Chapter Objectives

- Learn to implement secure protocols for given scenarios
- Explore use cases for secure protocols

Secure Protocols

- Protocols enable communication between components
- They are independent of vendor
- Act as a language that specifies how communications are to be conducted, and what can be communicated
- Protocols may have both secure and non/secure versions

DNSSEC

- The Domain Name Service (DNS) is a protocol for the translation of names into IP addresses
- The protocol uses UDP over port 53 for standard queries
- DNS is a hierarchical system of servers
- Requests and replies are sent in plaintext and are subject to spoofing
- DNSSEC (Domain Name System Security Extensions) is to use cryptography, enables origin authentication, authenticated denial of existence, and data integrity
- DNSSEC records are signed
- UDP 53 are size limited to 512 bytes, and DNSSEC packets can be larger – DNSSEC typically uses TCP port 53
**SSH**

- The *Secure Shell (SSH)* protocol is an encrypted remote terminal connection.
- SSH uses asymmetric encryption.
- Generally requires an independent source of trust with a server, such as manually receiving a server key.
- SSH uses TCP port 22 as its default port.

**S/MIME**

- MIME (Multipurpose Internet Mail Extensions) is a standard for transmitting binary data via an e-mail.
- They are sent as plaintext files, and any attachments need to be encoded with base64 encoding – no security.
- S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data.
- S/MIME is designed to provide cryptographic protections to e-mails and facilitate interoperability.

**SRTP**

- The *Secure Real-time Transport Protocol (SRTP)* is a network protocol for securely delivering audio and video over IP networks.
- It uses cryptography to provide encryption, message authentication and integrity, and replay protection to the RTP data.

**LDAPS**

- LDAP is the primary protocol for transmitting directory information e.g. Active Directory datasets.
- Lightweight Directory Access Protocol (LDAP) traffic is transmitted insecurely.
- You can make LDAP traffic secure by using it with SSL/TLS, known as LDAP Secure (LDAPS).
- LDAP is enabled over SSL/TLS by using a certificate from a trusted certificate authority (CA).
- LDAPS uses a TLS/SSL tunnel to connect LDAP services.
- This method was retired with LDAP v2, and replaced with Simple Authentication and Security Layer (SASL) in LDAP v3.
FTPS

- FTPS is the implementation of FTP over an SSL/TLS secured channel
- This supports complete FTP compatibility, yet provides the encryption protections enabled by SSL/TLS
- FTPS uses TCP ports 989 and 990

SFTP

- SFTP is the use of FTP over an SSH channel
- This leverages the encryption protections of SSH to secure FTP transfers
- Because of its reliance on SSH, it uses TCP port 22

SNMP v3

- The Simple Network Management Protocol version 3 (SNMP v3) is a standard for managing devices on networks
- I was developed specifically to address the security concerns and vulnerabilities of SNMP v1 and SNMP v2
- All versions of SNMP require ports 161 and 162 to be open on a firewall

SSL/TLS

- Secure Sockets Layer (SSL) is an encryption technology developed for transport-layer protocols across the Web
- It uses public key encryption methods to exchange a symmetric key for use in confidentiality and integrity
- The current version, V3, is outdated, having been replaced by the IETF standard TLS
- Transport Layer Security (TLS) is an IETF standard for encryption and replaces SSL – not compatible
- The standard port for SSL and TLS is undefined – it depends upon what the protocol that is being protected uses
**HTTPS**

- **Hypertext Transfer Protocol Secure (HTTPS)** is the use of SSL or TLS to encrypt a channel over which HTTP traffic is transmitted.
- Because of issues with all versions of SSL, only TLS is recommended for use.
- This uses TCP port 443.
- HTTPS is the most widely used method to secure HTTP traffic.

---

**Secure POP/IMAP**

- **Secure POP/IMAP** refers to POP3 and IMAP (respectively) over an SSL/TLS session.
- Secure POP3 utilizes TCP port 995.
- Secure IMAP uses TCP port 993.
- Encrypted data from the e-mail client is sent to server.
- TLS is the preferred protocol today.
- SMTP uses port 25, and SSL/TLS encrypted SMTP uses port 465.

---

**Use Cases**

- Various IETF working groups have been working to standardize some general-purpose security protocols.
- Some can be reused over and over instead of inventing new ones for each use case.
- SASL is a standardized method of invoking a TLS tunnel to secure a communication channel.
- This method is shown to work with a wide range of services, currently more than 15.

---

**Voice and Video**

- **Voice and video** are frequently streaming media and they have their own protocols for encoding data streams.
- To securely transfer this material, you can use the **Secure Real-time Transport Protocol (SRTP)**
Time Synchronization

- Network Time Protocol (NTP) is the standard for time synchronization across servers and clients
- NTP is transmitted over UDP port 123
- NTP has no assurance against a man-in-the-middle attack
- You could enclose all time communications using a TLS tunnel, although this is not an industry practice
- Since time is very important that port is always available and open for potential attacks

E-mail and Web

- E-mail and the Web are native plaintext-based systems
- HTTPS relies on SSL/TLS to secure web connections
- Use of HTTPS is widespread and common (msudenver.edu)
- E-mail is a bit more complicated to secure, and the best option is via S/MIME
- Lately there have been security issues not with the protocol but how TLS was attached and implemented with e-mail
- There are also industry requirements to retire unsafe version

File Transfer

- Secure file transfer can be accomplished via a wide range of methods, ensuring the confidentiality and integrity of file transfers across networks
- FTP is not secure but sFTP and FTPS are secure alternatives that can be used
- Metro only allows sFTP for file transfers – otherwise the connection will be refused

Directory Services

- Directory services use LDAP as the primary protocol
- When security is required, LDAPS is a common option
- Directory services are frequently found behind the scenes with respect to logon information
- Directory information is very important and needs to be protected
- It is challenging with cloud services using SSO solution
Remote Access

- Remote access is the means by which users can access computer resources across a network.
- Securing remote access can be done via many means.
- Organizations commonly use SSL/TLS.
- Depending upon the device being accessed, a variety of secure protocols exist.
  - Networking equipment: SSH is the secure alternative to Telnet.
  - Servers and other computer connections: access via VPN, or use of IPSec, is common.

Domain Name Resolution

- Domain name resolution is performed primarily by DNS.
- DNS is a plaintext protocol and DNSSEC is not widely used.
- DNSSEC has been available in Windows Active Directory domains since 2012.
- TCP and UDP port 53 can be used for DNS, with the need of firewall protection between the Internet and TCP port 53 to prevent attackers from accessing zone transfers.

Routing and Switching

- Routing and switching are the backbone functions of networking in a system.
- Managing the data associated with networking is the province of SNMP v3.
- It enables applications to manage data associated with networking and devices.
- Local access to the boxes may be accomplished by Telnet, although for security reasons SSH should be used instead.

Network Address Allocation

- Managing network address allocation requires multiple decision criteria, including the reduction of complexity and the management of device names and locations.
- SNMPv3 has many functions that can be employed to manage the data flows.
- IP addresses can be allocated either statically, or via DHCP.
- IP address allocation is part of proper network design – segmentation, traffic control.
Subscription Services

- Subscription services is the management of data flows to and from a system based on either a push (publish) or pull (subscribe) model.
- Managing data can be managed by using directory services.
- Software as a Service (SaaS) model.
- The actual software is hosted centrally, commonly in the cloud, and user access is based on subscriptions.
- This is becoming a common software business model.

Stay Alert!

There is no 100 percent secure system, and there is nothing that is foolproof!