Internet security

Technical Seminar under campus connect Programme with Infosys

Deepak Garg

Coordinator-Campus Connect Team

Computer Science & Engineering Department

Thapar Institute of Engineering & Technology, Patiala

Objectives

1. Introduction
2. Categories and classification
3. Loopholes
4. What you should take care of

Introduction

- ✓ Our private space is no longer private, every one has experienced the aggression in one way or another
- ✓ Security risks through internet are on the rise
- ✓ More and more frauds are coming into picture
- ✓ It is not difficult to remain secure but requires some effort on daily basis

Threat: Masquerade

- Attacker pretends to be someone else
  - Typically an authorized user or service personnel
- Attacker impersonates an organization
  - Party to a transaction
  - Front to collect credit cards or other information

Threat: Eavesdropping

- Attacker listens to a private communication as it is sent over the network
- Used to obtain valuable data or information required for Masquerade

Threat: Man-in-the-middle

- Attacker inserts itself between two parties and pretends to be one of the parties
- May be used in combination with Address Spoofing, Data Diddling, etc.

Threat: Address spoofing

- Attacker 'steals' a legitimate network address (an IP address) and uses it to impersonate the system that owns the address
- May be used in combination with Eavesdropping, Data Diddling, etc.

Threat: Data diddling

An attacker changes the data while enroute from source to destination

For example,

- Change amounts
- Change beneficiary account number

Threat: Dictionary attack

Attacker’s programs try a large set of likely combinations in order to guess a secret

For example,

- Common password values

Threat: Replay attack

Attacker captures one or more messages and communicates those messages again at a later time

Threat: Denial of service

- Attacker floods a system with bogus requests or tampers with legitimate requests
- Although the attacker may not benefit financially, service to legitimate users is disrupted

Threat: Trojan horse

- A Trojan Horse program hides within an apparently benign program
- When the apparently benign program runs it also runs the hidden program
- Typically these programs impact security
  - Allowing entry or changing access rights
  - Copying or destroying information

Threat: Virus or worm

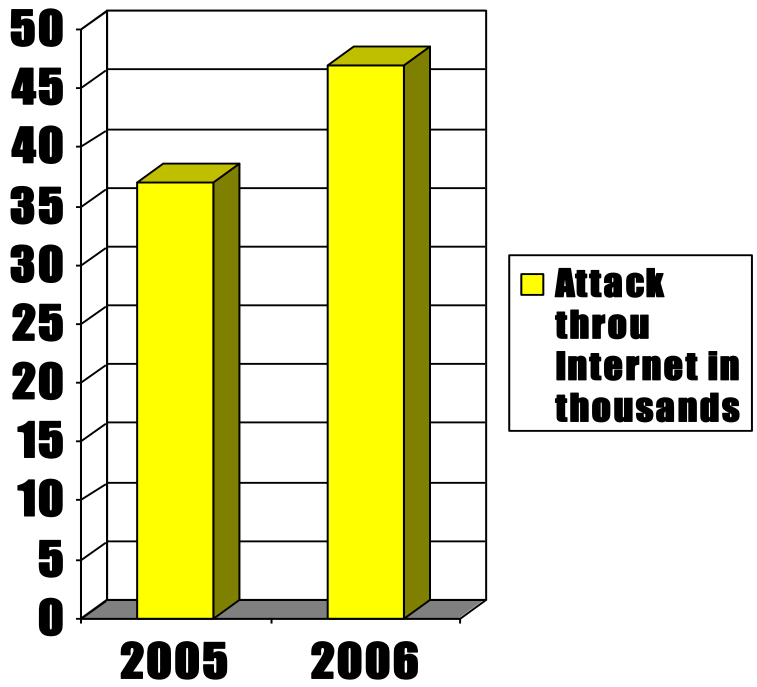
- Destructive or disruptive program with the ability to reproduce itself
- May travel via diskette, file, e-mail attachment, network, etc.
- Virus can be in programs, Word documents, Excel spreadsheets, Web pages, etc.

New Security Holes

Attacks through Internet on US organizations up by about 10%

Reported losses amount to about $100 million

(Ref: Computer Security Inst. & FBI, March 2006]

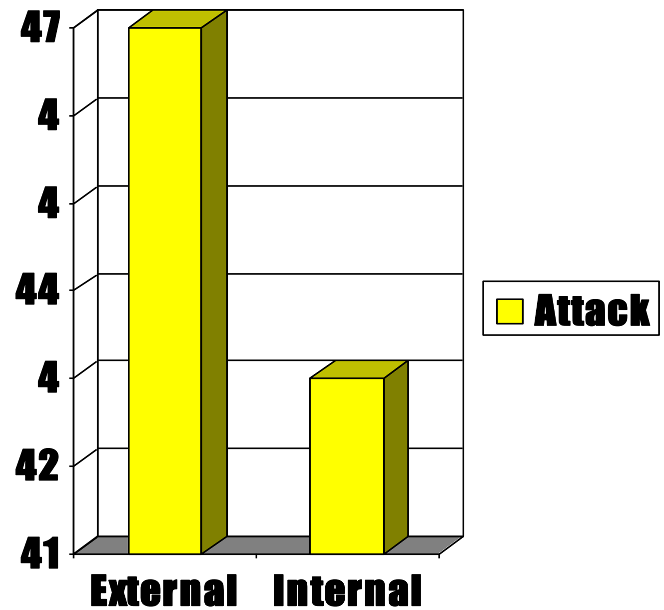


Increased Threat from Outside

47% experienced external attack against 43% internal attack

Dramatic rise in threat from outside due to increased Internet connectivity

(Ref: Computer Security Inst. & FBI, March 2006]



Common Security Risks

Hacker	**To test out someone's security system; steal data**
Businessman	**To discover a competitor's marketing strategy**
Accountant	**To embezzle money from a company**
Stockbroker	**To deny a promise made via e-mail**
Con man	**To steal credit card numbers for sale**
Student	**To have fun snooping on peoples' e-mail**
Terrorist	**To destroy data (say by virus attack)**

Security Problems

Common security problems relate to-

Access

Confidentiality

Authentication

Non-repudiation &

Integrity Control

Access

- Keeping important information out of the hands of unauthorized users (hackers) to avoid stealing or tampering
- For instance, preventing people from accessing remote services that they are not authorized to do
- Traditional implementation- lock
- Electronic implementation- password

Confidentiality

- Ensuring that the information or communication remains private (secret) as well as hiding the very existence of certain kinds of information
- For instance, preventing people from reading files that they are not permitted to do
- Traditional implementation- lock, seal
- Electronic implementation- permission, encryption

Authentication

Determining whom you are dealing with before revealing sensitive information or entering into a business deal

For instance, how to prove that whether the message "Pay ten thousand to X" is really from the Finance Manager or from X

Traditional implementation- signature, letter-head

Electronic implementation- digital signature, watermark

Non-repudiation

- People trying to deny that they sent certain messages
- For instance, how to prove that a customer really placed an order for 100 copies of a book @ Rs. 2000 when he later claims that the price was @ Rs. 1500
- Traditional implementation- signature
- Electronic implementation- digital signature

Integrity

- Preventing a legitimate message from being captured, tampered and replayed by an intruder
- For instance, how can you be sure that a received message is really the one sent by your counterpart and not something that a malicious adversary modified in transition or concocted
- Traditional implementation- registered mail
- Electronic implementation- cryptogram, steganogram

Security Tips

1. Use anti-virus software:

Your anti-virus software should be set to constantly monitor your system using “real-time monitoring,” and you should be sure your virus definitions are kept up to date.

Security Tips

2. Install hardware and software firewalls:
Your network should be behind a hardware firewall, particularly with a high-speed connection. Install a personal firewall to block any content that the hardware may miss.

Security tips

3. Create strong passwords:

A strong password is one that has at least 8 characters including letters, numbers, and other non-alphanumeric characters. Don’t use the same passwords for multiple registrations. Keep your passwords in a safe position or in a password protected file.

For example – **“A&Bh3cnJP&E”** looks like a complicated password, and much too hard to remember. But it comes from *“Ann and Bob have three children named Jason, Paul, and Elizabeth."*

A password like that would be very difficult to crack and impossible to guess. However, if you are Ann or Bob, you should remember it easily!

Security tips

4. **Establish a back-up schedule for important data:**
   Creating and maintaining a set schedule for backing up your data can prepare you for any unfortunate breach that could occur despite your best efforts to remain secure.

Security tips

5. Maintain up-to-date security patches:
Carefully review and install software patches as soon as they become available. This will help to reduce the amount of time that you are vulnerable to an attack.

Security tips

6. Use password-protected screen savers:

Reduce the chance that others are able to access your data by using a screen saver that activates after a short time and requires a password to return to the desktop.

Security tips

7. Check the settings in your e-mail client and web browser:
In your e-mail client you should use content filter settings to block unwanted e-mail. You can also set your Web browser to block cookies and unwanted JavaScript.

Security tips

8. Use safe e-mail and download practices:

Most computer viruses spread through e-mail or direct downloading to your computer. With this in mind, you should think carefully about everything that you download.

Security tips

9. A cookie is a small information file that a Web site puts on your hard drive in order to remember something about you later. Cookie keeps track your preferences when using a particular site. By using cookies, an on-line store like **Amazon** can keep track of what items you have placed in your shopping cart as you surf the site.

   In Internet Explorer, you can delete cookies by clicking on "Tools," scrolling down to "Internet Options," and clicking "Delete Cookies." Any website that requires cookies will simply replace them.

Security tips

10. Change your log-in password often. The simple act of changing your password will increase the likelihood that your e-mail remains secure

Security tips

11. Never open attachments from unknown sources. And be cautious about attachments from people you know. They may contain **Trojan horses**, **worms**, or **viruses**, which can seriously damage your personal or work computer. Make sure your virus checker scans all attachments from your friends before you open them; this is a common way for viruses to spread

Security tips

12. Always log out/sign off when you are finished with your computer. It's quick, easy, and may save your account from unwanted trespassers. If you are using a public terminal, exit the browser you are using when you are ready to end your Internet session. Be sure to clear your history and your **cookies**.

Security tips

13. A letter or e-mail from Nigeria (or sometimes another African country) offers the recipient the "opportunity" to share in a percentage of millions of dollars that the author is trying to transfer illegally out of Nigeria. The recipient is encouraged to send information to the scammer -- blank letterhead stationary, bank name, account numbers, and other identifying information using a fax provided in the letter.

Be advised that this is a scam and not a legitimate offer.

Security tips

14. E-mail has become the most widely used form of communication in the world. Millions of businesses and personal users rely on it for its speed and efficiency. Unfortunately, e-mail is often insecure.

Encrypting e-mail allows secure communication between the sender and recipient.

Security tips

15. Steganography

Many files, including images (.jpg, .bmp, .gif) and sound or music files (.mp3, .wav) contain unused data blocks. Steganography is the method of filling these unused blocks with a hidden message. Steganography is often used to send illegal or illicit messages including communications between terrorists or cyber-criminals.

Security tips

16. Identity theft, or impersonation fraud, occurs when someone assumes your identity to perform a fraud or other criminal act. The sources of information about you are so numerous that it can be difficult to prevent the theft of your identity

Security tips

Identity theft can be through

Stealing wallets, purses, or your mail, including bank and credit card statements, pre-approved credit offers, telephone calling cards, and tax information

- Stealing personal information you provide to an unsecured site on the Internet
- Rummaging through your trash and business trash for personal data
- Posing as someone who legitimately and legally needs information about you, such as employers or landlords
- Buying personal information from "inside" sources

Security tips

17. Your old hard drive likely contains sensitive information about you or your business.

When you "delete" files, even if you reformat the hard drive afterwards, the information in the files could still be recoverable.

Security tips

18. Pyramid Schemes

(also called “Ponzi schemes”) are illegal . Pyramid schemes are scams in which large numbers of people at the bottom of the pyramid pay money to a few people at the top. Each new participant pays for the chance to advance to the top and profit from payments of others who might join later.

Please note that pyramid scheme e-mails are frequently disguised as chain letters advertising new and legitimate business opportunities.

Security tips

19. Cyberspace has become rife with e-mails and websites offering “get-rich-quick” and “work-at-home” employment opportunities. Like any other scam, “work-at-home” fraud only exists because there are Internet users still falling for the same old tricks – users who are interested in getting something for nothing.

Security tips

20. Look For a Company's On-line Privacy Policy.

Most companies have an on-line privacy policy to inform users of their information collection practices. Always check this privacy policy before disclosing any personal information. If you are unable to locate this privacy policy, inquire about one, and request that the company post it to their website. Refuse to submit any personal information without reading a privacy policy first.

The race between good & bad will continue….
What remains to be seen is who will be ahead

Thanks!

Questions are welcome…