IPsec

Mahalingam Ramkumar
IPSec Goals

- Provide end-to-end security for IP payload
- SSL/TLS secures only the transport payload
  - only TCP HTTP payload originally
  - SSL/TLS can not be used for UDP
- SSL/TLS needs application to be rewritten
  - How about legacy apps?
- If OS supports IPSec at both end-points, all IP traffic can be encrypted /authenticated
- Routers do not have to be aware of IPSec
End-to-End Layers in the Protocol Stack

Unprotected IP packet

SSL Protects only Application Data

IPSec Protects entire IP payload in Transport Mode

IPSec Protects entire IP packet in Tunnel Mode

IPSec only, Transport mode

IPSec only, Tunnel mode
While routers do not care..
NATs do :(  
  • (Therein lies the main issue with IPSec)
Created as inherent part of IPv6
Nobody thought that IPv4 will still be used decades later
Later made compatible with IPv4 too
New IP protocol definition (51) in IP header for IPv4
Just another extension header in IPv6
IPv4 Header
Optional Headers – 1) Hop-by-Hop options 2) Routing Header 3) Fragment Header 4) AH  5) ESP  6) Dest. Options
IPsec

- IP Security (RFCs 2401, 2402, 2406)
- Transparent to higher (transport / application) layers
- Provides a virtual connection between two IP hosts
  - Security Association (SA)
  - Different SAs for different type of traffic flowing in different directions
- Not a single protocol
  - Provide algorithms + general framework
  - Up to hosts to choose appropriate methods
Applications

Secure branch office connectivity over the Internet
Secure remote access over the Internet
Establishing extranet and intranet connectivity with partners
Enhancing electronic commerce security
IPSec VPNs
Keep in mind end-to-end IPSec support may not be available
IPSec gateways?
IPsec Features

- Multiple services
  - Access Control
  - Data Integrity
  - Authentication
  - Protection from replay attacks
  - Confidentiality
  - Limited traffic flow confidentiality
- Multiple Algorithms
  - Not explicitly specified (can be negotiated / changed)
- Multiple Granularity
  - Ability to use IPSec for
    - Single TCP connection
    - All traffic between a pair of hosts
    - All traffic between two routers
Primary Modes and Services

Modes
- Transport Mode
- Tunnel Mode

Services
- Authentication only (AH – Authentication Header)
- Privacy (ESP – Encapsulated Security Payload)
IPSec Components

- Security Association Database (SAD)
  - A database of SAs indexed by SPI
- Security Policy Database (SPD)
  - A *rules* database that enables determination of SPI for outgoing packets
    - Rules that govern
      - Should IPSec should be used for this packet?
      - If so, which mode (trans/tunn)? Service? (ESP/AH)? What is the SPI?
- ISAKMP
  - Protocols for establishing SAs stored in SAD
Security Associations (SA)

- A one way relationship between a sender and a receiver.
  - Sequence number, algorithms, keys, lifetimes
- Uniquely identified by three parameters:
  - Security Parameter Index (SPI) (database index)
  - IP Destination address
  - Security Protocol Identifier (AH/ESP)
## AH / ESP in Transport / Tunnel Modes

<table>
<thead>
<tr>
<th></th>
<th>Transport Mode SA</th>
<th>Tunnel Mode SA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AH</strong></td>
<td>Authenticated IP payload and selected portions of IP header and IPv6 extension headers</td>
<td>Authenticated entire inner IP packet plus selected portions of outer IP header</td>
</tr>
<tr>
<td><strong>ESP</strong></td>
<td>Encrypts IP payload and any IPv6 extension header</td>
<td>Encrypts inner IP packet</td>
</tr>
</tbody>
</table>
Before AH
Transport Mode (AH)
Tunnel Mode (AH)
Authentication Header

Provides support for data integrity and authentication (MAC code) of IP packets. Guards against replay attacks. Sequence number incremented with each packet.

![IPSec Authentication Header diagram](image)

Figure 6.3 IPSec Authentication Header
End-to-End vs End-to-Intermediate Authentication
ESP (Encapsulating Security Payload)

ESP provides confidentiality services

![ESP Format Diagram]

*Figure 6.7 IPSec ESP Format*
Encryption and Authentication Algorithms

Encryption:
  Three-key triple DES
  RC5
  IDEA
  Three-key triple IDEA
  CAST
  Blowfish

Authentication:
  HMAC-MD5-96
  HMAC-SHA-1-96
ESP Encryption and Authentication

(a) Transport Mode
ESP Encryption and Authentication

(b) Tunnel Mode
Key Management

- ISAKMP (Internet Security Association Key Management Protocol)
  - Specifies protocols – formats, negotiation of security attributes
- Oakley Key Determination Protocol commonly used
  - Oakley – key exchange protocol: based on Diffie-Helman + features for addressing
    - Clogging attacks (addressed using cookies)
    - Replay attacks (nonces)
    - Secure exchange of public keys
      - Authenticated DH to thwart M-I-M attacks
ISAKMP

(a) ISAKMP Header

(b) Generic Payload Header

Figure 6.12 ISAKMP Formats
Combinations of SAs

SA
- Proposal (protocol to use – AH / ESP)
- Transform (transforms – algorithms)
- Key Exchange
- Identification (of communicating entities)
- Certificate
- Certificate Request
- Signature
- Nonce
- Notification (eg. delete SA)