Module 10
IPSec

Dr. Natarajan Meghanathan
Professor of Computer Science
Jackson State University, Jackson, MS 39232
E-mail: natarajan.meghanathan@jsums.edu
IPSec

- Before two machines send the messages using their IP addresses, they have to establish an IPSec SA (Security Association).
- IPSec SA
  - The two hosts A and B exchange their public-key certificates (that has their IP address and public-key certified).
  - All further communication are encrypted with the public key of the receiver (so that it can be decrypted only by the receiver with its private key).
  - The two hosts A and B negotiate on the encryption and keyed-hashing algorithms to use for confidentiality and integrity + authentication respectively.
  - The two hosts establish a session key (for integrity and authentication) using the public-key encryption based Diffie-Hellman key exchange mechanism.
  - Using the session key, the two hosts can then establish a secret key for confidentiality in communication.
  - IPSec SA is unidirectional: If machines A and B want to send messages back and forth, they have to establish an IPSec SA in each direction.
  - An IPSec SA from A to B is said to be outbound at A and inbound at B.
  - An IPSec SA from A to B is identified by the tuple <SPI, IP address of A> where SPI is the Security Parameter Index value, locally unique at A. The combination of the SPI with the IP address of the host makes the tuple globally unique.
IPSec

- The IPSec header is inserted in between the IP header and transport layer header. There is no need for support from any higher layers.

<table>
<thead>
<tr>
<th>IP Header</th>
<th>IPSec Header</th>
<th>TCP/ UDP Header</th>
<th>Data</th>
</tr>
</thead>
</table>

- IPSec headers:
  - **Authentication Header (AH):** used for integrity + authentication
  - **Encapsulated Security Payload Header (ESP):** used for confidentiality, integrity + authentication.

- IPSec Modes:
  - **Transport Mode:** When IPSec SA is directly established between the two end hosts. Message is secure all the way from the source host to the destination host
  - **Tunnel Mode:** When IPSec SA is established between the gateway routers of the two end hosts. Message is not secure in the source and destination networks. Need to use IP-in-IP encapsulation to encapsulate the IP datagram with the IP addresses of the two ultimate end hosts.
Typical IPSec Scenarios

**Transport Mode**

<table>
<thead>
<tr>
<th>IP Header</th>
<th>IPSec Header</th>
<th>TCP Header</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP _S, IP _D</td>
<td>SA: S -- D</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Tunnel Mode**

<table>
<thead>
<tr>
<th>IP Header</th>
<th>IPSec Header</th>
<th>IP Header</th>
<th>TCP Header</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP _R1, IP _R3</td>
<td>SA: R1 – R3</td>
<td>IP _S, IP _D</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IP4 Datagram with Authentication Header

Original IPv4 Datagram
- ver
- hlen
- TOS
- pkt len
- ID
- flgs
- frag offset
- TTL
- proto=TCP
- header checksum
- src IP address
- dst IP address
- TCP header (proto = 6)

New IPv4 Datagram
- ver
- hlen
- TOS
- pkt len + AH size
- ID
- flgs
- frag offset
- TTL
- proto=AH
- header checksum
- src IP address
- dst IP address
- SPI (Security Parameters Index)
- Sequence Number
- Authentication Data
- (variable length, padded if required)
- TCP header (proto = 6)
- TCP payload

Protected by AH Auth Data

Source: http://unixwiz.net/techtips/iguide-ipsec.html
IP4 Datagram with ESP Header

Original IPv4 Datagram

<table>
<thead>
<tr>
<th>ver</th>
<th>hlen</th>
<th>TOS</th>
<th>pkt len</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>flgs</td>
<td>frag offset</td>
<td></td>
</tr>
<tr>
<td>TTL</td>
<td>proto=TCP</td>
<td>header cksum</td>
<td></td>
</tr>
<tr>
<td>src IP address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst IP address</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TCP header (proto = 6)

TCP payload

New IPv4 Datagram

<table>
<thead>
<tr>
<th>ver</th>
<th>hlen</th>
<th>TOS</th>
<th>Pkt len + ESP Hdr len</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>flgs</td>
<td>frag offset</td>
<td></td>
</tr>
<tr>
<td>TTL</td>
<td>next=ESP</td>
<td>header cksum</td>
<td></td>
</tr>
<tr>
<td>src IP address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst IP address</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ESP

SPI (Security Parameters Index)
Sequence Number

TCP header +
TCP Payload (variable)

Encrypted Data
Authenticated Data

Source: http://unixwiz.net/techtips/iguide-ipsec.html