Unit – 4
Phishing and Identity Theft

Topics

4.1 Phishing : Introduction

4.2 Phishing methods : Dragnet, Rod-and-reel , Lobsterpot, Gillnet

4.3 Techniques of phishing

4.4 Phishing Toolkits and Spy Phishing

4.5 Phishing countermeasures

4.6 Personally Identifiable Information (PII)

4.7 Types of Identity theft

4.8 Techniques of Identity theft

4.9 Identity Theft Countermeasures

Phishing

- Phishing is the use of social engineering tactics to trick users into revealing confidential information.
- Facebook, HSBC, Paypal and Bank of America are the most targeted organizations in phishing attacks.
- US, India and China are the most targeted countries to launch phishing attack.
- Phishing is a type of deception (fraud) designed to steal your identity (i.e a kind of ID theft fraud).

Phishing

- it attracts netizens to reveal their personal information that can be used for Identity (ID) theft.

- ID theft involves unauthorized access to personal data.

- Phishing affect not only individuals but also all industries and businesses that have an online presence and do online transactions over Internet.

Phishing

- Internet scammers are using E-mail to fish (search) for passwords and financial data from sea of internet users.

- Definition of “Phishing” by Wikipedia
  - ***“It is the criminally fraudulent process of attempting to acquire sensitive information such as username, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.”***

Phishing

- In phishing, the phishers tries to get user to disclose valuable personal data by convincing to provide it under false pretense.

- **E-mails** are the popular medium used in phishing attacks and such E-mails are called as **Spam**.

- Spam is the abuse of electronic messaging system to send unsolicited bulk messages.

Phishing

- Two categories of E-mails
  - Spam E-mails
  - Hoax E-mails

Spam E-mails

- Also known as “junk E-mails” involves unwanted messages sent to numerous recipients .

- Spam E-mails grown since the early 1990s.

- Botnet, network of virus infected computers, are used to send about 80% of Spam.

- Types of Spam E-mails
  - **Unsolicited Bulk E-Mail (UBE) :**
    - » Synonym for spam
    - » Unsolicited Email send in large quantities
  - **Unsolicited Commercial E-Mail (UCE):**
    - » Unsolicited Emails are sent in large quantities from commercial perspective.
    - » Example : Advertising

Spam E-mails

- It is a popular medium for phishers

- To scam (cheat) users to enter personal information on fake website using E-mail forged to look like as if it is from a bank or other organizations such as
  - HSBC, Santander, Common Wealth Bank
  - eBay
  - Amazon
  - Facebook

Phishers tactic to get user information

- **Names of legitimate organizations**
  - Phishers might use a legitimate company’s name and incorporate the look and feel of its website into the Spam E-mail.

- **“From” a real employee:**
  - Real name of an official, who actually works for the organization, will appear in the “from” line or text of message.

Phishers tactic to get user information

- **URLs that “look right”:**
  - E-mail contain a URL (i.e Weblink) which seems to be legitimate website wherein user can enter information.
  - Website is a spoofed website that looks like real thing.

- **Urgent messages:**
  - Creating a fear to trigger a response.
  - Emails warn that failure to respond will result in no longer having access to E-mail accounts.

Phishers tactic to get user information

Examples of phases used to attract user to take action

- “Verify your account”
  - Organizations never ask user to send passwords, login names, PAN or SSN numbers or other information through emails.
  - Example : If email messages asking to update your credit card information, don’t respond without any confirmation of concern authority.
- “You have won the lottery”
- “If you don’t respond within 48 hours, your account will be closed”

Ways to reduce Spam E-mails

1. Share personal Email address with limited person and public websites.

2. Never reply or open any spam emails.

3. Disguise the email address on public website or groups by spelling out the sign “@” and DOT (.). Example, RajeevATgmailDOTcom. This prohibits phishers to catch valid email address while gathering email address through programs.

4. Use alternate email addresses for register for any personal or shopping website. Never use business email addresses for these sites.

5. Do not forward any emails from unknown recipients.
6. Make habit to preview an Email before opening it.
7. Never use email address as screen name in chat groups or rooms.
8. Never respond to spam email asking your email addresses from mailing distribution list.

Hoax Emails

- Attempts to deceive or trick user into believing or accepting that something is real, when the hoaxer (the person or group creating a hoax) knows it is false.

- It may or may not be spam emails.

- Websites can be used to check validity hoax emails.
  - www.breakthechain.org
  - www.hoaxbusters.org

SPAMBOTS

- An automated computer program or script developed, mostly in C programming, to send spam mails.

- Gather email addresses from internet, to build mailing lists to send unsolicited emails.

- Also known as web crawler,
  - They gather email addresses from numerous websites, chat room conversations, newsgroups.

Methods of phishing

1. Dragnet
2. Rod-and-reel
3. Lobsterpot
4. Gillnet

Dragnet

- Involves the use of spammed emails, bearing falsified corporate identification (e.g. corporate name, logos and trademarks), which addresses a large group of people to web sites or pop-up windows.

- Clicking on links in the body of email to take victims to the websites or pop-up windows where they are requested to enter bank or credit card account data or personal data.

- Dragnet phishers rely on false information included in email to trigger an immediate response by victims.

- Phishers do not identify specific prospective victims in advanced.

Rod-and-reel

- Phishers identify specific prospective victims in advance.
- Convey false information to them to prompt their disclosure of personal and financial data.
- Example:
  - Phony (fake) webpage, item’s cheaper price is displayed which the victims may be searching for and upon visiting the webpage, victims were asked for personal information before confirming transaction.

Lobsterpot

- Focus upon the use of spoofed website.

- Creating of bogus/phony website, similar to legitimate corporate ones.

- These attacks are known as “content injection phishing”.

- Once the netizens is into spoofed sites, phishers use their information for shopping, apply for new credit cards, access bank accounts etc.

Gillnet

- This technique rely on social engineering techniques
- Phishers introduce malicious code into emails and websites.
- Misuse browser functionality by injecting content.
- Example:
    - Malicious code will change settings in user’s systems so that users who want to visit legitimate banking websites will be redirected to a phishing site.

Phishing techniques

- Techniques used to launch phishing attacks
  1. URL (weblink) manipulation
  2. Filter evasion
  3. Website forgery
  4. Flash phishing
  5. Social phishing
  6. Phone phishing

URL (weblink) manipulation

- URLs are the weblinks (i.e. internet addresses) that direct the netizens/users to a specific website.

- In phishing attacks, URLs are usually supplied misspelled.

- Example: Instead of *www.abcbank.com*, URL is provided as *www.abcbank1.com*, or *www.abbank.com.*

- Users use lobsterpot method to make difference of one or two letters in the URLs, which is ignored by netizens.

- Phishers use homograph attack for URL manipulation.

URL (weblink) manipulation

- **Homograph attack :**
  - Meaning of homograph is
    - Two words are spelled the same way but differ in meaning.
    - E.g. right

  - Phishers use homograph attack on the internationalized Domain Name (IDN) to deceive the netizens by redirecting them on the phony/fake website which looks like the original website.

  - E.g. “0” (zero) and “O” (o alphabet in uppercase), l (L in lowercase) and “I” (i alphabet in uppercase).

  - Instead of www.GOOGLE.com, it is www.G00GLE.com

Filter Evasion

- This technique use graphics (i.e. images) instead of text to prevent from netting such emails by anti-phishing filters.

- These filters are inbuilt into the web browsers.

- Example:
  - Internet Explorer version 7 has inbuilt “Microsoft phishing filter”. One can enable it during installation or it cab be enabled post-installation. It is important to note that it is *not enabled* by default.

  - Firefox 2.0 and above has inbuilt “Google Phishing Filter”. It is enabled by default.

  - Opera phishing filter

Website forgery

- Phishers direct the netizens to website designed or developed by him, to login into website, by altering browser address bar through javascript.
- As the netizens logs into the fake website, phishers gets confidential information very easily.
- Another technique used is “cloaked” URL- domain forwarding and inserting control characters into URL .

Flash phishing

- Anti-phishing toolbars are installed/enabled to help checking the webpage content for signs of phishing, but limitation is that do not analyze flash objects at all.
- Phishers use it to try to like the legitimate website.
- Netizens believe that website is clean and is a real website because anti-phishing toolbar is unable to detect it.

Social phishing

- Phishers attract users to reveal sensitive data using systematic manner
  - Phishers sends mail as it is sent by a bank asking to call them back because there was a security breach.
  - Victim calls the bank on the phone numbers displayed in the mail.
  - Phone number provided in the mail is a false and victim gets redirected to the phisher.
  - Phisher speaks with victim in the similar fashion/style as a bank employee, asking to verify that the victim is the customer of the bank.
    - Example : “Sir, we need to make sure that you are our customer. Could you please supply your credit card information so that I can verify your identity?”
  - Phishers get the required details.

Phone phishing

- Phishers can use a fake caller ID data to make it appear that the call is received from a trusted organization to attract users to reveal their personal information such as account numbers and passwords.

- Example: phishing attack launched on “Android market” website.
  - A malware writer succeeded to list a rogue phishing application called *09Droid* on the android market website.
  - The application posed to be a shell for mobile banking applications, instead being used to obtain (steal) online banking credentials.

Phishing toolkits and spy phishing

- A phishing toolkit is a set of scripts/programs that allows a phisher to automatically set up phishing websites.

- Is used to spoof the legitimate websites of different brands including graphics (i.e. images and logos) displayed on these websites.

- Phishers use Hypertext Preprocessor (PHP) to develop the phishing kits.

- Free phishing kits also called **DIY** (Do It Yourself) phishing kit which may hide backdoors through which the phished information is sent to recipients.

Phishing toolkits and spy phishing

Phishing toolkits	Description
Rock Phish	This phishing toolkit is popular in the hacking community since 2005. It is used to launch phishing attacks. Allow a single website with multiple DNS names to host a variety of phished webpages, covering numerous organizations and institutes.
Xrenoder Trojan Spyware	It reset the homepage and search settings to point to other websites usually for commercial purposes or porn traffic.
Cpanel Google	It is a spyware that modifies the DNS entry in the host's file to point to its own website. If Google gets redirected to its website, a netizen may end up having a version of a website prepared by phisher.

Phishing countermeasures

- To avoid being a victim of phishing attack, countermeasures are

1. Keep antivirus up to date
2. Do not click on hyperlinks in emails
3. Take advantages of anti-Spam software
4. Verify https (SSL)
5. Use anti-Spyware software
6. Get educated
7. Use the Microsoft Baseline Security Analyzer (MBSA)
8. Firewall
9. Use backup system images
10. Do not enter sensitive information or financial information into pop-up windows
11. Secure the hosts file
12. Protect against DNS Pharming attacks

SPS algorithm

- SPS (Sanitizing Proxy System) algorithm is used to thwart (prevent) against phishing attack.

- Using this, removing the part of the content that entices the netizens into entering their personal information.

- SPS sanitize all HTTP responses from suspicious URLs.

SPS algorithm

Characteristics of SPS algorithm

- Two-level filtering:
  - Composed of strict URL filtering and HTTP response sanitizing.
- Flexibility of the rule set:
  - Algorithm distinguish between legitimate website and other suspicious websites based on rule set.
- Simplicity of the filtering algorithm:
  - Described into 20 steps and easily apply SPS functions into existing proxy implementation, browser plug-ins or personal firewall.

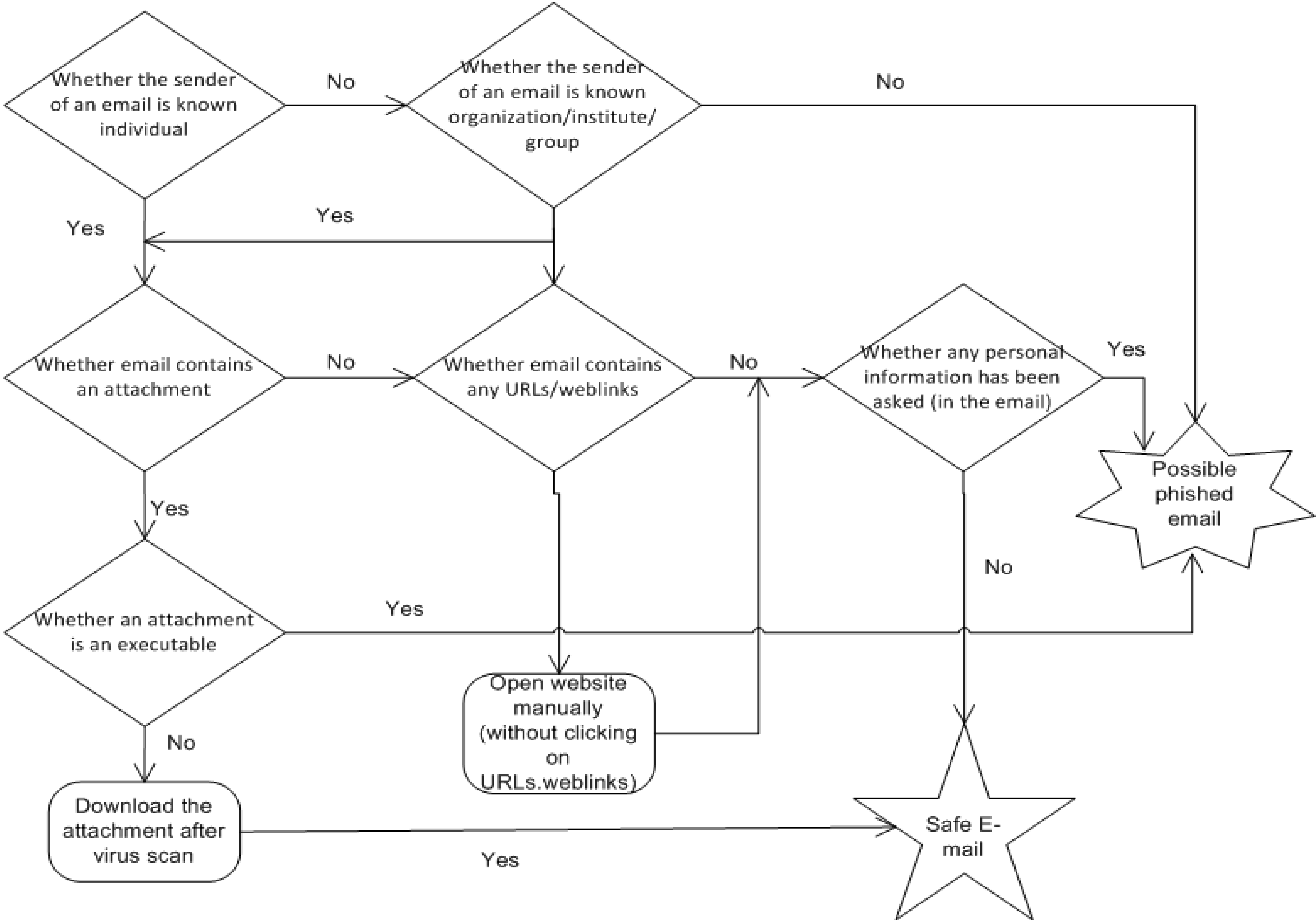
- Accountability of HTTP response sanitizing:
    - SPS prevents netizens from disclosing their personal information to phishing sites by removing malicious HTTP headers or HTML tags from HTTP response.

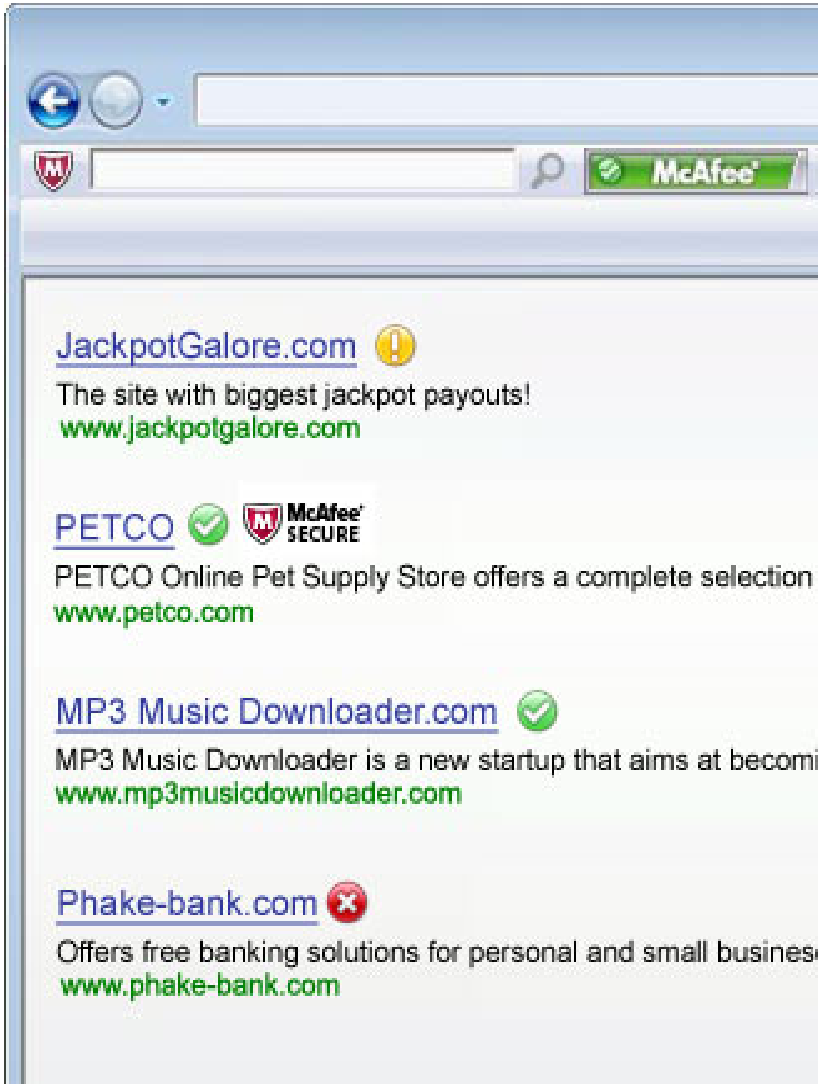
- Robustness against both misbehavior of novice users and evasion techniques:
    - SPS built-in proxy server can protect netizens from web spoofing.

Anti-Phishing plug-ins

Plug-in names	Description
Netcraft Toolbar	It offers protection from phishing attacks
TrustWatch	It has a toolbar for Internet Explorer users as well as Firefox users.
ScamBlocker	It helps protect users from latest phishing threats.
PhishNet 1.2	It protect users from web phishing scams.
SpoofStick	It helps users to detect spoofed (fake) websites.
Google Safe Browsing	It is used as an extension to Firefox. It will alert when a webpage tries asking for user’s personal or financial information.
Windows Internet Explorer’s Phishing filter	Available in IE 7. It helps protect users from entering phishing sites.

Flowchart of phishing attack


Whether the sender of an email is known individual
No
Whether the sender of an email is known organization/institute/ group
No
Yes
Yes
Whether email contains an attachment
No
Whether email contains any URLs/weblinks
No
Whether any personal information has been asked (in the email)
Yes
Possible phished email
Yes
No
Whether an attachment is an executable
Yes
Open website manually (without clicking on URLs.weblinks)
No
Download the attachment after virus scan
Yes
Safe E-mail

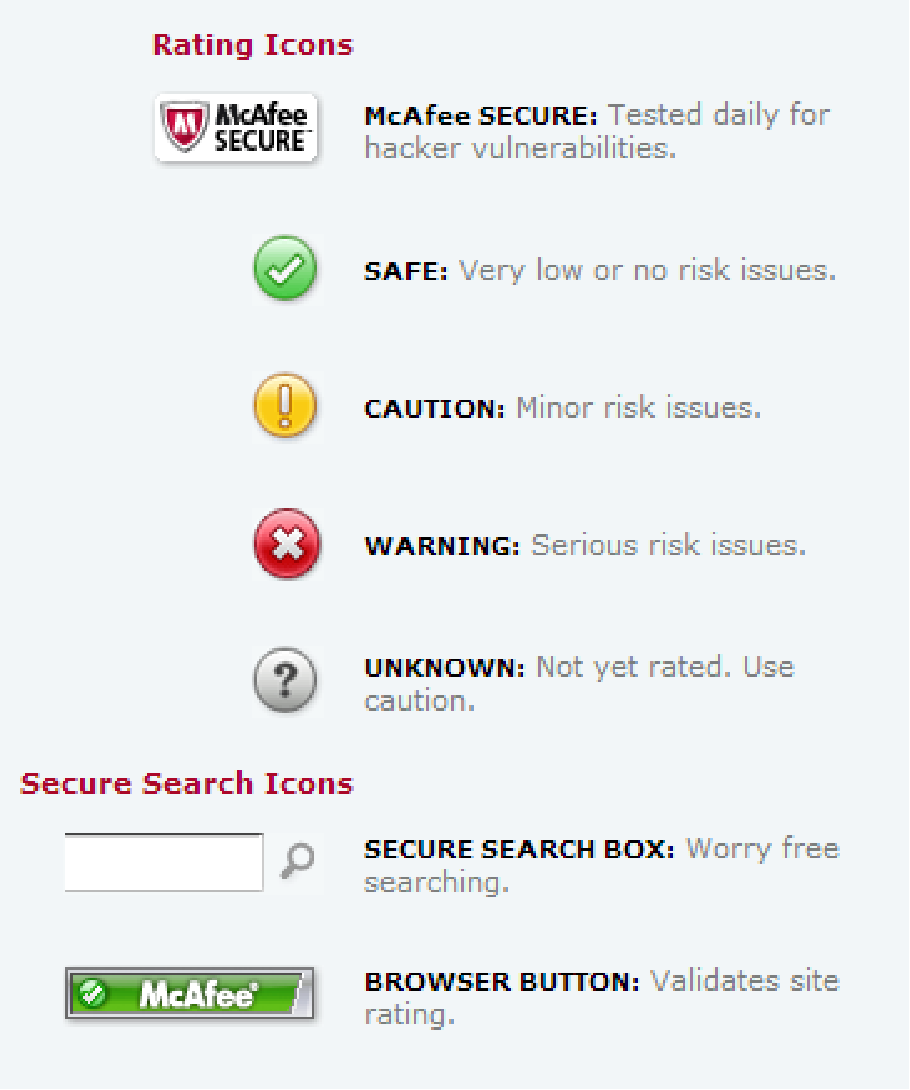


JackpotGalore.com ⚠
The site with biggest jackpot payouts!
www.jackpotgalore.com

PETCO ✓ McAfee SECURE
PETCO Online Pet Supply Store offers a complete selection
www.petco.com

MP3 Music Downloader.com ✓
MP3 Music Downloader is a new startup that aims at becomi
www.mp3musicdownloader.com

Phake-bank.com ✗
Offers free banking solutions for personal and small busines
www.phake-bank.com



Rating Icons

McAfee SECURE — **McAfee SECURE:** Tested daily for hacker vulnerabilities.

✓ **SAFE:** Very low or no risk issues.

⚠ **CAUTION:** Minor risk issues.

✗ **WARNING:** Serious risk issues.

? **UNKNOWN:** Not yet rated. Use caution.

Secure Search Icons

SECURE SEARCH BOX: Worry free searching.

McAfee — **BROWSER BUTTON:** Validates site rating.

- McAfee SiteAdvisor software is a free web security plug-in that provides website security ratings based on the search results

Identity Theft (ID theft)

- ID theft is a fraud involving another person’s identity for an illicit purpose.
- Phishing and identity theft are related offences.
- Identity theft occurs when someone uses another's personally identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.
- ID theft is a punishable offense under the Indian IT Act.
- **Identity Theft Resource Center (ITRC)** is a non-profitable organization situated in USA, the objective is to extend the support to the society to spread awareness about this fraud.

Identity Theft (ID theft)

- Federal Trade Commission (FTC) has provided statistics about identity theft:

- Credit card fraud (26%)
  - Occur when someone acquires the victim's credit card number and uses it to make purchase.

- Bank fraud(17%)
  - E.g. Cheque theft, ATM pass code theft

- Employment fraud (12%)
  - Attacker borrows the victim's valid SSN to obtain a job.

- Government fraud (9%)
  - SSN, driver license and income tax fraud.

- Loan fraud(5%)
  - Occur when attacker applied for a loan on the victim's name.

Personally Identifiable Information (PII)

- Information which can be used to uniquely identify.

- Uniquely Identifiable Information are
  - Full name
  - National Identification Number (e.g. SSN)
  - Telephone number and mobile phone number
  - Driver’s license number
  - Credit card number
  - Digital identity (e.g. Email address, online account ID and password)
  - Birthdate/ birth day
  - Birthplace
  - Face and fingerprints

Personally Identifiable Information (PII)

- Fraudsters may search an individual by combine with other personal information to identify
  - First or last name
  - Age
  - Country, state or city of residence
  - Gender
  - Name of the school/college/workplace
  - Job position, grades and/or salary

Personally Identifiable Information (PII)

- Information can be classified
  1. Non-classified information
  2. Classified information

Non-classified information

- Public information
  - Information that is the matter of public record or knowledge

- Personal information
  - Information belongs to a private individual.

  - But they may share with others for personal or business reasons.

  - e.g. addresses, telephone numbers and email addresses

Non-classified information

- Routine business information
  - Information do not required any special protection
  - May be routinely shared with inside or outside of the business.
- Private information
  - Information can be private if associated with an individual and can object in case of disclosure
  - E.g. SSN, Credit card number, financial information

Non-classified information

- Confidential business information
  - Information which, if disclosed, may harm the business
  - E.g. sales and marketing plans, new product plans, notes related with inventions.

Classified information

- Confidential
  - Information that required protection and unauthorized disclosure could damage national security.

  - E.g. information about strength of armed forces and technical information like guns.

- Secrete
  - Information require protection and unauthorized disclosure could seriously damage security.

  - E.g. national security policy, military plans or intelligence operations.

Classified information

- Top secret
  - Information required highest degree of protection and unauthorized disclosure
  - E.g. important plans and cryptologic intelligence system.
- ID theft fraudsters target to gain access to private, confidential, secret and top secret information.

Types of identity theft

1. Financial identity theft
2. Criminal identity theft
3. Identity cloning
4. Business identity theft
5. Medical identity theft
6. Synthetic identity theft
7. Child identity theft

Financial identity theft

- Includes
  - bank fraud
  - credit card fraud
  - Tax refund fraud
  - Mail fraud

- Occurs when fraudster makes a use of someone's identifying details, such as
    - Name, SSN, bank account details

- Example
    - Fraudsters open a new credit card account in the victim's name and card charges up, payment is neglected.
    - Leaving the victim with bad credit history.
    - Open bank accounts, multiple credit cards, purchase vehicle etc.

Financial identity theft

- Process of recovering from crime is expensive and time-consuming.

- Before a crime is detected, fraudster is capable of running up hundreds to thousands of dollars on victim’s name.

- This type of fraud often destroys a victim’s credit.

Criminal Identity theft

- it involves taking over someone’s identity to commit a crime such as
  - Enter into a country
  - Get special permits
  - Hide one’s own identity
  - Commit acts of terrorism

- These criminal activities are
    - Computer and cybercrime
    - Organized crime
    - Drug trafficking
    - Smuggling
    - Money laundering

Criminal Identity theft

- Fraudster uses the victim’s name upon an arrest or during a criminal investigation.

- This may place the victim’s name into countrywide or statewide criminal database record.

- Personal information given by a fraudster to a law enforcement officer may include counterfeited document such driver’s license, birth certificate etc.

Identity cloning

- Identity cloning is the act of a fraudster living a natural and usual life similar to a victim’s life, may be at a different location.

- Instead of stealing personal information for financial gain or commit crimes in the victim’s name, identity clones compromised the victim’s life by actually living and working as the victim.

- ID clones may even pay bills regularly, get engaged and married and start a family.

Identity cloning

- Identity clone will obtain as much personal information about victim as they can attain.

- They look to find
    - What city and state the victim was born
    - what street he/she grew up on,
    - Where he/she attended school, college etc.
    - What relationships he/she may have involved in
    - Information concerning victim’s parents and other family members.

- These information used when fraudster are on the move or asked about the victim’s life.

Business Identity theft

- It is extremely important to protect Business Sensitive Information (BSI).
- BSI is the information about business or organization.
- BSI is a “sensitive asset” for organization.
- If it is compromised through alteration, corruption, loss, misuse or unauthorized disclosure could cause serious damage to the organization.
- Business ID theft may fuel economic and industrial espionage – which is associated industries such as telecommunication, computer software and hardware, biotechnology, transportation etc.

Business ID theft countermeasures

1. Secure your business premises with locks and alarms
2. Put your business records under lock and key
3. Be cautious (careful) on the phone
4. Limit access to your IT systems
5. Protect IT systems from hackers
6. Create awareness that internet is a dangerous place
7. Avoid broadcasting information
8. Create and enforce organization-wide information security policy
9. Disconnect the access of ex-employees immediately

Synthetic identity theft

- Fraudster will take parts of personal information from many victims and combine them.

- The new identity is not any specific person, but all the victims can be affected when it is used.

Child identity theft

- Parents might sometimes steal their children's identity to open credit card accounts, bank accounts, take out loans because their own credit history is insufficient or too damaged

Medical identity theft

- Fraudsters use someone’s medical information or medical history on their medical record, increase the possibility of patient being treated incorrectly because of incorrect medical record.

- In this type fraud, fraudster has stolen the victim’s identity and receive treatment.

Techniques of ID theft

1. Human-based methods
2. Computer-based methods

Human-based methods

- Direct access to information
  - People who have earned a certain degree of trust.
  - House cleaners, babysitters, nurses, friends or roommates can obtain legitimate access to a business or to a residence to steal the required personal information.
- Dumpster diving
  - Retrieving documents from trash (garbage)
- Theft of a purse or wallet
  - Purse or wallet often contains bank credit cards, debit cards, driving license
- Mail theft
- Shoulder surfing
- False or disguised ATM’s
- Dishonest or mistreated employees
- Telemarketing and fake telephone calls

Computer-based methods

- Backup theft
- Hacking
- Unauthorized access to system and database theft
- Phishing
- Pharming
  - It is an attack aiming to redirect a website’s traffic to another bogus website.
  - An attacker cracks vulnerability in an ISP DNS server and hijacks the domain name of a commercial site and using it redirect to fake website.
- Redirectors
  - Malicious programs that redirects user’s network traffic to unknown location.
- Hardware

Identity theft countermeasures

1. Monitor your credit closely
2. Keep records of your financial data and transactions
3. Install security software
4. Use an updated web browser
5. Be wary of email attachments and instant messages
6. Store sensitive data securely
7. Shred documents
8. Protect your PII
9. Stay alert to the latest scams

Tools used to protect your online identity

Tools	Description
Anti Tracks	Set of tools appear to protect your online identity, sensitive data and maintaining integrity of your system by hiding system's IP address, secure locking and hiding important files and folders .
Privacy Eraser Pro	It protect internet privacy by cleaning up all the tracks of internet and computer activities support by web browsers. Features of this utility are: • Erase Browser Cache Files, browser history, cookies, browser address bar history • File shredder • Cleaning free disk space • Speed up the system
MyPrivacy	It removes your personal information such as name, address, age, phone and other related information. It helps by continuously monitoring internet to remove footprint on internet.
Seppukoo	It is an anti-social network failing to destroy your identity.
Web 2.0 suicide machine	It completely roots out your identity from servers of social networking websites such as MySpace, Twitter and LinkedIn.

Steganography

- Steganograpgy comes from two Greek words

  Steganos meaning “covered”

  Graphein meaning “to write”

  that means “concealed writing”

- Method that attempts to hide the existence of a message or communication.

- it is an art and science of hiding information in such a way that no one apart from the intended recipient knows the existence of the message.

- Also known as data hiding, information hiding and digital watermarking.

Steganography

- **Digital watermarking** is the process of embedding information into a digital signal.
- Example : audio, pictures or video

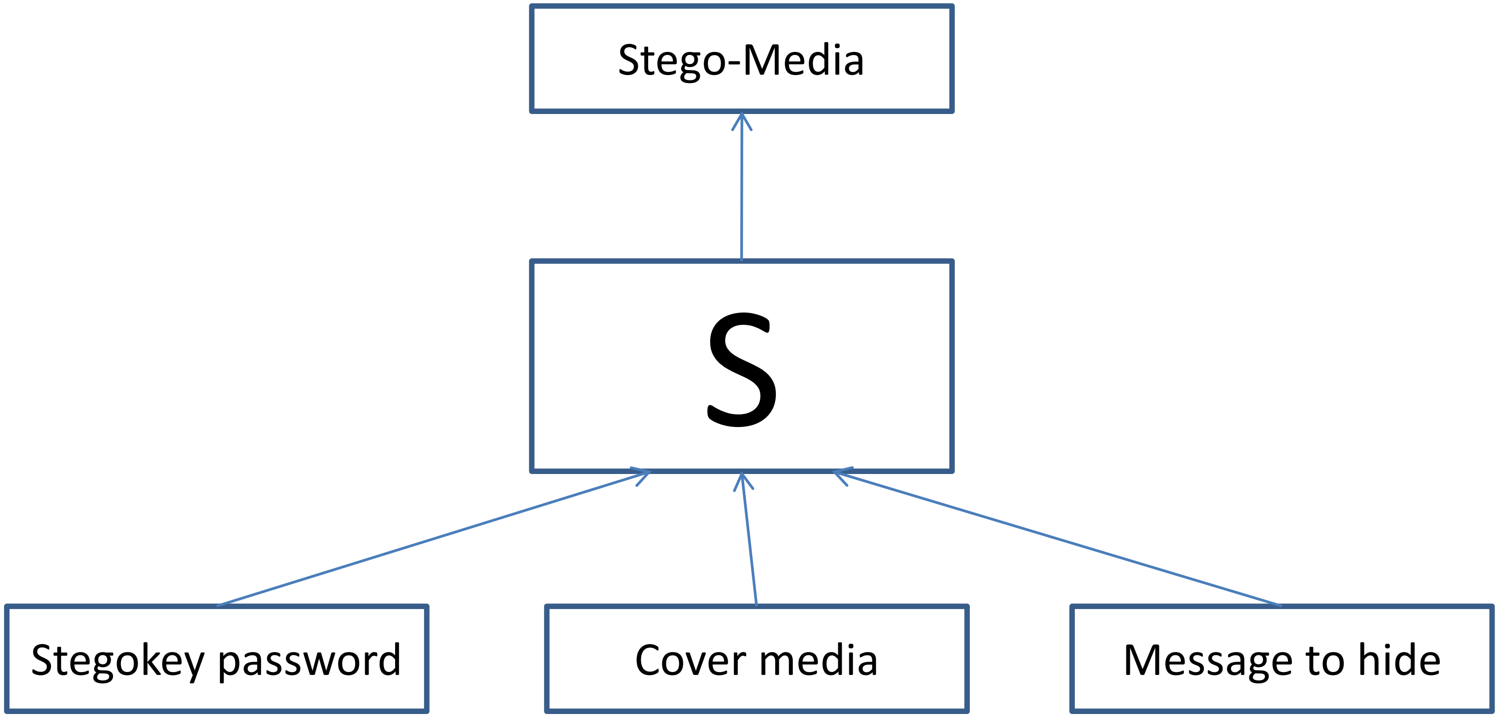
- Terrorist use steganography techniques to hide their communication in images on the internet.

- It is different with cryptography where content is obscured.

- Steganography hides text in plain sight (i.e. image) , while cryptography scrambles plaintext (original message) into ciphertext (coded message)

Steganography

- Cover medium + Embedded message + Stegokey = Stego-medium



Steganography tools

- Disi-Steganography
- Invisible folder
- Invisible secrets
- Stealth files
- Hermetic stego
- DriveCrypt Plus (DCPP)
- MP3Stego
- MSU StegoVideo

Steganalysis

- Steganalysis it the art and science of detecting messages that are hidden in images, audio/video files using steganography.
- Goal of steganalysis
    - to identify suspected packages and to determine whether or not they have a payload encoded into them
    - if possible recover it

Steganalysis tools

- StegAlyzerAS
- StegAlyzerSS
- StegSpy
- Stegdetect
- Stegsecrete
- Visual Steganographic Laboratory (VSL)

DoS Attacks

- DoS stands for Denial-of-Service
- It attempt to make a machine or network resource unavailable to its intended users.
- It is a type of criminal act, the attacker floods the bandwidth of the victim’s network or fills his e-mail box with spam mail.
- **A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.**

DoS Attacks

- Attackers target sites or services hosted on high-profile web servers such as
    - banks, credit card payment gateways, mobile phone networks etc.
- Buffer overflow technique is used to commit such kind of criminal act.
- IP address spoofing refers to creation of IP packets with a forged (spoofed) source IP address with purpose of
    - Concealing the ID of sender
- Attacker spoofs the IP address and floods the network of the victim with repeated requests.
- As IP address is fake, the victim machine keeps waiting for response from attacker's machine for each request. This consumes the bandwidth of network which then fail to serve the legitimate requests.

DoS Attacks

- United States Computer Emergency Response Team defines symptoms of DoS attack are
  - Unusually slow network performance (opening files or accessing websites)
  - Unavailability of a particular websites
  - Inability to access any website
  - Dramatic increase in the number of spam emails received (i.e. email bomb)

DoS Attacks

- Goal of DoS is not to gain unauthorized access to system or data, but to prevent intended users of a service from using it.

- A DoS attack do
  - Flood a network with traffic, thereby preventing legitimate network traffic.
  - Disrupt connections between two systems, thereby preventing access to a service.
  - Prevent a particular individual from accessing a service.
  - Disrupt service to a specific system or person.

Classification of DoS attacks

1. Bandwidth attacks
2. Logic attacks
3. Protocol attacks
4. Unintentional DoS attack

Bandwidth attacks

- Bandwidth means amount of data transferred in a second.
- Loading any website takes certain time.
- Loading consumes some amount of memory.
- Every site is given with a particular amount of bandwidth for its hosting.
- Example
    - If visitors consumes all 50 GB bandwidth then the hosting of the site can ban (disallow) this site.
    - Attacker opens 100 pages of a site and keeps on refreshing and consuming all the bandwidth, the site becomes out of service.

Logic attacks

- This kind of attack can exploit vulnerabilities in network software such as web server or TCP/IP stack.

Protocol attacks

- Protocols are rules that should be followed to send data over network.

- These kind of attacks exploit a specific feature or implementation bug of some protocol installed at the victim’s system to consume excess amounts of its resources.

Unintentional DoS attack

- A website ends up denied due to its popularity.
- Example : news story
- Regular users, potentially hundreds of thousands of people, click that link within a few hours.

Types/levels of DoS attack

- Flood attack
- Ping of death attack
- SYN attack
- Teardrop attack
- Smurf attack
- Nuke

Flood attack

- Also known as ping flood.
- Attacker sending number of ping packets using "ping" command, which result into more traffic than the victim can handle.
- Very simple to launch.
- Difficult to prevent from it.

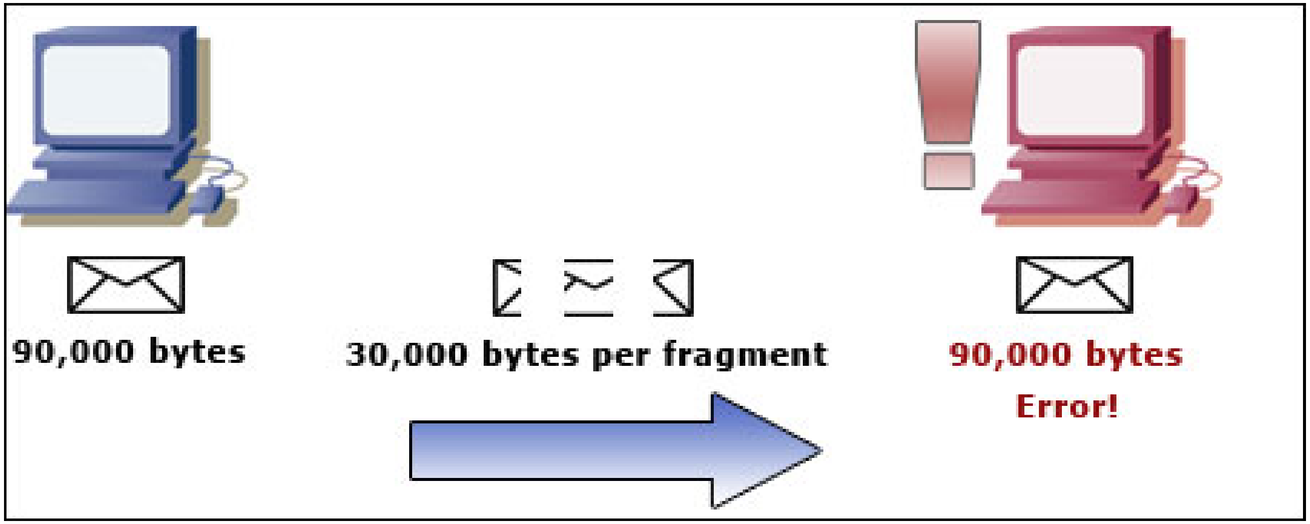
Ping of death attack

- Ping of death attack sends oversized Internet Control Message Protocol(ICMP) packets.

- Used by networked computer OS to send error messages to victim
  - E.g. requested service is not available, host or router could not be reached
- Maximum packet size allowed is of 65536 bytes.

- Upon receiving the oversized packet will crash, freeze or reboot, resulting DoS.

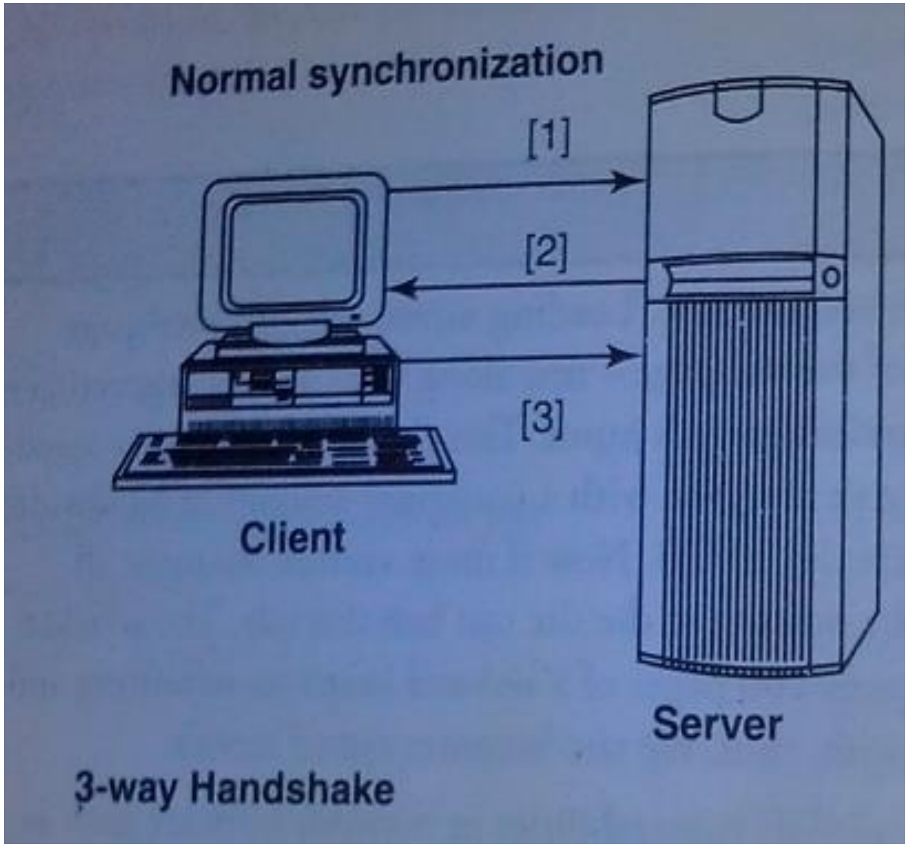
Ping of death attack



- Sending a ping of this size is against the rules of the TCP/IP protocol, but hackers can bypass this by cleverly sending the packets in fragments.
- When the fragments are assembled on the receiving computer, the overall packet size is too large. This will cause a buffer overflow and crash the device.

SYN attack

- Also termed as TCP SYN flooding.
- In Transmission Control Protocol (TCP), handshaking of network connection is done with SYN and ACK messages.



3-way handshake:

▪ Client sends synchronize(SYN) packet to web server

▪ Server sends synchronize acknowledgement (SYN-ACK)

▪Client replies with an acknowledgement packet, the connect is established.

SYN attack

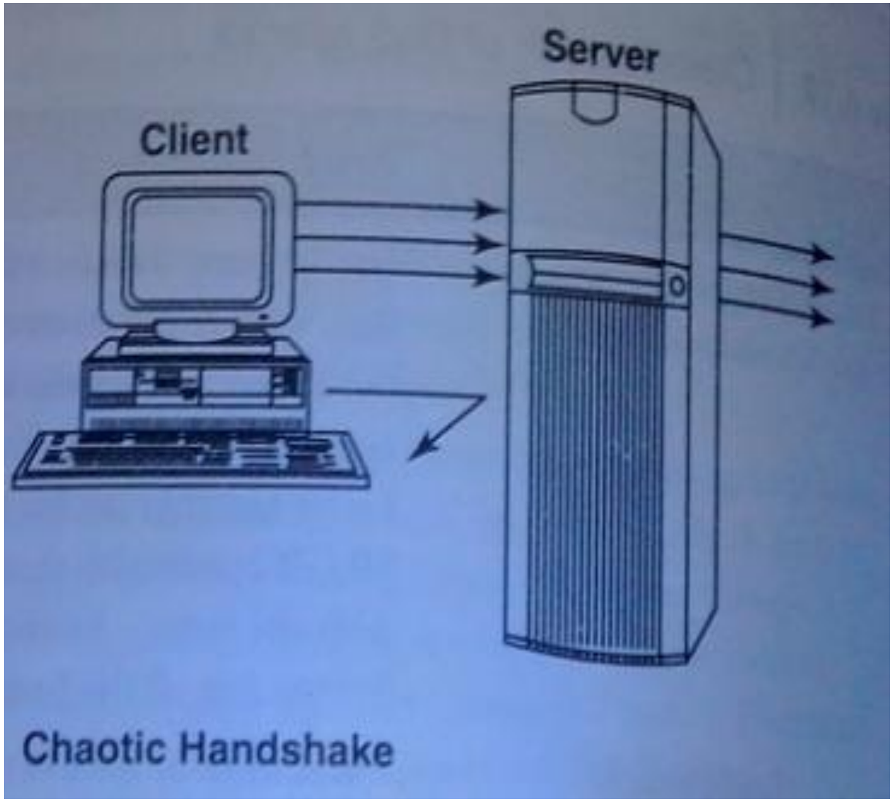
- An attacker initiates TCP connection to the server with an SYN (using legitimate or spoofed source address).

- The server replies with an SYN-ACK.

- The client then does not send back an ACK, causing the server (i.e target system) to allocate memory for pending connection and wait.

- This fills up the buffer space for SYN messages on server, preventing other system on network from communicating with the target system.

SYN attack



Chaotic Handshake

- client sends multiple SYN packets to web server – all with bad addresses

- Server sends SYN-ACK to in correct addresses.

- Legitimate user is denied access because queue is full and additional connections cannot be accepted.

Teardrop attack

- Teardrop attack is an attack where fragmented packets are forged to overlap each other when the receiving host tries to reassemble them.

- IP's packet fragmentation algorithm is used to send corrupted packets to confuse the victim and may hang the system.

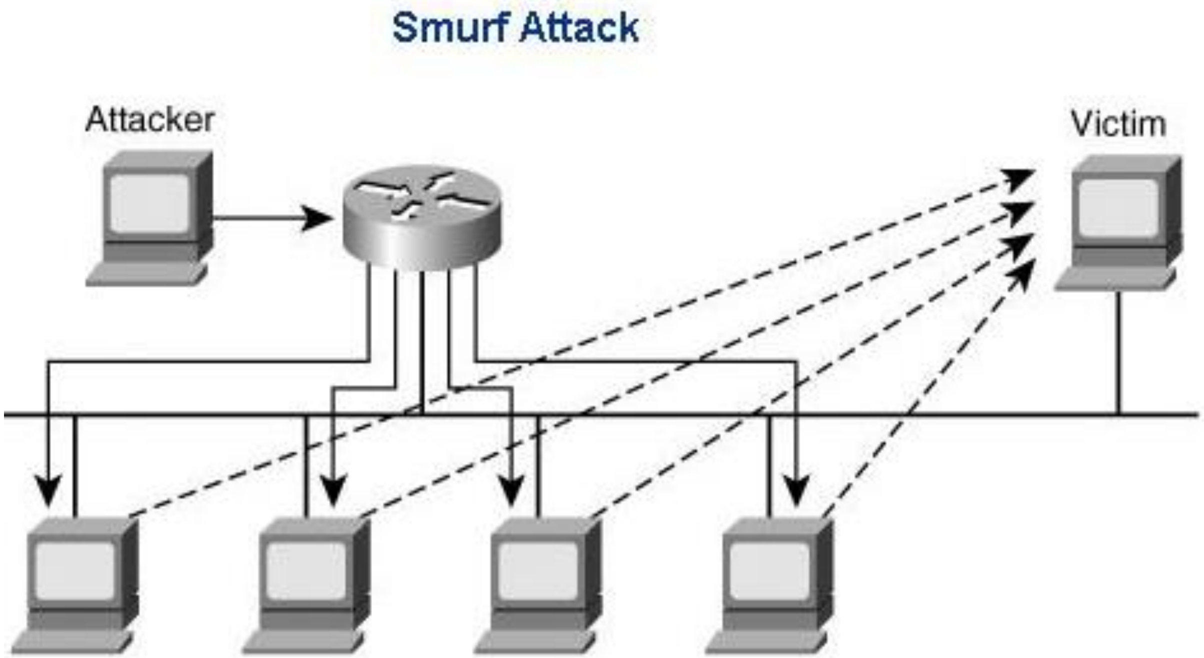
- This attack can crash various OSs due to bug in their TCP/IP fragmentation reassembly code.

- Operating systems such as Windows NT, Windows 95, and even Linux versions prior to version 2.1.63 are vulnerable to the teardrop attack.

Smurf attack

- Generating significant computer network traffic on a victim network.
- Floods a target system via spoofed broadcast ping messages.
- Attacker sends a ICMP echo request (ping) to a broadcast address.
- Every host on the network receives the ICMP echo request and send back an ICMP echo response to the target system.

Smurf attack



Nuke attack

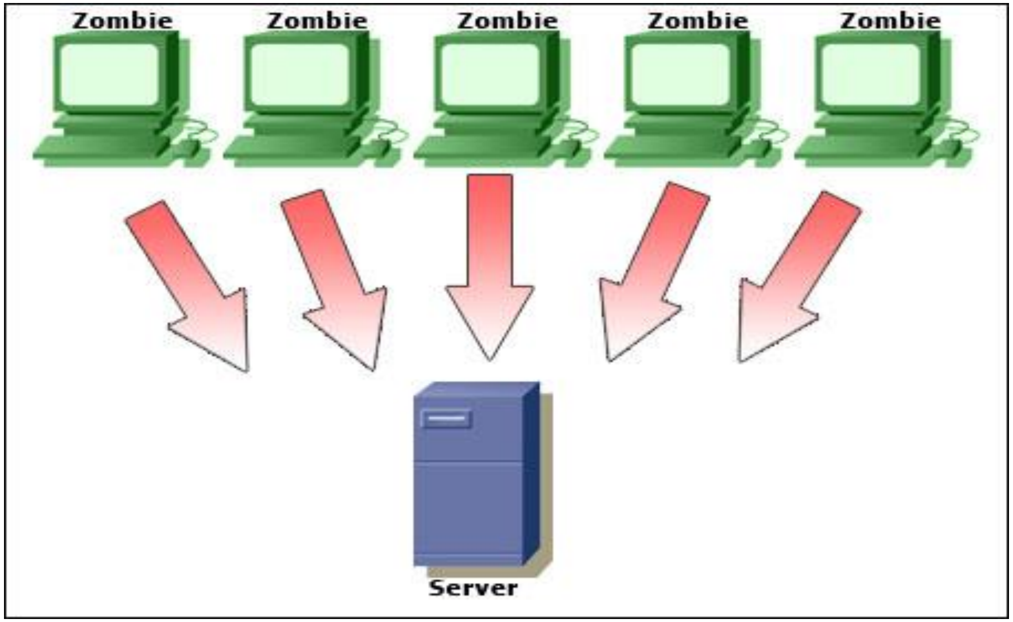
- Old DoS attack against computer networks consisting of fragmented or invalid ICMP packets sent to the target.
- It is achieved by using modified ping utility to repeatedly send corrupt data, to slow down.

Tools used to launch DoS attack

- Jolt2
- Nemesy
- Targa
- Crazy Pinger
- SomeTrouble

DDoS attack

- DDoS stands for Distributed Denial-of-Service attack.
- A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system.



DDoS attack

- Attacker
  - Use your computer to attack another computer.
  - Force your computer to send huge amount of data to a website or send spam to particular email addresses.

- The attack is “distributed” because attacker is using multiple computers to launch the DoS attack.

- Malware can carry DDoS attack mechanism.

- Example : **MyDoom** is a malware that carry DDoS attack.

Tools used to launch DDoS attack

- Trinoo
- Tribe Flood Network (TFN)
- Stacheldraht
- Shaft
- MStream

How to protect from DoS/DDoS attacks

1. Implement router filters.
2. If such filters are available for your system, install patches to guard against TCP SYN flooding.
3. Disable any unused or inessential network service. This can limit the ability of an attacker to take advantage of these services to execute a DoS attack.
4. Enable quota systems on your OS.
5. Observe system performance and baselines for regular activity. Use baseline to determine unusual levels of disk activity, CPU usage or network traffic.
6. Routinely examine your physical security with regard to your current needs.
7. Use tools to detect changes in configuration information or other files.
8. Invest in redundant and fault-tolerant network configuration.
9. Establish and maintain regular backup schedules and password policies.

Tools for detecting DoS/DDoS attacks

- Zombie Zapper
- Remote Instruction Detector (RID)
- Security Auditor’s Research Assistant (SARA)
- Find_DDoS
- DDoSPing

Difference between DoS and DDoS attack

DoS attack	DDoS attack
In a DoS attack, one computer and one internet connection is used to flood a server with packets, with the aim of overloading the targeted server’s bandwidth and resources.	A DDoS attack, uses many devices and multiple Internet connections, often distributed globally into what is referred to as a botnet.

PDoS attack

- PDoS stands for Permanent Denial-of-Service attack.

- A PDoS attack damages a system so badly that it requires replacement or reinstallation of hardware.

- It is pure hardware sabotage.

SQL injection

- Also known as SQL insertion attack.
- SQL is a database computer language designed for managing data in RDBMS.
- SQL injection is a code injection technique that exploits a security vulnerability occurring in database.
- Attack target the SQL server – i.e database servers use to store confidential data.

SQL injection

- The objective behind SQL injection attack is
  - To obtain information while accessing a database table that may contain confidential data.

- During SQL injection attack, malicious code is inserted into a web form field or website's code to make a system execute command shell or other arbitrary commands.

- Just as a legitimate user enters queries and additions to the SQL database via a web form, the attacker can insert commands to the SQL server through the same web form field.

SQL injection

- Web pages take parameters from web user and make SQL query to the database.

- For example:
  - When a user logs in with username and password, an SQL query is sent to the database to check if a user has valid name and password.
  - With SQL injection, it is possible for an attacker to send username and password field that will change the SQL query.

Steps for SQL injection attack

1. Attacker looks for the web pages that allow submitting data, i.e login page, search page, feedback etc. Also looks for webpage that display HTML commands such as POST or GET by checking site’s source code.

2. To check source code of any website, right click on web page and click “view source”.

   attacker checks source code and looks for “FORM” tag to find vulnerability.

   ```
   <FORM action=search.asp method=post>
        <input type=hidden name=A value=C>
   </FORM>
   ```

3. Attacker inputs a single quote under the text box provided on the web page to accept the username and password. This checks whether user-input variable is sanitized or interpreted literally by server. If response is an error message such as “a” = “a” then website found to be vulnerable to an SQL injection attack.

4. Attacker use SQL commands such as SELECT statement to retrieve data from database or INSERT statement to add information to the database.

- Example of variable field text attacker uses on web page to test SQL vulnerabilities

Blah’ or 1=1- -
Login: blah’ or 1=1- -
Password:: blah’ or 1=1- -
http://search/index.asp?id=blah’ or 1=1- -

Double dashes near the end of the command tell SQL to ignore the rest of the command as a comment.

Blind SQL injection

- It is used when a web application is vulnerable to an SQL injection but the result of the injection are not visible to the attacker.

Using SQL injection

- Attackers can
  - Obtain some basic information if the purpose of the attack is reconnaissance
    - To get a directory listing
    - To ping an IP address
  - May gain access to the database by obtaining username and passwords.
  - Add new data to the database
    - Execute INSERT command
  - Modify data currently in the database.
    - Execute UPDATE command

- **mySQLenum**
  - It is a command line automatic blind SQL injection tool for web application that uses MYSQL server as its back-end.
  - The main objective is to provide an easy-to-use command line interface.

Tools used for SQL server penetration

- Automated tools are used
  - To find database vulnerabilities
  - To protect the database applications

Tools	Description
AppDetectivePro	Network-based, discovery and vulnerability assessment scanner. It examines, reports and fixes security holes and misconfigurations. It identify user rights and privilege levels based on security methodology.
DbProtect	It enables organizations with complex, heterogeneous environments to optimize database security and manage risk. It integrates database asset management, vulnerability management, audit and threat management, policy management.

Tools used for SQL server penetration

Tools	Description
Database Scanner	It is an integrated part of Internet Security Systems' (ISS) Dynamic Threat Protection Platform that assess online risks by identifying security vulnerabilities in database applications. It quickly scan and generate reports with all information needed to correctly configure and secure database.
SQLPoke	It is an NT-based tool that locates Microsoft SQL (MSSQL) server and tries to connect with default System Administrator (SA) account. A list of commands are executed.
NGSSQLCrack	It can guard against weak passwords. This is a password cracking utility to identify user accounts with weak passwords.
MSSQLFP	Stands for Microsoft SQL Server Fingerprint. It is used to identifies SQL version and vulnerable versions.

How to prevent SQL injection attack

- SQL injection attacks occur due to poor website administration and coding.

- Steps to prevent SQL injection
  1. Input validation
  2. Modify error reports
  3. Other preventions

How to prevent SQL injection attack

1. Input Validation
   - User inputs to be checked and cleaned any characters or string that could be used maliciously. Eg. ; , -- , select, insert can be used to perform SQL injection attack.
   - Numeric values should be checked.
   - Keep all text boxes and form fields as short as possible to limit the length of user input.

How to prevent SQL injection attack

2. Modify error reports
   - SQL errors should not be displayed to outside users and to avoid this, developer should handle error reports.
   - These errors display full query pointing to the syntax error and attacker can use it for further attack.

How to prevent SQL injection attack

3. Other preventions

- Default system account for SQL server 2000 should never be used.
- Isolate database server and web server. Both should reside on different machines.
- Most often attacker make use of store procedures such as xp_cmdshell and xp_grantlogin in SQL injection attack. So extended store procedures are not used.

Buffer Overflow

- Buffer is a contiguous allocated chunk of memory such as an array or pointer in C.

- Buffer overflow or buffer overrun, is an anomaly where a process stores data in a buffer outside the memory.

- This may result in
  - erratic program behavior
  - memory access errors
  - incorrect results
  - program termination
  - breach of system security

Buffer overflow

- Buffer overflow occurs when a process or program tries to store more data in a buffer (temporary data storage area) than it was intended to hold and result is corrupting or overwriting the valid data held in them.

- Bounds checking can prevent buffer overflows.

- In C and C++, no automatic bounds checking on buffer.
- Example

```
int main()
{           int buffer[10];
            buffer[20]=10;
}
```

This is successfully compile but result is an unexpected behaviour.

Types of buffer overflow

1. Stack-Based Buffer Overflow
2. Heap Buffer Overflow

Stack-Based Buffer Overflow

- Occur when a program writes to a memory address on the program's call stack outside the intended data structure – fixed length buffer.

- Characteristics of stack-based programming
  1. "Stack" is a memory space in which automatic variables are allocated.

  2. Function parameters are allocated on the stack and are not automatically initialized by the system, so they have garbage until they are initialized.

  3. Once a function has completed its cycle, reference to the variable in the stack is removed. (i.e if function is called multiple times, its local variables and parameters are recreated and destroyed each time the function is called and exited.)

Stack-Based Buffer Overflow

- The attacker exploit stack-based buffer overflows to manipulate program in various ways by overwriting

1. A local variable that is near the buffer in memory on the stack to change the behaviour of program that may benefit the attacker.

2. Return address in a stack frame. Once the function returns, execution will resume at the return address as specified by the attacker, usually a user input-filled buffer.

3. A function pointer, or exception handler, which is subsequently executed.

Stack-based buffer overflow

- Factors to overcome the exploits are

1. Null bytes in addresses
2. Variability in the location of shell code
3. Differences between environment

Shell code is a small piece of code used in exploitation of software vulnerability.

Heap Buffer Overflow

- Occurs in the heap data area.

- Overflow occurs when an application copies more data into a buffer than the buffer was designed to contain.

- Vulnerable to exploitation if it copies data to buffer without first verifying that source will fit into destination.

- Characteristics of stack-based and heap-based programming:
  1. “Heap” is a “free store” that is memory space, when dynamic objects are allocated.
  2. The heap is the memory space dynamically allocated new(), malloc(), and calloc() functions.
  3. Dynamically created variables (i.e declared variables) are created on heap before execution and stored in memory until the life cycle of object has completed.

- Exploitation is performed
  - By corrupting data to override internal structures such as linked list pointers.
  - Pointer exchange to override program function

How to minimize Buffer Overflow?

1. Assessment of secure code manually
2. Disable stack execution
3. Compiler tools
4. Dynamic run-time checks
5. Tools are used to detect/ protect buffer overflow

Tools used to protect buffer overflow

1. StackGuard
2. ProPolice
3. LibSafe