

---

# Lectures 12

## Advances Security

Computer Systems Administration  
TE2003



# Lecture overview

- At the end of lecture 12 students can identify, describe and discuss:
  - Security requirements
  - Security policy
  - Security components
  - Applying security

# Security Requirements

- Security policy
  - Comprehensive statement about the level of security required and how this security will be achieved
- Is the computer located at a home or a business?
- Is there full-time Internet access?
- Is the computer a laptop?

# Security Policy

A collection of rules, guidelines, and checklists:

- Define an acceptable computer usage statement.
- Identify the people permitted to use the computer equipment.
- Identify devices that are permitted to be installed on a network, as well as the conditions of the installation.
- Define the requirements necessary for data to remain confidential on a network.
- Determine a process for employees to acquire access to equipment and data.
- Might also provide detailed information about how to proceed in case of an emergency
  - Breach in security
  - Theft
  - Data loss

# Security Hardware

The security policy should identify hardware and equipment that can be used to prevent theft, vandalism, and data loss

- To **restrict access** to premises, you might use biometrics, door locks, ...
- To **protect the network infrastructure**, you might secure rooms, setup detection for unauthorized use of wireless, and/or setup hardware firewalls
- To **protect individual computers**, you might use cable locks, laptop docking station locks and/or lockable cases
- To **protect data**, you might use lockable HD carriers and/or USB security dongles

# Security Applications

Security applications protect the operating system and software application data

- Software Firewall
- Intrusion Detection Systems (IDS)
- Application and OS Patches
- Anti-virus software and anti-malware software

# Security Techniques

Use **encrypted passwords** to login to the network

Monitor network activity through **logging and auditing**

Set up **data encryption over wireless**

Encryption methods include:

- Hash encoding uses an algorithm to track tampering
- Symmetric encryption uses a key to encode/decode data
- Asymmetric encryption uses one key to encode and another key to decode
- VPN creates a virtual “secure tunnel”

# Access Control Devices

## Physical access control devices

- Locks, conduit, card key, video surveillance, guards
- **Two-factor** (Username/password + something else ) identification methods for access control
  - Smart card
  - Security key fob
  - Biometric device

# Firewall Types

- Protect data and equipment on a network from unauthorized access
- Modes for filtering network data traffic
  - Packet filter
  - Proxy firewall
  - Stateful packet inspection
- Some applications may not operate properly unless the firewall is configured correctly for them

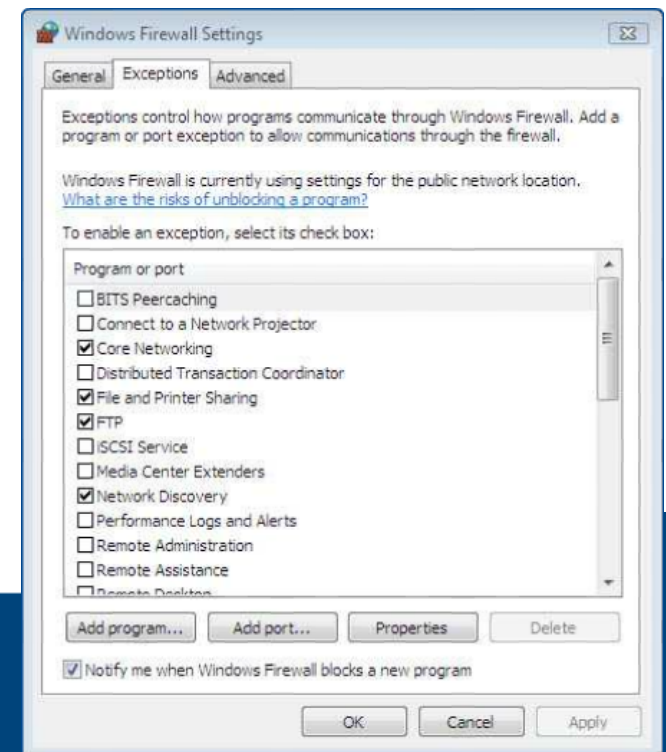
Hardware Firewall	Software Firewall
Free-standing and uses dedicated HW	Available as 3rd party SW and cost varies
Initial cost for HW and SW updates can be costly	Included in some operating systems
Multiple computers can be protected	Typically protects only the computer it is installed on
Little impact on the computer performance	Uses the CPU, potentially slowing the computer

# Configure Security Settings

- Setting levels of permissions on folders and files
  - Use FAT or NTFS to configure folder sharing or folder-level permissions for users with network access
  - Use file-level permissions with NTFS to configure access to files
- Securing wireless access points
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access 2 (WPA2)
  - MAC address filtering
  - Unused wireless connections
  - Service Set Identifier (SSID) Broadcasting
  - Wireless antenna

# Configure Firewall

- A **restrictive firewall** policy
  - open only the required ports
- A **permissive firewall** policy
  - open all ports except those explicitly denied
- Configure a **software** firewall manually or to run automatically.
- Configure a **hardware** firewall by indicating what is filtered by port type, port number, source address, and/or destination address.



# Protect Against Malware

- Run software scanning programs to detect and remove the malicious software.
- Anti-virus, anti-spyware, anti-adware, and phishing programs
  - Phishing attacks trick the user into providing the personal information. A user's data can be sold and/or used fraudulently.



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

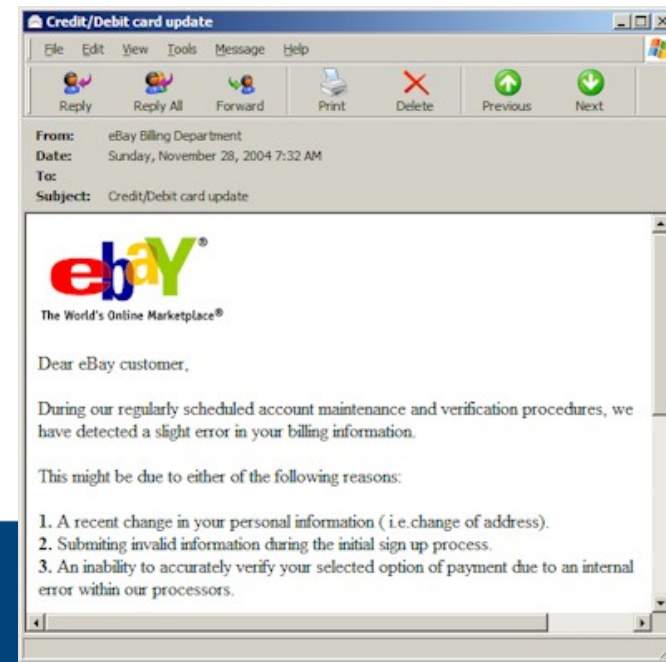
If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,  
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.



# Data Backups

- Goal of a good backup is to have the data ready for you quickly in case of a crash
- Do you need to do a full backup every night?
  - Most files won't change
  - Too time consuming

	Description
<b>Full or Normal Backup</b>	Archives all selected files
<b>Incremental Backup</b>	Archives all selected files that have changed since last full or incremental backup. It marks files as having been backed up.
<b>Differential Backup</b>	Archives everything that has changed since last full backup. It does not mark files as having been backed up.
<b>Daily Backup</b>	Archives all selected files that have changed on the day of the backup
<b>Copy Backup</b>	Archives all selected files

