Protokół IPsec

Patryk Czarnik

Wydział Matematyki, Informatyki i Mechaniki
Uniwersytet Warszawski

Bezpieczeństwo sieci komputerowych – MSUI 2009/10

Standard IPsec

IPsec (od *IP security*) to standard opisujący kryptograficzne rozszerzenia protokołu IP.

- Implementacja obowiązkowa w IPv6, opcjonalna w IPv4.
- Główne funkcjonalności to szyfrowanie i kryptograficzne uwierzytelnianie pakietów IP.
- Historia:
  1. 1995 — wersja obecnie nieużywana,
  2. 1998 — zmiany w szczegółach niekompatybilne wstecz,
  3. 2005 — rozszerzenia drugiej wersji,
  4. przyszłość — prawdopodobnie uproszczenia i dostosowanie standardu do istniejącej praktyki.

Usługi zapewniane przez IPsec

- Poufność (szyfrowanie) transmisji.
- Zapewnienie integralności danych w pakiecie.
- Uwierzytelnianie pochodzenia danych.
- Zabezpieczenie przed atakami polegającymi na powtórnym przesłaniu pakietu (lub całej „nagranej” transmisji).
- Ograniczone zabezpieczenie przed analizą ruchu.
- Kontrola dostępu.
- IPsec jest jednym ze sposobów na zbudowanie VPN (bezpiecznej wirtualnej sieci).

Składowe standardu IPsec

Uwierzytelnienie, szyfrowanie, wymiana klucza

- **AH (*Authentication Header*)** – nagłówek dodawany do pakietu IP, zawierający dane służące do uwierzytelnienia (i kontroli integralności).
- **ESP (*Encapsulating Security Payload*)** – szyfrowanie oryginalnego pakietu IP i obudowanie w pakiet ESP
  - tryb transportowy – podmiana zawartości pakietu IP na zaszyfrowaną,
  - tryb tunelowy – zanurzenie pakietu ESP w nowy pakiet IP
- **IKE (*Internet Key Exchange*)** – uniwersalny algorytm wymiany klucza

Specyfikacje

Specyfikacja IPsec jest zapisana w dokumentach RFC. Są to między innymi:

Temat	wersja 1998	wersja 2005
Opis architektury systemu	RFC 2401	RFC 4301
Opis protokołu AH	RFC 2402	RFC 4302 oraz 4305
Opis protokołu ESP	RFC 2406	RFC 4303 oraz 4305
Algorytm wymiany klucza (IKE)	RFC 2409	RFC 4306

Pełna lista m.in. na `http://en.wikipedia.org/IPsec`

Niskopoziomowość

- IPsec działa na poziomie sieci (OSI 3), w odróżnieniu od TLS, SSL, SSH itp., działających na poziomie sesji (lub aplikacji wg niektórych źródeł).
- Może być wykorzystywany przez dowolne protokoły warstwy transportowej działające nad IP (TCP i UDP).
- Nie może polegać na własnościach zapewnianych przez TCP (pewności dostarczenia i (de)fragmentacji).
- Wymaga implementacji na niskim poziomie (w jądrze systemu).

Sposoby implementacji IPsec

- Zintegrowany z implementacją IP, wymaga to dostępu do kodu źródłowego.
- Wstawiony pomiędzy implementację IP a sterowniki sieciowe, nie jest wtedy wymagany dostęp do kodu źródłowego.
- Zaimplementowany na specjalnej karcie z procesorem kryptograficznym, czasem karty tego typu mogą posiadać własny adres IP.

Security Association

- Abstrakcyjny kanał komunikacji w IPsec:
  - jednokierunkowy,
  - dla ustalonych nadawcy i odbiorcy,
  - z określonymi aspektami szyfrowania
  - i aktualnym kontekstem.
- Idetyfikowany przez:
  - adres IP odbiorcy (może być unicastowy, broadcastowy lub multicastowy),
  - liczbę nazywaną *Security Parameter Index* (SPI),
  - identyfikator protokołu bezpieczeństwa (ESP lub AH).

Security Association

- Abstrakcyjny kanał komunikacji w IPsec:
  - jednokierunkowy,
  - dla ustalonych nadawcy i odbiorcy,
  - z określonymi aspektami szyfrowania
  - i aktualnym kontekstem.
- Idetyfikowany przez:
  - adres IP odbiorcy (może być unicastowy, broadcastowy lub multicastowy),
  - liczbę nazywaną *Security Parameter Index* (SPI),
  - identyfikator protokołu bezpieczeństwa (ESP lub AH).

Parametry ustalone przez SA

- Algorytm uwierzytelniania (oraz jego tryb pracy) użyty w nagłówku AH (obowiązkowe w przypadku AH).
- Klucze użyte w AH (obowiązkowe w przypadku AH).
- Algorytm szyfrowania (oraz jego tryb pracy) i transformacja użyte nagłówku ESP (obowiązkowe w przypadku ESP).
- Klucze użyte w ESP (obowiązkowe w przypadku ESP).
- Informacja o obecności i rozmiarze wektora kryptograficznej synchronizacji lub inicjalizacji dla algorytmu szyfrowania (obowiązkowe w przypadku ESP).
- Algorytm uwierzytelnienia (i jego tryb) użyty dla transformacji ESP (opcjonalny dla ESP).
- Klucz użyty w powyższym (opcjonalny dla ESP).

Parametry ustalone przez SA (c.d.)

- Czas życia klucza lub czas ponownej negocjacji klucza (opcjonalny).
- Czas życia danego SA (opcjonalny).
- Adres nadawcy SA, może zawierać adres grupowy, jeśli dana SA jest używana przez więcej niż jednego nadawcę (opcjonalny).
- Poziom poufności zaszyfrowanych danych (wymagany w przypadku systemów oferujących wiele poziomów poufności).

Mechanizm uzgadniania kluczy odwołuje się jedynie do pojęcia SPI, dlatego jest ono wyspecyfikowane osobno.

Bazy danych

Systemy korzystające z IPsec posiadają dwie bazy danych:

- **SPD (*Security Policy Database*)** – zawiera informacje o mechanizmach, jakie powinny być zastosowane do pakietów wychodzących i przychodzących,
- **SAD (*Security Association Database*)** – zawiera parametry związane z SA:
  - algorytm szyfrowania lub uwierzytelniania,
  - klucze szyfrowania lub uwierzytelniania,
  - czas życia SA,
  - licznik pakietu SA,
  - informacje co należy robić w przypadku przepełnienia licznika.

Selektory

Baza SPD pozwala wybrać sposób przetwarzania pakietów na podstawie tak zwanych **selektorów**. Zdefiniowane są następujące typy selektorów:

- adres docelowy,
- adres źródłowy,
- nazwa użytkownika (np. `binladen@alkaida.org`) lub komputera, zarówno DNS jaki i według X.500,
- poziom poufności danych,
- protokół transportowy,
- porty źródłowy i docelowy.

IKE – *Internet Key Exchange*

- Planowany do różnorakich zastosowań (nie tylko IPsec)
- Bardzo ogólnie sformułowany
- W przypadku IPsec rezultatem jest utworzenie SA
- Możliwe tryby ustalania klucza:
  - hasło znane obu stronom (*shared secret*)
  - podpisy RSA
  - certyfikaty X.509
- Dwie wersje:
  - IKE (koniec 1998)
  - IKEv2 (koniec 2005)

ESP – *Encapsulating Security Payload*

- Zapewnienie poufności i nienaruszalności pakietów IP.
- Szyfrowanie może dotyczyć tylko segmentu warstwy transportowej (*transport-mode ESP*) lub całego pakietu (*tunneling mode ESP*).
- Najczęściej stosowane algorytmy: DES, 3DES, AES.
- Numer wśród protokołów IP: 50

Pakiet ESP (w trybie transportowym)

- **SPI** – 32 bity,
- **numer sekwencyjny pakietu** – 32 bity,
- **dane** – zmienna długość,
- **uzupełnienie** – od 0 do 255 bajtów,
- **długość uzupełnienia** – 8 bitów,
- **następny nagłówek** – 8 bitów; określa typ pakietu, który jest transportowany, zgodnie z numerami protokołów IP (np. 6=TCP)
- **dane uwierzytelniające** – zmiennej długości.

Tryb transportowy i tunelowy ESP

Tryb transportowy ESP

- obejmuje szyfrowanie samych danych użytkowych, pozostawiając oryginalny nagłówek IP
- nagłówek ESP jest umieszczany bezpośrednio przed nagłówkiem transportowym (TCP / UDP/ ICMP)

Tryb tunelowy ESP

- cały oryginalny pakiet jest szyfrowany (wraz z nagłówkiem IP), a następnie wysyłany w polu danych nowego pakietu IP
- nowy nagłówek zawiera informacje wystarczające do przekazania pakietu na miejsce, ale nie do analizy ruchu
- wygodny sposób tworzenia VPN i bezpiecznego łączenia sieci lokalnych przez internet

Tryb transportowy i tunelowy ESP

Tryb transportowy ESP

- obejmuje szyfrowanie samych danych użytkowych, pozostawiając oryginalny nagłówek IP
- nagłówek ESP jest umieszczany bezpośrednio przed nagłówkiem transportowym (TCP / UDP/ ICMP)

Tryb tunelowy ESP

- cały oryginalny pakiet jest szyfrowany (wraz z nagłówkiem IP), a następnie wysyłany w polu danych nowego pakietu IP
- nowy nagłówek zawiera informacje wystarczające do przekazania pakietu na miejsce, ale nie do analizy ruchu
- wygodny sposób tworzenia VPN i bezpiecznego łączenia sieci lokalnych przez internet

AH – *Authentication Header*

- Zapewnienie (tylko) integralności danych
- Uwierzytelnienie bez szyfrowania
- Minimalne algorytmy uwierzytelnienia:
  - HMAC-MD5
  - HMAC-SHA1
- Numer wśród protokołów IP: 51

AH – nagłówek uwierzytelniania

- **następny nagłówek** – 8 bitów; określa typ pakietu (np. IPv4, IPv6, TCP),
- **długość** – 8 bitów; długość całego AH w słowach 32-bitowych (minus 2),
- **zarezerwowane** – 16 bitów,
- **SPI** – 32 bity,
- **numer sekwencyjny pakietu** – 32 bity,
- **dane uwierzytelniające** – zmiennej długości.

Dane uwierzytelniające w nagłówku

- Dane uwierzytelniające są wyliczane dla całego pakietu IP, z poniższymi zastrzeżeniami.
- Dla pól nagłówka, których wartość może ulec zmianie w czasie przesyłania pakietu, na czas wyliczania przyjmowane są wartości zerowe.

Dane uwierzytelniające w nagłówku – IPv4

- W IPv4 za „zmienne” uważa się pola:
  - typ usługi (TOS),
  - czas życia (TTL),
  - przesunięcie fragmentu (FO),
  - suma kontrolna nagłówka,
  - niektóre opcje, w zależności od tego czy mogą się zmieniać.
- Jako „stałe” są natomiast traktowane adresy nadawcy i odbiorcy, co powoduje nie działanie AH przy translacji adresów IP (NAT itp.).
- Rozwiązaniem jest połączenie AH z trybem tunelowym ESP.

AH + ESP

Uwierzytelnienie można łączyć z szyfrowaniem na dwa sposoby:

- Szyfrowanie przed uwierzytelnianiem:
  - najpierw szyfrujemy pakiet,
  - potem dla całego wyliczamy nagłówek uwierzytelniający,
  - możliwy tryb transportowy (o ile po drodze nie ma translacji adresów IP) i tunelowy ESP.
- Uwierzytelnianie przed szyfrowaniem:
  - najpierw dla oryginalnego pakietu wyliczamy AH,
  - potem szyfrujemy wraz z całym pakietem,
  - możliwy tylko tryb tunelowy ESP (bo chcemy zaszyfrować też nagłówek AH).

AH + ESP

Uwierzytelnienie można łączyć z szyfrowaniem na dwa sposoby:

- Szyfrowanie przed uwierzytelnianiem:
  - najpierw szyfrujemy pakiet,
  - potem dla całego wyliczamy nagłówek uwierzytelniający,
  - możliwy tryb transportowy (o ile po drodze nie ma translacji adresów IP) i tunelowy ESP.
- Uwierzytelnianie przed szyfrowaniem:
  - najpierw dla oryginalnego pakietu wyliczamy AH,
  - potem szyfrujemy wraz z całym pakietem,
  - możliwy tylko tryb tunelowy ESP (bo chcemy zaszyfrować też nagłówek AH).