Module 4: Introduction to Cyberspace and Cyber Crime

Content

- Cyberspace
- Internet
- WWW
- Cyber Crime
- Classification:

Classification

- Phishing
- Email Spoofing
- Credit Card Fraud
- Password Cracking
- Cyberstalking
- Social Engineering
- Virus and Trojan Horse

INTRODUCTION

❖The internet in India is growing rapidly. It has given rise to new opportunities in every field, we can think of, be it entertainment, business, sports or education.

❖There’re two sides to a coin. Internet also has it’s own disadvantages, that is Cyber crime, illegal activity committed on the internet.

Cyberspace

- Cyberspace is where users virtually travel through matrices of data.
- It is virtual environment
- It is the place where human interact over computer networks.
- Now the term “cyberspace” is used to describe the Internet and other computer networks.
- In terms of Computer Science, “cyberspace” is a world wide network of computer networks that uses TCP/IP for communication to facilitate transmission and exchange of data.
- Cyberspace is a place where we chat, explore , watch movies, buy items, research and, etc.

CYBER CRIME

- Crime committed using a computer and the internet to steal data or information.
- Illegal imports.
- Malicious programs.

Another definition

- *"Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that target the security of computer systems and the data processed by them".*
- Hence cybercrime can sometimes be called as *computer-related crime, computer crime, E-crime, Internet crime, High-tech crime….*

Cybercrime specifically can be defined in number of ways…

- A crime committed using a computer and the internet to steal a person's identity(identity theft) or sell contraband (smuggled goods) or stalk (spying) victims or disrupt operations with malicious programs.
- Crimes completed either on or with a computer
- Any illegal activity through the Internet or on the computer.
- All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW.
- Cybercrime refers to the act of performing a criminal act using cyberspace as communication vehicle.

Motives behind cybercrime

- Greed
- Desire to gain power
- Publicity
- Desire for revenge
- A sense of adventure
- Looking for thrill to access forbidden information
- Destructive mindset

Classification of cybercrimes

1. Cybercrime against an individual
2. Cybercrime against property
3. Cybercrime against organization
4. Cybercrime against Society

1. Cybercrime against an individual

- Electronic mail spoofing and other online frauds
- Phishing,
- spamming
- Cyber defamation
- Cyber stalking and harassment
- password sniffing and so on.

2.Cybercrime against property

- Credit card frauds
- Intellectual property(IP) crimes
- Internet time theft

3.Cybercrime against organization

- Unauthorized accessing of computer
- Password sniffing
- Denial-of-service attacks
- Virus attack/dissemination of viruses
- Trojan Horse
- Computer network intrusions

4.Cybercrime against Society

- Forgery
- Cyber terrorism
- Web jacking (Hackers gaining access and control of a website by taking over a domain)

Phishing

- The fraudulent practice of sending emails purporting to be from reputable companies in order to convince individuals to reveal personal information, such as passwords, OTP, and credit card numbers.
- Phishing Steals personal and financial data and also can infect systems with viruses.
- A method of online ID theft


1.
Attacker sends phishing
mail to target
Hacker
Target
2.
Victim clicks on
Phishing link and
visits fake website
3.
Hacker collects
important credentials
4.
Hacker uses
victim's credentials
to access private
information
Original Website
Phishing Website

How Phishing works?

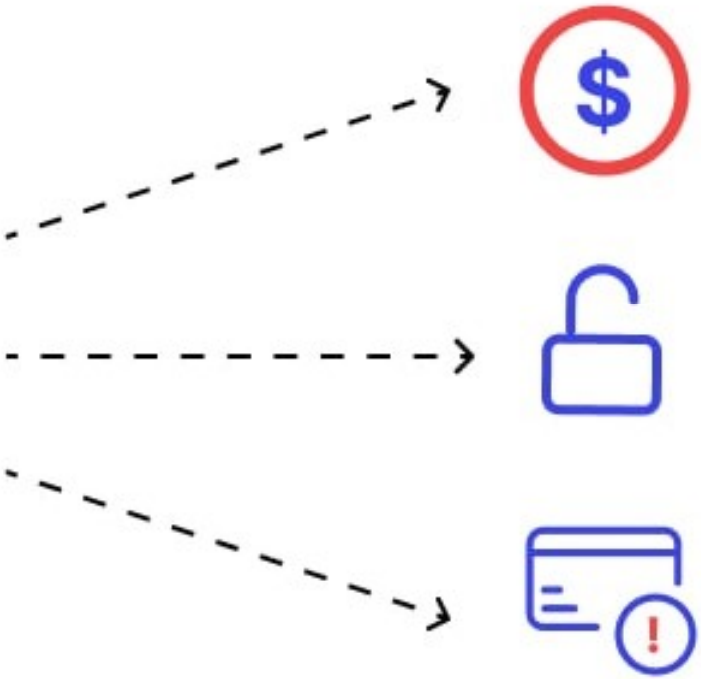
- Planning : use mass mailing and address collection techniques- spammers
- Setup : Email/ webpage to collect data about the target
- Attack : send a phony message to the target that appears to be from a reputable source.
- Collection: record the information obtained from victim.
- Identity theft and fraud: use information to commit fraud or illegal purchases

E-Mail Spoofing

- E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.
- To send spoofed e-mail, senders insert commands in headers that will alter message information.
- Thus, someone could send spoofed e-mail that appears to be from you with a message that you didn't write.
- For example, spoofed e-mail may purport(especially falsely) to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information -- any of which can be used for a variety of criminal purposes.

Email spoofing

The recipient thinks the letter came from a friend or legitimate company because the header of the letter has been changed



Fake email from a friend with a malicious link

Fake email from CEO demanding confidential company data

Fake email from the seller asking for bank details

Credit card frauds

- **Credit card fraud** is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction.
- The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.

Credit card Frauds in Mobile and wireless computing Era

- Credit card fraud is common attack in M-commerce and M-banking.
- **Credit card fraud** is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction.
- Credit card fraud is primarily the unauthorized, illegal use of your credit card to either obtain goods without paying for them or obtain funds from your account by way of a cash withdrawal.
- The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account

Tips to prevent Credit card Frauds

- Avoid Giving out Your Credit Card Information
- Report Lost or Stolen Credit Cards Immediately
- Review Your Billing Statements Each Month
- Be Safe with Your Credit Card Online : Don't click on email links from anyone that looks like your bank, credit card company, or other business who uses your personal information, even if the email looks legitimate.
- Make Strong Passwords and Keep Them Safe
- Check Gas Stations and ATMs for Credit Card Skimmers(Device): These skimmers capture and store your credit card information.
- **Visually inspect ATM machines before using them.**

Tips to prevent Credit card Frauds

- keep a watchful eye on all your accounts and your credit reports.
- Use mobile payment apps for in-store shopping: to avoid skimming.
- Be careful about giving your information over the phone.
- Don't send your information in the mail, via email or in a text.
- Don't save your credit card information online and in smart phone.
- Use a virtual credit card number online.
- Avoid unsecure websites.
- Use a virtual private network on public Wi-Fi

Tips to prevent Credit card Frauds

- The best way to prevent both credit card fraud and identity theft is to ensure your sensitive information is secured as much as possible.

Trojan horse

- It is a type of malicious software (malware) developed by hackers to disguise as legitimate software to gain access to target users' systems.
- A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer.
- Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems.
- Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system.

Trojan horse

- Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an e-mail attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else.
- Trojan horses are one of the most common methods a computer criminal uses to infect your computer and collect personal information from your computer.

Trojan horse

- **Trojan horse actions include:**
  - Deletes Data
  - Copies data
  - Modifies Data
  - Blocks Data
  - Disrupts the performance of the target computers or networks

Social Engineering

- It is the technique to influence and persuasion to deceive people to obtain information or perform some action.
- A social engineer uses phone call or Internet to get them to do something that is against the security practices and/or policies of the organization.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationship with insiders.
- The goal of social engineer is to fool someone into providing valuable information or access to that information.

Classification of social engineering

- Human based social engineering: person to person interaction to get required/desired information,
- Computer based social engineering: Using software and Internet to get required/desired information (Sending an e-mail and asking user to re-enter password to confirm it)

Human based social engineering

- Impersonating an employee or valid user
- Posing as an important user (CEO, CTO, High level manager)
- Using third person: An attacker pretends to have permission from an authorized source to use a system.
- Calling technical support: help desk.
- Shoulder surfing: : it is the technique of gathering username and password by watching over person's shoulder while he/she logs into the system.
- Dumpster diving: It involves looking in the trash for information written on pieces of paper or computer printouts. [PAN number, Debit/Credit numbers and so on]

Computer based social engineering

- Fake –emails
- E-mail attachments
- Pop-up windows

Note:

Social engineering also considered as passive information gathering methods.

Cyberstalking

- **Cyberstalking** is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization.
- Types:
  1. Online stalkers: Interaction using Internet, E-Mail, Chat rooms.
  2. Offline stalkers: Following victim, watching daily routine of the victim, searching on news groups/ personal websites/face book.

Cyberstalking is a technologically-based "attack" on one person who has been targeted specifically for that attack for reasons of anger, revenge or control. Cyberstalking can take many forms, including: harassment, embarrassment and humiliation of the victim.

Cyberstalking: How it works

1. Personal information gathering about victim.
2. Establish contact with victim through phone to threaten/harass.
3. Establish contact with victim through E-mail and sending repeated e-mails to threaten/harass the victim.

Password cracking

- Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.
- Usually an attacker follows a common approach –
  - Repeatedly making guesses for the password
- Password cracker purpose
  - To recover a forgotten password
  - To check easily crackable password by system admin
  - To gain unauthorized access to a system

Password Cracking

- Manual Password Cracking
  - Log in with different passwords
  - Attacker follows the following Steps
    - Find a valid user account such as an Admin or Guest
    - Create a list of possible passwords
    - Rank the passwords from high to low probability
    - Try again until a successful password if found

Password Cracking

- Password can be guessed sometimes with knoweldge of user's personal information
  - Bank (none)
  - The words like "Password", "passcode" & "admin"
  - Asdf, qwerty etc (series of letter from QWERTY Keyboard)
  - User's name or login name
  - Name of users' friend /relative / pet
  - User's birthplace or date of birth, or a relative's or a friend
  - User's vehile number, office number, residence number or mobile number
  - Name of a celebrity who is considered to be an idol
  - Simple modification of one of the preceding, such as suffixing a digit, particularly 1 or reversing the order of letter.

Password Cracking

- Attacker also writes script file(automated program) which will be executed to try each password in a list.
- Password are not stored as plain text
- To ensure confidentiality
  - One way hashing
    - Password text converted to unique hash value & stored in database/system
    - Each time entered password is converted into hash value and compares with the stored hash value for authentication.
  - Trying password generated hash value with stored hash values
- Password cracking tools
- www.defaultpassword.com -
- www.oxid.it/cain.html - used in Microsoft OS, cracks the password by sniffing the network, cracking encrypted password, brute force attacks, decoding scrambled password & recovering wireless network keys
- www.openwall.com/john - Open source – Fast password cracker, primary purpose is to detect weak password.
- www.freeworld.tch.org/thc-hydra - very fast network logon cracker
- www.aircrack-ng.org – used for wireless networks. WPA 1 or WPA 2 networks
- www.10phtcrack.com – used to crack windows passwords from hashes . Has methods to generate password guess.

Password Cracking Classification

- Online Attacks
  - Script file (automated program) try each possible password
  - Man in the middle attack(MITM) also termed as bucket-brigade attack or Janus Attack.
- Offline Attacks - **Offline Password Cracking** is an attempt to recover one or more passwords from a password storage file that has been recovered from a target system
  - Requires access to computer & copying the password file
  - Analyzing the password file.
  - Dictionary Attack – Attempts to match all the word from the dictionary to get the password – Eg : Administrator
  - Hybrid Attack – Substitute numbers and symbols to get the password – Eg : Adm**ı**n**ı**strator
  - Brute Force Attack – Attempts all possible combination of letter or nubers
- Non-electronic attacks(e.g – Social Engineering, shoulder surfing and dumpster diving)

Strong, Weak and Random Password

- Self Study & Discussion

Password Cracking

- General Guidelines applicable to the password policies, which can be implemented organization-wide are as follows
  - Password and user logon ID should be unique to each authorized user
  - Password should consist of 8 alphanumeric characters(no common names or phrases)
  - Avoid weak password(there should be computer controlled list or rules to identify weak password)
  - Password should be changed every 30/45 days or less
  - User Account should be frozed(locked) after five failed logon attempts
  - Session should be suspended after 15 minutes of idle period and needs to reenter password
  - Logon ID & Password should be suspended after a specified period of non-use
  - For high-risk systems, after excessive violations, the system should generate and alarm and be able to simulate a continuing session(with dummy data) for the failed user (to keep this user connected while personal attempt to investigate the incoming connection)

Password Cracking

- Password guidelines to avoid being victim of getting their personal E-Mail accounts hacked/attacked by the attackers.
  - Password used for business E-Mail account, personal E-Mail accounts and banking/financial user accounts should be kept separate.
  - Password length
  - Password should be change every 30/45 days
  - Password should not be shared with anyone
  - Password used previously should not be used while renewing the password.
  - Passwords should not be stored in PDA (Mobile Devices)
  - Avoid victim of phishing attacks by avoiding fake link to change password (check the legitimacy of the E-Mail)
  - Avoid victim of Smishing attacks(SMS based phishing)
  - In case accounts is hacked contact immediate the respective agencies or institutes .

Thank You!