SNS COLLEGE OF ENGINEERING

KURUMBAPALAYAM (PO), COIMBATORE – 641 107
ACCREDITED BY NAAC-UGC WITH 'A' GRADE
APPROVED BY AICTE & AFFILIATED TO ANNA UNIVERSITY, CHENNAI

Department of Artificial Intelligence & Data Science

Course Name:19AD511 Cyber Security

III YEAR/V SEMESTER

UNIT-III DEFENSE SECURITY COUNTER MEASURES

Cryptography in Network Security

Cryptography in Network Security

- There are two broad classes of encryption:
- symmetric (secret key) and
- asymmetric (public key) systems.
- The first of those is the cryptographic workhorse, used for bulk encryption of large quantities of data. That description perfectly fits network traffic, and that is exactly how it is used.
- The second class of cryptographic algorithms excels at establishing a trustworthy relationship between two parties who may not previously have had one, which also applies naturally in a networking situation.
- In this section we describe how those two approaches can provide security strength in a network.

Modes of Network Encryption

Link Encryption

- In link encryption, data are encrypted just before the system places them on the physical communications link.
- In this case, encryption occurs at layer 1 or 2 in the OSI model. Similarly, decryption occurs just as the communication arrives at and enters the receiving computer.
- The data travel in plaintext through the top layers of the model until they are encrypted just prior to transmission, at level 1.
- Addressing occurs at level 3. Therefore, in the intermediate node, the encryption must be removed in order to determine where next to forward the data, and so the content is exposed.

Link Encryption

- In link encryption, data are encrypted just before the system places them on the physical communications link.
- In this case, encryption occurs at layer 1 or 2 in the OSI model.
- Similarly, decryption occurs just as the communication arrives at and enters the receiving computer. the data travel in plaintext through the top layers of the model until they are encrypted just prior to transmission, at level 1.
- Addressing occurs at level 3. Therefore, in the intermediate node, the encryption must be removed in order to determine where next to forward the data, and so the content is exposed

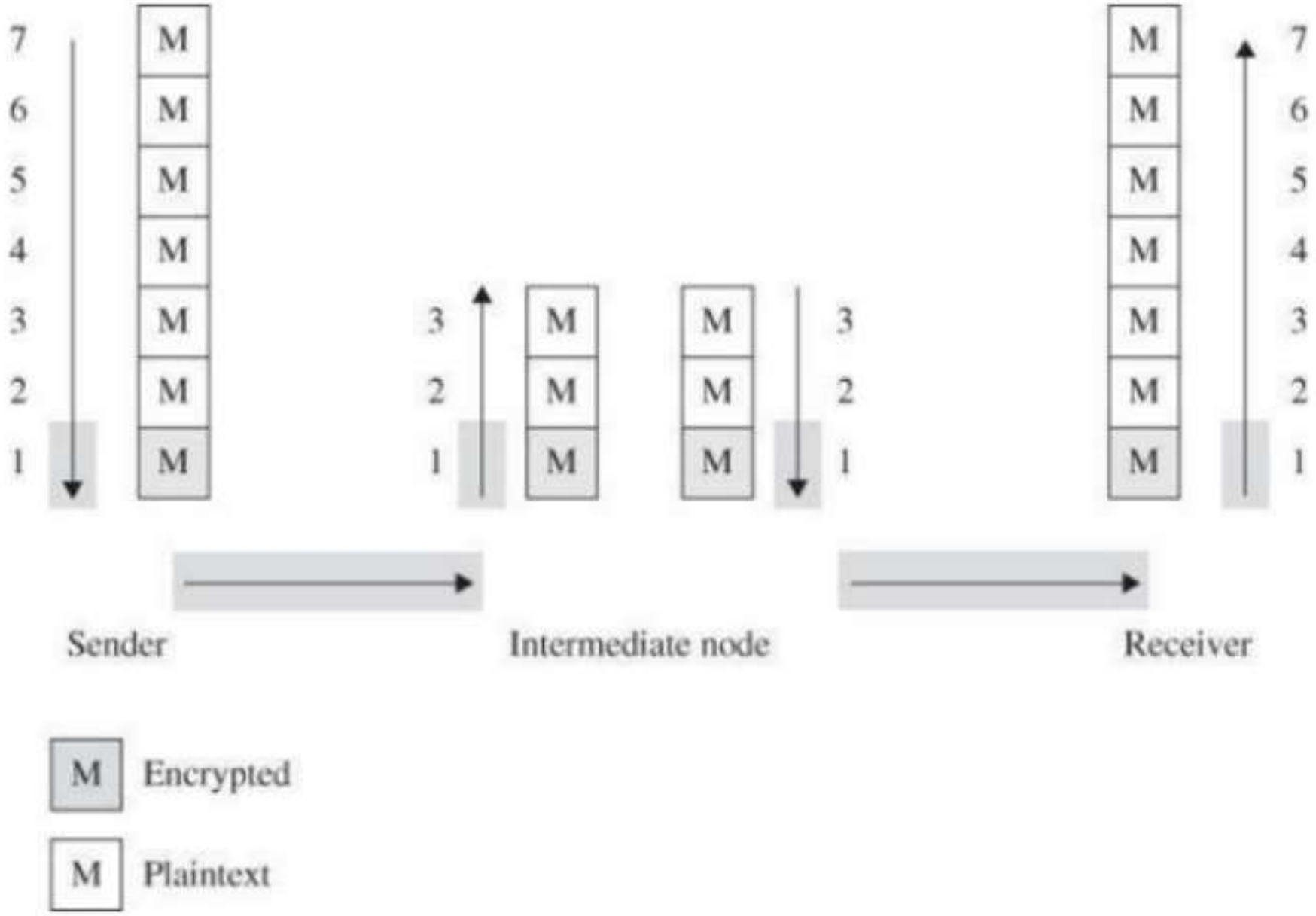

FIGURE 6-36 Model of Link Encryption

End-to-End Encryption

- End-to-end encryption provides security from one end of a transmission to the other.
- The encryption can be applied between the user and the host by a hardware device.
- Alternatively, the encryption can be done by software running on the host computer.
- In either case, the encryption is performed at the highest levels, usually by an application at OSI level 7, but sometimes 5 or 6.

End-to-end Encryption

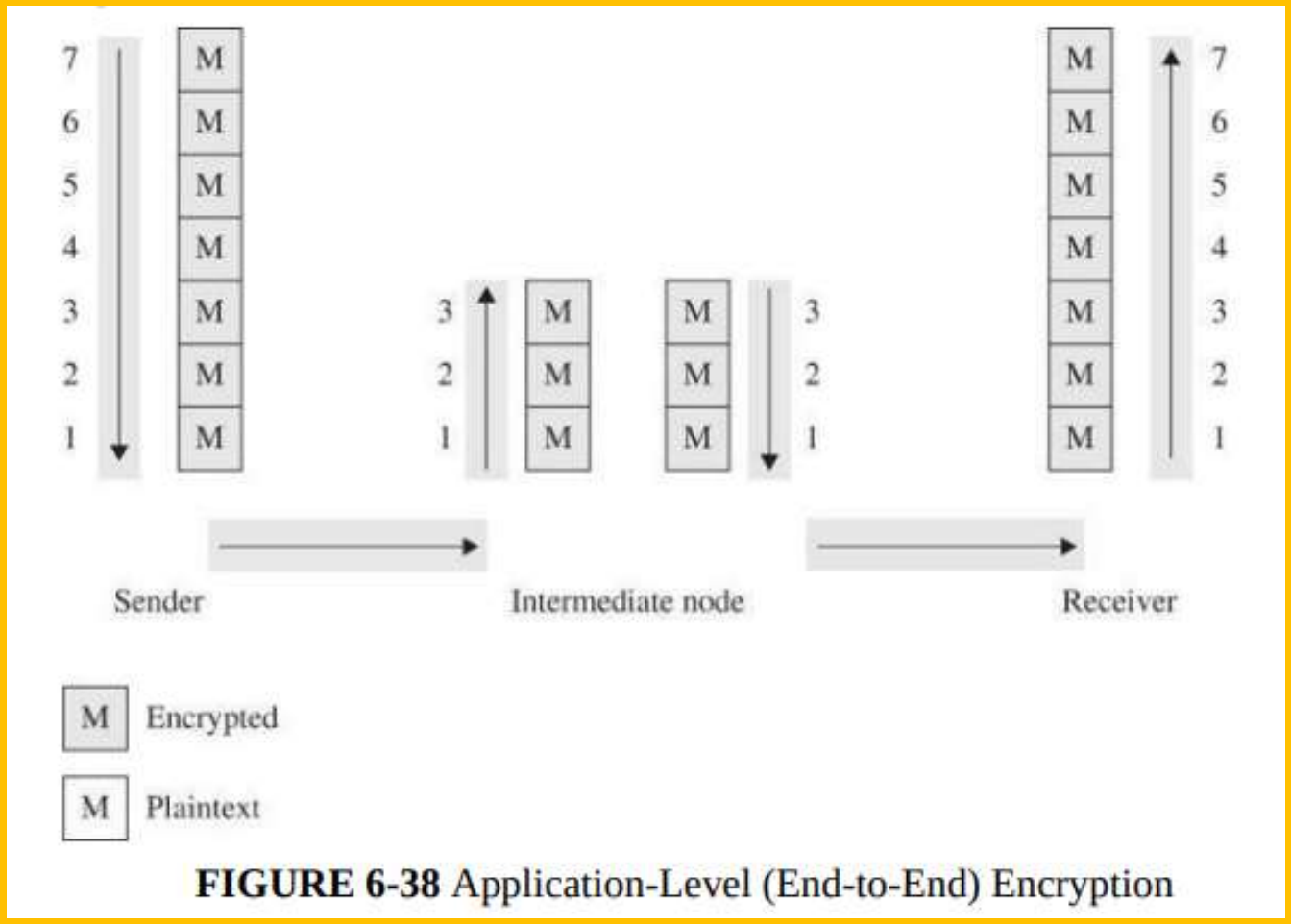

FIGURE 6-38 Application-Level (End-to-End) Encryption

COMPARISION OF link and End-to-end Encryption

Link Encryption	End-to-End Encryption
Security within hosts	
Data partially exposed in sending host	Data protected in sending host
Data partially exposed in intermediate nodes	Data protected through intermediate nodes
Role of user	
Applied by sending host	Applied by user application
Invisible to user	User application encrypts
Host administrators select encryption	User selects algorithm
One facility for all users	Each user selects
Can be done in software or hardware	Usually software implementation; occasionally performed by user add-on hardware
All or no data encrypted	User can selectively encrypt individual data items
Implementation considerations	
Requires one key per pair of hosts	Requires one key per pair of users
Provides node authentication	Provides user authentication

TABLE 6-3 Comparison of Link and End-to-End Encryption

Browser Encryption

- Browsers can encrypt data for protection during transmission. The browser and the server negotiate a common encryption key, so even if an attacker does hijack a session at the TCP or IP protocol level, the attacker, not having the proper key, cannot join the application data exchange.

1. SSH Encryption

- SSH (secure shell) is a pair of protocols (versions 1 and 2) originally defined for Unix but now available under most operating systems.

- SSH provides an authenticated and encrypted path to the shell or operating system command interpreter.

- Both SSH versions replace Unix utilities such as Telnet, rlogin, and rsh for remote access. SSH protects against spoofing attacks and modification of data in communication.

1. SSL and TLS Encryption

- The Secure Sockets Layer (SSL) protocol was originally designed by Netscape in the mid-1990s to protect communication between a web browser and server. It went through three versions: SSL 1.0 (private), SSL 2.0 (1995), and SSL 3.0 (1996). In 1999, the Internet Engineering Task Force upgraded SSL 3.0 and named the upgrade TLS, for transport layer security. TLS 1.0, which is sometimes also known as SSL 3.1, is documented in Internet RFC 2246; two newer versions are named TLS 1.1 (RFC 4346, 2006) and TLS 1.2 (RFC 5246, 2008). The acronym SSL is often used to represent both the SSL and TLS protocol suites.

SSL and TLS Encryption

The Secure Sockets Layer (SSL) protocol was originally designed by Netscape in the mid-1990s to protect communication between a web browser and server.

It went through three versions: SSL 1.0 (private), SSL 2.0 (1995), and SSL 3.0 (1996). In 1999, the Internet Engineering Task Force upgraded SSL 3.0 and named the upgrade TLS, for transport layer security.

TLS 1.0, which is sometimes also known as SSL 3.1, is documented in Internet RFC 2246; two newer versions are named TLS 1.1 (RFC 4346, 2006) and TLS 1.2 (RFC 5246, 2008). The acronym SSL is often used to represent both the SSL and TLS protocol suites.

Cipher Suite

- Client and server negotiate encryption algorithms, called the cipher suite, for authentication, session encryption, and hashing.
- To allow for expansion and deprecation of algorithms over time, the first to open an interaction, often the client, states its preferred algorithms, and the second party responds with the highest one on that list it can handle.

SSL Session

- Because SSL is commonly used with web pages, it is often referred to as HTTPS (HTTP Secure), and you will see the https: prefix in the address bar of a browser, as well as a closed padlock in the corner whenever SSL is in operation.
- To use SSL, the client requests an SSL session.
- The server responds with its public key certificate so that the client can determine the authenticity of the server.
- The client returns a symmetric session key encrypted under the server’s public key. Both the server and client compute the session key, and then they switch to encrypted communication, using the shared session key.

Onion Routing

- Onion routing is a technique for anonymous communication over a computer network.
- In an onion network, messages are encapsulated in layers of encryption, analogous to layers of an onion.
- There is a large set of preventive measures and best practices to make web browsing safer and more secure for users.
- Let’s say that you send an HTTPS request to a server and someone intercepts that request but that person can’t know what that message says because it’s encrypted.