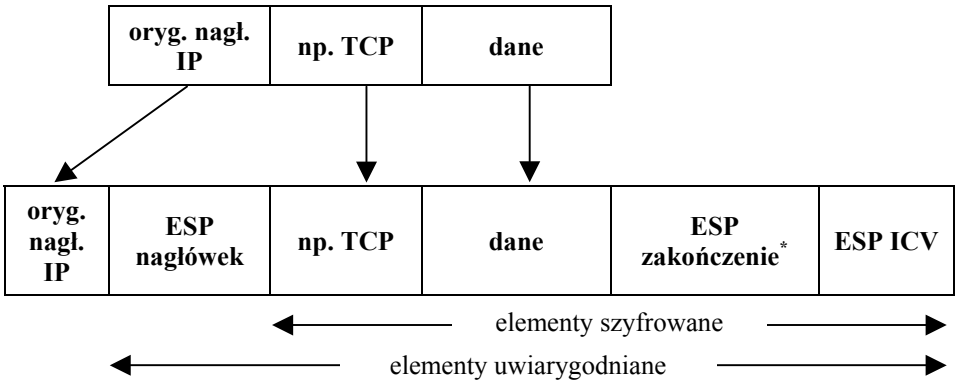
Nagłówek IP bezpośrednio poprzedzający nagłówek ESP w polu określającym protokół zawiera wartość 50.

6. Tryby pracy środowiska IPSec

IPSec wykorzystuje dwa tryby przesyłania danych przez sieć: tryb transportowy i tryb tunelowy. Tryb transportowy jest wykorzystywany do utworzenia bezpiecznego łącza pomiędzy dwoma hostami. W protokole IPv4 nagłówek zabezpieczający (tzn. AH lub ESP) jest umieszczany po oryginalnym nagłówku i jego ewentualnych opcjach, a przed danymi protokołów warstwy wyższej. Struktura pakietu IPSec w trybie transportowym dla nagłówka AH jest pokazana na rysunku 4, a dla nagłówka ESP na rysunku 5.



Rys.4. Konstrukcja pakietu IPSec z nagłówkiem AH w trybie transportowym



* pole obejmuje pola: uzupełnienie, długość uzupełnienia i następny nagłówek nagłówka ESP

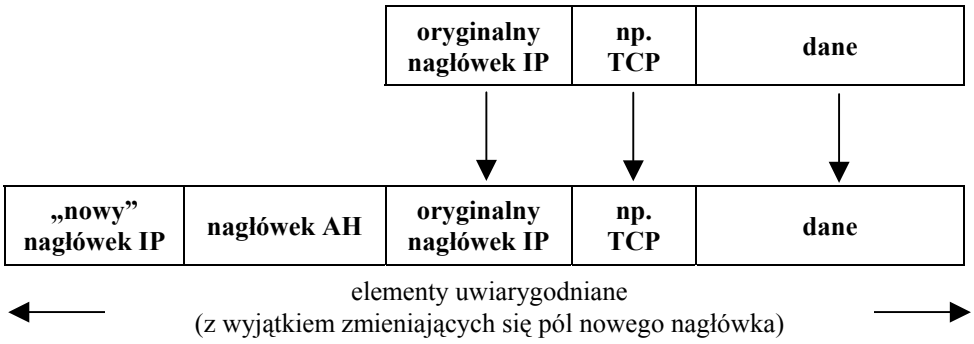
Rys.5. Konstrukcja pakietu IPSec z nagłówkiem ESP w trybie transportowym

Pomiędzy dwoma węzłami, z których przynajmniej jeden funkcjonuje jako bezpieczna brama (tzn. przekazuje odkodowany ruch sieciowy na drugą stronę bramy), musi[4] być stosowany tryb tunelowy do realizacji bezpiecznych łączy. Ten tryb może być również wykorzystywany do bezpiecznej transmisji pomiędzy dwoma hostami.

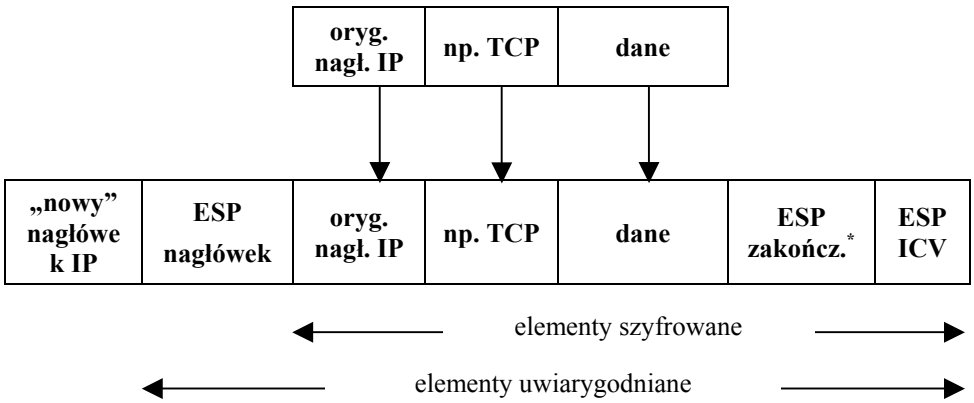
W trybie tunelowym cały oryginalny pakiet IP razem z oryginalnym nagłówkiem jest zapakowany w innym pakiecie IP i może być zakodowany. Z tego względu tunelujące routery w „zewnętrznym" nagłówku umieszczają niezbędne adresy IP do przesłania pomiędzy sobą pakietów. Dane

[4] Konieczność stosowania trybu tunelowego wynika z problemów defragmentacji pakietów w przypadku istnienia kilku bram bezpieczeństwa prowadzących do jednego docelowego węzła.

z „zewnętrznego" nagłówka nie są kodowane. W trybie tunelowym mogą być wykorzystywane zarówno nagłówki AH jak i ESP. Stosowanie trybu tunelowego powoduje zwiększenie długości pakietu o około 20 bajtów w stosunku do trybu transportowego. Sposób tworzenia pakietu IPSec w trybie tunelowym wykorzystującym nagłówek AH jest podany na rysunku 6, a nagłówek ESP na rysunku 7.



Rys.6. Konstrukcja pakietu IPSec z nagłówkiem AH w trybie tunelowym



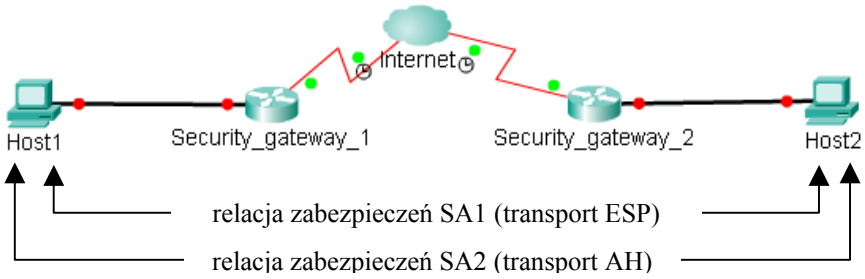
* pole obejmuje pola: uzupełnienie, długość uzupełnienia i następny nagłówek nagłówka ESP

Rys.7. Konstrukcja pakietu IPSec z nagłówkiem ESP w trybie tunelowym

7. Złożone relacje zabezpieczeń

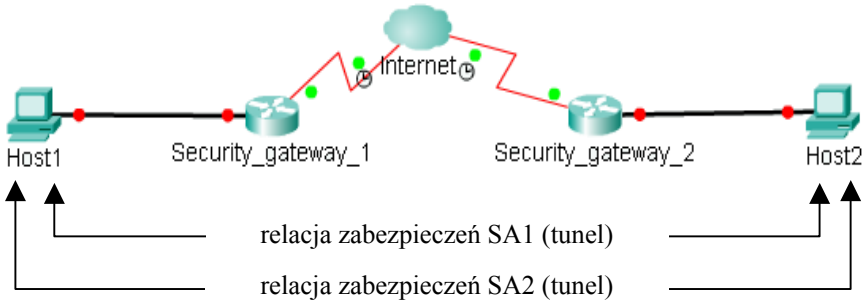
Datagram IP transmitowany poprzez jedną relację zabezpieczeń umożliwia wykorzystanie dokładnie jednego z dwóch protokołów: AH albo ESP. Występują sytuacje, w których wymagane są zabezpieczenia transferu niemożliwe do spełnienia przy wykorzystaniu jednego protokołu. W takich przypadkach można zastosować kombinację relacji zabezpieczeń (*ang. SA bundle*). Kombinacje takie można uzyskać następującymi sposobami:

1. Użycie dwóch protokołów zabezpieczeń dla jednego datagramu IP (*ang. transport adjacency*) w trybie transportowym.

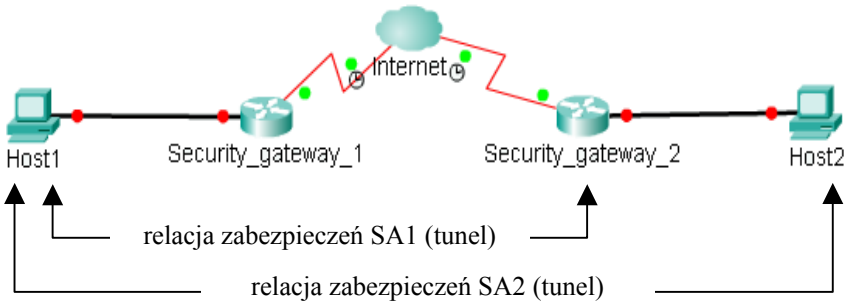


Rys.8. Kombinacja zabezpieczeń w trybie transportowym

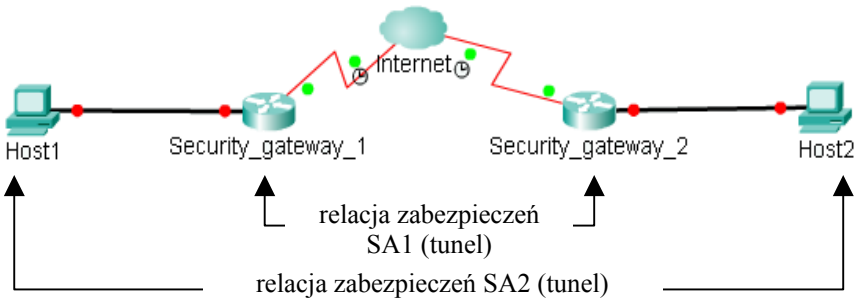
2. Wielokrotne tunelowanie - wewnętrzny i zewnętrzny tunel musi wykorzystywać ten sam protokół AH albo ESP, tzn. AH wewnątrz AH albo ESP wewnątrz ESP. Może występować w trzech podstawowych wariantach:
   - oba końce w obu relacjach zabezpieczeń są takie same (rysunek 9);
   - jeden koniec w obu relacjach zabezpieczeń jest taki sam (rysunek 10);
   - żaden z końców obu relacji zabezpieczeń nie jest taki sam (rysunek 11).



Rys.9. Kombinacja zabezpieczeń w trybie tunelowym (wariant 1)

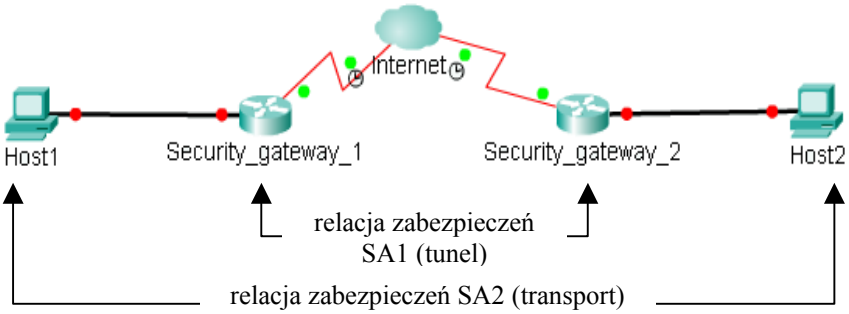


Rys.10. Kombinacja zabezpieczeń w trybie tunelowym (wariant 2)



Rys.11. Kombinacja zabezpieczeń w trybie tunelowym (wariant 3)

3. Rozwiązania mieszane – przykład jest podany na rysunku 12



Rys.12. Tryb transportowy przenoszony w trybie tunelowym

8. Bazy danych zabezpieczeń

W modelu bezpieczeństwa oferowanym w środowisku IPSec istotną rolę odgrywają dwie bazy danych:

- baza danych protokołów bezpieczeństwa SPD (*ang. Security Policy Database*) – określa, który rodzaj ruchu sieciowego podlega procedurom IPSec;
- baza danych relacji zabezpieczeń SAD (*ang. Security Association Database*) – określa parametry każdej aktywnej relacji zabezpieczeń.

Baza danych SPD umożliwia sklasyfikowanie całego ruchu sieciowego na ruch:

- wchodzący (*ang. inbound*);
- wychodzący (*ang. outbound*);

oraz

- podlegający ochronie IPSec;
- niepodlegający ochronie IPSec.

Na podstawie zawartości bazy danych SPD w stosunku do każdego pakietu wchodzącego lub wychodzącego podejmowana jest jedna z poniższych decyzji:

- odrzuć – pakiet nie może opuścić hosta, ani przejść przez bramę bezpieczeństwa ani być przekazany do aplikacji;
- pomiń procedury IPSec przy przekazywaniu pakietu;
- zastosuj procedury IPSec – w tym przypadku baza SPD wskazuje stosowane usługi bezpieczeństwa, protokoły i algorytmy.

Datagramy wychodzące są wysyłane z zastosowaniem ochrony lub bez ochrony. Decyzja odrzucenia lub akceptacji wchodzącego datagramu bazuje na szeregu kryteriów, które mogą zachodzić na siebie lub przeczyć sobie. W takich sytuacjach decyduje kolejność przetwarzania kryteriów. Kluczowe znaczenie ma sposób określania reguł, według których podejmowane są powyższe decyzje. Nie są one precyzyjnie opisane – RFC2401 podaje tylko wymagania, które muszą spełniać aplikacje pracujące w środowisku IPSec.

Zapisy w bazie danych SPD służą ponadto do kontrolowania całego ruchu sieciowego związanego ze środowiskiem IPSec, a w szczególności ruchu związanego z zarządzaniem kluczami (np. ISAKMP). Z tego względu w bazie SPD muszą znaleźć się zapisy definiujące ten typ ruchu.

Każda aktywna relacja zabezpieczeń posiada jeden zapis w bazie danych SAD. Przy przetwarzaniu pakietów wychodzących odpowiednie zapisy są wskazywane przez zapisy w bazie danych SPD (w przypadku braku w bazie SAD relacji wskazywanej przez zapisy bazy SPD uruchamiana jest procedura tworzenia relacji zabezpieczeń, a po jej utworzeniu tworzony jest odpowiedni zapis w bazie SAD). Przy przetwarzaniu pakietów wchodzących zapisy bazy SAD są indeksowane przy pomocy zewnętrznego adresu docelowego z pakietu, typu protokołu IPSec (tzn. AH lub ESP) i wartości pola SPI.

Każdy zapis w bazie SAD musi ponadto zawierać dane, które zostały wynegocjowane w trakcie tworzenia relacji zabezpieczeń. Te dane są niezbędne dla strony wysyłającej do konstrukcji poprawnego pakietu, a stronie odbierającej do sprawdzenia szeroko rozumianej poprawności odebranego pakietu. Zapisy bazy danych SAD obejmują następujące pola:

- licznik numeru sekwencyjnego – 32-bitowa liczba używana do tworzenia pola „numer sekwencyjny" w nagłówkach AH i ESP;
- wskaźnik przepełnienia licznika numeru sekwencyjnego – wystąpienie takiego zdarzenia powoduje deaktywację aktualnej relacji zabezpieczeń i wymusza procedurę negocjacji nowej relacji;
- okno „anti replay" – 32-bitowa liczba używana do określenia, czy przychodzący pakiet nie jest powtórzeniem wcześniejszego pakietu;
- dla AH: algorytm uwierzytelniania, klucze, itp. (jeżeli wybrano usługę AH);
- dla ESP: algorytm szyfrowania, klucze, wektor inicjujący (IV), tryb wykorzystania wektora IV itp. (jeżeli wybrano usługę szyfrowania ESP);
- dla ESP: algorytm autentykacji, klucze, itp. (jeżeli wybrano usługę autentykacji ESP);
- czas życia relacji zabezpieczeń – może być określony jako upływ czasu lub jako licznik przesłanych bajtów od momentu zainicjowania relacji; po wyczerpaniu czasu życia bieżąca relacja jest przerywana i może być negocjowana nowa relacja; w przypadku wykorzystywania obu sposobów określania czasu życia relacji wyczerpanie pierwszego powoduje renegocjację nowej relacji;
- tryb pracy IPSec (tunelowy, transportowy lub „wildcard" tzn. wybierany przez aplikację;
- wartość parametru PMTU (*ang. Path Maximum Transfer Unit*) i parametru czas starzenia PMTU.

9. Zarządzanie kluczami kryptograficznymi

Oferowane przez środowisko IPSec usługi autentykacji i zabezpieczania pakietów wymagają kluczy kryptograficznych. Obie strony relacji zabezpieczeń muszą dysponować odpowiadającym sobie danymi umożliwiającymi realizację wymienionych usług. Każda ze stron musi dbać o ich aktualność i zabezpieczyć przed niepowołanym dostępem. Istotnym problemem jest dystrybucja kluczy pomiędzy oboma stronami relacji zabezpieczeń. Dystrybucja kluczy nie jest elementem środowiska IPSec, ale jest niezbędna do poprawnego funkcjonowania usług IPSec. Wymiana danych dotyczących kluczy może być realizowana manualnie lub automatycznie.

Manualna dystrybucja kluczy polega na tym, że administrator generuje odpowiednie dane dla obu stron każdej relacji i instaluje odpowiednie dane po obu stronach każdej relacji. Dystrybucja danych musi się odbywać bezpiecznym kanałem – nie może to być na przykład publiczne niezabezpieczone łącze internetowe. Ten sposób jest bardzo uciążliwy dla administratora, nie jest pewny i często jest źródłem kłopotów w komunikacji na skutek błędów administratora polegającego na instalacji po obu stronach relacji nieodpowiadających sobie danych.

Zalecanym sposobem dystrybucji kluczy na potrzeby środowiska IPSec jest wykorzystanie protokołu wymiany kluczy kryptograficznych w Internecie IKE (ang. Internet Key Exchange)[5]. Protokół ten implementuje specyfikacje dotyczące wymiany kluczy kryptograficznych zgodnie ze strukturą ISAKMP (*ang. Internet Security Association and Key Management Protocol*)[6] i umożliwia wymianę utajnionych kluczy i innych danych związanych ze wszystkimi algorytmami wykorzystywanymi przez zabezpieczenia IPSec przy wykorzystaniu publicznych łączy internetowych. Przy wykorzystaniu tego protokołu oba końce połączenia muszą autentykować się wzajemnie. IKE dopuszcza tutaj wiele sposobów uwierzytelniania. Aktualnie wykorzystywane są następujące mechanizmy negocjacji:

- *Pre-shared keys* - takie same klucze preinstalowane są na każdym hoście. IKE autentykuje każdy węzeł przez wysyłanie skrótów na podstawie tych kluczy;
- *Public key cryptography* - każda strona generuje pseudo losowy numer i koduje go wykorzystując klucz publiczny drugiej strony.
- *Digital signature* (podpis elektroniczny) - każde urządzenie podpisuje cyfrowo zbiór danych i wysyła je do drugiej strony.

[5] Szczegółowy opis można znaleźć w dokumencie RFC 2409.
[6] Szczegółowy opis można znaleźć w dokumencie RFC 2408.

Każdy z podanych mechanizmów negocjacji ma zalety i wady. Pierwszy sposób przerzuca na administratora obowiązek bezpiecznego przekazania kluczy do zainstalowania na wszystkich hostach. Takie rozwiązanie jest dosyć wygodne tylko w przypadku małych rozmiarów[7] zabezpieczanej sieci. Dwa pozostałe rozwiązania umożliwiają automatyzację wymiany kluczy przy wykorzystaniu kluczy publicznych i metody Diffie'go-Hellmana. Istotnym elementem jest certyfikat dla wykorzystywanego klucza publicznego. W drugiej metodzie certyfikat nie jest generowany albo jest generowany przez stronę wysyłającą. Z punktu widzenia bezpieczeństwa dwa pierwsze rozwiązania nie są dostateczne. Najpewniejszym mechanizmem jest stosowanie podpisu elektronicznego, ale jego stosowanie wymaga dostępu centrum certyfikacji (*ang. Certificate Authority*).

Praca została zrealizowana w ramach projektu PBW 864/2003

Literatura:

[1] Chapman D. W., Fox A.: *Cisco Secure PIX Firewalls*, Wydawnictwo MIKOM, Warszawa, 2002.

[2] Harkins D., Carrel D.: *The Internet Key Exchange (IKE),* Network Working Group, RFC 2409, 1998.

[3] Held G., Hundley K.: *Listy dostępu rutenów Cisco – przewodnik specjalistyczny*. Wydawnictwo PLJ, Warszawa, 2001.

[4] IPsec and IKE Administration Guide, Sun Microsystems, Inc., 2003.

[5] Kaeo M.: *Tworzenie Bezpiecznych Sieci*, Wydawnictwo MIKOM, Warszawa, 2000.

[6] Kent S., Atkinson R.: *IP Authentication Header*. Network Working Group, RFC 2402, 1998.

[7] Kent S., Atkinson R.: *IP Encapsulating Security Payload*. Network Working Group, RFC 2406, 1998.

[8] Kent S., Atkinson R.: *Security Architecture for the Internet Protocol*. Network Working Group, RFC 2401, 1998.

[9] Maughan D., Schertel M., Schneider M., Turner J.: *Internet Security Association and Key Management Protocol (ISAKMP)*, Network Working Group, RFC 2408, 1998.

[10] Protokół IPSec - bezpieczeństwo w Internecie, Biuletyn informacyjny Integrator, Solidex, Nr 11-12/1998.

Recenzent: : prof. dr hab. inż. Włodzimierz Kwiatkowski
Praca wpłynęła do redakcji 20.12.2004.

[7] To znaczy sieci obejmującej małą liczbę hostów położonych na niewielkim geograficznie obszarze