End-to-End Encryption Methods

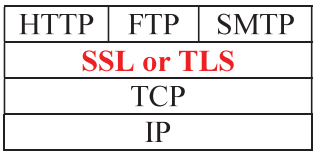
Encryption by Application

Applications are encrypted on a case by case basis.

Secure Shell (SSH): Provides an authenticated and encrypted remote login and file transfer capability.
Can tunnel XWindows, ftp, POP-3, IMAP-4, … replaces RCP, rlogin, rsh
Authenticates before allowing connection
Generates a public/private key pair; notifies partner systems of public key
SSH protocol negotiates the encryption algorithm: DES, IDEA, AES and the authentication algorithm: public key & Kerberos.
SSH2: Can negotiate between 3DES, IDEA, Blowfish, Twofish, Arcfour, Cast
SSHv2 is more secure than SSHv1, which has numerous exploits
Uses port 22 for all applications
SSH is free or minimal cost for commercial version

Secure Sockets Layer (SSL): Protects communication above the transport level: Web
Certificate-based system created by Netscape to protect web page communications
Implemented by Netscape & Microsoft Explorer and other browsers – widely available
When SSL & HTTP used together is called **HTTPS**
Standardized in IETF as **Transport Layer Security (TLS)** which is nearly equal to SSLv3 but incompatible (RFC 2246)
URL name starts as https:// - also key or lock icon displays at bottom corner.

SSL protocol negotiates the security algorithm:
Confidentiality: DES, 3DES, AES, RC4
Integrity: MD5, SHA-1
Authentication: RSA, Diffie-Hellman
Non-Repudiation: Digital Signature
Both Netscape and Internet Explorer allow you to configure SSL parms
Steps include:
Customer generates session key which is encrypted & sent to server using server's public key
Client initiates negotiation of security parms. However server may negotiate to lesser security
Client authenticates server certificate using public key encryption and possibly vice versa



Secure Hypertext Transport Protocol (SHTTP): Extends HTTP protocol to protect each message sent between 2 computers.
Summarize the difference between HTTP and HTTPS

HTTP	HTTPS
URL begins with "http://"	URL begins with "https://"
It uses port 80 for communication	It uses port 443 for communication
Unsecured	Secured
Operates at Application Layer	Operates at Transport Layer
No encryption	Encryption is present
No certificates required	Certificates required

Pretty Good Privacy (PGP): Email encryption method
Available in 1991, currently free but also became a commercial product in 1996
Public Keys can be registered under email names at:
ldap://certsaver.pgp.com
http://pgpkeys.mit.edu:11371
Point your PGP utility at one of them
Web of Trust: Trust that that the keys you get in email (from people you know) or in a list via email (from people you know) is authentic
Senders can put their PGP public key at the bottom of their email messages.
Not endorsed by NSA, but good for private use
Uses RSA or Diffie-Hellman public key encryption for key exchange
Uses IDEA, 3DES, or CAST for message encryption
Uses MD5 hashing algorithm for integrity
Authentication provided via public key certificates – generated as part of PGP
Nonrepudiation provided via digitally signed messages.

<table>
<tr><td rowspan="2">Kerberos</td><td>S/MIME</td><td>PGP</td><td>SET</td></tr>
<tr><td colspan="2">SMTP</td><td>HTTP</td></tr>
<tr><td>UDP</td><td colspan="3">TCP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

Secure Multipurpose Internet Mail Extensions (S/MIME): An Internet standard for secure email attachments
MIME: Protocol specification dictates how multimedia data and email attachments are transferred: E.g., Header=Image, subtype=jpeg.
Used for encryption and digital signatures
Encrypts many types of attachments: spreadsheets, graphics, presentations, movies, sound.
Uses public key certificates, in X.509 format, for authentication and key exchange
Can negotiate from a set of encryption algorithms: DES, AES, RC2
Integrated into many commercial email packages, including sendmail.

Secure Electronic Transaction (SET): Protects credit card transactions on the Internet
Requested by MasterCard and Visa in 1996
Provides trust by use of X.509 digital certificates
Ensures privacy & secure communications

Discussion: What info is visible (unencrypted) in the SSL packets? In the PGP or S/MIME packets?