IPSEC

Bronislav ŠOPÍK, Master Degree Programme (5)
Dept. of Computer Systems, FIT, BUT
E-mail: xsopik00@stud.fit.vutbr.cz

Supervised by: Dr. Cvrček Daniel

ABSRACT

IPSec is an internet standard of a protocol providing data authentication, integrity and confidentiality for data that are transferred between two peers across the network. IPSec provides data security at the packet level.

1 ÚVOD

IPSec je definován jako otevřený standard s cíle zvýšit zabezpečení privátní, bezpečné komunikace přes IP (Internet Protocol) sítě pomocí kryptografické bezpečnostní služby. IPSec podporuje integritu dat, utajení dat, ověření původu dat a opakovanou ochranu, na síťové úrovni. Jelikož je IPSec integrovaný v internetové vrstvě (vrstva 3 v ISO/OSI modelu), tak transparentně podporuje všechny protokoly v TCP/IP, a není tedy třeba ani konfigurovat bezpečnost samostatně pro jednotlivé aplikace využívají TCP/IP.

IPSec poskytuje ochranu proti:

- síťovým útokům z nedůvěryhodných počítačů, útoky mohou mít za následek odepření služby aplikací, služeb nebo sítě
- poškození dat
- krádeži dat
- uživatelsky-doporučeným krádežím
- kontrole nad servery, jinými počítači a sítí

2 IPSEC AH A ESP PROTOKOLY

IPSec protokoly, Authentication Header (AH) a Encapsulation Security Payload (ESP), poskytují data a shodnou ochranu pro každý IP paket. AH protokol je IPSec protokol, který poskytuje autentizaci původu dat, integritu dat a anti-opakující se ochranu pro celý paket (IP hlavičku a data přenášená v paketu, kromě polí v IP hlavičce, která je povolena měnit při přenosu). AH může být použit samostatně nebo v kombinaci s ESP protokolem nebo v IPSec tunelovém módu. Tunelový mód je používán k ochraně síť ↔ síť (brána ↔ brána) provozu mezi sítěmi, stejně jako jednotlivých klientů. Odesílací brána zapouzdří celý IP datagram a

přidá novou IP hlavičku a pak zabezpečí nový paket jedním z IPSec bezp. protokolů.

ESP protokol je IPSec protokol, který poskytne utajení dat, autorizaci původu dat, integritu dat a Anty-opakovací ochranu pro ESP provoz. ESP protokol může být použit samostatně v kombinaci s AH protokolem ne v IPSec tunelovém módu.

IPSec AH A ESP PROTOKOLY V TRANSPORTNÍM MÓDU IPSec protokoly poskytnou data ochrany pro každý paket přidáním jejich vlastní hlavičky bezpečnostního protokolu do každého paketu. Tato část popisuje jak AH a ESP chrání IP pakety když je IPSec použita v transportním módu.

IPSec v transportním módu používáme k ochraně provozu v end-to-end komunikacích (např. komunikace mezi klientem a serverem). IPSec v transportním módu také můžeme použít pro základní filtrování paketů (statické povolení nebo zakázání provozu na kombinaci adres zdroje a cíle, na IP protokolu a na TCP a UDP portech). IPSec transportní mód zapouzdří originální IP náklad s IPSec hlavičkou (AH či ESP).

IPSec AH a ESP PROTOKOLY V TUNEL MÓDU IPSec tunel mód primárně chrání provoz proti sítím, jejichž spojení prochází přes nedůvěryhodnou cestu. Tunel mód lze užít například k:

- Ustanovení brána ↔ brána tunelu mezi sítěmi, které nepodporují L2TP/IPSec VPN (Virtual Private Network) spojení.
- Ochraně provozu end-to-end, pokud jeden z konců nepodporuje IPSec. Je možné zabezpečit data k počítači, který podporuje tunel mód a je umístěn bezprostředně před počítačem, který IPSec nepodporuje.

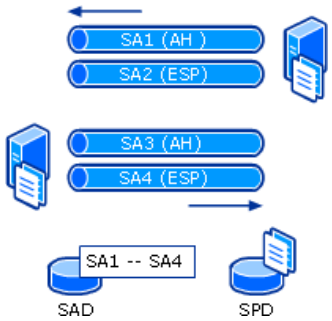
S tunel módem je celý IP paket zapouzdřen s AH nebo ESP hlavičkou a přidanou IP hlavičkou. IP adresy vnější IP hlavičky jsou koncové body tunelu a IP adresy v zapouzdřené hlavičce je finální zdrojová a cílová adresa.

Můžeme použít oba ESP a AH protokoly v kombinaci, když tunel poskytuje utajení pro IP paket procházející tunelem a integritu a autentizaci pro celý paket.

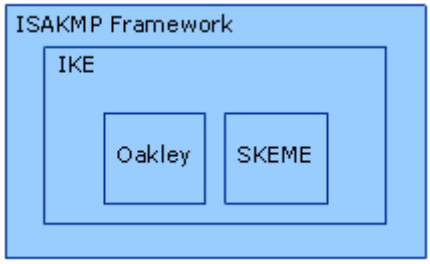
3 BEZPEČNOSTNÍ ASOCIACE

Bezpečnostní asociace (BA) jsou kombinací vzájemně kompatibilních politik a klíčů. Politiky definují jaké bezpečnostní služby, mechanismy a klíče se musí použít k ochraně komunikace mezi klienty IPSec. Každá BA je pro jednosměrné, jednoduché spojení. Jelikož jsou BA definovány jenom pro jednosměrnou komunikaci, každá IPSec sezení vyžaduje dvě BA (odchozí a příchozí data).

BA pro IPSec-bezpečnou komunikaci požadují dvě databáze: security policy database (SPD) a security association database (SAD). SPD uchovává bezpečnostní požadavky nebo politiky potřebné pro ustanovení BA. SPD je používána při zpracování příchozích i odchozích paketů. IPSec kontroluje vstupní pakety pro dodržení bezpečnostní specifikací. Odchozí pakety jsou zabezpečeny opět podle lokálně definované politiky. SAD obsahuje parametry pro všechny aktivní BA. Obrázek 1 ukazuje spojení mezi BA, SPD a SAD.



Obr. 1: *BA, SPD a SAD Architektura*

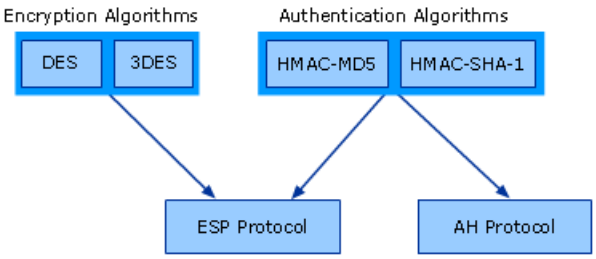


Obr. 2: *Architektura protokolů ISAMKP, IKE, Oakley a SKEME*

IPSec vyžaduje podporu správy BA a správy klíčů. Internet Security Association and Key Management Protocol (ISAKMP) definují kostru pro autorizaci a výměnu klíčů s poskytnutím procedur pro vyjednání, ustanovení, změnu a mazaní BA. Nedefinuje však konkrétní výměnu klíčů: jedná se jen o kostru protokolu.

IPSec umožňuje jak manuální, tak i automatickou správu BA a klíčů. IKE je standardní protokol automatické správy klíčů pro IPSec. Je to hybridní protokol, který spojuje části z Oakley protokolu pro výměnu klíčů a SKEME protokolu klíčových technik. Obrázek 2 ukazuje vztahy mezi ISAMKP, IKE, Oakley a SKEME protokoly.

Dva autorizační nebo klíčové hash algoritmy HMAC-MD5 (Hash Message Authentication Code - MD5) a HMAC-SHA-1 jsou užívány s oběma AH a ESP protokoly. DES a 3DES kódovací algoritmus je užíván s ESP. Obrázek 3 ukazuje vztahy mezi autorizačními a kódovacími algoritmy a AH a ESP protokoly.



Obr. 3: *IPSec Protokoly a algoritmy pro autorizaci a kódování*

4 DALŠÍ PRÁCE

V rámci diplomové práce se budeme dále věnovat právě správě klíčů, konkrétně z pohledu implementací a jejich vzájemné interoperabilitě. Pro tyto účely jsem již začali provádět praktické testy. Uvědomujeme si, že IPSec je životně závislý právě na správě klíčů, která ovšem standardem není nijak pokryta.

LITERATURA

[1] IEFT: IPSec standard - http://www.ietf.org/html.charters/ipsec-charter.html