

IPsec

použití v praxi

Vladimír Kotal <vlada@openbsd.cz>

Motivace

- potřeba bezpečnostních technologií
 - autentizace
 - kontrola integrity
 - konfidentialita
 - kontrola přístupu

Co chceme

- zabezpečit 3. vrstvu transparentně
- VPNs
 - host–host (transport mode)
 - host–gw
 - gw–gw (tunnel mode)
- správa klíčů seprátně (IKE)
- adaptabilní (výběr šifer)

Protokoly za IPsec

- IETF (ipsec, ipseckey, ipsps WGs)
 - AH (Authentication Header)
 - ESP (Encap. Security Payload)
 - ISAKMP (IPsec key management protocol)
 - IKE (Internet Key Exchange)

Security architecture for IP

- RFC 2401 (dnes bis-00)
 - zavedení pojmů, jejich zpracování
 - SA, SPD, SAD
 - IP traffic processing
 - PMTU a IPsec

Security Association

- SA = (SPI, DstAddr, Sec. proto)
 - -> jednoznačná identifikace
- pouze pro jeden směr
- buď pro AH nebo ESP (oba => 2xSA)

AH (Auth. header)

- RFC 2402
- ochrana
 - identity
 - integrity
 - proti replay útokům
- IP | AH = { NextHdr, paylen, SPI, seq#, ICV }
- AH samotná, s ESP nebo tunnel mode

AH header location

- IPv4
 - za IP hl., před hl. vyššího proto (TCP), před příp. IPsec hlavičky
 - IP | AH | TCP | Data
- IPv6
 - za hop-by-hop, frag, routing hl.
 - IP | h-b-h,fr,rout,dest* ext. | AH | dest* ext. | TCP | Data

Sémantika AH

- IPv4 & IPv6
 - transport mod – autentizováno vše až na mutable pole v IP hdr
 - tunel mod – autent. vše až na mutable pole ve vnější IP hdr

AH a crypto algoritmy

- ICV computation
 - závisí na SA (alg.)
 - unicast: MACs (DES) nebo 1way hash fce (MD5, SHA1)
 - multicast: 1way h.fce + assym sig. alg.

ESP (Encr. sec. payload)

- RFC 2406
- to samé co AH + konfidentialita (ale!)
- z pohledu útočníka:
 - $IP | ESP = \{ SPI, seq \#, data \}$
- on the wire format:
 - $IP | ESP | TCP | ESP \text{ trailer} | ESP \text{ auth.}$
 - $ESP = \{ SPI, seq\#, payload, padding, auth. \}$

ESP header location

- transport
 - IPv4 { IP | ESP | TCP | payload | ESP trailer | ESP auth. }
 - IPv6 { IP | h-b-h,fr,rout,dest* ext. | ESP | dest* ext. | TCP | Data | ESP trailer | ESP auth. }
- tunnel mode – analogicky

Sémantika ESP

- tunnel mode
 - autentizováno
 - { ESP hdr | (orig IPhdr*) | TCP | Data | ESP trailer }
 - šifrováno
 - { (orig IP hdr*) | TCP | Data | ESP trailer }

Kombinace AH + ESP

- pouze jeden alg. pro SA
- SA bundle = sekvence SA
- mnoho různých kombinací
- bundles
 1. transport adjacency
 2. iterated tunneling
 3. kombinace (1) a (2)

SPD, SAD (I)

- in kernel struktury
- SAD
 - typ (AH, ESP)
 - algoritmus (např. hmac-sha1)
 - src/dst addr
 - zivotnost klicu
 - zivotnost samotneho SA
 - sekvencni cislo, anti replay win, ...

SPD, SAD (2)

- SPD
 - určuje jaké IPsec služby pro jaké datagramy
 - outbound, inbound
 - SPD entry je tzv. selektor (src/dst IP addr/port range, protocol, IPv6 mobility header type range, ICMP msg type range, sensitivity level (IPSO/CIPSO labels))
 - SPD entry obsahuje ukazatele do SAD

ISAKMP/IKE

- RFC 2408
- manuální výměna klíčů SA nestačí (anti-replay, konfigurovatelnost)
- ISAKMP používá protokoly pro výměnu klíčů, preferovaný je IKE
- vyjednat lze parametry SA, použití certifikátů, ...
- Phase 1 (bezpečný kanál)
- Phase 2 (vyjednání a ustavení SA)

ISAKMP (2)

- ISAKMP has SAs too !
 - pro ochranu trafficku mezi ISAKMP servery (phase 1)
- payloads (SA, transform, key exchange, identification, hash, delete)
- exchanges (base, identification, aggressive, auth., informational)

Obecné schema

1. bootstrap ISAKMP SA (main-aggressive mode)
2. use Quick mode v rámci ISAKMP SA pro vyjednání (AH nebo ESP) SA
3. používej SA pro komunikaci než vyprší, rekeying

Praxe

- různé implementace
 - IPsec
 - KAME, Keromytis
 - IKE/ISAKMP
 - isakmpd, raccon, FreeS/WAN

Net/FreeBSD

- SPD v kernelu (`setkey(3)`)
- kernel se vyžaduje od userlandu ustavení SA
- racoon: hierarchický config file

setkey(3)

- SPD, SAD management

- `setkey -c << EOF`
`flush;`
`spdflush;`

```
spdadd $my_addr 0.0.0.0/0 any -P out ipsec  
        esp/tunnel/$my_addr-$gateway/use;  
spdadd 0.0.0.0/0 $my_addr any -P in ipsec  
        esp/tunnel/$gateway-$my_addr/use;  
EOF
```

Session 1 (static keys)

- IPsec v IPv6 povinně, ale...
- AH example
 - `fec0::1 <-> fec0::2`

Session II (dynamic keying)

- racoon type config
- 192.168.0.1 <-> 192.168.0.2
- remote anonymous # IKE phase 1
{
 proposal {
 # parametry pro návrh SA
 }
}
sainfo anonymous # IKE phase 2
{
 # SA
}

Novinky

- NAT/firewall traversal
- IKE support for SCTP
- nové šifry (AES, SHA-2)

Konec