IPsec as a Real-Time Protocol

A real-time protocol is one where parties negotiate interactively to authentication each other and establish a session key.
- The conversation protected using the session key is called security association.
- Examples: IPsec, SSL/TLS, SSH
  - Public key based.

Security at Layer 4 vs. 3

Pros and Cons

Security at layer 4 (SSL/TLS/SSH)
- No need to change OS
  - Applications have to be modified
  - No way to tell TCP layer whether newly received data is bogus or real
  - Such as a sequence number attack.

Security at layer 3 (IPsec)
- Transparent to applications
  - OS needs to modified
  - Security is in terms of IP addresses
  - IPsec authentication cannot distinguish between users.

IPsec User Model

- Alice and Bob sets up a secure channel
  - Called Security Association
- Then rely on IPsec to protect the channel.

What does IPsec Accomplish?

- Encrypted traffic
- Connectionless Integrity
- Anti replay
- More secure authentication based on source IP address
- Enforced access control based on a policy database
- Similar to set up two firewalls between two ends.
Main Pieces

- **AH & ESP**
  - IP header extensions for carrying cryptographically protected data
- **IKE**
  - A protocol for establishing security associations (SA) and establishing session keys
  - Not required for IPsec but recommended
    - IKE also supports manual SAs/keying

---

IPsec Deployment

- Individual host: an end system can implement its own protection end-to-end or hop-by-hop
- Host community: a single security gateway (e.g., a firewall) can protect an entire domain of hosts
- Pairings: host-to-host, host-to-gateway, gateway-to-gateway
  - Or combined

---

Security Association

- An unidirectional cryptographically protected connection
  - Communication between Alice and Bob consists of two SAs, one for each direction
- Each end remembers:
  - Id of the other end
  - A cryptographic key
  - Sequence number currently being used
  - Cryptographic services being used
    - Integrity only, encryption only, or both
    - Which cryptographic algorithms

---

Security Association Database

- A security association database (SAD) is used to remember those info above for every active security association
  - Indexed by security parameter index (SPI)
- Thus an IPsec-capable node knows how to communicate with a given destination
  - A packet from Alice to Bob should tell Bob the SPI value that Bob can use to locate the Alice-Bob SA entry in his SAD

---

AH & ESP

- **AH** provides integrity protection
  - For payload and some fields in IP header
- **ESP** provides encryption and/or integrity protection
  - For payload
  - The encryption algorithm can be "null" or others

---

![Diagram: Overview of IPsec](image.png)
A Side Effect of IPsec on Firewall

- If a packet is protected using ESP, a firewall won’t be able to inspect the payload of the packet
  - A firewall has even no idea whether the payload is encrypted or not
    - Recall the encryption algorithm could be “null”

Two IPsec Modes

- Transport mode
- Tunnel mode

Transport Mode

- IP header
- rest of packet

Tunnel Mode

- IP header
- rest of packet
- New IP header
- IPsec
- IP header
- rest of packet

Mode Selection

- Transport mode is most logical when applying IPsec for end-to-end communication
- A tunnel mode is good for firewall-to-firewall, or end-to-firewall

An Example of Using Tunnel Mode

- IP: src=F1, dst=F2
- ESP
- IP: src=A, dst=B
Format of IPsec-Protected Packets

• A field in the IP header points to AH header or ESP header
  – “Protocol” field in IPv4
  – “Next header” field in IPv6
  
  – ESP = 50
  – AH = 51
  – (TCP = 6, UDP = 17)

IPv4 Datagram Format

<table>
<thead>
<tr>
<th>Field</th>
<th>Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP protocol version</td>
<td>1</td>
</tr>
<tr>
<td>header length</td>
<td>1</td>
</tr>
<tr>
<td>“type” of data-max number</td>
<td>2</td>
</tr>
<tr>
<td>remaining hops (decremented</td>
<td>4</td>
</tr>
<tr>
<td>at each router)</td>
<td></td>
</tr>
<tr>
<td>upper layer protocol</td>
<td>4</td>
</tr>
<tr>
<td>to deliver payload to</td>
<td></td>
</tr>
<tr>
<td>Options (if any)</td>
<td></td>
</tr>
<tr>
<td>total datagram length</td>
<td>32</td>
</tr>
<tr>
<td>packet version index</td>
<td>16</td>
</tr>
<tr>
<td>length</td>
<td>8</td>
</tr>
<tr>
<td>Internet checksum</td>
<td>16</td>
</tr>
<tr>
<td>time to live</td>
<td>32</td>
</tr>
<tr>
<td>source IP address (32 bit)</td>
<td>12</td>
</tr>
<tr>
<td>destination IP address</td>
<td>12</td>
</tr>
<tr>
<td>destination IP address</td>
<td>12</td>
</tr>
<tr>
<td>data (variable length,</td>
<td>65535</td>
</tr>
<tr>
<td>typically a TCP or UDP</td>
<td></td>
</tr>
<tr>
<td>segment)</td>
<td></td>
</tr>
</tbody>
</table>

AH - Authentication Header

<table>
<thead>
<tr>
<th>Field</th>
<th>Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>next header</td>
<td>1</td>
</tr>
<tr>
<td>payload length</td>
<td>1</td>
</tr>
<tr>
<td>unused</td>
<td>2</td>
</tr>
<tr>
<td>SPI (security parameter</td>
<td>4</td>
</tr>
<tr>
<td>index)</td>
<td></td>
</tr>
<tr>
<td>sequence number</td>
<td>4</td>
</tr>
<tr>
<td>authentication data</td>
<td></td>
</tr>
</tbody>
</table>

ESP - Encapsulating Security Header

<table>
<thead>
<tr>
<th>Field</th>
<th>Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPI (security parameter</td>
<td>4</td>
</tr>
<tr>
<td>index)</td>
<td></td>
</tr>
<tr>
<td>sequence number</td>
<td>4</td>
</tr>
<tr>
<td>IV (initialization vector)</td>
<td>4</td>
</tr>
<tr>
<td>data</td>
<td></td>
</tr>
<tr>
<td>padding</td>
<td>1</td>
</tr>
<tr>
<td>padding length</td>
<td>1</td>
</tr>
<tr>
<td>next header / protocol</td>
<td></td>
</tr>
<tr>
<td>type</td>
<td></td>
</tr>
<tr>
<td>authentication data</td>
<td></td>
</tr>
</tbody>
</table>

AH Fields

• Next header
  – Same as “protocol” field in IPv4
  – If TCP follows the AH header, this field is 6
• Payload length:
  – The size of the AH header (in 32-bit chunks)
• SPI
  – For the recipient to locate the SA entry in its SAD
• Sequence number:
  – For anti-replay purpose
• Authentication data
  – Cryptographic integrity check
  – Those immutable and mutable-but-predictable fields in an IP header are also protected

ESP Fields

• Same fields as in AH header:
  – SPI, sequence number, next header
• Initialization vector
  – Needed for some encryption algorithms
  – for example, when CBC mode is used (see next slide)
• Data: protected data, probably encrypted
• Padding: many 0’s mainly in order to
  – make data be a multiple of a block size
  – Maybe required by adopted cryptographic algorithms
  – Or make [data, padding, padding length, next header] a multiple of four octets
More on the Data Field in an ESP Header

- In Tunnel Mode
  - Begin at the IP header
- In Transport Mode
  - Begin at the IP payload
  - Begin at TCP header if a TCP payload

Security Policy Database

- An ordered list of SPD entries
- Each SPD entry specifies a policy: **applicability**, **disposition**, and **protection**
- Applicability: which packets are subject to policy
- Disposition: discard, bypass, or apply IPsec
- Protection: what kinds of SA to apply under this policy

An Example of SPD entry

- Outbound SPD entry example:
  - IP: source=175.34.*.* destination=98.34.32.6
  - Protocol = 6 (TCP)
  - Port: source any, destination=80
  - Disposition = IPsec
  - Protection = Details on what kind of SA to set up (e.g. ESP tunnel mode, DES, ...)
- Similarly an inbound SPD entry can be defined