Internet Security
- IPSec, SSL/TLS, SRTP -

29th. Oct. 2007
Lee, Choongho
chlee@mmlab.snu.ac.kr
Introduction (1/2)

◆ **Security Goals**
  - Confidentiality
  - Data authentication
  - Data integrity

◆ **Internet Security Protocols**

```
<table>
<thead>
<tr>
<th>Application</th>
<th>SRTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL / TLS</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>UDP</td>
</tr>
<tr>
<td>IP/IPSec</td>
<td></td>
</tr>
<tr>
<td>Data Link</td>
<td></td>
</tr>
<tr>
<td>Physical</td>
<td></td>
</tr>
</tbody>
</table>
```
Security Protocol Architecture

- Encapsulation

[Diagram showing encapsulation process]

- Session (Association) Establishment

[Diagram showing session establishment process]

* MAC: Message Authentication Code
**IP Security Protocol (IPSec)**
- To provide IP packet security at network layer
- Designed by IETF
- Optional for IPv4
- Mandatory for IPv6

**Security service**
- Confidentiality - Encrypting traffic
- Integrity
- Authenticating the peers
- Anti-replay
**IPSec Parts (1/2)**

- **Connection Setup**
  - Internet Key Exchange (IKE)
    - Initial negotiation to agree upon the encryption mechanism, keys, etc.
  - Security Association (SA)
    - A one-directional relationship between sender and receiver
    - Two-way secure exchange of IP packets requires two (or more) SAs
    - SA parameters
      - Lifetime of this SA
      - AH/ESP Information: authentication/encryption algorithm, keys, lifetime
      - Protocol Mode
      - Sequence number counter
  - The actual choice of encryption and authentication algorithms is left to the IPSec administrator
Data transfer

- Extension headers that follow the main IP header
- Authentication Header (AH)
  - Data integrity & authentication
  - Protecting the IP payload and all header fields of an IP datagram except for mutable fields
- Encapsulating Security Payload (ESP)
  - ESP Header + ESP Trailer
  - Data confidentiality
  - Integrity & Authentication (Optional)
  - Not protect IP header
**IPSec - Protocol Mode (1/2)**

- **Transport mode**
  - Protection for upper-layer protocols
  - Only the payload is encrypted
  - Host-to-host

- **Tunnel mode**
  - Protection of entire IP packet
  - New outer IP packet for routing
  - Network-to-network (secure tunnels b/w routers), host-to-network, host-to-host
  - Used for Virtual Private Network (VPN)
**IPSec - Protocol Mode (2/2)**

### Transport Mode

- **Site Network**
- **Secure Connection**
- **Site Network**
- **Secure on the Internet**

- **Extra Software May be Required**
- **Security in Site Network**

### Tunnel Mode

- **Site Network**
- **Tunneled Connection**
- **Site Network**

- **No Extra Software**
- **No Security in Site Network**
- **IPsec Gateway**
- **Secure on the Internet**
- **IPsec Gateway**
- **No Security in Site Network**
- **No Extra Software**
**IPSec – AH + Two mode**

Transport Mode:

- IP hdr
- AH (..., Seq. Num., ICV)
- upper layer data

*ICV*: Integrity Check Value

Tunnel Mode:

- New IP hdr
- AH (..., Seq. Num., ICV)
- IP hdr
- upper layer data

*Integrity*:

(only header fields that are not changed or are changed in a predictable manner)
IPSec – ESP + Two mode

Transport Mode

Tunnel Mode

* ICV : Integrity Check Value
Contents

- Introduction
- IPSec
- SSL / TLS
- SRTP
- Conclusion
Secure Sockets Layer (SSL) / Transport Layer Security (TLS)

- SSL v3.0 with minor change -> TLS 1.0
- Connection-oriented data confidentiality and integrity, and optional client and server authentication
- Applications
  - Web browsing, e-mail, Internet faxing, instant messaging and other data transfers
SSL / TLS 구조 (1/3)
**Record Layer Protocol**

- Record: exchanging unit
- Encapsulates the data to be exchanged
- Each record has a content type field, a length field, a TLS version field

*MAC: Message Authentication Code*
◆ **Handshake Protocol (content type 22)**
  - Client and server authentication
  - Establish cryptographic keys (for encryption and MAC)
  - Negotiation of cryptographic algorithms

◆ **ChangeCipherSpec Protocol (content type 20)**
  - The Client tells The server
    - “Everything I tell you from now on will be encrypted”

◆ **Alert Protocol (content type 21)**
  - Warning, Fatal Error

◆ **Application Protocol (content type 23)**
  - Application Data
SSL / TLS Handshake (1/3)

CLIENT

- Client Hello
- Certificate
- Client Key Exchange
- Certificate Verify
- [changecipherstransfer]
- Finished

SERVER

- Hello Request
- Server Hello
- Certificate
- Server Key Exchange
- Certificate Request
- Server Hello Done
- [changecipherstransfer]
- Finished

✓ start handshake, protocol version, algorithms
✓ authentication server + exchange (pre)master secret
✓ client authentication
✓ end handshake, integrity verification

Optional
SSL / TLS Handshake (2/3)

◆ **ClientHello**
  - The highest TLS protocol version a client supports, a random number, a list of suggested cipher suites and compression methods

◆ **ServerHello**
  - The chosen protocol version, a random number, cipher suite, and compression method from the choices offered by the client

◆ **Server Certificate (optional)**
  - The Server sends its Certificate

◆ **Server Key Exchange (optional)**
  - The Server sends this when Server Certificate is not enough for the client to generate premaster secret.

◆ **CertificateRequest (optional)**
  - The server requests the client’s Certificate

◆ **Server Hello Done**
  - Indicating it is done with handshake negotiation
SSL / TLS Handshake (3/3)

- **Client Certificate (optional)**
  - The Client sends its Certificate

- **Client Key Exchange**
  - PreMasterSecret, public key, or nothing

- **Certificate Verify (optional)**
  - The Client sends its certificate verification

- **ChangeCipherSpec**
  - The Client tells The server
    - “Everything I tell you from now on will be encrypted

- **Finished**
  - Encrypted message
  - The Server attempts to decrypt the Client’s Finished message and verify
    - If this is fails, the handshake is considered to have failed and the connection should be torn down
Real-time Transport Protocol (RTP)
- Standardized packet format for Transporting the multimedia datastream
- Sending packets via UDP
- RTP packet fields
  - Payload-type identification
  - Sequence number
  - Time stamp
- Position in the protocol stack
  - Transport protocol that is implemented in the application layer
- Used for VoIP

RTP Control Protocol (RTCP)
- Is used to monitor QoS
Secure Real-time Transport Protocol (SRTP)

- An extension to RTP Profile for Audio and Video Conferences
- Security services
  - Confidentiality of the RTP payload
  - Message authentication and integrity
  - Replay protection
- All provided features (encryption, authentication)
  - Optional
  - Separately enabled/disabled

Secure RTCP (SRTCP)

- Provides Security for RTCP
SRTP (2/3)

- **SRTP needs an external key management protocol**
  - For exchange a master key
  - Multimedia Internet KEYing (MIKEY) : Rely on certificates
  - ZRTP : Not require certificates or alike

- **Key Derivation**
  - One single master key
  - Key derivation function
    - All other necessary session keys are generated from master key
    - Periodically regenerate session keys
    - Reduce key management overhead

- **Data Encryption**
  - Advanced Encryption Standard (AES)
    - Only a single cipher for SRTP
  - NULL cipher
    - Does not perform any encryption
SRTP (3/3)

◆ **Authentication, integrity**
  - Over packet payload and the packet header

◆ **Replay protection**
  - Maintain the indices of previously received message
  - Compare them with the index of each new received message
  - Admit the new message only if it has not been played before
Conclusion

◆ **Security Protocol at different layers**
  - IPSec
  - SSL / TLS
  - SRTP / SRTCP

◆ **Providing Security Service**
  - Where?
  - Which service?
  - How?

◆ **Other Considering Points**
  - Reduce overhead
  - Reduce Handshake time
  - Throughput Rate
  - Etc.