Component 4: Introduction to Information and Computer Science

Unit 8b: Security

Unit Objectives

- List and describe common security concerns
- Describe safeguards against common security concerns, including firewalls, encryption, virus protection software and patterns, programming for security, etc.
- Describe security concerns for wireless networks and how to address them
- List security concerns/regulations for health care applications
- Describe security safeguards used for health care applications

Mitigating Security Issues

- Create a security policy
- Authenticate users
- Firewalls
- Antivirus software
- Intrusion Protection Systems
- Encrypt communications & stored data
- Audit adherence to security policies

Security Policy

- Most policies contain provisions related to:
  - Security definition
  - Enforcement
  - User access to the network, devices, software, & data
  - Password management
  - E-mail & Internet use
  - Antivirus software
  - Backup and recovery
  - Intrusion detection
  - Auditing
  - Others

Authentication Factors - Proving Your Identity

- Something you know
  - Username and password
- Something you have
  - Smart cards and employee badges
- Something you are (biometrics)
  - Fingerprints, retinal scans, etc.

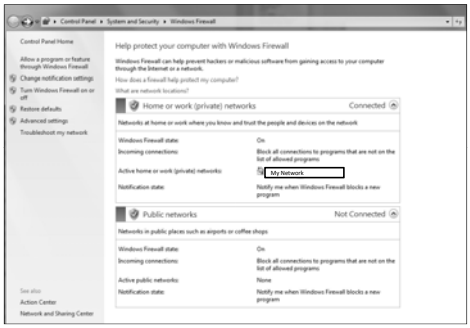
Factor Authentication

- One factor authentication
  - Simplest authentication process
  - Username and password needed
- Two factor authentication
  - Username and password needed
  - Need one of other authentication types
    - Such as smart card or fingerprint reader
- Three factor authentication
  - All three authentication types used
    - Such as username/password and smart card and fingerprint reader

Firewalls

- Software and/or hardware that blocks unauthorized communications on a computer.
- Windows OS all provide Windows Firewall.
- Routers provide basic firewall protection.
  - Most ISP routers act as firewalls.
- Inspects each piece of communication.
- Permits or denies traffic based on rules.
  - For example, you will not be able to connect to your brother's PC to copy shared photos unless his firewall is configured to allow the communication.

Windows Firewall Example



Antivirus (AV) Software

- Detects and removes malware.
  - Can also protect against adware & spyware.
- Requires current virus pattern definitions.
  - Cost of approx. $50/year.
- Searches all computer files for virus signatures.
- Monitors for malicious computer activity.
  - For example, if a running program attempts to perform some odd action, the AV software will stop and quarantine the program.

Common Antivirus Software Vendors

- Avast! - http://www.avast.com/index
- AVG - http://free.avg.com/us-en/homepage
- HouseCall - http://housecall.trendmicro.com/
- Kaspersky - http://usa.kaspersky.com/
- McAfee - http://www.mcafee.com/us/
- Symantec - http://www.symantec.com/index.jsp

Intrusion Protection Systems (IPS)

- Similar to firewall functionality – but more!
- Hardware and/or software that monitors all network traffic for malicious activity.
  - Works to stop intrusions and alert network administrators.

The Cisco Secure Intrusion Detection System (formerly NetRanger), is an enterprise-scale, real-time, intrusion detection system designed to detect, report, and terminate unauthorized activity throughout a network.
Approximate cost: $700

Encryption

- Makes communication unreadable to unauthorized viewers.
  - Uses electronic private and public key set.
- Authorized viewers provided with encryption key, with ability to encrypt and decrypt messages.
  - Medical office encrypts data using its private key.
  - Patient decrypts data using the medical office's public key.
- Encryption keeps data confidential.
  - Entities never share their private key.

Encryption Example

Encrypting a Microsoft Excel 2010 document makes the spreadsheet unreadable to anyone who tries to open it without the encrypting password.

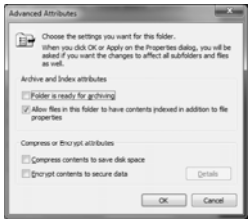
Any Microsoft Office file can be encrypted (password protected) in this way.

Encryption Example (cont'd)

Opening an encrypted document requires the user to enter the password used to encrypt it.

If the user does not enter the correct password, the encrypted document cannot be opened. Entering the correct password allows the document to be decrypted so that it can be viewed.

Encryption Example (cont'd)



Any file on a Windows-based PC can be encrypted.
To encrypt a document:

1. Create a new folder.
2. Right-click the folder and select Properties.
3. Click Advanced.
4. Click Encrypt contents to secure data.
5. All files placed in this folder will be encrypted.

Audit Security Policy Practices

- Is organization doing what it says it will do?
  - If nurses are to log off nursing stations when they leave the station, is this being done?
  - Is the database server kept up to date with critical updates?
  - Is all access of medical records logged?
  - Are backups being done regularly and stored according to the security policy?
  - Do employees adhere to e-mail policies?
  - Others?

Additional Steps to Take...

- Educate employees
  - Don't open unsolicited attachments.
  - Users lock screens when not at station.
  - Don't click on popup ads while surfing.
  - Report strange activity to network admins.
- Create secure software applications
  - Only authenticated & authorized use of software.
  - Non-repudiation of network actions.
    - Means that a user or device cannot deny having done something.

Additional Steps to Take...

- Use of password policies
  - Password complexity.
  - Passwords changed regularly (60 days, etc.).
  - No reuse of old passwords.
  - Passwords not written down anywhere.
- Domain-based network environment
  - Server manages users, devices, and policies.
  - No use of network assets unless part of domain.
  - Restricted number of network administrators.

Additional Steps to Take...

- Physical security of assets
  - Servers bolted to floor/wall in locked room.
  - No unauthorized physical access of equipment.
  - Devices password protected at all times.
  - UPS and power surge equipment utilized.
  - No access to data without authentication.
- Validation of data entered into database
  - All database entries validated before stored in database.
  - Test for expected and unexpected database entries.