IPSEC: AH and ESP

Markus Hidell
mahidell@kth.se

Based on material by Vitaly Shmatikov, Univ. of Texas, and by the previous course teachers
Reading

• Kaufman, chapter 16-17
TCP/IP Example
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
Operating system layers

- SSL (Secure Socket Layer) changes the API to TCP/IP
  - Applications change, but OS doesn't
- IPSec implemented in OS
  - Applications and API remain unchanged (at least in theory)
- To make full use of IPSec, API and apps have to change!
  - and accordingly also the applications
Overview of IPsec

• Authenticated Keying
  - Internet Key Exchange (IKE)
    • Next lecture

• Data Encapsulation
  - ESP: IP Encapsulating Security Payload (RFC 4303)
  - AH: IP Authentication Header (RFC 4302)

• Security Architecture (RFC 4301)
  - Tunnel/transport Mode
  - Databases (Security Association, Policy, Peer Authorization)
IPsec: Network Layer Security

**IPsec = AH + ESP + IKE**

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

- **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

• Authentication and encapsulation can be used separately or together

• Either provided in one of two modes
  - Transport mode
  - Tunnel mode
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
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**
Tunnel Mode Illustration

IPsec protects communication on the insecure part of the network
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

  
  | IP header (gateway) | IPSec header | IP header (real dest) | TCP/UDP header + data |
Security Association (SA)

- One-way sender-recipient relationship
  - Manually configured or negotiated through IKE
- SA determines how packets are processed
  - Cryptographic algorithms, keys, AH/ESP, lifetimes, sequence numbers, mode (transport or tunnel) - read Kaufman!
- SA is uniquely identified by \{SPI, dst IP addr, flag\}
  - SPI: Security Parameter Index
    - Chosen be destination (unless traffic is multicast...)
  - Flag: ESP or AH
  - Each IPsec implementation keeps a database of SAs
  - SPI is sent with packet, tells recipient which SA to use
Sending and Receiving IPsec Packets

• When Alice is sending to Bob:
  - Consult “security policy database” (SPD) to check if packet should protected with IPsec or not (“selector” fields)
  - SPD provides pointer to the associated SA entry in the security association database (SAD)
  - SA provides SPI, algorithm, key, sequence number, etc.
  - Include the SPI in the message

• When Bob receives a message:
  - Lookup the SA based on the destination address and SPI (In a multicast message the address is not Bob's own)
  - Find algorithm, key, sequence number, etc.
  - After decrypting message, verify that packet matches “selector” in the policy database (SPD)
Encapsulation Formats

- **AH**
  - Authentication Header
  - Only provides integrity

- **ESP**
  - Encapsulating Security Payload
  - Provides integrity and/or privacy

AH in transport mode

```
Original IP header  | AH   | TCP header | Data
```
AH: Authentication Header

- RFC 4302
- 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)

AHv2, RFC 4302

Let authentication header implement IP integrity by holding a hash of a shared secret and the content of an IP packet
AH and IP Header

- **Mutable fields**
  - may change
    - Service type
    - Fragm. offset
    - TTL
    - Header checksum
- **Predictable fields**
  - may change in a predictable way
    - Dst address (source routing)
- **Immutable fields**
  - will not change
    - the rest....

Mutable fields can’t be included in the AH’s end-to-end integrity check
Authentication Header Format

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

<table>
<thead>
<tr>
<th>Next header (TCP)</th>
<th>Payload length</th>
<th>Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Security parameters index (SPI)
- Sequence number
- ICV: Integrity Check Value
  (HMAC of IP header, AH, TCP payload)

Identifies security association (shared keys and algorithms)

Anti-replay

Authenticates source, verifies integrity of payload
ESP: Encapsulating Security Payload

- RFC 4303
- 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 Security Guarantees Diagram]

- Encrypted (inner)
- Authenticated (outer)
ESP Packet

- Security Parameters Index (SPI)
- Sequence Number
- Payload Data (variable)
- Padding (0 - 255 bytes)
- Authentication Data (variable)

- 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 Internet
Use Cases Summary

- **Host-Host**
  - Transport mode
  - *(Or tunnel mode)*

- **Gateway-Gateway**
  - Tunnel mode

- **Host-Gateway**
  - Tunnel mode