# Introduction to Cyber Security

Module 4

# Network Security

# Part B

# Internet Security Protocols

After studying this topic, you should be able to:

- Provide an overview of MIME.
- Understand the functionality of S/MIME and the security threats it addresses.
- Explain the key components of SSL.
- Discuss the use of HTTPS.
- Provide an overview of IPsec.

# Secure Email and S/MIME

- S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security.
- **MIME:**

✓ MIME is an extension to the old RFC 822 specification of an Internet mail format.

✓ RFC 822 defines a simple header with To, From, Subject, and other fields that can be used to route an e-mail message through the Internet and that provides basic information about the e-mail content.

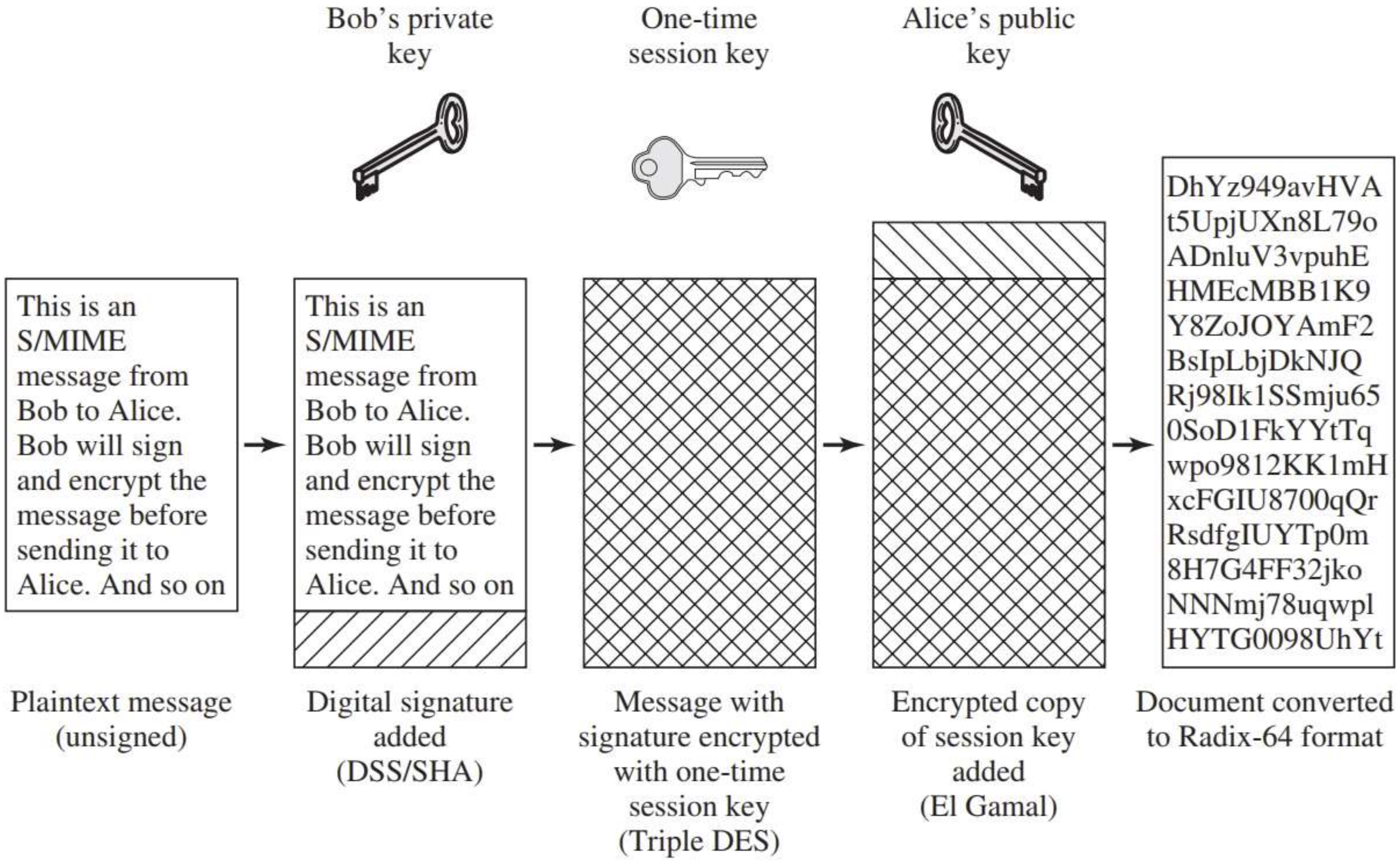
✓ RFC 822 assumes a simple ASCII text format for the content.

# MIME

- MIME provides a number of new header fields that define information about the body of the message, including the format of the body and any encoding that is done to facilitate transfer.
- Most important, MIME defines a number of content formats, which standardize representations for the support of multimedia e-mail.
- Examples include text, image, audio, and video.

# S/MIME

- S/MIME is defined as a set of additional MIME content types and provides the ability to sign and/or encrypt e-mail messages.

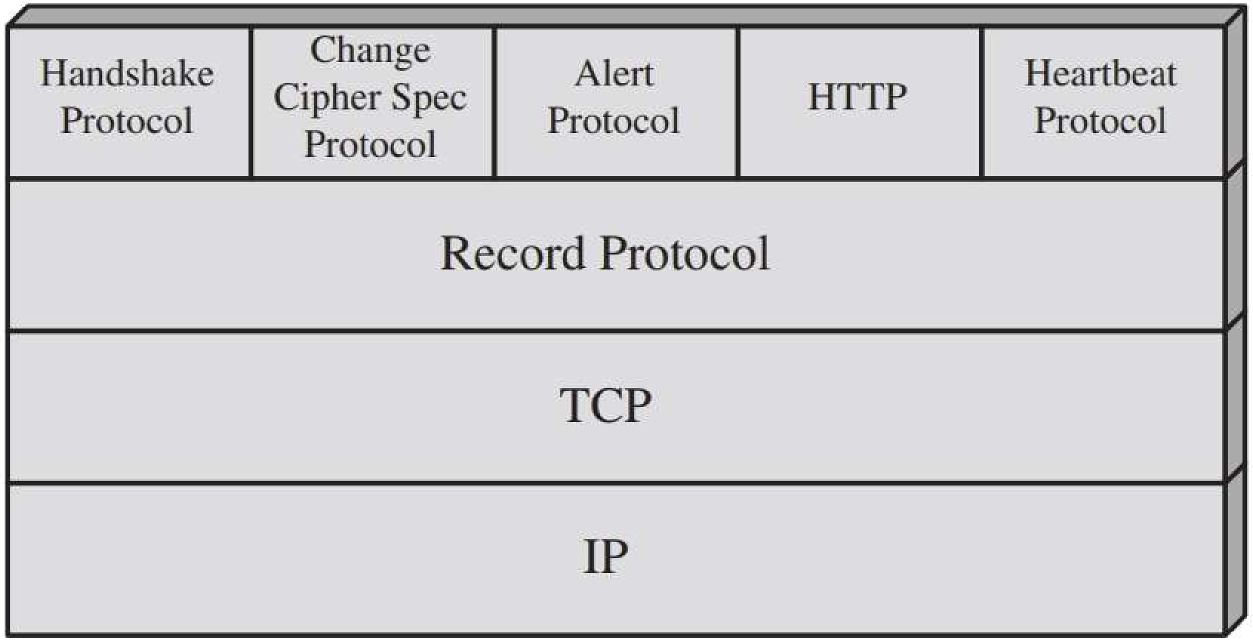


Bob's private key
One-time session key
Alice's public key
This is an S/MIME message from Bob to Alice. Bob will sign and encrypt the message before sending it to Alice. And so on
This is an S/MIME message from Bob to Alice. Bob will sign and encrypt the message before sending it to Alice. And so on
DhYz949avHVA
t5UpjUXn8L79o
ADnluV3vpuhE
HMEcMBB1K9
Y8ZoJOYAmF2
BsIpLbjDkNJQ
Rj98Ik1SSmju65
0SoD1FkYYtTq
wpo9812KK1mH
xcFGIU8700qQr
RsdfgIUYTp0m
8H7G4FF32jko
NNNmj78uqwpl
HYTG0098UhYt
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

# SSL and TLS

**Transport Layer Security (TLS) Architecture:**

- ✓ TLS is designed to make use of TCP to provide a reliable end-to-end secure service.
- ✓ TLS is not a single protocol but rather two layers of protocols



SSL/TLS Protocol Stack

# HTTPS

- HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server.
- The HTTPS capability is built into all modern Web browsers. Its use depends on the Web server supporting HTTPS communication.
- A normal HTTP connection uses port 80. If HTTPS is specified, port 443 is used, which invokes SSL.

# Contd…

- When HTTPS is used, the following elements of the communication are encrypted:

✓ URL of the requested document

✓ Contents of the document

✓ Contents of browser forms (filled in by browser user)

✓ Cookies sent from browser to server and from server to browser

✓ Contents of HTTP header

# IPv4 and IPv6 Security

- IP-level security encompasses three functional areas: authentication, confidentiality, and key management.
- The key management facility is concerned with the secure exchange of keys.
- The current version of IPsec, known as IPsecv3, encompasses authentication and confidentiality.
- Key management is provided by the Internet Key Exchange standard, IKEv2.

# Honeypots

- A further component of intrusion detection technology is the honeypot.
- Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.
- Honeypots are designed to:

✓ Divert an attacker from accessing critical systems.

✓ Collect information about the attacker’s activity.

✓ Encourage the attacker to stay on the system long enough for administrators to respond.

- These systems are filled with fabricated information designed to appear valuable but that a legitimate user of the system would not access.

# Contd…

- Thus, any access to the honeypot is suspect.
- The system is instrumented with sensitive monitors and event loggers that detect these accesses and collect information about the attacker's activities.
- Because any attack against the honeypot is made to seem successful, administrators have time to mobilize and log and track the attacker without ever exposing productive systems.
- The honeypot is a resource that has no production value. There is no legitimate reason for anyone outside the network to interact with a honeypot.
- Thus, any attempt to communicate with the system is most likely a probe, scan, or attack.

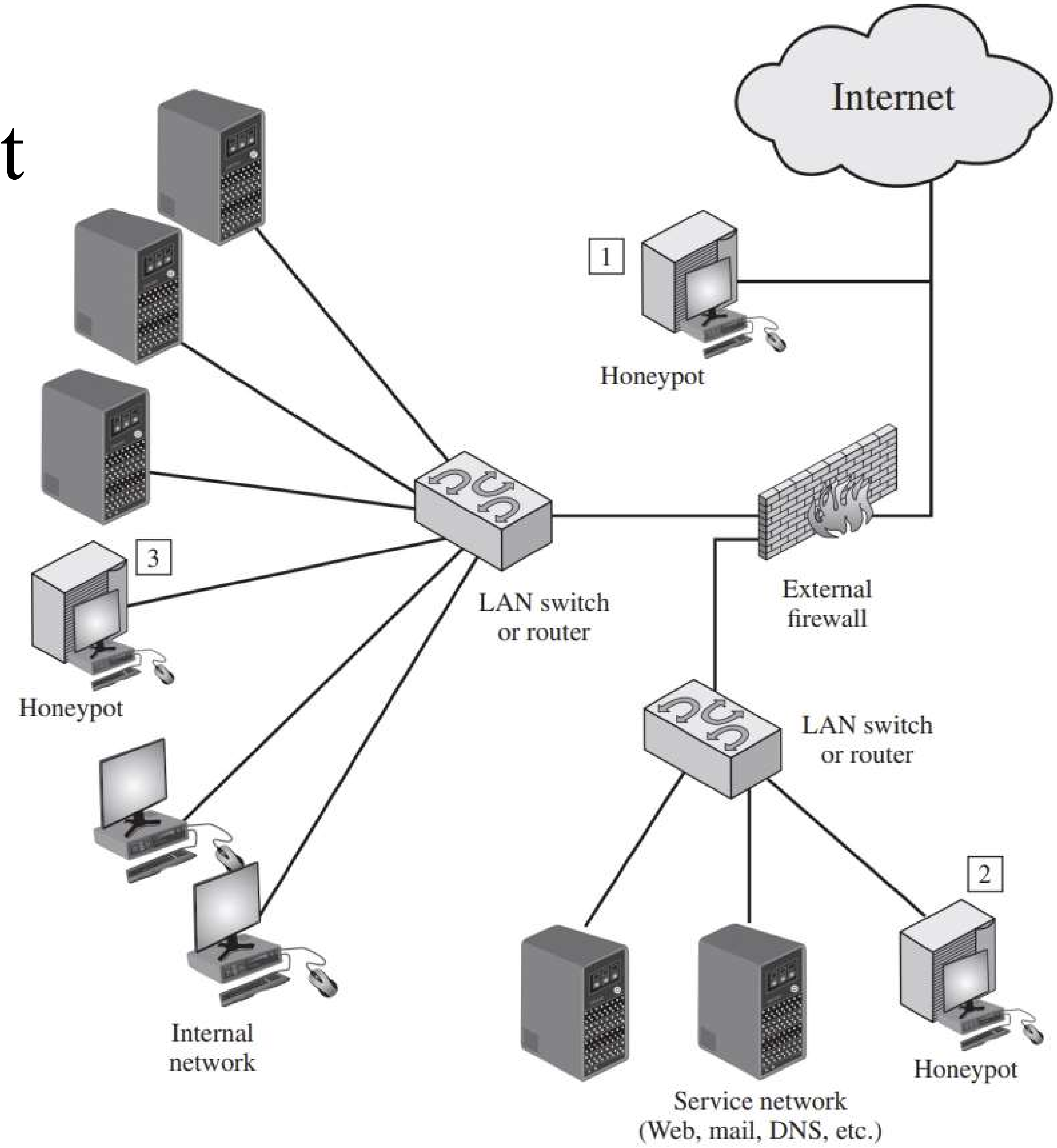
# Contd…

- Conversely, if a honeypot initiates outbound communication, the system has probably been compromised.
- Honeypots are typically classified as being either low or high interaction.

✓ **Low interaction honeypot:** Consists of a software package that emulates particular IT services or systems well enough to provide a realistic initial interaction, but does not execute a full version of those services or systems.

✓ **High interaction honeypot:** Is a real system, with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers.

# Deployment Locations


Internet
1
Honeypot
External firewall
LAN switch or router
3
Honeypot
Internal network
LAN switch or router
2
Honeypot
Service network (Web, mail, DNS, etc.)