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

The body is itself an encapsulated message that conforms to RFC 822.

Text images

Bob's private key

Alice's public key

Plaintext message (unsigned)

Derived private key

One-time session key

Derived public key

Extracted copy of session key added (ElGamal)

Digest of message with signature encrypted with one-time session key (Triple DES)

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

Digital signature added (MD5/SHA)

Figure 22.1  Typical S/MIME Process for Creating an S/MIME Message

Table 22.1

<table>
<thead>
<tr>
<th>Type</th>
<th>Subtype</th>
<th>mime Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>Plain</td>
<td></td>
<td>Unformatted text; may be ASCII or ISO-8859. Provides greater format flexibility.</td>
</tr>
<tr>
<td>Multipart</td>
<td>Mixed</td>
<td></td>
<td>The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order they appear in the mail message.</td>
</tr>
<tr>
<td></td>
<td>Parallel</td>
<td></td>
<td>The different parts are delivered only in that order. It is defined for delivering the parts to the receiver.</td>
</tr>
<tr>
<td></td>
<td>Alternative</td>
<td></td>
<td>The different parts are alternative versions of the same message. The server is ordered to pass them to the recipient only if the recipient's mail system should display the 'best' version to the user.</td>
</tr>
<tr>
<td>Digest</td>
<td></td>
<td></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></td>
<td>The body is itself an encapsulated message that conforms to RFC 822.</td>
</tr>
<tr>
<td></td>
<td>Partial</td>
<td></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</td>
<td></td>
<td>Contains a pointer to an object that exists elsewhere.</td>
</tr>
<tr>
<td>Image</td>
<td>jpg</td>
<td>jpeg</td>
<td>The image is in JPEG format, JPG encoding.</td>
</tr>
<tr>
<td></td>
<td>gif</td>
<td>gif</td>
<td>The image is in GIF format.</td>
</tr>
<tr>
<td>Video</td>
<td>mpeg</td>
<td>mpeg</td>
<td>MPEG format.</td>
</tr>
<tr>
<td>Audio</td>
<td>Basic</td>
<td></td>
<td>Single-channel 8-bit 8 kHz raw encoding at a sample rate of 8 kHz.</td>
</tr>
<tr>
<td>Application</td>
<td>PostScript</td>
<td></td>
<td>Adobe PostScript.</td>
</tr>
<tr>
<td></td>
<td>script-_module</td>
<td>General binary data consisting of 8-bit bytes.</td>
<td></td>
</tr>
</tbody>
</table>
Signed and Clear-Signed Data

- 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 EIGamal
  - EIGamal 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**
  - Signed 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

Figure 22.3 Simple Example of DKIM Deployment
Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

- 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 RFC 4346: Transport Layer Security (TLS)

Two Implementation choices:

- Provided as part of the underlying protocol suite
- Embedded in specific packages

Figure 22.4 SSL/TLS Protocol Stack

TLS Concepts

TLS Session
- An association between a client and a server
- Created by the Handshake Protocol
- Define a set of cryptographic security parameters
- Used to avoid the expensive negotiation of new security parameters for each connection

TLS Connection
- A transport (in the OSI layering model definition) that provides a suitable type of service
- Peer-to-peer relationships
- Transient
- Every connection is associated with one session
Change Cipher Spec Protocol

- One of four TLS specific protocols that use the TLS 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

Alert Protocol

- Conveys TLS-related alerts to peer entity
- Each message consists of two bytes
- Alert messages are compressed and encrypted
- 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, TLS immediately terminates the connection
- Other connections on the same session may continue, but no new connections on this session may be established
Handshake Protocol

- Most complex part of TLS
- 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

Heartbeat Protocol

- A periodic signal generated by hardware or software to indicate normal operation or to synchronize other parts of a system
- Typically used to monitor the availability of a protocol entity
- Defined in 2012 in RFC 6250
- Runs on top of the TLS Record Protocol
- Use is established during Phase 1 of the Handshake Protocol
- Each peer indicates whether it supports heartbeats
- Serves two purposes:
  - Assures the sender that the recipient is still alive
  - Generates activity across the connection during idle periods

Figure 22.6 Handshake Protocol Action

Client

Server

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.
SSL/TLS Attacks

Attacks on the Handshake Protocol

Attacks on the record and application data protocols

Four general categories:

Attacks on the PKI

Other attacks

Attacks on the Handshake Protocol

Attacks on the record and application data protocols

Four general categories:

Attacks on the PKI

Other attacks

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
  o Search engines do not support HTTPS
  o 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

Figure 22.7 The Heartbleed Exploit

Source: BAE Systems
IP Security (IPsec)

- Various application security mechanisms
  - S/MIME, 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

**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

Applications of IPsec

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establishing extranet and intranet connectivity with partners
- Enhancing electronic commerce security
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

VPN's want both authentication and encryption

Also an authentication-only function, implemented using an Authentication Header (AH)
- Because message integrity is only provided by ESP, the use of AH is limited to peers that have identical 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
Transport and Tunnel Modes

Transport Mode

- Extends to the payload of an IP packet
- Typically used for end-to-end communication between two hosts
- ESP 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
- A number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec

Summary

- Secure E-mail and S/MIME
  - MIME
  - S/MIME
- DomainKeys identified mail
  - Internet mail architecture
  - DKIM strategy
- SSL and TLS
  - TLS architecture
  - TLS protocols
  - TLS attacks
  - SSL/TLS attacks
- HTTPS
  - Connection institution
  - Connection closure
- IPv4 and IPv6 security
  - IP security overview
  - The scope of IPsec
  - Security associations
  - Encapsulating security payload
  - Transport and tunnel modes