Module 10

Security Fundamentals

Objectives

1. The Importance of Security
2. 2.1 Common Prevention Methods
3. 2.2 Security Threats

THE IMPORTANCE OF SECURITY

Bad News

1. Security is the number one thought on most computer users minds these days.
2. It is thought that over 150,000,000 computers are currently being remotely controlled by attackers
3. Your computer is probed looking for vulnerabilities on average of every 39 seconds
4. The U.S. has highest number of infected computers and more attacks originate in U.S. than any other country (25.5%)

Kaspersky Security Bulletin 2012

Hackers

1. In the early days hackers:
   A. Worked alone
   B. Wanted show off abilities
   C. Created nuisance worms and viruses
2. Now hackers:
   A. Are organized international groups
   B. Motive by financial gain
   C. Steal confidential information instead of destroy
   D. Create customized malware

Why The Increase In Attacks?

1. Speed of attacks
2. More sophisticated attacks
3. Simplicity of attack tools
4. Faster detection weaknesses
5. Delays in user patching
6. Distributed attacks
7. User confusion

User Confusion

1. Confusion over different attacks: Worm or virus? Adware or spyware? Rootkit or Trojan?
2. Confusion over different defenses: Antivirus? Firewall? Patches?
3. Users asked to make security decisions and perform technical procedures:
   A. Will you grant permission to open this port?
   B. Is it safe to unquarantine this attachment?
   C. Should I install this add-in?

User Misconceptions

"I don't have anything on my computer a hacker would want."

"I have antivirus software so I'm protected."

"My Apple computer is safe."

"My IT person takes care of security here at work."

"Mobile devices are immune."

The Importance of Security

1. Private information, passwords, financial data, computer equipment, and other information is placed at risk if proper security procedures are not followed
2. A technician's primary responsibilities include physical, data, and network security

Security Threats

1. Types of attacks to computer security:
   - A. **Physical**
     - Theft, damage, or destruction to computer equipment
   - B. **Digital**
     - Removal, corruption, denial of access, unauthorized access, or theft of information
2. Potential threats to computer security:
   - A. **Internal threats**
     - Employees can cause a malicious threat or an accidental threat
   - B. **External threats**
     - Outside users can attack in an unstructured or structured way

COMMON PHYSICAL AND DIGITAL SECURITY METHODS

Physical Security

1. Lock doors
2. Badges
3. Key fobs
4. RFID badges
5. RSA token – performs two-factor authentication for a user to a network resource
6. Securing physical documents and passwords
7. Shredding documents

Biometrics

1. Used to identify humans by their characteristics or traits
2. Security feature preventing access to a device
3. Types
   1. A. Fingerprint scanner
   2. B. Voice Recognition
   3. C. Optical Scanner
   4. D. Retinal Scanner
4. Avoid false positives

Smart Cards

1. Can provide identification, authentication, data storage and application processing
2. Individuals can increase security and convenience when using smart cards designed to work between services
3. A single smart card can be programmed with multiple banking credentials, medical information, driver’s license information, and loyalty programs

Digital Security

1. Antivirus
2. Antispyware
3. User authentication/strong passwords
4. Firewalls
5. Directory/folder permissions

Strong Passwords

1. Difficult to break
2. Have at least 15 characters but 6-8 characters is average
3. Should be a random combination of letters, numbers, and special characters
4. Should be replaced with new passwords at least every 30-60 days
5. Should not be reused for 12 months
6. Should not be duplicated passwords or used for multiple accounts

Firewall

1. **Two-way personal software firewall** or **Stateful Packet Inspection (SPI)** - Inspects network traffic passing through it and denies/permits passage based on rules
2. Restricts what can come in and go out of your computer across the network
   A. Stops bad stuff from coming in
   B. Stops a compromised computer from infecting other computers on network
3. An **application-aware firewall** allows user to specify which desktop applications can connect to the network

DIGITAL SECURITY THREATS

Malware

1. Application designed specifically to damage or disrupt a system. It is used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems
2. Can appear in the form of code, scripts, active content, or other software
3. Includes: viruses, worms, trojan horses, rootkits, spyware, adware, keyloggers, and other malicious programs
4. Anti-virus, anti-malware, and firewalls are relied upon by homes and businesses to safeguard against malware attacks which help in identifying and preventing the continued spread in the network

Virus

1. Program with malicious intent
2. Attaches itself to other documents or software and then executes it malicious payload when the document is opened or program is launched
3. Rely on actions by users to run or spread themselves to another computer

Worm

1. Program designed to take advantage of vulnerability in applications or operating systems
2. Once worm has exploited the vulnerability on one system, it immediately searches for another computer to infect (sends out email from a clients address book)
3. Can travel by itself and does not require any user action to start

Trojan Horse

1. Program advertised as performing one activity but actually does something else (or it may perform both the advertised and malicious activities)
2. Appears harmless but is there to cause malicious intent
3. A program that contains hidden code that attacks the computer system

Rootkit

1. Software that activates each time your system boots up
2. Designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer
3. Difficult to detect because they are activated before the Operating System has completely booted up
4. Often allows the installation of hidden files, processes, hidden user accounts, etc. in the operating system
5. Can intercept data from network connections, microphone, webcam, and keyboard

Zombies & Botnets

1. One of the more common types of malware today carried by Trojan horses, worms, and viruses
2. Program puts infected computer under remote control of an attacker without user's knowledge
3. Zombie - Infected and controlled computer (robot)
4. Botnet - Thousands of zombies manipulated under remote control
   A. Once under the control of a single hacker (bot herder), botnets can be used for many different collective purposes

Denial of Service (DoS)

1. Prevents users from accessing normal services
2. Sends enough requests to overload a resource or even stopping its operation
3. **Ping of Death** is a series of repeated pings intended to crash the receiving computer
4. **E-mail Bomb** is a large quantity of e-mail that overwhelms the e-mail server preventing users from accessing legitimate e-mail
5. **Distributed DoS** is an attack launched from many computers (Botnet)

Grayware , Adware, and Spyware

1. **Grayware** is a general classification for applications that behave in a manner that is annoying or undesirable
2. Typically installed without the user’s knowledge or consent to:
   - A. Collect information stored on the computer
   - B. Change the computer configuration
   - C. Open new windows on the computer
3. **Adware** automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used
4. **Spyware** is installed to intercept or take partial control over the user's interaction with the computer

Social Engineering

Relies on deceiving someone to obtain secure information or gain access to secure areas

1. **Shoulder surfing** – Observing someone to get information
   - Defense: Privacy filters, shields or anti-glare devices
2. **Dumpster diving** – Stealing mail or documents from individuals
   - Defense: Shredders or destroy information
3. **Tailgating** – Following an authorized person through an entrance without using a badge to defeat security
   - Defense: Turnstiles and mantraps (designed to entrap a human)

Social Engineering

1. Never give out a username or password
2. Always ask for the ID of the unknown person and validate
3. Restrict access of unexpected visitors
4. Escort all visitors through the facility

Phishing

1. Sending an e-mail or displaying a Web page that falsely claims to be from a legitimate business in an attempt to trick you into surrendering personal information
2. Users are:
   A. Asked to respond to an e-mail
   B. Directed to a fake web site
   C. Asked to update personal information, such as passwords, credit card numbers, Social Security numbers, bank account numbers, or other information
   D. Asked for information a legitimate organization already has on record

Recognize Phishing Attacks

1. **Deceptive Web links** – Link to Web site embedded in e-mail should not have an @ sign in the middle of the address
2. **E-mails that look like web sites** – Phishers often include vendor information to make the e-mail look like a legitimate vendor web site as a way to convince the you that the message is genuine
   A. Presence of logos does not mean that e-mail is legitimate
   B. Users should never log on to a Web site from a link in an e-mail but instead should open new browser window and type legitimate address

Recognize Phishing Attacks

1. **Fake sender’s address** – Because sender addresses can be forged easily, an e-mail message should not be trusted simply because the sender’s e-mail address appears to be valid
2. **Generic greeting** – Many phishing e-mails begin with a general opening such as “Dear PayPal Member” and include a invalid account number
3. **Popup boxes and attachments** – Legitimate e-mails from vendors never contain a popup box or an attachment
4. **Urgent request** – Many phishing e-mails try to make you act immediately to catch you off guard

Be Aware

1. User Education
   A. Education & awareness
   B. Smart behavior
   C. Technology

2. Principle of least privilege

Summary

In the module we discussed:

1. The importance of security
2. Types of security threats
3. Physical security threats and prevention
4. Digital security threats and prevention
5. Social engineering threats and prevention

Glossary and Terms

1. **Hacker** – A person that weaknesses in a computer system or network.
2. **Physical attacks –** Theft, damage, or destruction to equipment/
3. **Digital attacks** – Removal, corruption, denial of access, unauthorized access, or theft of data.
4. **Internal threats** – Employees or internal users that cause an attack.
5. **External threats –** Outside users that attack in an unstructured or structured way.
6. **Biometrics** – A device used to identify humans by their characteristics or traits.
7. **Firewall** – A hardware or software device that restricts what can come in and go out of your computer across the network.

Glossary and Terms

8. **Malware** - Application designed specifically to damage or disrupt a system. It is used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.
9. **Virus** – Program with malicious intent that relies on actions by users to run or spread themselves to another computer.
10. **Worm** – A program designed to take advantage of vulnerability in applications or operating systems that can travel by itself and does not require any user action to start.
11. **Trojan Horse** – A program advertised as performing one activity but actually does something else.
12. **Rootkit** – Malicious software that activates each time your system boots up.
13. **Zombie** – An infected and attacker controlled computer (robot).
14. **Botnet** - Thousands of zombies manipulated under remote control.

Glossary and Terms

15. **DoS** – Denial of Service. Prevents users from accessing normal services by sending enough requests to overload a resource or even stopping its operation.
16. **Ping of Death** – A series of repeated pings intended to crash the receiving computer.
17. **E-mail Bomb** – A large quantity of e-mail that overwhelms the e-mail server preventing users from accessing legitimate e-mail.
18. **DDoS** – Distributed Denial of Service. An attack launched from many computers (Botnet)
19. **Grayware** – A general classification for applications that behave in a manner that is annoying or undesirable.
20. **Adware** – Software that automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.

Glossary and Terms

21. **Spyware** – Software installed to intercept or take partial control over the user's interaction with the computer.
22. **Keylogger** – A type of surveillance software that has the capability of recording every keystroke you make.
23. **Social Engineering** – The manipulation of people into performing actions or divulging personal or confidential information.
24. **Shoulder surfing** – Observing someone to get information.
25. **Dumpster diving** – Stealing mail or documents from individuals.
26. **Tailgating** – Following an authorized person through an entrance without using a badge to defeat security.
27. **Phishing** – Attempting to acquire personal or confidential information by masquerading as a trustworthy entity in an electronic communication.