Review

- Chapter 1: Basic Concepts and Terminology
- Chapter 2: Basic Cryptographic Tools
- Chapter 3 – User Authentication
- Chapter 4 – Access Control Lists
- Chapter 5 – Database Security (skipped)
- Chapter 6 – Malicious Software
- Networking Basics (not in book)
- Chapter 7 – Denial of Service
- Chapter 8 – Intrusion Detection
- Chapter 9 – Firewalls and Intrusion Prevention
- Chapter 10 – Buffer Overflow
- Chapter 11 – Software Security
- Chapter 12 – OS Security
- Chapter 22 – Internet Security Protocols
Chapter 22

Internet Security
Protocols and Standards
MIME and S/MIME

MIME

• extension to the old RFC 822 specification of an Internet mail format
  – RFC 822 defines a simple heading with To, From, Subject
  – assumes ASCII text format
  – provides a number of new header fields that define information about the body of the message

S/MIME

• Secure/Multipurpose Internet Mail Extension
  • security enhancement to the MIME Internet e-mail format
    – based on technology from RSA Data Security
    – provides the ability to sign and/or encrypt e-mail messages
<table>
<thead>
<tr>
<th>Type</th>
<th>Subtype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>Plain</td>
<td>Unformatted text; may be ASCII or ISO 8859.</td>
</tr>
<tr>
<td></td>
<td>Enriched</td>
<td>Provides greater format flexibility.</td>
</tr>
<tr>
<td>Multipart</td>
<td>Mixed</td>
<td>The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.</td>
</tr>
<tr>
<td></td>
<td>Parallel</td>
<td>Differs from Mixed only in that no order is defined for delivering the parts to the receiver.</td>
</tr>
<tr>
<td></td>
<td>Alternative</td>
<td>The different parts are alternative versions of the same information. They are ordered in increasing faithfulness to the original, and the recipient's mail system should display the &quot;best&quot; version to the user.</td>
</tr>
<tr>
<td></td>
<td>Digest</td>
<td>Similar to Mixed, but the default type/subtype of each part is message/rfc822.</td>
</tr>
<tr>
<td>Message</td>
<td>rfc822</td>
<td>The body is itself an encapsulated message that conforms to RFC 822.</td>
</tr>
<tr>
<td></td>
<td>Partial</td>
<td>Used to allow fragmentation of large mail items, in a way that is transparent to the recipient.</td>
</tr>
<tr>
<td></td>
<td>External-body</td>
<td>Contains a pointer to an object that exists elsewhere.</td>
</tr>
<tr>
<td>Image</td>
<td>jpeg</td>
<td>The image is in JPEG format, JFIF encoding.</td>
</tr>
<tr>
<td></td>
<td>gif</td>
<td>The image is in GIF format.</td>
</tr>
<tr>
<td>Video</td>
<td>mpeg</td>
<td>MPEG format.</td>
</tr>
<tr>
<td>Audio</td>
<td>Basic</td>
<td>Single-channel 8-bit ISDN mu-law encoding at a sample rate of 8 kHz.</td>
</tr>
<tr>
<td>Application</td>
<td>PostScript</td>
<td>Adobe Postscript</td>
</tr>
<tr>
<td></td>
<td>octet-stream</td>
<td>General binary data consisting of 8-bit bytes.</td>
</tr>
</tbody>
</table>
## S/MIME Content Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Subtype</th>
<th>smime Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multipart</td>
<td>Signed</td>
<td></td>
<td>A clear-signed message in two parts: one is the message and the other is the signature.</td>
</tr>
<tr>
<td>Application</td>
<td>pkcs7-mime</td>
<td>signedData</td>
<td>A signed S/MIME entity.</td>
</tr>
<tr>
<td></td>
<td>pkcs7-mime</td>
<td>envelopeData</td>
<td>An encrypted S/MIME entity.</td>
</tr>
<tr>
<td></td>
<td>pkcs7-mime</td>
<td>degenerate signedData</td>
<td>An entity containing only public-key certificates.</td>
</tr>
<tr>
<td></td>
<td>pkcs7-mime</td>
<td>CompressedData</td>
<td>A compressed S/MIME entity.</td>
</tr>
<tr>
<td></td>
<td>pkcs7-signature</td>
<td>signedData</td>
<td>The content type of the signature subpart of a multipart/signed message.</td>
</tr>
</tbody>
</table>
Typical S/MIME Process

This is an S/MIME message from Bob to Alice. Bob will sign and encrypt the message before sending it to Alice.

Plaintext message (unsigned)

Digital signature added (DSS/SHA)

Message with signature encrypted with one-time session key (Triple DES)

Encrypted copy of session key added (El Gamal)

Document converted to Radix-64 format

Figure 22.1 Typical S/MIME Process
S/MIME Cryptographic Algorithms

• default algorithms used for signing messages are DSS and SHA-1
• RSA public-key encryption algorithm can be used with SHA-1 or the MD5 message digest algorithm for forming signatures
• radix-64 or base64 mapping is used to map the signature and message into printable ASCII characters
S/MIME Public Key Certificates

• default algorithms used for encrypting S/MIME messages are 3DES and ElGamal
  – ElGamal is based on the Diffie-Hellman public-key exchange algorithm
• if encryption is used alone radix-64 is used to convert the ciphertext to ASCII format
• basic tool that permits widespread use of S/MIME is the public-key certificate
• S/MIME uses certificates that conform to the international standard X.509v3
S/MIME Functions

- **enveloped data**: encrypted content and associated keys
- **signed data**: encoded message + signed digest
- **clear-signed data**: cleartext message + encoded signed digest
- **signed and enveloped data**: nesting of signed and encrypted entities
DomainKeys Identified Mail (DKIM)

• specification of cryptographically signing e-mail messages permitting a signing domain to claim responsibility for a message in the mail stream

• proposed Internet Standard (RFC 4871: DomainKeys Identified Mail (DKIM) Signatures)

• has been widely adopted by a range of e-mail providers
Figure 22.2 Function Modules and Standardized Protocols Used Between Them
Example of DKIM Deployment

Figure 22.3 Simple Example of DKIM Deployment

DNS = domain name system
MDA = mail delivery agent
MSA = mail submission agent
MTA = message transfer agent
MUA = message user agent
Secure Sockets Layer (SSL)

- one of the most widely used security services
- general-purpose service implemented as a set of protocols that rely on TCP
- subsequently became Internet standard RFC2246: Transport Layer Security (TLS)

Two implementation choices:
- provided as part of the underlying protocol suite
- embedded in specific packages
Figure 22.4  SSL Protocol Stack
SSL Record Protocol Operation

Figure 22.5  SSL Record Protocol Operation
SSL Change Cipher Spec Protocol

• one of three SSL specific protocols that use the SSL Record Protocol
• is the simplest
• consists of a single message which consists of a single byte with the value 1
• sole purpose of this message is to cause pending state to be copied into the current state
• hence updating the cipher suite in use
SSL Alert Protocol

- Conveys SSL-related alerts to peer entity.
- Alert messages are compressed and encrypted.
- Each message consists of two bytes:
  - First byte takes the value warning (1) or fatal (2) to convey the severity of the message.
  - Second byte contains a code that indicates the specific alert.
- If the level is fatal, SSL immediately terminates the connection.
- Other connections on the same session may continue, but no new connections on this session may be established.
SSL Handshake Protocol

- most complex part of SSL
- is used before any application data are transmitted
- allows server and client to:
  - authenticate each other
  - negotiate encryption and MAC algorithms
  - negotiate cryptographic keys to be used

- comprises a series of messages exchanged by client and server
- exchange has four phases
Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4
Change cipher suite and finish handshake protocol.

Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

Figure 22.6 Handshake Protocol Action
HTTPS
(HTTP over SSL)

• combination of HTTP and SSL to implement secure communication between a Web browser and a Web server
• built into all modern Web browsers
  – search engines do not support HTTPS
  – URL addresses begin with https://
  – documented in RFC 2818, HTTP Over TLS
  – agent acting as the HTTP client also acts as the TLS client
  – closure of an HTTPS connection requires that TLS close the connection with the peer TLS entity on the remote side, which will involve closing the underlying TCP connection
IP Security (IPsec)

- various application security mechanisms
  - S/MIME, PGP, Kerberos, SSL/HTTPS
- security concerns cross protocol layers
- would like security implemented by the network for all applications
- authentication and encryption security features included in next-generation IPv6
- also usable in existing IPv4
IPsec

- general IP security mechanisms
- provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet

Provides:

**authentication**
- assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header and that the packet has not been altered in transit

**confidentiality**
- enables communicating nodes to encrypt messages to prevent eavesdropping by third parties

**key management**
- concerned with the secure exchange of keys
- provided by the Internet exchange standard IKEv2
IPsec Uses
Benefits of IPsec

• when implemented in a firewall or router, it provides strong security to all traffic crossing the perimeter
• in a firewall it is resistant to bypass
• below transport layer, hence transparent to applications
• can be transparent to end users
• can provide security for individual users
• secures routing architecture
The Scope of IPsec

provides two main functions:

- a combined authentication/encryption function called Encapsulating Security Payload (ESP)
- key exchange function

VPNs want both authentication and encryption

also an authentication-only function, implemented using an Authentication Header (AH)

- because message authentication is provided by ESP, the use of AH is included in IPsecv3 for backward compatibility but should not be used in new applications

specification is quite complex
- numerous RFC's
  2401/4302/4303/4306
Security Associations

• a one-way relationship between sender and receiver that affords security for traffic flow
  – if a peer relationship is needed for two-way secure exchange then two security associations are required

• is uniquely identified by the Destination Address in the IPv4 or IPv6 header and the SPI in the enclosed extension header (AH or ESP)

Defined by 3 parameters:

- Security Parameter Index (SPI)
- IP Destination Address
- Protocol Identifier
Encapsulating Security Payload (ESP)

Figure 22.7 IPSec ESP Format
Transport and Tunnel Modes

- transport mode protection extends to the payload of an IP packet
- typically used for end-to-end communication between two hosts
- ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header

- tunnel mode provides protection to the entire IP packet
- the entire original packet travels through a tunnel from one point of an IP network to another
- used when one or both ends of a security association are a security gateway such as a firewall or router that implements IPsec
- with tunnel mode a number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec
Summary

• secure E-Mail and S/MIME
• DomainKeys Identified Mail
  – Internet mail architecture
  – DKIM strategy
• Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
  – SSL architecture
  – SSL record protocol
  – change cipher spec protocol
  – alert protocol
  – handshake protocol
• HTTPS
  – connection initiation
  – connection closure
• IPv4 and IPv6 security
  – IP security overview
  – scope of IPsec
  – security associations
  – encapsulating security payload
  – transport and tunnel modes