HNDIT11062 – Web Development

Week 12: Protecting data in the internet

Objectives

- Explain the different types of computer crime and the difficulties of discovery and prosecution.
- Describe the aspects of securing corporate data.
- Explain the threats to personal privacy posed by computers and the Internet.
- Describe actions you can take to maximize your privacy.

Introduction

- Computer virus have become today's headline news
- With the increasing use of the Internet, it has become easier for virus to spread
- Virus show us loopholes in software
- Most virus are targeted at the MS Windows OS

Internet Use for

Security Basics

- What does it mean to be secure?
  - "Include protection of information from theft or corruption, or the preservation of availability, as defined in the security policy." - The Wikipedia
- Types of Security
  - Network Security
  - System and software security
  - Physical Security
- Very little in computing is inherently secure, you must protect yourself!
  - Software cannot protect software (maybe hardware can)
  - Networks can be protected better than software

Goals of Computer Security

- Integrity:
  - Guarantee that the data is what we expect
- Confidentiality
  - The information must just be accessible to the authorized people
- Reliability
  - Computers should work without having unexpected problems
- Authentication
  - Guarantee that only authorized persons can access to the resources

Privacy

- The ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves by selectively.

Authentication

- The act of establishing or conforming something(or someone) as authentic, that is, that claims made by or about the thing are true.

Who is vulnerable?

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations
- **ANYONE ON THE NETWORK**

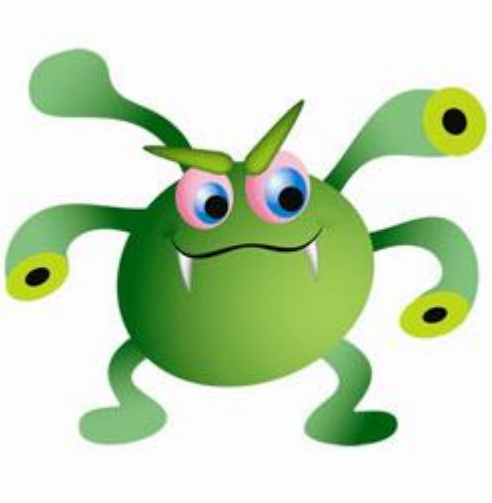
Enemies

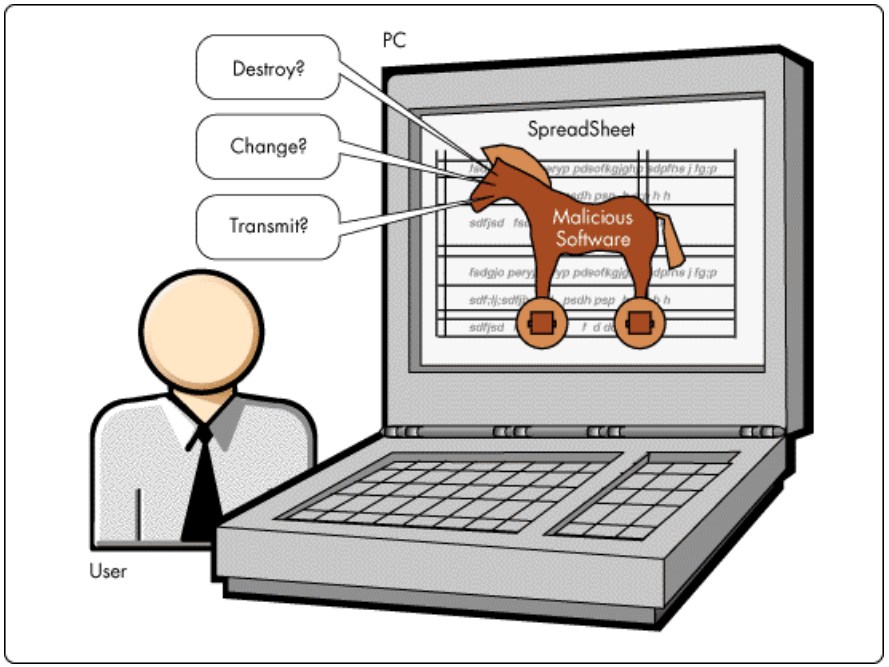
- **Hackers**
  - Access systems in an unauthorized manner.
  - Hackers have no malicious intent (i.e., they do not intend to cause harm).
  - They are only motivated by curiosity, personal satisfaction, or gaining reputation etc.

- **Crackers**
  - Individuals who cause damages to information systems with a malicious intent often for financial gains.

Malicious Software

- Malicious software, commonly known as malware, is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, trojans, spyware, adware and rootkits, etc., which steal protected data, delete documents or add software not approved by a user.





Types of Vulnerabilities

- **Virus**
  - A malicious code that infects software on a computer, thereby causing undesired results, such as changing system settings, deleting files, disabling functions, and some even hardware damage (flashing the CMOS).
  - A virus spread by making copies of itself and spreading.
  - It may spread between files or disks, but the defining character is that it can recreate itself on it's own without traveling to a new host.

- First virus was created to show loopholes in software

Symptoms of Virus Attack

- Computer runs slower than usual
- Computer no longer boots up
- Screen sometimes flicker
- PC speaker beeps periodically
- System crashes for no reason
- Files/directories sometimes disappear
- Denial of Service (DoS)

➢ You can protect your machine by using an updated anti-virus software.

Virus through the Internet

- Today almost 87% of all viruses are spread through the internet (source: ZDNet)
- Transmission time to a new host is relatively low, on the order of hours to days

Types of Vulnerabilities…(cont.)

- **Worms**
  - Has similar properties to a virus
  - Spread over network connection
  - Worms replicate
  - Has the capability of moving from location to location(PC to PC) thereby doing some damage and going somewhere else.
  - Can spread and cause damage on its own without attaching to another program
  - Even if you scan your machine, the worm will not be found
  - First worm released on the Internet was called Morris worm, it was released on Nov 2, 1988.
  - Recent e.g. CodeRed, BugBear, SoBig etc.

Macro

- Specific to certain applications
- Comprise a high percentage of the viruses
- Usually made in WordBasic and Visual Basic for Applications (VBA)

Types of Vulnerabilities…(cont.)

- **Trojans**
  - A class of software that enters into your system pretending to be something else, or a part of another software.
  - Hidden
  - Leaks information
  - Usually does not reproduce
  - Keyloggers, adware, spyware, could all enter into your system as trojans.

Types of Vulnerabilities…(cont.)

- **Spyware**
  - This is a class of applications that spy on the users activities.
  - They may provide others access to your system, display unwanted banner ads, or steal your confidential information

Symptoms

• Targeted Pop-ups	SPYWARE
• Slow Connection	SPYWARE / TROJAN
• Targeted E-Mail (Spam)	SPYWARE
• Unauthorized Access	TROJAN HORSE
• Spam Relaying	TROJAN HORSE
• System Crash	SPYWARE /TROJAN
• Program Customisation	SPYWARE

Effects

- Allows remote access
  - To spy
  - To disrupt
  - To relay a malicious connection, so as to disguise the attacker's location (spam, hacking)
  - To access resources (i.e. bandwidth, files)
  - To launch a DoS attack

Operation

- Listen for connections
- Memory resident
- Start at boot-up
- Disguise presence
- Rootkits integrate with kernel
- Password Protected

Similarities / Differences

Spyware	Trojan Horses
Commercially Motivated	**Malicious**
Internet connection required	**Any network connection required**
Initiates remote connection	**Receives incoming connection**
Purpose: To monitor activity	**Purpose: To control activity**
Collects data and displays pop-ups	**Unauthorized access and control**
Legal	**Illegal**
Not Detectable with Virus Checker	**Detectable with Virus Checker**
Age: Relatively New (< 5 Years)	**Age: Relatively Old (> 20 Years)**
Memory Resident Processes	
Surreptitiously installed without user's consent or understanding	
Creates a security vulnerability	

Types of Vulnerabilities…(cont.)

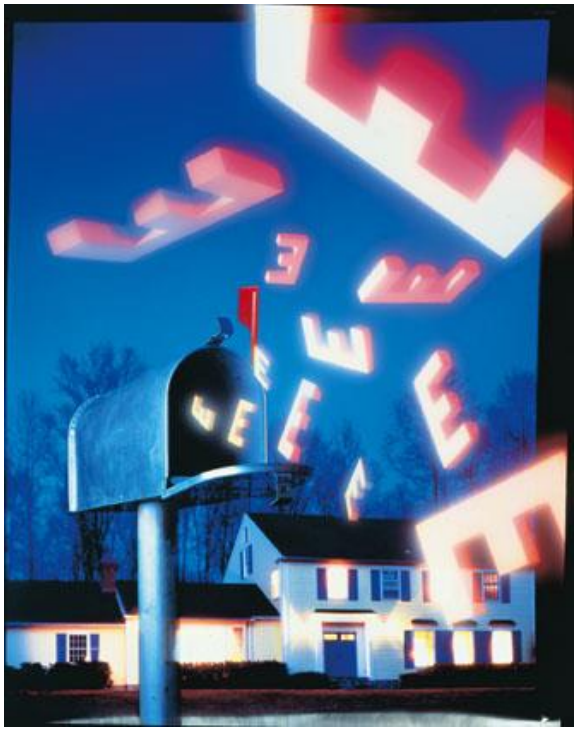
- **Spam**
  - Spam is “unsolicited” email – email that is sent without permission.
  - This normally consists of credit cards, stock reports, etc.
  - Replying to a spammer and asking him not to sent emails is pointless.
  - Best thing to do is to use a spam filter , which filter out the spam mail and send it to another folder, or delete it.
- **Adware**
  - This is software that courses various advertisements to display on your system as pop-ups or pop-unders while you are browsing on-line.
- **Keyloggers**
  - This is software/hardware that monitors your keystrokes and records them/publishes them.
  - This attempt to capture passwords, credit card numbers, and other sensitive information.

Web Attacks

- Phishing
  - An evil website pretends to be a trusted website
  - Example:
    - You type, by mistake, “mibank.com” instead of “mybank.com”
    - mibank.com designs the site to look like mybank.com so the user types in their info as usual
    - BAD! Now an evil person has your info!
- SQL Injection
  - Interesting Video showing an example
- Cross Site Scripting
  - Writing a complex Javascript program that steals data left by other sites that you have visited in same browsing session

Need to know:
Web Programming, Javascript, SQL

Junk e-mail

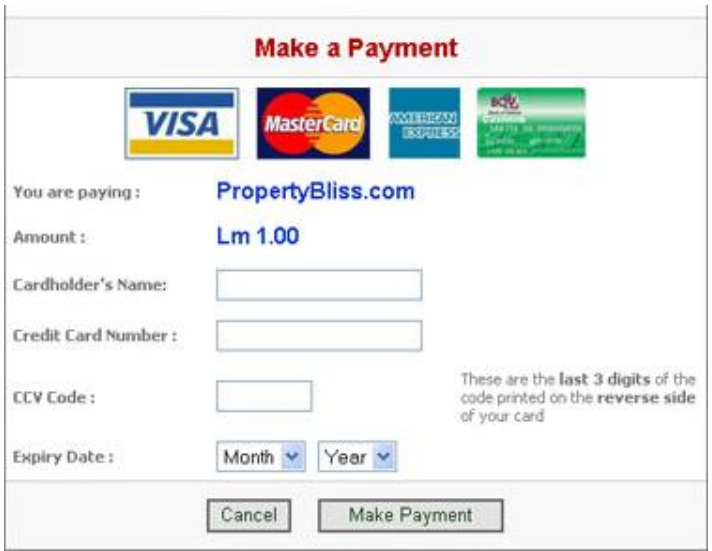


- Cheaper than snail mail
- Spamming
  - Sends e-mail messages to “everyone”
  - Abandons the originating site

- Help eliminate junk e-mail
  - Do not complete a member profile with online service
  - Do not fill in registration forms unless the purveyor promises not to sell or exchange your information
  - Never respond to spamming
- Use filter software

Identity Theft

- In the Internet sometimes you have to disclose your personal information such as name, telephone numbers and email addresses
- To make online purchases you need to give your credit card number
- However, you got to be careful when you disclose your personal information over the Internet



Identity Theft (cont.)

- Identity theft is the act of using someone's Identity and good reputation by another individual for financial gains
- One of the fastest growing crimes in United States
- A popular way to obtain private information is by using phishing scams
- In phishing scams attacker sends an email to the victim which looks like a legitimate request for victims personal information

Preventing Identity Theft

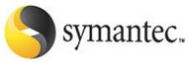
- Do not disclose your private information over emails
- Always check whether a website is a trusted one before you enter any sensitive information
- Always check whether the website supports secure transactions (others cannot see the information you send to secure sites)
- Always read privacy policies given on websites

Network and Web Site Security

- Tools such as passwords, firewalls, intrusion detection systems, and virus scanning software should be used to protect a network and Web site.

Preventing Malicious Software

- Always use a virus scanner and keep it up to date with latest updates
- Enable auto-protect features of your virus scanner
- Use a spyware scanner to scan and remove spyware and update it regularly
- Never download content from unknown web sites
- Never open email attachments coming from unknown sources

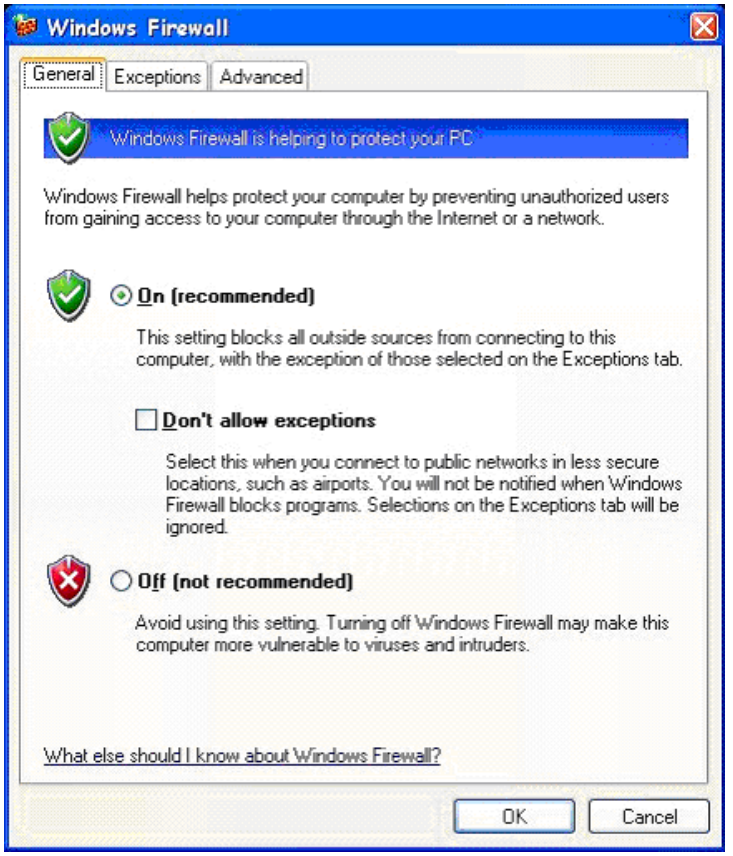


Don't let it expire

Preventing Malicious Software (cont.)

- Use a personal firewall
- Keep your operating system updated with latest updates and patches
- Never click “yes” in unknown popup ads that appear.

  Always close them using “x” on the upper right hand corner



Attacks on Passwords

- Brute force attack
  - Here the attacker tries all possible combinations for a password until he gets the correct one
  - There are programs written to do this task

- Dictionary attack
  - The attacker tries all the words in a dictionary with the hope of discovering the password (including names, places, etc.)
  - There are dictionaries of frequently used passwords that can be used for this purpose

Attacks on Passwords…(cont.)

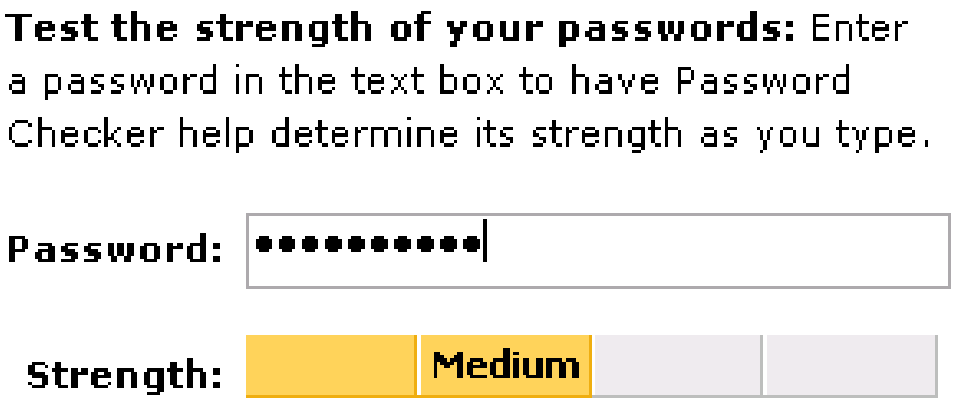
- Keystroke Monitoring
  - Attacker tries to obtain a password by looking at your key strokes while you enter your password

- Dumpster diving
  - Attacker searches through trash bins with the hope of finding written down passwords or other confidential information

Strong Passwords

- Passwords are not stored in clear-text (i.e., readable) format in your computer
- It is possible for someone to find out your password either by guessing it or by carrying out a password attack.
- Cannot be easily guessed by others or cracked by password cracking programs
- Strong passwords are essential to protect your information

For example, “sdfo839f” is a good password



Password Best Practices

- Always use a password of a minimum of eight characters
- Do not use your name, birthday, name of a close relative as your password since these can be easily guessed
- Use non-dictionary words for your password
- Always use a combination of uppercase/lowercase characters, numbers.
- Use at least one special character in your password

  (e.g., !,#,$,@)
- Change your password at least twice every month
- Never write down your password in books, pieces of paper, diary etc.
- Never send your password via email or disclose it to someone even if you trust that person

Privacy

Monitoring by Web Sites

Cookies

- A Cookie is a small text file sent to the user from a website.
  - **Contains Website visited**
  - **Provides client-side personalisation**
  - **Supports easy Login**
- Cookies are controlled by…
  - **Website's Application Server**
  - **Client-side Java Script**
- The website is effectively able to 'remember' the user and their activity on previous visits.

Cookie

- Stores information about you
- Located on your hard drive
- Beneficial uses
  - Viewing preferences
  - Online shopping
  - Secure sites retain password in cookie
- Controversial use
  - Tracking surfing habits for advertisers
- Can set browser to refuse cookies or warn before storing
- Software available to manage cookies

Web Proofing

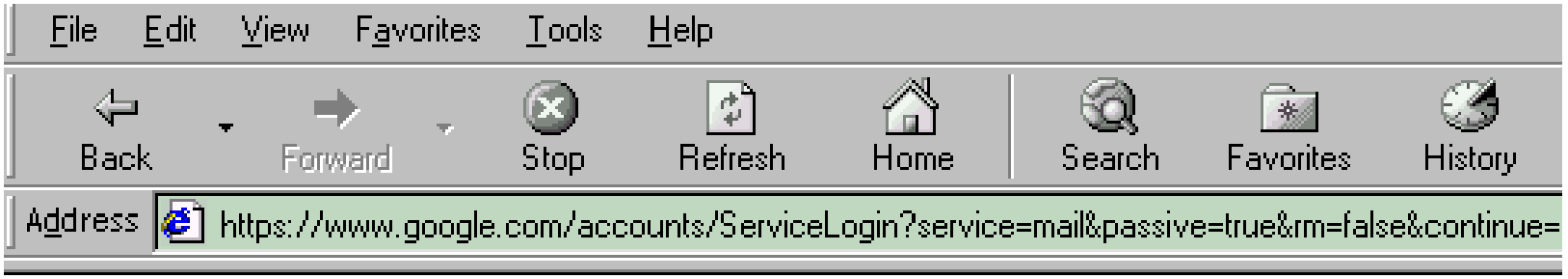
- The process of tracking the behavior of users including
  - the sites they go to
  - How much time they spend there
  - What they do there etc.

Protection/Prevention

- Knowledge
- Proper configurations
- Run only necessary programs
- Anti-virus software

Identifying Secure Websites

- Secure websites have a URL starting with https://



- There is a closed padlock icon at the bottom of the browser status bar

Solutions

Short Term

- Firewall
- Virus Checker
- Spyware Remover
- Frequent OS updates
- Frequent back-up
- Learning problems

Long Term

- Add Spyware to Anti-Virus
- Automatic maintenance
- Legislation
- Education on problems
- Biometric access
- Semantic web (and search)

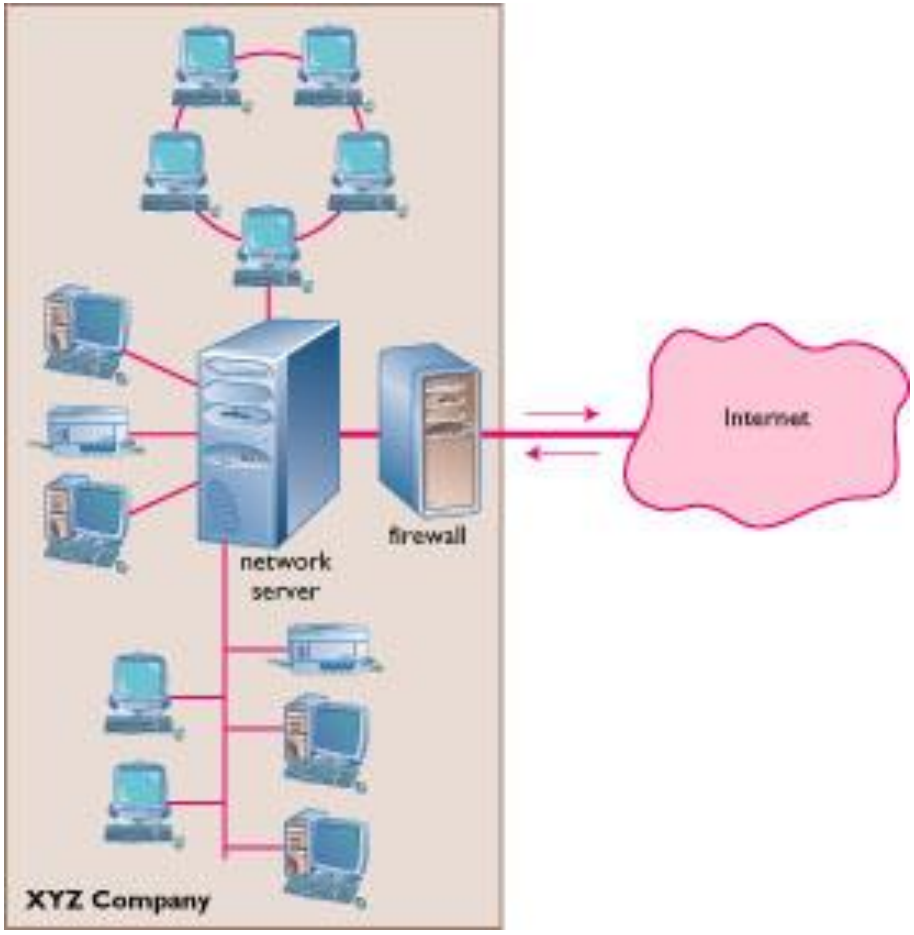
Internet Security

Firewall

- Dedicated computer that governs interaction between internal network and the Internet

Encryption

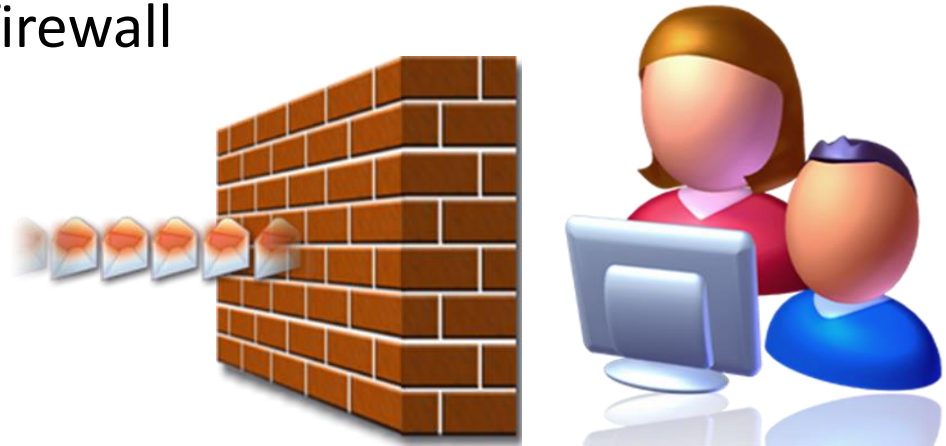
- Data Encryption Standard (DES)



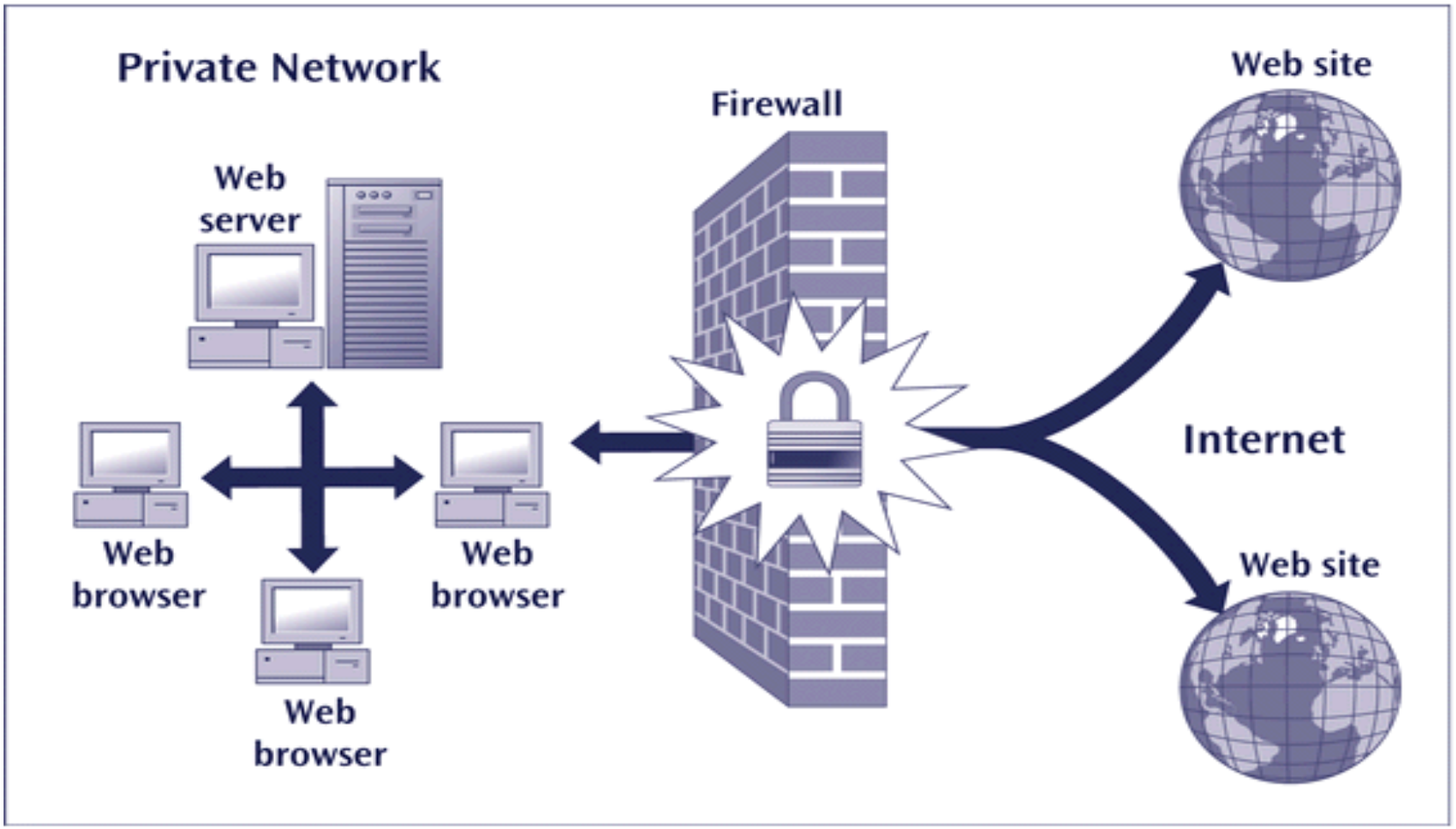
Internet Security

- Purpose of Security
  - Keeping anyone from doing things you do not want them to do to, with, on, or from your computers or an peripheral devices
  - Protecting corporate network from illegal Internet access
- Strategies for a secure Network
  - Strategy: building firewall

MacAfee
Norton

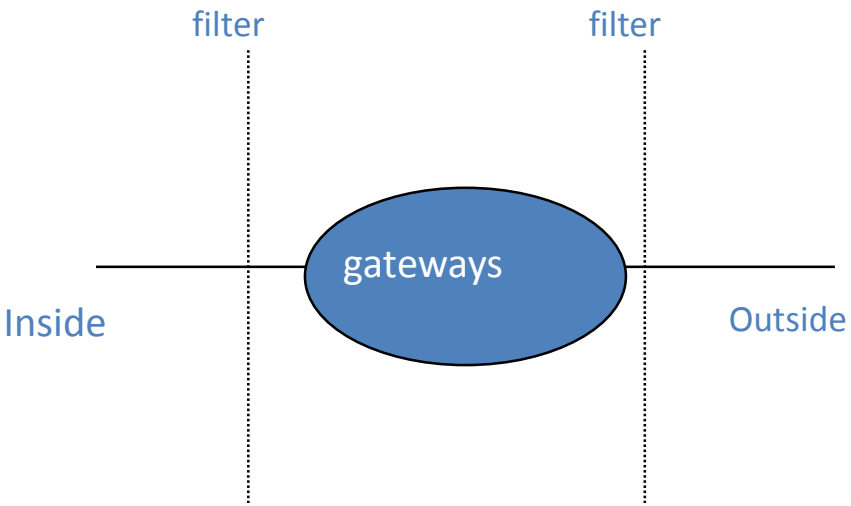


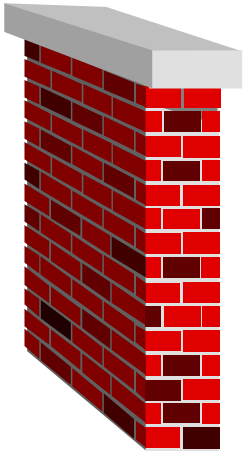
Firewall


Private Network
Web server
Web browser
Web browser
Web browser
Firewall
Web site
Internet
Web site

What is a Firewall?

- A firewall is hardware, software, or a combination of both that is used to prevent unauthorized programs or Internet users from accessing a private network and/or a single computer





What is a Firewall?...(cont.)

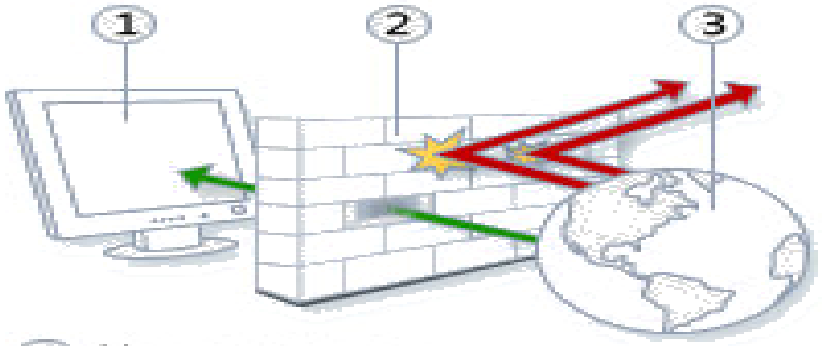
- A firewall is software or hardware that checks information coming from the Internet or a network, and then either blocks it or allows it to pass through to your computer, depending on your firewall settings.
- A firewall can help prevent hackers or malicious software (such as worms) from gaining access to your computer through a network or the Internet. A firewall can also help stop your computer from sending malicious software to other computers.
- A firewall isn't the same thing as an antivirus program. To help protect your computer, you need both a firewall and an antivirus and anti-malware program.

Hardware vs. Software Firewalls

- Hardware Firewalls
  - Protect an entire network
  - Implemented on the router level
  - Usually more expensive, harder to configure
- Software Firewalls
  - Protect a single computer
  - Usually less expensive, easier to configure

How does a software firewall work?

- Inspects each individual “packet” of data as it arrives at either side of the firewall
- Inbound to or outbound from your computer
- Determines whether it should be allowed to pass through or if it should be blocked



Firewall Rules

- Allow – traffic that flows automatically because it has been deemed as “safe” (Ex. Meeting Maker, Eudora, etc.)
- Block – traffic that is blocked because it has been deemed dangerous to your computer
- Ask – asks the user whether or not the traffic is allowed to pass through

What a personal firewall can do

- Stop hackers from accessing your computer
- Protects your personal information
- Blocks “pop up” ads and certain cookies
- Determines which programs can access the Internet

♣ ***Role***

♦ **A firewall shields the Internal corporate network from the Internet**

♦ **The Internal network works normally**

What a personal firewall cannot do

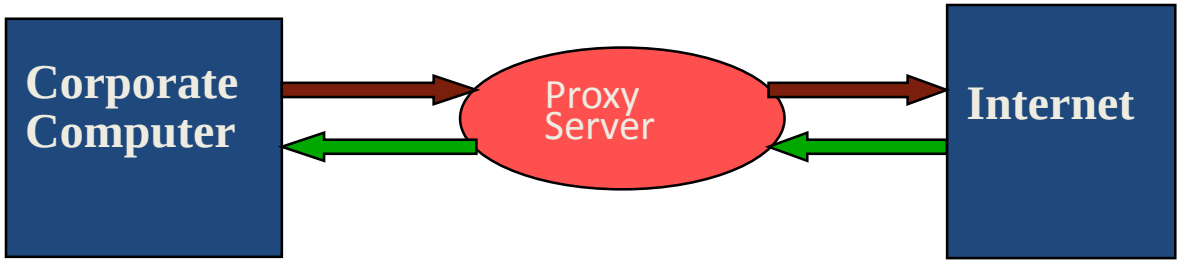
- Cannot prevent e-mail viruses
  - Only an antivirus product with updated definitions can prevent e-mail viruses
- After setting it initially, you can forget about it
  - The firewall will require periodic updates to the rule sets and the software itself

Examples of personal firewall software

- ZoneAlarm <www.zonelabs.com>
- BlackICE Defender <http://blackice.iss.net>
- Tiny Personal Firewall <www.tinysoftware.com>
- Norton Personal Firewall <www.symantec.com>

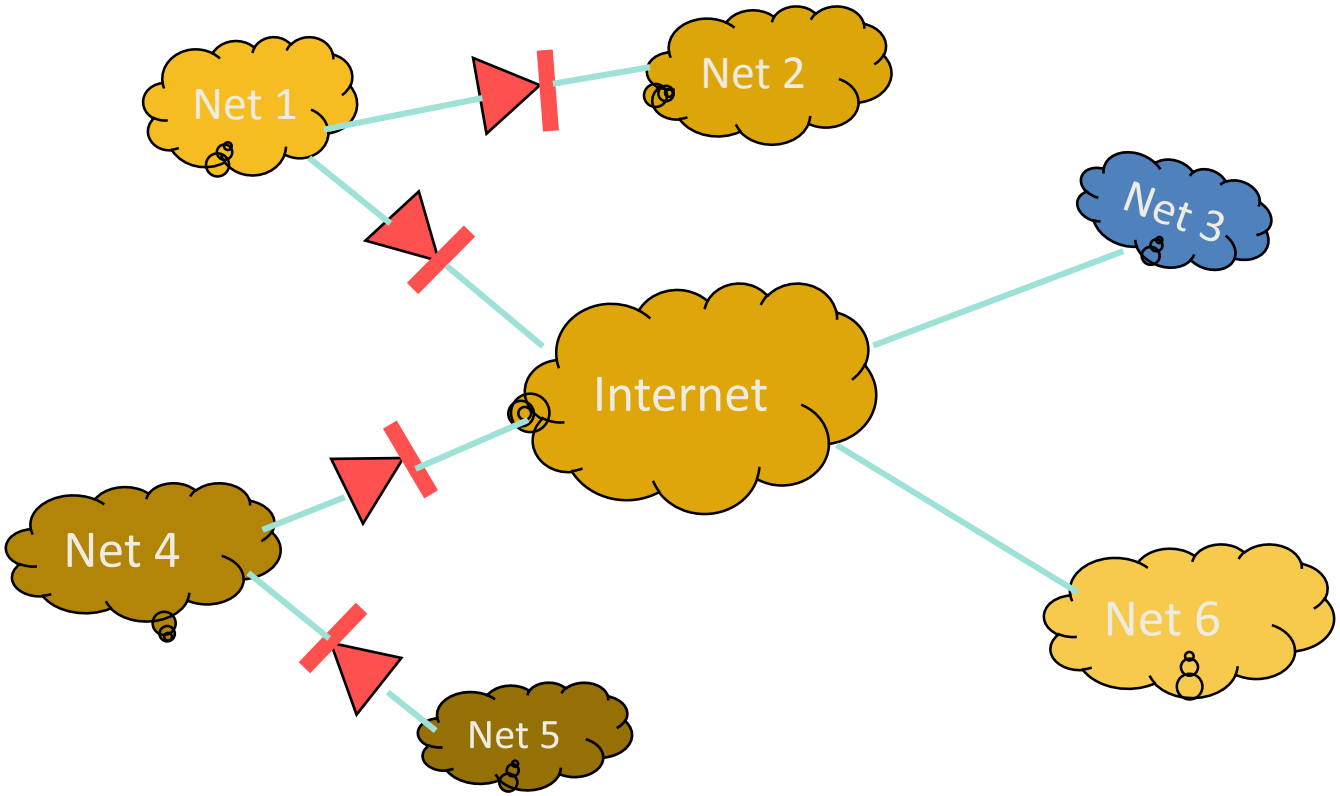
How Firewall Works

- Proxy Server (an example)
  - step 1: A request from a corporate network
  - step 2: That request being Sent to proxy server
  - step 3: A proxy server sends the request to the targeted Internet server
  - step 4: The internet server fulfilled the request and sends the answer back to proxy server
  - step 5: The proxy server sends the answer back to the corporate network



Building Firewall

- Positioning Firewalls



Limitations of Firewall

- No protection against problems with higher level protocols
- The degree of protection against threads depends on how carefully the gateway code is written
- Any information that passes inside can trigger problems
- At best, a firewall provides only a convenient single place to apply a corrective filter.

Cryptography

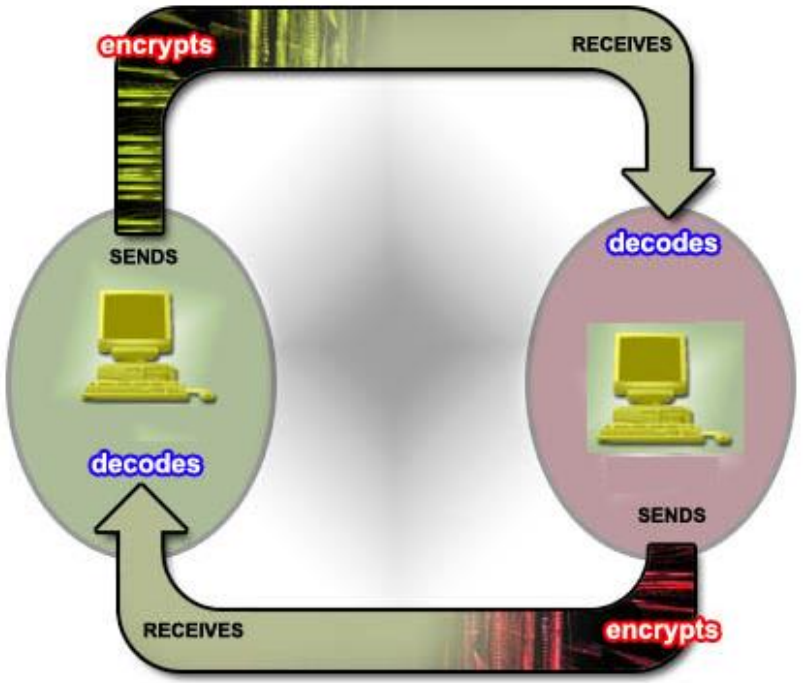
- Simply – secret codes
- Encryption
  - Converting data to unreadable codes to prevent anyone form accessing this information
  - Need a “key” to find the original data – keys take a few million-trillion years to guess
- Public keys
  - An ingenious system of proving you know your password without disclosing your password. Also used for digital signatures
  - Used heavily in SSL connections
- Hashing
  - Creating fingerprints of documents

Need to know:
Mathematics, number theory, cryptographic protocols

Encryption

- Encryption makes your data unreadable to others
- Encryption takes your normal messages (called clear text) and changes it to an unreadable format called cipher text
- Example:

  Take the word “Hello” and replace each letter by three letters ahead in the alphabet.
  You end up with “Khoor”
  which is unreadable



Cryptography

Cryptography

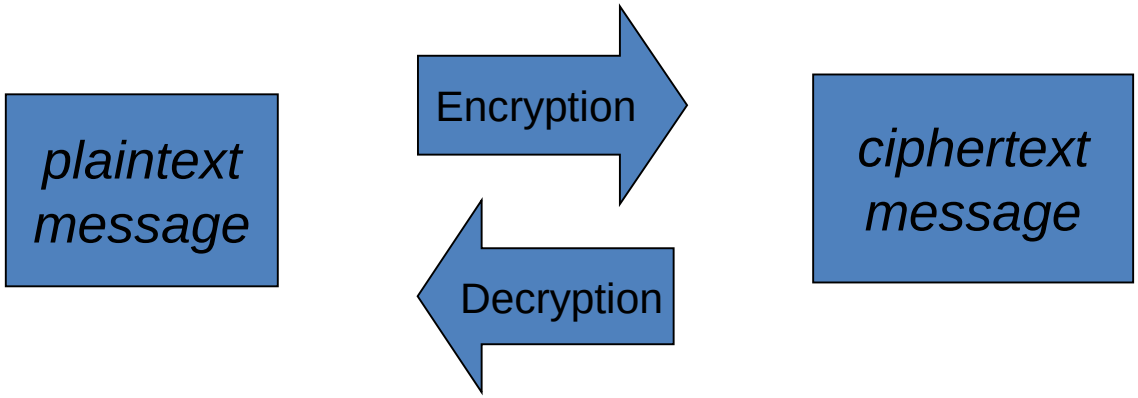
The field of study related to encoded information (comes from Greek word for "secret writing")

Encryption

The process of converting plaintext into ciphertext

Decryption

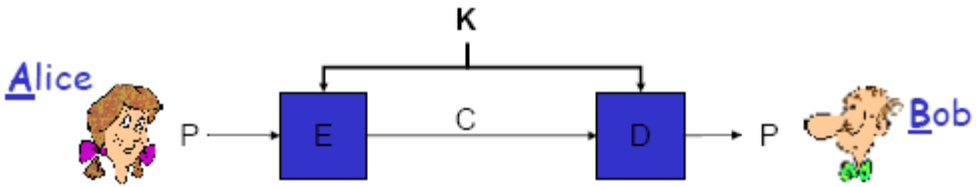
The process of converting ciphertext into plaintext



Encrypted(Information) cannot be read

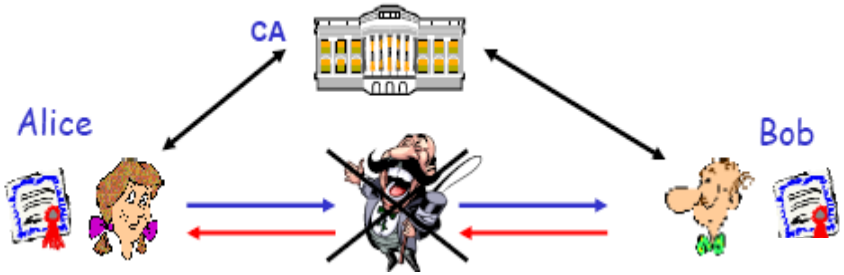
Decrypted(Encrypted(Information)) can be

Cryptographic Protocols



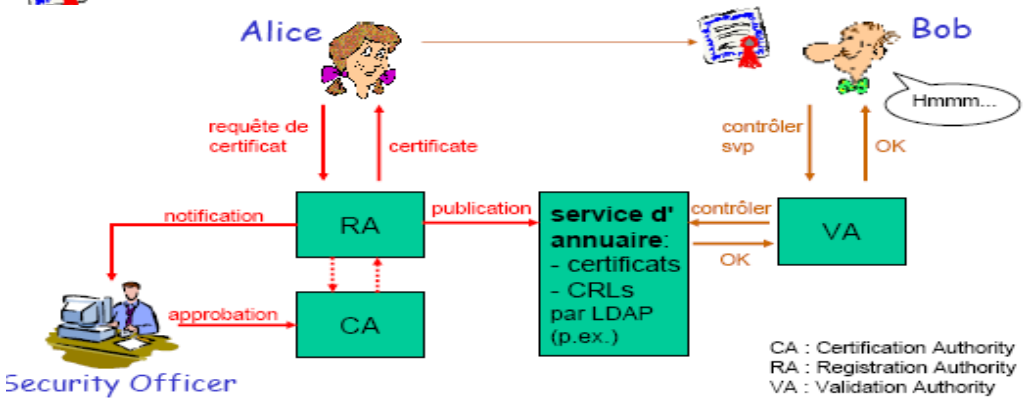
Symmetric encryption

Asymmetric encryption



Authentication

Public Key Infrastructure



How can you achieve security?

- Many techniques exist for ensuring computer and network security
  - Cryptography
  - Secure networks
  - Antivirus software
  - Firewalls
- In addition, users have to practice “safe computing”
  - Not downloading from unsafe websites
  - Not opening attachments
  - Not trusting what you see on websites
  - Avoiding Scams

Transaction Security and Data Protection

- Use a predefined key to encrypt and decrypt the data during transmission.
- Use the secure sockets layer (SSL) protocol to protect data transmitted over the Internet.
- Move sensitive customer information such as credit card numbers offline or encrypting the information if it is to be stored online.

Transaction Security and Data Protection - internal

- Remove all files and data from storage devices including disk drives and tapes before getting rid of the devices.
- Shred all hard-copy documents containing sensitive information before trashing them.
- Security is only as strong as the weakest link.

Chapter Review

- What is Computer Security?
- What is Network Security?
- What is Internet Security?
- What are the technologies design to protect network connections and data transfer over the internet?
- When we doing instant chatting (Skype, gtalk, etc.) viruses can attack our machine. How could that happen and how can we avoid it?
- What does antivirus software do?
- Briefly explain term Data Encryption with its process.
- How can you protect your privacy on the Internet? Briefly explain.