Chapter 19 — IP Security

If a secret piece of news is divulged by a spy before the time is ripe, he must be put to death, together with the man to whom the secret was told.

— The Art of War, Sun Tzu

IP Security

- have a range of application specific security mechanisms
  - eg. S/MIME, PGP, Kerberos, SSL/HTTPS
- however there are security concerns that cut across protocol layers
- would like security implemented by the network for all applications

IP Security

- general IP Security mechanisms
- provides
  - authentication
  - confidentiality
  - key management
- applicable to use over LANs, across public & private WANs, & for the Internet
- need identified in 1994 report
  - need authentication, encryption in IPv4 & IPv6

IP Security Uses

Benefits of IPSec

- in a firewall/router provides strong security to all traffic crossing the perimeter
- in a firewall/router is resistant to bypass
- is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users
- secures routing architecture
**IP Security Architecture**

- Specification is quite complex, with groups:
  - Architecture
    - RFC 4301 Security Architecture for Internet Protocol
  - Authentication Header (AH)
    - RFC 4302 IP Authentication Header
  - Encapsulating Security Payload (ESP)
    - RFC 4303 IP Encapsulating Security Payload (ESP)
  - Internet Key Exchange (IKE)
    - RFC 4306 Internet Key Exchange (IKEv2) Protocol
  - Cryptographic algorithms
  - Other

**IPSec Services**

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
  - A form of partial sequence integrity
- Confidentiality (encryption)
- Limited traffic flow confidentiality

**Transport and Tunnel Modes**

- Transport Mode
  - To encrypt & optionally authenticate IP data
  - Can do traffic analysis but is efficient
  - Good for ESP host to host traffic
- Tunnel Mode
  - Encrypts entire IP packet
  - Add new header for next hop
  - No routers on way can examine inner IP header
  - Good for VPNs, gateway to gateway security

**Transport and Tunnel Mode Protocols**

**Security Associations**

- A one-way relationship between sender & receiver that affords security for traffic flow
- Defined by 3 parameters:
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier
- Has a number of other parameters
  - Seq no, AH & EH info, lifetime etc
- Have a database of Security Associations
Security Policy Database

- relates IP traffic to specific SAs
- match subset of IP traffic to relevant SA
- use selectors to filter outgoing traffic to map
- based on: local & remote IP addresses, next layer protocol, name, local & remote ports

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Local IP</th>
<th>Port</th>
<th>Remote IP</th>
<th>Port</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>12.1.1.2</td>
<td>*</td>
<td>20.1.1.2</td>
<td>560</td>
<td>NAK</td>
<td>TUN</td>
</tr>
<tr>
<td>ICMP</td>
<td>12.1.1.2</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>BYPASS</td>
</tr>
<tr>
<td>DNS</td>
<td>12.1.1.2</td>
<td>*</td>
<td>23.1.2.1</td>
<td>560</td>
<td>NAK</td>
<td>Protect DNS traffic</td>
</tr>
</tbody>
</table>
| TCP      | 12.1.1.2 | 562  | 24.1.1.2  | 560  | NAK    | Encrypt to server)
| TCP      | 12.1.1.2 | *    | 24.1.1.2  | 560  | NAK    | BYPASS  |

Encapsulating Security Payload (ESP)

- provides message content confidentiality, data origin authentication, connectionless integrity, an anti-replay service, limited traffic flow confidentiality
- services depend on options selected when establish Security Association (SA), net location
- can use a variety of encryption & authentication algorithms

Encryption & Authentication Algorithms & Padding

- ESP can encrypt payload data, padding, pad length, and next header fields
  - if needed have IV at start of payload data
- ESP can have optional ICV for integrity
  - is computed after encryption is performed
- ESP uses padding
  - to expand plaintext to required length
  - to align pad length and next header fields
  - to provide partial traffic flow confidentiality

Anti-Replay Service

- replay is when attacker resends a copy of an authenticated packet
- use sequence number to thwart this attack
- sender initializes sequence number to 0 when a new SA is established
  - increment for each packet
  - must not exceed limit of $2^{32} - 1$
- receiver then accepts packets with seq no within window of $(N-W+1)$

Combining Security Associations

- SA's can implement either AH or ESP
- to implement both need to combine SA's
  - form a security association bundle
  - may terminate at different or same endpoints
  - combined by
    - transport adjacency
    - iterated tunneling
  - combining authentication & encryption
    - ESP with authentication, bundled inner ESP & outer AH, bundled inner transport & outer ESP
Combining Security Associations

IPSec Key Management
- handles key generation & distribution
- typically need 2 pairs of keys
  – 2 per direction for AH & ESP
- manual key management
  – sysadmin manually configures every system
- automated key management
  – automated system for on demand creation of keys for SA's in large systems
  – has Oakley & ISAKMP elements

Oakley
- a key exchange protocol
- based on Diffie-Hellman key exchange
- adds features to address weaknesses
  – no info on parties, man-in-middle attack, cost
  – so adds cookies, groups (global params), nonces, DH key exchange with authentication
- can use arithmetic in prime fields or elliptic curve fields

ISAKMP
- Internet Security Association and Key Management Protocol
- provides framework for key management
- defines procedures and packet formats to establish, negotiate, modify, & delete SAs
- independent of key exchange protocol, encryption alg, & authentication method
- IKEv2 no longer uses Oakley & ISAKMP terms, but basic functionality is same

IKEV2 Exchanges

ISAKMP
- Initiator's Security Parameter Index (SPI)
- Responder's Security Parameter Index (SPI)
- Message ID
- Length
- Next payload

- RESERVED
- Payload length
- Generic Payload Header
IKE Payloads & Exchanges

- have a number of ISAKMP payload types:
- payload has complex hierarchical structure
- may contain multiple proposals, with multiple protocols & multiple transforms

Cryptographic Suites

- variety of cryptographic algorithm types
- to promote interoperability have
  - RFC4308 defines VPN cryptographic suites
    - VPN-A matches common corporate VPN security using 3DES & HMAC
    - VPN-B has stronger security for new VPNs implementing IPsecv3 and IKEv2 using AES
  - RFC4869 defines four cryptographic suites compatible with US NSA specs
    - provide choices for ESP & IKE
    - AES-GCM, AES-CBC, HMAC-SHA, ECP, ECDSA

Summary

- have considered:
  - IPSec security framework
  - IPSec security policy
  - ESP
  - combining security associations
  - internet key exchange
  - cryptographic suites used