Jak funguje IPSEC ?

Vložil/a pan_r [1], 7 Prosinec, 2005 - 13:32

- Encryption [2]
- Networks & Protocols [3]
- Security [4]

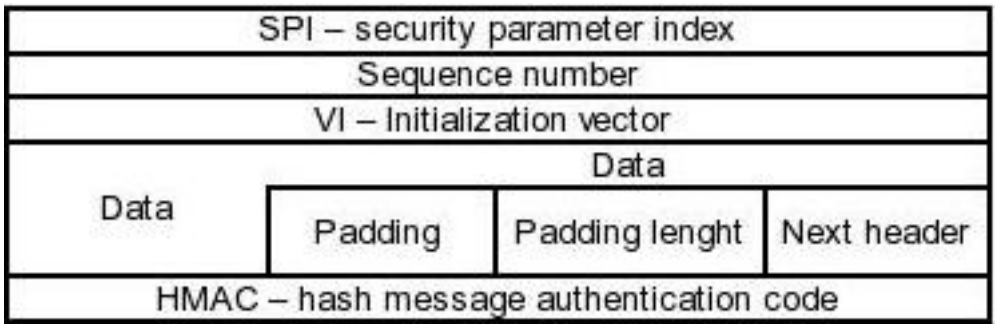
Článek zabývající se teorií protokolu IPSEC, jeho obsahem a popisem funkcí.

IPSEC – Internet Security Protocol

Jedná se o bezpečnostní mechanizmus, který je založen na kryptografické bázi. Je to jakési rozšíření týkající se třetí síťové vrstvy referenčního modelu ISO/OSI. Výzkum začal kolem roku 1992, nejprve byl vyvinut pro IP ve verzi 6 jehož je standardně součástí a poté byl začleněn i do ipv4 jako nepovinný. Nasazen do provozu byl roku 1995. IPSEC je jakási množina zahrnující řadu funkcí a protokolů jako jsou AH,ESP,IPCOMP,ISAKMP. Tento mechanizmus ovlivňuje každý paket, na který je aplikován. Může být použit s jakýmkoli protokolem postaveným nad IP výše. IPSEC podporuje řadu šifrovacích a hašovacích funkcí jako jsou SHA-1,SHA-2,MD5,...

Encapsulating Security Payload (ESP)

Jedná se o jeden z protokolů, který zajišťuje možnost ověření autentičnosti (authentication), podobně jako AH, ovšem ne v takové míře, ESP ověřuje jen data. Jeho stěžejní vlastnost je to, že zabraňuje odposlechu obsahu přenášených dat pomocí symetrických šifrovacích algoritmů, zpočátku jen NULL a DES, nyní podporuje silnějších, mezi něž patří např. 3DES, AES, Blowfish ... Další možnost využití má při ověření integrity.



1. ESP hlavička

ESP hlavička se skládá z několika částí:

První pole v ESP hlavičce specifikuje SPI - security parametr index. Tento index jednoznačně určuje SA - security association, která se použije při vybaleni obsahu paketu.

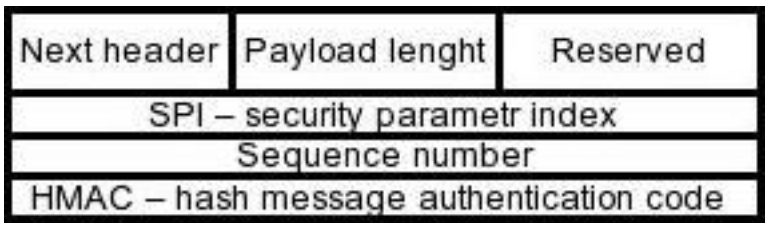
Druhé pole obsahuje sekvenční číslo, které se využívá jako obrana před replay útoky. Použití anti replay obrany je závislé na možnostech obou uzlu. Dle RFC dokumentu operační systém může, ale nemusí implementovat tuto funkci. Anti replay obrana může být použita pouze tehdy, je-li použita funkce na ověření autentičnosti (authentication).

Třetí pole určuje inicializační vektor, který je použit při šifrovacím procesu, v případě nepoužití by byl symetricky algoritmus oslaben vůči frekvenčnímu útoku.

Ve čtvrtém poli jsou obsažena data, která jsou potřeba v případě, že délka hlavičky není násobkem 32 bitů u ipv4 nebo u ipv6 násobkem 64 bitů doplnit (padding) potřebné bloky dat, protože IPSEC používá blokové šifry. Část pole označené jako padding lenght slouží k uložení délky doplněných bloků. Pole next header je ukazatelem na další hlavičku. Na závěr je přidán výsledek HMAC algoritmu zajišťující integritu dat. Tato funkce je aplikovaná na payload IP, hlavička je vynechána, protože v ní dochází při cestě paketu sítí ke změnám, které jsou dané charakteristikou síťové implementace.

Authentication Header (AH)

Umožňuje ověřeni pravosti (authentication) ve vetším rozsahu než ESP tím, že ověřuje větší množství polí paketu. Při obdržení paketu obsahujícího AH a kladně vyhodnoceným kontrolním součtem si můžeme být jisti ve dvou věcech a to, že paket nebyl modifikován (integrita) při cestě sítí, a že pochází od důvěryhodného zdroje (autentičnost). Oproti ESP nešifruje obsah. Podobně jako ESP nabízí možnost ochrany před tzv. replay útoky pomocí sekvenčního čísla, jehož hodnota se s každým odeslaným paketem inkrementálně zvětšuje.



2. AH hlavička

AH hlavička se skládá:

Celá hlavička je dlouhá 24 bajtu. První část pole má bajt jeden a je ukazatelem na další hlavičku. Druhá část pole udává délku payloadu pomocí jednoho bajtu a poslední dva bajty jsou rezervované. V tunel módu, kde je zapouzdřen celý IP datagram, má celé pole hodnotu 4 bajty. Pokud se jedna o transport, mód má hodnotu plných 6 bajtu.

Další pole obsahuje 32 bitů dlouhé číslo Security Parameter Index (SPI). Tento index určuje SA (security association) stejně jako u ESP.

Třetí pole je 32 bitové sekvenční číslo sloužící jako anti replay ochrana . Konec hlavičky je tvořen 96 bity kódovým hašem, který zaručuje integritu paketu.

Původně byl protokol AH určen jen pro kontrolu autentičnosti a ESP pro šifrování. Ostatní funkce byly dodatečně přidány dle potřeb. Implementace nám umožňuje použití různých variací AH a ESP.

Aby bylo možné zapouzdření a vybalení paketu s ESP nebo AH je potřeba tajný klíč, algoritmus a další udaje Tyto informace jsou uloženy v Security Association (SA).Daná SA může být použita vždy jen pro jeden směr (input, output) a pro jeden protokol AH, ESP nikoliv pro oba zároveň. Implementačně je kombinace možná , proto je v takových případech zapotřebí tzv. SA bundle.

Jednotlivé SA jsou uloženy v centrální databázi zvané Security Assocciation Database (SAD).

security association obsahuje:

* zdrojovou a cílovou IP adresu nebo rozsah adres
* IPSEC protokol (AH nebo ESP),IPCOMP
* algoritmus, klíč

* security parameter index (SPI) číslo, které jednoznačně identifikuje SA
* IPSEC mód (tunel nebo transport)
* velikost posuvného okna (u anti-replay obrany)
* životnost SA, klíče

SA obsahuje pouze informace o tom, jak trafik chránit, nikoliv však jaký. Tyto specifikace jsou obsaženy v Security Police (SP), jejich seznam je sdružen v Security Police Database (SPD), Tato databáze si udržuje ukazatel na SAD.

SP obvykle udává tyto parametry:

* Zdrojovou a cílovou adresu. V transportním módu se tyto adresy shodují s adresou uvedenou v SA, na rozdíl od tunel módu, kde se můžou lišit!
* Chráněný protokol a port. Ne všechny implementace dovolují definovat konkrétní protokol. V těchto případech jsou chráněny všechny pakety pocházející z uvedených IP adres.
* ukazatel na SA
* priorita politiky (use,require)

ISAKMP/IKE

Protokoly AH a ESP potřebují pro svou činnost několik SA (pro daný směr a protokol), klíč, algoritmus a další. Tyto parametry je možné nastavit manuálně. Ovšem klíče a šifrovací algoritmus musí být sdílený mezi články ve VPN síti a výměna klíčů pro symetrické šifry je kritický problém. Proto byl vynalezen způsob pro automatické vyjednání klíčů a dalších podrobností zajištujících bezpečné spojení a to pomocí Internet Security Association Key Management (ISAKMP), který je implementačně nezávislý tím , že umožňuje pro výměnu použít libovolný protokol. ISAKMP umožňuje zabezpečené spojení od začátku do konce relace včetně výměny klíčů pomocí Internet Key Exchange (IKE) protokolu, který řeší mnoho problémů týkajících se výměny klíčů.

Tento protokol má dvě fáze:

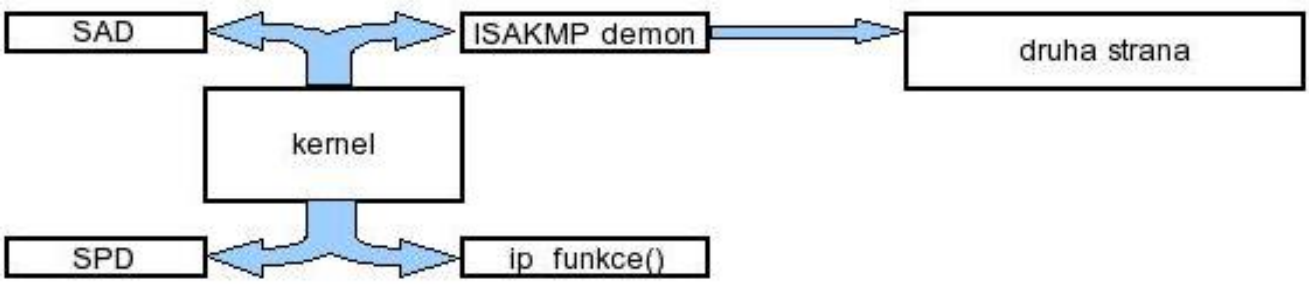
První fáze stanovuje ISAKMP SA (SA v kontextu tohoto protokolu), aby byl chráněn proces výměny a dohod. Bezpečnost v první fázi je zaručena pomocí algoritmu (RSA) a X.509 certifikátu.

Tato fáze podporuje dvě metody:

* hlavní mód (main mode)
* agresivní mód (aggresive mode)

Oba módy zaručují nastavení ISAKMP SA. Ovšem agresivní mód je metoda navržená k tomu, aby zaručila společný přenos v jedné zprávě SA, klíče a důvěryhodnost informace vztahující se k datům. Touto kombinací zkracuje počet přenosu na úkor toho, že neumožňuje ochranu identity, která je právě z technického hlediska nemožná. Agresivní mód má využití pouze při malé šířce pásma.

V druhé fázi si obě strany vymění potřebná data a dohodnou se na vzájemně akceptovatelných podmínkách SA. Tajný symetrický klíč je vyměněn za použití Diffiho-Hellmanova schématu pro výměnu klíče.



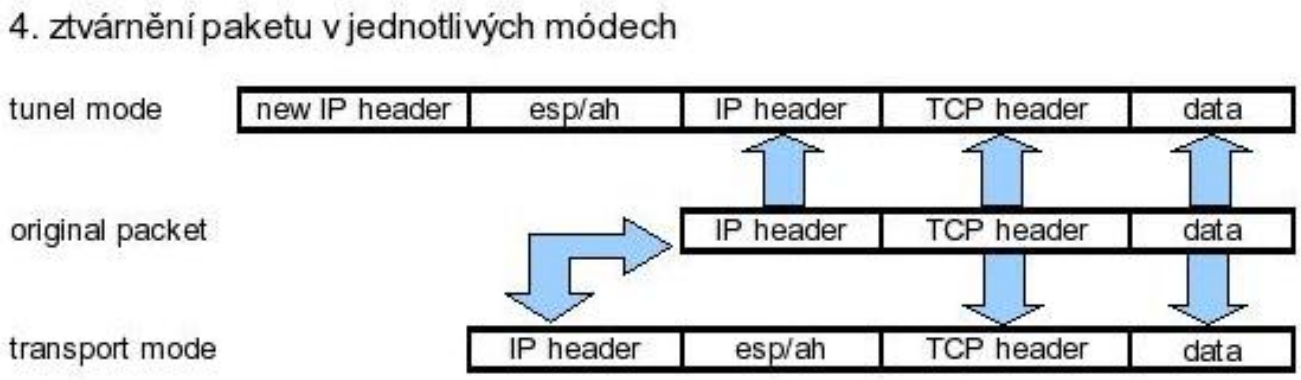
3. jedna z implementací chránící paket pomoci IPSEC

Před opuštěním paketu kernel zjistí z SPD jak má s paketem zacházet v případě, že SPD obsahuje ukazatel na příslušnou SA , kernel aplikuje danou politiku a odešle. V případě , že SPD neobsahuje ukazatel na SA , je kernelem zavolán ISAKMP démon pro její vyjednání. ISAKMP démon vyjedná danou SA, kterou uloží do databáze, kernel použije a aplikuje na paket a odešle v případě, že vyprší limit při dotazování ISAKMP démona na SA druhé stany, kernel paket zahodí. Takto je to implementováno v systémech FreeBSD a NetBSD.

Druhou možností je použití démona, který se stará o výměnu klíčů a vyjednání SA, nedostává od kernelu požadavky na vyjednání SA. V případě, že v SPD není ukazatel na příslušnou SA, paket je zahozen. Takto je to implementováno v OpenBSD.

IPSEC podporuje dva režimy:

* transportní (transport mode) – slouží například k propojeni dvou uzlů
* tunel (tunnel mode) – využití mezi dvěma VPN bránami



Rozdíly mezi módy jsou v aplikaci. V tunel módu je paket plně zapouzdřen včetně IP hlavičky uzlu. V transport módu jsou zapouzdřena jenom data z IP datagramu a to tak , že se vloží hlavička ESP nebo AH mezi hlavičku IP a payload.

URL článku: https://security-portal.cz/clanky/jak-funguje-ipsec

Odkazy:
[1] https://security-portal.cz/users/panr
[2] https://security-portal.cz/category/tagy/encryption
[3] https://security-portal.cz/category/tagy/networks-protocols
[4] https://security-portal.cz/category/tagy/security