REVIEW LESSON

MTA Course: 98-367 Security Fundamentals
Lesson name: Understanding Operating System Security 2.5_B
Topic: Understand encryption (Part 2)
(One 50-minute class period)
File name: SecurityFund_RL_2.5_B

Lesson Objective

2.5_B: Understand core security principles. *This objective may include, but is not limited to:* VPN, public key and private key, encryption algorithms, certificate properties, certificate services, PKI/certificate services infrastructure, token devices.

Preparation Details

Instructor preparation activities

- Make copies of Student Activity SecurityFund_SA_2.5_B

Resources, software, and additional files needed for this lesson

- SecurityFund_PPT_2.5_B
- SecurityFund_SA_2.5_B
- SecurityFund_SA_2.5_B_Key
- Internet access

Teaching Guide

Essential Vocabulary

certificate—a public key certificate, usually just called a certificate, is a digitally signed statement that's commonly used for authentication and to secure information on open networks. A certificate securely binds a public key to the entity that holds the

corresponding private key. The issuing CA digitally signs the certificates, and they can be issued for a user, a computer, or a service.

certification authority (CA)—an issuer of digital certificates, the cyberspace equivalent of identity cards. A certificate authority may be an external issuing company (such as VeriSign) or an internal company authority that has installed its own server (such as the Microsoft® Certificate Server) for issuing and verifying certificates. A CA is responsible for providing and assigning the unique strings of numbers that make up the "keys" used in digital certificates for authentication and to encrypt and decrypt sensitive or confidential incoming and outgoing online information.

point-to-point tunneling protocol (PPTP)—a tunneling protocol first supported in Windows® NT 4.0 and Windows 98. PPTP is an extension of point-to-point protocol (PPP) and leverages the authentication, compression, and encryption mechanisms of PPP. Client support for PPTP is built-in to the Windows XP remote access client.

layer 2 tunneling protocol with Internet protocol security (L2TP/IPSec)—a combination of PPTP and Layer 2 Forwarding (L2F), a technology proposed by Cisco Systems, Inc. Rather than having two incompatible tunneling protocols competing in the marketplace and causing customer confusion, the IETF mandated that the two technologies be combined into a single tunneling protocol that represents the best features of PPTP and L2F.

private key—one of two keys in public key encryption. The user keeps the private key secret and uses it to encrypt digital signatures and to decrypt received messages.

public key—one of two keys in public key encryption. The user releases this key to the public, who can use it for encrypting messages to be sent to the user and for decrypting the user's digital signature.

public key infrastructure (PKI) —refers to the set of hardware, software, people, policies, and procedures necessary to create, manage, store, distribute, and revoke certificates based on public key cryptography. The characteristic operation of PKI is known as certification (the issuance of certificates). PKI certification provides a framework for the security feature known as authentication (proof of identification).

token devices—a security token (or sometimes a hardware token, hard token, authentication token, USB token, cryptographic token, or key fob) may be a physical device that an authorized user of computer services is given to ease authentication. The term may also refer to software tokens.

virtual private network (VPN)—nodes on a public network such as the Internet that communicate among themselves using encryption technology so that their messages are as safe from being intercepted and understood by unauthorized users as if the nodes were connected by private lines.

Lesson Sequence

Activating prior knowledge/lesson staging (Anticipatory Set: 10 minutes, Slide 3)

1. Student prompt (see PowerPoint® slide 3)
    - On a sheet of paper, list information that is stored in a "certificate". Why is each piece of the information important?
    - Give students a few minutes to research, allowing them to work until they have finished.
    - As time permits, call on a few students to report to the group with their responses.

Lesson activity (40 minutes, slides 4–11)

1. Teacher Instruction (20 minutes)
    - Use the included PowerPoint slideshow to review various types of encryption.
    - At the end of the slideshow, ask the students to discuss the overall importance of data, user, password, and access encryption. Small group discussions may be beneficial.
        - Show the presentation and give the students a few minutes to process the information and come up with their answers/opinions.
        - Have each pair of students share their answers with the whole group.

2. Guided Practice (20 minutes) (Use the SecurityFund_SA_2.5_B document and Slide 13)
    - Students complete the worksheet identifying the different types of encryption requirements and deciding which applications are appropriate for different situations.
    - If time allows, you may review all or part of the worksheets and discuss student responses to the questions.

Assessment/lesson reflection (10 minutes, slide 14)

1. Use the "History Lesson" as a "ticket out the door" to encourage students to review the lesson concepts in terms of this information and to provide an opportunity for additional questions. The last slide in the PowerPoint facilitates this exercise.

2. Tell students to write any questions they have or any topics about which they would like more assistance.

3. After class, look through the student responses and follow up with any student requiring additional help.

Microsoft resources and Web links

- **TechNet: Certificates**
  http://technet.microsoft.com/en-us/library/cc700805.aspx
- **TechNet: Data Encryption**
  http://technet.microsoft.com/en-us/library/cc785633(WS.10).aspx
- **TechNet: PKI Technologies**
  http://technet.microsoft.com/en-us/library/cc779826(WS.10).aspx
- **TechNet: Configuring Authentication for Exchange ActiveSync®**
  http://technet.microsoft.com/en-us/library/bb430770.aspx