14 - IPSec

Sicurezza all livello applicazione:

- pros: disegnato per le richieste dell'applicazione
- cons: richiede molteplici meccanismi di sicurezza
  Sicurezza al livello trasporto
- pros: interfaccia comune a servizi di sicurezza
- cons: potrebbe richiedere modifiche minori alle applicazioni
  Sicurezza al livello rete
- pros: funziona anche con applicazioni security-ignorant
- cons: potrebbe richiedere modifiche modifiche all'OS

IPSec è una famiglia di protocolli di IETF per rendere sicure le applicazioni su internet
Debolezze e attacchi IP:

- mancanza di integrità - ip spoofing
- mancanza di autenticazione - ip spoofing
- mancanza di confidenzialità - packet sniffing

I protocolli IPSec sono stati progettati sia per IPv4 (supporto opzionale) che per IPv6 (supporto obbligatorio)
Protocollo basato su extension headers
Specificazione complessa
Protocolli base: AH, ESP, IKE

IPSec applicazioni

- VPN in internet
- accesso sicuro e provato tramite internet
- stabilizzazione di connettività extranet e intranet con partners
  - comunicazioni sicure con altre organizzazioni garantendo autenticazione e confidenzialità fornendo un meccanismo di scambio chiavi
- migliorare la sicurezza di applicazioni di alto livello
  - ecommerce

Benefici

- Quando applicato a un firewall o router provvede forte sicurezza su tutto il traffico che attraversa il perimetro
  - nessun impatto con il traffico interno
- trasparente alle applicazioni (sotto TCP/IP)
- nessun bisogno di cambiare software di un utente o sistema quando IPSec è implementato nel firewall o router
- trasparente agli utenti finali
  - nessun bisogno di addestrare gli utenti ai meccanismi di sicurezza

Protocolli

- authentication header (AH) per integrità dei messaggi e autenticità
- Encapsulating security payloads (EPS), per confidenzialità (combinato con authentication/encryption)
- Internal security e Key Management Protocol (IKE), per scambio chiavi
- AH/ESP sono applicati ogni pacchetto
  - supportano due modelli di utilizzo:
    - transport mode
    - tunnel mode

Transport mode

- Provvede protezione ai protocolli di livello superiore (IP packets payload)
- normalmente usato per end to end communication
  AH in transport mode
- autentica l' IP payload e porzioni selezionate dell' IP header
  ESP in transport mode

- cripta e opzionalmente autentica l'IP payload
- IP header non protetto

Tunnel mode

- provvede protezione per tutto l'IP packet
- normalmente usato per le comunicazioni "gateway to gateway"
  Funzionamento:
- AH/ESP headers sono aggiunti all'IP packet
- l'intero pacchetto è trattato come payload di un nuovo IP packet uscente con un nuovo IP header
  I pacchetti viaggiano attraverso un tunnel
- nessun router nella strada è in grado di esaminare il pacchetti originale

Transport mode

- basso overhead
- alcune informazioni possono essere sniffate (es utente che si connette all'host)
  Tunnel mode
- più sicuro
- entità intermedie
- alto overhead

Tunnel mode esempio

- Host A vuole comunicare con l'host B sulla rete N_B
- A genera un pacchetto con A come sender e B come destinazione
- Il pacchetto è instradato al security gateway (firewall con IPSec) della rete N_A
- Il security gateway incapsula il pacchetto in un IP header uscente con N_A come sender e N_B come destinazione
- Il pacchetto sicuro viene instradato dalla rete pubblica (internet) fino al security gateway della rete N_B
- il security gateway estrae, decripta e autentica il pacchetto originale
- Il pacchetto originale è strato instradato e consegnato a B nella rete N_B