IPSec

EJ Jung
TCP/IP Example

End System Y

Router 1

LAN, WAN, or point-to-point link

Router 2

End System Y

LAN

Application
TCP
IP
LLC
MAC
Physical

Application
TCP
IP
LLC
MAC
Physical

Application
TCP
IP
LLC
MAC
Physical

Application
TCP
IP
LLC
MAC
Physical
IP Security Issues

- Eavesdropping
- Modification of packets in transit
- Identity spoofing (forged source IP addresses)
- Denial of service

- Many solutions are application-specific
  - TLS for Web, S/MIME for email, SSH for remote login
- IPSec aims to provide a framework of open standards for secure communications over IP
  - Protect every protocol running on top of IPv4 and IPv6
IPSec: Network Layer Security

IPSec = AH + ESP + IPcomp + IKE

- **Protection for IP traffic**
  - AH provides integrity and origin authentication
  - ESP also confidentiality

- **Compression**

- **Sets up keys and algorithms for AH and ESP**

AH and ESP rely on an existing **security association**
- Idea: parties must share a set of secret keys and agree on each other’s IP addresses and crypto algorithms

**Internet Key Exchange (IKE)**
- Goal: establish security association for AH and ESP
- If IKE is broken, AH and ESP provide no protection!
IPSec Security Services

- Authentication and integrity for packet sources
  - Ensures connectionless integrity (for a single packet) and partial sequence integrity (prevent packet replay)
- Confidentiality (encapsulation) for packet contents
  - Also partial protection against traffic analysis
- Authentication and encapsulation can be used separately or together
- Either provided in one of two modes
- These services are transparent to applications above transport (TCP/UDP) layer
IPSec Modes

- **Transport mode**
  - Used to deliver services from host to host or from host to gateway
  - Usually within the same network, but can also be end-to-end across networks

- **Tunnel mode**
  - Used to deliver services from gateway to gateway or from host to gateway
  - Usually gateways owned by the same organization
    - With an insecure network in the middle
Transport Mode vs. Tunnel Mode

- **Transport mode** secures packet payload and leaves IP header unchanged

<table>
<thead>
<tr>
<th>IP header (real dest)</th>
<th>IPSec header</th>
<th>TCP/UDP header + data</th>
</tr>
</thead>
</table>

- **Tunnel mode** encapsulates both IP header and payload into IPSec packets

<table>
<thead>
<tr>
<th>IP header (gateway)</th>
<th>IPSec header</th>
<th>IP header (real dest)</th>
<th>TCP/UDP header + data</th>
</tr>
</thead>
</table>
IPSec in Transport Mode

- End-to-end security between two hosts
  - Typically, client to gateway (e.g., PC to remote host)
- Requires IPSec support at each host
IPSec in Tunnel Mode

- Gateway-to-gateway security
  - Internal traffic behind gateways not protected
  - Typical application: virtual private network (VPN)
- Only requires IPSec support at gateways
Security Association (SA)

- One-way sender-recipient relationship
- SA determines how packets are processed
  - Cryptographic algorithms, keys, IVs, lifetimes, sequence numbers, mode (transport or tunnel)
- SA is uniquely identified by SPI (Security Parameters Index)...
  - Each IPSec keeps a database of SAs
  - SPI is sent with packet, tells recipient which SA to use
- ...destination IP address, and
- ...protocol identifier (AH or ESP)
SA Components

- Each IPSec connection is viewed as one-way so two SAs required for a two-way conversation
  - Hence need for Security Parameter Index
- Security association (SA) defines
  - Protocol used (AH, ESP)
  - Mode (transport, tunnel)
  - Encryption or hashing algorithm to be used
  - Negotiated keys and key lifetimes
  - Lifetime of this SA
  - ... plus other info
Security Association Issues

- How is SA established?
  - How do parties negotiate a common set of cryptographic algorithms and keys to use?

- More than one SA can apply to a packet!
  - E.g., end-to-end authentication (AH) and additional encryption (ESP) on the public part of the network.
Figure 6.10  Basic Combinations of Security Associations
AH: Authentication Header

- Sender authentication
- Integrity for packet contents and IP header
- Sender and receiver must share a secret key
  - This key is used in HMAC computation
  - The key is set up by IKE key establishment protocol and recorded in the Security Association (SA)
    - SA also records protocol being used (AH) and mode (transport or tunnel) plus hashing algorithm used
    - MD5 or SHA-1 supported as hashing algorithms
Recap: MAC

Figure 3.2 Message Authentication Using a One-Way Hash Function
HMAC in IPSec

HMAC for AH Authentication (RFC 2104)

- Secret Key
- nul pad
- 0x3636363636...
- Magic numbers
- XOR’d key
- Message to hash (full IP packet)
- hash function
- XOR’d key
- intermediate hash
- hash function
- Integrity Check Value in the AH header

222f47a2983a56556f2292b5e1e08c2d
AH sets mutable fields to zero and predictable fields to final value and then uses this header plus packet contents as input to HMAC.
AH in Transport Mode

Before AH is applied

IPv4
original IP header | TCP | Data
IPv6
original IP header | extension headers (if present) | TCP | Data

IPv4
original IP header | AH | TCP | Data

IPv6
original IP header | hop-by-hop, dest, routing, fragment | AH | dest | TCP | Data

authenticated except for mutable fields

authenticated except for mutable fields
AH in Tunnel Mode

Before AH is applied

- IPv4: orig IP hdr, TCP, Data
- IPv6: orig IP hdr, extension headers (if present), TCP, Data
Authentication Header Format

- Provides integrity and sender authentication
- Authenticates portions of the IP header
- Anti-replay service (to counter denial of service)
- No confidentiality

**Authentication Header Format**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next header (TCP)</td>
<td>Identifies security association (shared keys and algorithms)</td>
</tr>
<tr>
<td>Payload length</td>
<td></td>
</tr>
<tr>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>Security parameters index (SPI)</td>
<td>Anti-replay, verifies integrity of payload</td>
</tr>
<tr>
<td>Sequence number</td>
<td></td>
</tr>
<tr>
<td>ICV: Integrity Check Value</td>
<td></td>
</tr>
<tr>
<td>(HMAC of IP header, AH, TCP payload)</td>
<td>Authenticated source, verifies integrity of payload</td>
</tr>
</tbody>
</table>
Prevention of Replay Attacks

- When SA is established, sender initializes 32-bit counter to 0, increments by 1 for each packet
  - If wraps around $2^{32}-1$, new SA must be established
- Recipient maintains a sliding 64-bit window
  - If a packet with high sequence number is received, do not advance window until packet is authenticated
ESP: Encapsulating Security Payload

- Adds new header and trailer fields to packet
- Transport mode
  - Confidentiality of packet between two hosts
  - Complete hole through firewalls
  - Used sparingly
- Tunnel mode
  - Confidentiality of packet between two gateways or a host and a gateway
  - Implements VPN tunnels
ESP Security Guarantees

- **Confidentiality** and integrity for packet payload
  - Symmetric cipher negotiated as part of security assoc
- **Optionally** provides authentication (similar to AH)
- Can work in transport...

...or tunnel mode
ESP Packet

- **Identifies security association (shared keys and algorithms)**
- **Anti-replay**
- **TCP segment (transport mode) or entire IP packet (tunnel mode)**
- **Pad to block size for cipher, also hide actual payload length**
- **Type of payload**
- **HMAC-based Integrity Check Value (similar to AH)**
Virtual Private Networks (VPN)

- ESP is often used to implement a VPN
  - Packets go from internal network to a gateway with TCP/IP headers for address in another network
  - Entire packet hidden by encryption
    - Including original headers so destination addresses are hidden
  - Receiving gateway decrypts packet and forwards original IP packet to receiving address in the network that it protects

- This is known as a VPN tunnel
  - Secure communication between parts of the same organization over public untrusted Internet
ESP Together With AH

- AH and ESP are often combined
- End-to-end AH in transport mode
  - Authenticate packet sources
- Gateway-to-gateway ESP in tunnel mode
  - Hide packet contents and addresses on the insecure part of the network
- Significant cryptographic overhead
  - Even with AH