IPsec

IT443 – Network Security Administration
Instructor: Bo Sheng

Securing Networks

<table>
<thead>
<tr>
<th>Layer</th>
<th>Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>(spread-Spectrum, quantum crypto, etc.)</td>
</tr>
<tr>
<td>Link</td>
<td>(IEEE802.1x, IEEE802.10)</td>
</tr>
<tr>
<td>Network</td>
<td>(IPSec, IKE)</td>
</tr>
<tr>
<td>Transport</td>
<td>(SSL/TLS)</td>
</tr>
<tr>
<td>Applications</td>
<td>(ftp, telnet, mail, PGP)</td>
</tr>
</tbody>
</table>

IPsec Objectives

- Why do we need IPsec?
  - IP V4 has no authentication
    - IP spoofing
    - Payload could be changed without detection.
  - IP V4 has no confidentiality mechanism
    - Eavesdropping
  - Denial of service (DoS) attacks
    - Cannot hold the attacker accountable due to the lack of authentication.

IPsec Objectives

- IP layer security mechanism for IPv4 and IPv6
  - Not all applications need to be security aware
  - Can be transparent to users
  - Provide authentication and confidentiality mechanisms.

IPsec Architecture

SPD: Security Policy Database; IKE: Internet Key Exchange; SA: Security Association; SAD: Security Association Database.
IPsec Architecture

- Can be implemented in:
  - Host or gateway
- Can work in two Modes:
  - Tunnel mode
  - Transport mode
- Hosts can implement IPsec to connect to:
  - Other hosts in transport or tunnel mode
  - Or gateways in tunnel mode
- Gateways to gateways:
  - Tunnel mode

Authentication Header (AH)

- Data integrity:
  - Entire packet has not been tampered with
- Authentication:
  - Can “trust” IP address source
  - Use MAC to authenticate
- Anti-replay feature

Encapsulated Security Protocol (ESP)

- Confidentiality for upper layer protocol
- Partial traffic flow confidentiality (Tunnel mode only)
- Data origin authentication and connectionless integrity (optional)

Tunnel Mode

- ESP applies only to the tunneled packet
- AH can be applied to portions of the outer header

Transport Mode

- New IP Header
- AH or ESP Header
- Org IP Header
- TCP
- Data

Encrypted/Autenticated

- Encrypted Tunnel
Transport Mode

- IP header
- IP options
- IPsec header
- Higher layer protocol

Real IP destination

- ESP protects higher layer payload only
- AH can protect IP headers as well as higher layer payload

Security Association (SA)

- An association between a sender and a receiver
  - Consists of a set of security related parameters
    - E.g., sequence number, encryption key
- One way relationship
- Determine IPsec processing for senders
- Determine IPsec decoding for destination
- SAs are not fixed! Generated and customized per traffic flows

Security Parameters Index (SPI)

- A 32-bits string assigned to an SA.
- Carried in AH and ESP headers to enable the receiving system to select the SA under which the packet will be processed.

- SPI + Dest IP address + IPsec Protocol
  - Uniquely identifies each SA in SA Database (SAD)

SA Database (SAD)

- Holds parameters for each SA
  - Sequence number counter
  - Lifetime of this SA
  - AH and ESP information
  - Tunnel or transport mode

- Every host or gateway participating in IPsec has their own SA database

SA Bundle

- More than 1 SA can apply to a packet

- Example: ESP does not authenticate new IP header. How to authenticate?
  - Use SA to apply ESP w/out authentication to original packet
  - Use 2nd SA to apply AH

Security Policy Database (SPD)

- Decide
  - What traffic to protect?
  - Has incoming traffic been properly secured?
- Policy entries define which SA or SA Bundles to use on IP traffic
- Each host or gateway has their own SPD
- Index into SPD by Selector fields
  - Selectors: IP and upper-layer protocol field values.
  - Examples: Dest IP, Source IP, Transport Protocol, IPsec Protocol, Source & Dest Ports, …
Outbound Processing

Is it for IPsec? If so, which policy entry to select?

IP Packet

SPD (Policy)

SA Database

Determine the SA and its SPI

IPsec processing

SPI & IPsec Packet

Send to B

Inbound Processing

From A

Original IP Packet

Use SPI to index the SAD

SA Database

SPI & Packet

Was packet properly secured?

IP Packet

SPD (Policy)

Issues

• Firewalls
  – IPsec encrypts information used by firewalls to filter traffic (e.g., port number)

• AH mutable/immutable/predictable fields:
  – Some fields get modified by the intermediate routers and can’t be protected by the AH
  – Mutable: type of service, flags, fragment offset, TTL, header checksum
  – Mutable but predictable fields are included in the AH computation using their expected value at the destination (e.g., destination address even when using source routing)

Internet Key Exchange

• Why do we need Internet key management
  – AH and ESP require encryption and authentication keys

  • Process to negotiate and establish IPsec SAs between two entities

Security Principles

• Basic security principle for session keys
  – Compromise of a session key
    • Doesn’t permit reuse of the compromised session key.
    • Doesn’t compromise future session keys and long-term keys.

• Perfect forward secrecy (PFS)
  – Compromise of current keys (session key or long-term key) doesn’t compromise past session keys.
  – Concern for encryption keys but not for authentication keys.

A Note about IKE

• IKE v2 was introduced in RFC 4306 (December 2005)

• IKE v2 does not interoperate with IKE v1
  – Both version can unambiguously run over the same UDP port

• IKE v2 combines the contents of previously separate documents
  – ISAKMP
  – IKE v1
  – DOI
  – NAT
  – …
IKE Overview

• A separate RFC has been published for IKE – RFC 2409
• Request-response protocol
  – Initiator
  – Responder
• Two phases
  – Phase 1: Establish an IKE (ISAKMP) SA
    • Essentially the ISAKMP phase 1
    • Bi-directional
  – Phase 2: Use the IKE SA to establish IPsec SAs
    • Key exchange phase
    • Directional

A Clarification About PFS

• In RFC 2409:
  – When used in the memo Perfect Forward Secrecy (PFS) refers to the notion that compromise of a single key will permit access to only data protected by a single key.
  – The key used to protect transmission of data MUST NOT be used to derive any additional keys.
  – If the key used to protect transmission of data was derived from some other keying material, that material MUST NOT be used to derive any more keys.