Computer Fundamentals

Lecture # 9:

Cyber Crime

Today's Aim

- Different aspects of Cyber Crimes
- DoS Attack
- Viruses
- Pirated Software
- Victims of Cyber Crimes

DoS (Denial of service) – A Case Study

- is an attempt to make a machine or network resource unavailable to its intended user
- Feb 7, 2000 – DoS
- No Response from Yahoo's Server
- Hit- Rate higher than on an Important Event
- No Computer Got Broken Into
- No User Data was Manipulated

Three Phases of DoS

- Search
  - SW used to search weak servers which are used as Drones
  - Drones are used to Scan other servers
- Arm
  - Conquered Drones Loaded with the DoS SW
  - The attack may either be ‘triggered’ (Command Dependent) or ‘scheduled’ (Time Dependent)

Three Phases of DoS

- Attack
  - At the Wake-up Call, Drones Release Large no. of Packets
  - Packets are Similar with no Quality Info
  - Responding to Packets Overburdens the Destination Servers

Neutralizing DoS

- Key Characteristics of Incoming Packets Analyzed
- Packets Filtering
- IP Address Spoofing (**IP address spoofing** or **IP spoofing** refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender)
- For the DoS Attack of Feb 2007, Neutralizing took 3 hours.

- A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate (lawful) users of a service from using that service.
- There are two general forms of DoS attacks: those that crash services and those that flood services.

- A DoS attack can be perpetrated (carry out) in a number of ways. The five basic types of attack are:
- Consumption of computational resources, such as bandwidth, disk space, or processor time.
- Disruption of configuration information, such as routing information.

Continued…

- Disruption of state information, such as unsolicited (not requested) resetting of TCP sessions (see next slide).
- Disruption of physical network components.
- Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

TCP Session function

When you connect to another computer or device on a network or the Internet, a link between you and that machine must be created to be able to pass any data (files, email, web, etc).

That link is called a TCP session. It does many things, like make sure the machines you want to connect to is really the one you want to (there are millions of computers on the Internet).

Also checks that every data you receive or send is not corrupted or lost. If it happens, then sends the data segment again.

It also checks if the other machines is still online. If it's not, your computer will tell you that you have lost connection, or something like that.

Various aspects of Cyber Crimes

- Unauthorized Access
- Info Theft
- E-Mail Bombing & Spoofing
- Denial of Service
- Virus/Worm Attacks
- Logic Bombs(In a computer program, a logic bomb, also called *slag code*, is programming code, inserted intentionally, that is designed to execute (or "explode") under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command.)
- Trojan Attacks (Web hacking)
- Software Piracy
- Cyber Stalking (**It** is the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization.)

Victims

- Individuals
- Organizations
- Countries
- Societies

Victims – Individuals

- Harassment via e-mails.
- Cyber-stalking.
- Dissemination (broadcasting without f/back) of obscene (utterly ridiculous) material
- Defamation.
- Unauthorized control/access over computer system.
- Email spoofing
- Cheating & Fraud
- Computer Vandalism (**a** program that performs malicious function such as extracting a user's password or other data or erasing the hard disk.)

Victims – Organizations

- Unauthorized control/access over computer system
- Possession of unauthorized information.
- Cyber terrorism against the government organization.
- Distribution of pirated software etc.

Victims – Countries

- Vulnerable sectors include:
  - Telecom
  - Finance
  - Defense Related Systems

Victims – Societies

- Trafficking
- Financial crime e.g., credit card frauds
- Sale of illegal articles
- Online gambling

Cyber War

- California's 911 Service shut down
- US Navy Warship controlled by Hackers
- US NSA hired 35 Hackers to Check DoD's N/W's Security
- Wiki Leaks

Cyber Warfare

Cyberwarfare refers to politically motivated hacking to conduct sabotage (deliberately destroying). It is a form of information warfare sometimes seen as analogous to conventional warfare, although this analogy is controversial for both its accuracy and its political motivation.
U.S. government security expert Richard A. Clarke, in his book *Cyber War* (May 2010), defines "cyberwarfare" as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.

- A Threat
- An Opportunity
- Nations Involved

A Look at the Most Common Cyber Crimes

E- Mail Bombing

- Similar to DoS
- Purpose - Overloading of destination account
- Can Shut-down a poorly-designed eMail system/ server
- Can tie up the telecom channel for long periods
- Defense: email filtering

Email Spoofing

- Using Forgery (illegal modifications) to Use Someone Else's Account Name
- Purpose:
  - Revenge
  - Financial Frauds
- Defense:
  - Confirmation With the Sender

Unauthorized Access

- Sometimes Referred to as Hacking
- Purpose:
  - Steal info
  - Plant malicious programs
  - Delete Files
- Defense:
  - Intrusion detectors(An **intrusion detection system** (**IDS**) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station.)
  - Complex Passwords

Credit Card Fraud

- eCommerce server break-in
- Using Stolen Credit Card No.s:
  - Online Shopping
  - Credit Card Auction
- Defense:
  - Single-use credit card numbers
  - Single Transaction Credit Card Numbers

Piracy

- Using SW Without Author's Permission
- Using SW for Unauthorized Use
- Defense: Authentication Techniques

Industrial Espionage(Spying)

- Spying over a Competitors Business
- Monitors data coming in and out of your private network
- Defense:
  - Private networks
  - Encryption
  - Network Sniffers (is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network)

Web Store Spoofing

- Fake Web stores
- Customers' Credit Card Info Obtained
- Defense: Never Trust A Stranger

Virus

- Self-replicating SW (replicate itself and spread from one pc to another)
- Elusive (difficult to describe)
- Dependent(Executable-infecting viruses are dependent on users exchanging software or boot-able floppies, so they spread rapidly in computer hobbyist circles.)
- Infects files on a computers through:
  - Storage Media
  - Networks

Virus Classification

- Malicious
  - May destroy or broadcast private data
  - May clog-up (obstructed) the communication channels
  - May tie-up the microprocessor to stop it from doing useful work
- Harmless
  - e.g., funny prompts, annoying but cause no system crash

Virus Anatomy(structure wise analysis)

- Transmission Mechanism
  - Travel Through Hosts
  - Become Active when Host File Executed
- Payload(The payload is what the computer virus is programmed to do. Some viruses do nothing more than copy themselves onto another PC, much like a real virus does from host to host. This is the simplest payload that a virus can have. However, just like viruses in nature, some computer viruses have a greater effect - maybe they steal files or data or allow someone else to take control over the PC while some will destroy some or all of the data on the computer.)
  - Contains Malicious Instructions
    - Infection propagation component
    - Actual destructive component

Other Virus-Like Programs

- Trojan Horses
- Logic- and Time- Bombs
- Worms

Trojan Horses

- Stand-alone programs
  - A **Trojan horse**, or **Trojan**, is a malicious application that appear as a legitimate file or helpful program but whose real purpose is, for example, to grant a hacker unauthorized access to a computer. Trojans do not attempt to inject themselves into other files like a computer virus. Trojan horses may steal information, or harm their host computer systems
- Types:
  - Password Trojans
  - Privileges- Elevating Trojans
  - Key Loggers
  - Destructive Trojans
  - Joke Programs
  - Back Orifice
  - NetBus

Logic- or Time- Bombs

- A **logic bomb** is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database in a company)
- Execution Event Predetermined
- Example events:
  - Command
  - Time

Worms

- Independent Programs
- Harmless Instructions
- Harmful duplication
- Types:
  - Rabbits
  - Octopus

World famous Worms & Viruses

- 1988 – the Internet Worm
- 1989 – the Span Network Worm
- 1997 – the Tree Christmas Worm
- 1998 – Chernobyl
- 1999 – Melissa, ExploreZip
- 2000 – “The Love Bug”
- 2000 – Pakistani Brain