REVIEW LESSON

MTA Course: 98-367 Security Fundamentals
Lesson name: Wireless Security 1.4
Topic: Understand wireless security
(One 50-minute class period)
File name: SecurityFund_RL_1.4

Lesson Objective

1.4: Understand wireless security. *This objective may include but is not limited to:* advantages and disadvantages of specific security types; keys; SSID; MAC filters.

Preparation Details

Prerequisite student experiences and knowledge

This MTA Certification Exam Review lesson is written for students who have learned about security fundamentals. Students who do not have the prerequisite knowledge and experiences cited in the objective will find additional learning opportunities using resources such as those listed in the Microsoft® resources and Web links at the end of this review lesson.

Resources, software, and additional files needed for this lesson

- SecurityFund_PPT_1.4
- A wireless connection installed on each computer and configured with a local access point
- Examples that your students can recognize and associate with the different wireless access points and routers

Teaching Guide

Essential Vocabulary

media access control (MAC)—in the IEEE 802.x specifications, the lower of two sublayers that make up the ISO/OSI data link layer. The MAC manages access to the physical network, delimits frames, and handles error control.

MAC filters—a Wi-Fi network access point can be configured so that only preauthorized nodes, based upon their MAC addresses, may connect.

service set identifier (SSID)—a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS (the communicating stations, or nodes, on a wireless LAN). An SSID is also referred to as a *network name* because essentially it is a name that identifies a wireless network.

Wi-Fi protected access (WPA)—a Wi-Fi standard that was designed to improve upon the security features of WEP.

wired equivalent privacy (WEP)—an encryption algorithm system included as part of the 802.11 standard, developed by the Institute of Electrical and Electronics Engineers as a security measure to protect wireless LANs from casual eavesdropping.

Lesson Sequence

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

1. Have students open the "Network Places" icon on their personal or lab computer. Click on Properties and investigate the wireless connection. Have them record their findings.
2. Give students a few minutes to research, allowing them to work until they have finished.
3. As time permits, call on a few students to report to the group with their responses.

Lesson activity (40 minutes)

1. Teacher Instruction (20 minutes)
    - Use the included PowerPoint® slideshow to review the different types of wireless security.
    - At the end of the slideshow, have the students answer the Review Questions. Small-group discussions may be beneficial.
        - Show the question and give the students 1 minute to process the question and come up with answers.

- Then give the students 2 minutes to discuss answers with a partner.
- Finally, have each pair of students share their answers with the whole group.
- Repeat for each additional review question.

2. Guided Practice (20 minutes)

   Have students make a chart, identifying the different types of wireless security and deciding which technology is appropriate for different situations.

   - If time allows, you may review all or part of the assignment, discussing student responses to the questions.

Assessment/lesson reflection (10 minutes)

1. The last slide in the PowerPoint facilitates this exercise.
2. On the same paper they used for the Anticipatory Set, tell students to complete a survey in the building, summarizing the steps to find and identify a rogue (unauthorized) Wi-Fi access point. What tools would you use? Recommend?

   - Be sure to give ample time for students to write their summaries.
   - If time allows, pick a few students to read their summaries.

3. At the bottom of the page, tell students to write down any questions they have or any topics about which they would like more assistance.
4. After class, look through the student responses and follow up with any student requiring additional help.

Microsoft resources and Web links

- **TechNet Magazine: Security Watch: A Guide to Wireless Security**
  http://technet.microsoft.com/en-us/magazine/2005.11.securitywatch.aspx
- **WINDOWS®: What are the different wireless network security methods?**
  http://windows.microsoft.com/en-US/windows-vista/What-are-the-different-wireless-network-security-methods