CYBER CRIME, HACKING AND VIRUSES

Prepared By:

Kazi Jahidur Rahman

Assistant Professor

Dept. of Computer Science and Engineering

University of Rajshahi

Cell: 01728385822

E-mail: kazi.jahid@yahoo.com

Web: http://www.ru.ac.bd/cse/

Cyberspace

- Metamorphic space of computer systems and computer networks.
- Here electronic data are stored and online communication takes place.
- An apparent perception of object experienced daily by the operators of Information and Communication Technology throughout the world.
- The term was originated in science fiction.

Cyber Crime

- **Also known as E-crime.**
- **Almost conventional crime in nature committed by using computer and ICT with an intention to make social disorder.**
  - **Hacking**
  - **Unauthorized access to a computer system**
  - **Distributing software to commit a crime**
  - **Launching a denial of service attack intentionally or causing a computer system to deny service to any authorized user.**

Modern Computer Crimes

- **Can be based on malicious code such as a virus, email virus, worm or Trojan horse.**
  - ***Also known as Passive Attacks***
- **Or actively perpetrated by knowledgeable individuals, who attempt to exploit network, computer, and software flaws**
  - ***Also known as Active Attacks***

It is crime, because.....

- Damage a home computer
- Bring down a business
- Weaken the telecom, financial, or even defense-related systems of a country
- Defame the social elite or reputed person.
- Cheat with needy people and make financial loss.

and many more……

Types of cyber crimes.....

- Financial crimes
- Cyber pornography
- Sale of illegal articles
- Online gambling
- Intellectual property crimes
- Email spoofing
- Forgery
- Cyber defamation
- Cyber stalking

Financial crimes

- Credit card fraud
  - A thief somehow breaks into an eCommerce server and gets hold of credit numbers and related information
  - The thief then uses that info to order stuff on the Internet
  - Alternatively, the thief may auction the credit card info on certain Web sites setup just for that purpose

Financial crimes....

- Cheating
  - Punjab National Bank was cheated to the tune of Rs. 1.39 crore through false debits and credits in computerized accounts.

Cyber Pornography....

- Designing and building pornographic websites to gain financial benefits by producing the advertisement of illegal or sexual items, medicines or costumes.
- Publish or print pornographic magazines using computers and the internet to download photographic pictures, videos, writings etc.
- Storing and carrying pornographic contents in computers, mobile phones and others portable devices.

Sale of illegal articles....

- Sale of Narcotics
- Sale of weapons
- Sale of illegal medicine

  [This can be done by posting information on websites, auction websites, and bulletin boards or simply by email communication.]

Online gambling....

Many websites offer online gambling. In most of the cases, these are actually….

- Fronts of money laundering
- Related with drug trafficking

Intellectual property crimes...

- Software piracy
- Copyright infringement
- Trademarks violation
- Theft of source code
- Registering domain under different fictitious names.

Software Piracy

- Using a piece of SW without the author's permission or employing it for uses not allowed by the author is SW piracy
- For whatever reason, many computer users do not consider it to be a serious crime, but it is!
- Only the large rings of illegal SW distributors are ever caught and brought to justice
- Defense: Various authentication schemes. They, however, are seldom used as they generally annoy the genuine users

Email spoofing.....

- Email which appears to originate from one source but actually has been sent from another source.

Case study: once numerous customers of a bank decided to withdraw their money and close their accounts. It was revealed that someone sent out spoofed emails to customers stating..”The bank was in very bad shape financially. It could close operations at any time.” The email appeared to have from the bank itself.

Forgery.....

- Using sophisticated computers, high quality printers and scanners, counterfeit….
  - Currency notes
  - Postage and revenue stamps
  - certificates
  - Mark sheets etc…..

Cyber defamation....

- Sending derogatory, defamatory and obscene email about someone or company.
- Posting or publishing any content on the website which is defamatory for any company or personnel.
- Posting defamatory objects about someone or any company or any organization on social blogging sites.
- Super imposing on nude pictures or something like that.

Cyber stalking....

Abnormal or illegal movements of a person across the internet. The person sends the messages on the bulletin boards frequently to the victim. He can enter into the chat-rooms and disturbs the victim by constantly sending emails.

Mail Bombing

- A stream of large-sized eMails are sent to an address, overloading the destination account
- This can potentially shut-down a poorly-designed eMail system or tie up the telecom channel for long periods
- Defense: eMail filtering

Break-Ins

- Hackers are always trying to break-in into Internet-connected computers to steal information or plant malicious programs
- Defense: Intrusion detectors

Industrial Espionage

- Spies of one business monitoring the network traffic of their competitors
- They are generally looking for info on future products, marketing strategies, and even financial info
- Defense: Private networks, encryption, network sniffers

Web Store Spoofing

- A fake Web store (e.g. an online bookstore) is built
- Customers somehow find that Web site and place their orders, giving away their credit card info in the process
- The collected credit card info is either auctioned on the Web or used to buy goods and services on the Web

HACKING

- Hacking is the practice of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose.
- The person who is consistently engaging in hacking activities, and has accepted hacking as a lifestyle and philosophy of their choice, is called a **hacker**.

- White hat hacker: A white hat hacker breaks security for non-malicious reasons, for instance testing their own security system. The term "white hat" in Internet slang refers to an ethical hacker. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement. Often, this type of 'white hat' hacker is called an ethical hacker.

- Black hat hacker: A Black Hat Hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain. Black Hat Hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network.

- Grey hat hacker: A grey hat hacker is a combination of a Black Hat and a White Hat Hacker. A Grey Hat Hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been hacked. Then they may offer to repair their system for a small fee.

- Script kiddie: A script kiddie (or skiddie) is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept—hence the term script (i.e. a prearranged plan or set of activities) kiddie (i.e. kid, child—an individual lacking knowledge and experience, immature).

- Hacktivist: A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks.

Denial-of-Service Attacks

- Denial-of-Service (DoS) attack
  - Prevents legitimate users from accessing network resources
- Some forms do not involve computers
- Attacks do not attempt to access information
  - Cripple the network
  - Make it vulnerable to other type of attacks
- Performing an attack yourself is not wise
  - Only need to prove attack could be carried out

Distributed Denial-of-Service Attacks

- Attack on a host from multiple servers or workstations
- Network could be flooded with billions of requests
  - Loss of bandwidth
  - Degradation or loss of speed
- Often participants are not aware they are part of the attack
  - Attacking computers could be controlled using Trojan programs

Hacking Techniques

- Port scanner/ vulnerability scanner
- Password cracking
- Packet sniffer
- Spoofing attack/ phishing
- Key-loggers
- Trojan horse
- Viruses
- worms

Port Scanner

- A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number.

Password Cracking

- Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.

Packet sniffer

- A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

Spoofing attack/phishing

- A spoofing attack involves one program, system, or website successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another program. The purpose of this is usually to fool programs, systems, or users into revealing confidential information, such as user names and passwords, to the attacker.

Key-loggers

- A key logger is a tool designed to record ('log') every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to confidential information typed on the affected machine, such as a user's password or other private data.

Trojan Horses

- Unlike viruses, they are stand-alone programs
- The look like what they are not
- They appear to be something interesting and harmless (e.g. a game) but when they are executed, destruction results

Viruses

- Self-replicating SW that eludes detection and is designed to attach itself to other files
- Infects files on a computers through:
  - USB flash disks, Floppy disks, CD-ROMs, or other removable media
  - The Internet or other networks
- Viruses cause tens of billions of dollars of damage each year
- One such incident in 2001 – the LoveBug virus – had an estimated cleanup/lost productivity cost of US$8.75 billion
- The first virus that spread world-wide was the *Brain* virus, and was allegedly designed by someone in Lahore

One Way of Classifying Viruses

- Malicious
  - The type that grabs most headlines
  - May destroy or broadcast private data
  - May create jam on the communication channels
  - May tie-up the up to stop it from doing useful work
- Neutral
  - May display an annoying, but harmless message
  - May hop from one computer to another while searching for and destroying malicious viruses

Anatomy of a Virus

A virus consists of 2 parts:

- Transmission mechanism
- Payload

Transmission Mechanism

- Viruses attach themselves to other computer programs or data files (termed as *hosts*)
- They move from one computer to another with the *hosts* and spring into action when the *host* is executed or opened

Payload

- The part of the virus that generally consists of malicious computer instructions
- The part generally has two further components:
  - Infection propagation component:
    - This component transfers the virus to other files residing on the computer
  - Actual destructive component:
    - This component destroys data or performs or other harmful operations

Some Commonsense Guidelines

- Download softwares from trusted sites only
- Do not open attachments of unsolicited eMails
- Use flash disks, floppy disks and CDROMs that have been used in trusted computers only
- When transferring files from your computer to another, use the write-protection notches
- Stay away from pirated softwares
- Regularly back your data up
- Install Antivirus SW; keep it and its virus definitions updated

Antivirus

- Kind of software designed for detecting viruses & inoculating
- Continuously monitors a computer for known viruses and for other tell-tale signs like:
  - Most – but, unfortunately not all – viruses increase the size of the file they infect
  - Hard disk reformatting commands
  - Rewriting of the boot sector of a hard disk
- The moment it detects an infected file, it can automatically inoculate it, or failing that, erase it

Other Virus-Like Programs

- There are other computer programs that are similar to viruses in some ways but different in some others
- Three types:
  - Trojan horses
  - Logic- or time-bombs
  - Worms

Logic- or Time-Bombs

- It executes its payload when a predetermined event occurs
- Example events:
  - A particular word or phrase is typed
  - A particular date or time is reached

Worms

- Harmless in the sense that they only make copies of themselves on the infected computer
- Harmful in the sense that it can use up available computer resources (i.e. memory, storage, processing), making it slow or even completely useless

Spyware

- Sends information from the infected computer to the attacker
  - Confidential financial data
  - Passwords
  - PINs
  - Any other stored data
- Can registered each keystroke entered
- Prevalent technology
- Educate users about spyware

Figure 3-2 A spyware initiation program

Adware

- Similar to spyware
  - Can be installed without the user being aware
- Sometimes displays a banner
- Main goal
  - Determine user's online purchasing habits
  - Tailored advertisement
- Main problem
  - Slows down computers

Protecting Against Malware Attacks

- Difficult task
- New viruses, worms, Trojan programs appear daily
- Malware detected using antivirus solutions
- Educate your users about these types of attacks

Figure 3-3 Detecting a virus

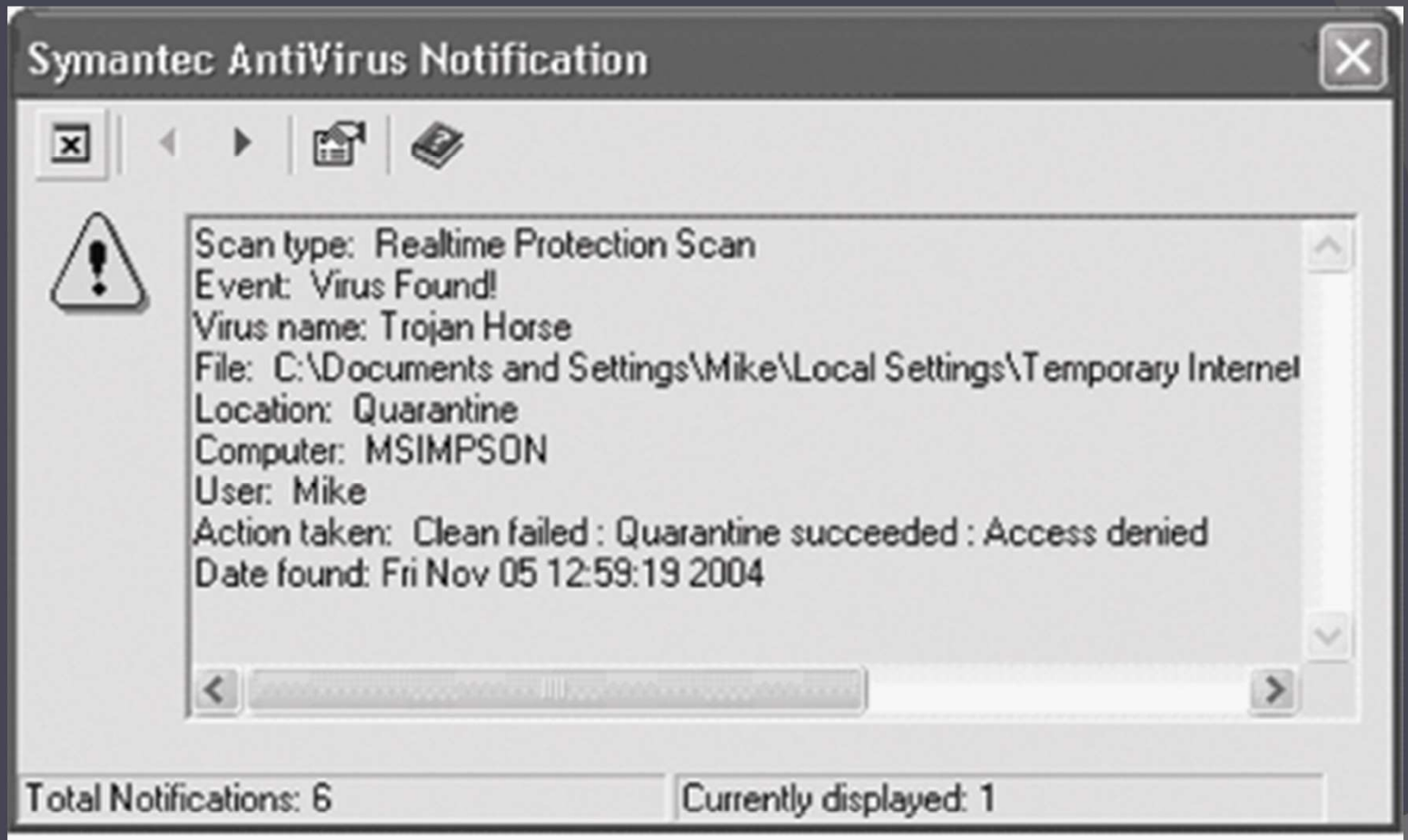

Figure 3-4 Detecting a Trojan program

Educating Your Users

- Structural training
  - Most effective measure
  - Includes all employees and management
- E-mail monthly security updates
  - Simple but effective training method
- Recommend that users update virus signature database
  - Activate automatic updates

Educating Your Users

- SpyBot and Ad-Aware
  - Help protect against spyware and adware
- Firewalls
  - Hardware (enterprise solution)
  - Software (personal solution)
  - Can be combined
- Intrusion Detection System (IDS)
  - Monitors your network 24/7

The Role of Security and Penetration Testers

- Hackers
  - Access computer system or network without authorization
  - Breaks the law; can go to prison
- Crackers
  - Break into systems to steal or destroy data
  - U.S. Department of Justice calls both hackers
- Ethical hacker
  - Performs most of the same activities but with owner's permission

The Role of Security and Penetration Testers (continued)

- Script kiddies or packet monkeys
  - Young inexperienced hackers
  - Copy codes and techniques from knowledgeable hackers
- Programming languages used by experienced penetration testers
  - Practical Extraction and Report Language (Perl)
  - C
- Script
  - Set of instructions that runs in sequence

How to prevent Cyber crime

- Technical prevention
- Network administrator
  - Tasks
  - Role in the company organisation chart
  - Personal data and privacy

How to prevent Cyber crime

- Update Operating System
- Antivirus protection
- Anti-spam and Trojan protection
- Home banking and Internet banking
- Good legal policies
- Use secured protocol for net surfing.

How to prevent Cyber crime

Using the computer at workplace – between efficiency and privacy

- Include the Policy on how to use Internet at workplace as a part of the labour contract
- Training the employees on usage of Internet and software
- Training the employees on how they should treat confidential information and the essential passwords

Cyber Forensics

- Finding password protected information
- Finding encrypted information and contents
- Tracing the source of Email
- Tracking software piracy
- Recovering deleted data
- Matching information
- Remotely monitoring computer and preserving digital evidence to present in the court.

E-Evidence/Digital Evidence

- **Digital evidence** or **electronic evidence** is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required.

E-Evidence Types

The use of digital evidence has increased in the past few decades as courts have allowed the use of

- e-mails,
- digital photographs,
- ATM transaction logs,
- word processing documents,
- instant message histories,
- files saved from accounting programs

E-Evidence types

- spreadsheets,
- internet browser histories,
- databases,
- the contents of computer memory,
- computer backups,
- Global Positioning System tracks,
- logs from a hotel's electronic door locks,
- digital video or audio files.

What to do with a cybercrime case ?

- To report it or not ?
- Confidential information ; Public image
- Be careful with digital evidences !
  - *Digital evidence is not obvious*
  - *It is very "fragile" (can be easily modified or can disappear)*
  - *Special protection measures are required in order to collect, seize or examine such evidence*

End of Lecture

Thanks to all.