RV College of Engineering ®

Go, change the world

22EM106-Introduction to Cyber Security

UNIT- II

Chapter-2:Cyber Offenses How Criminals Plan Them

Text Book:

Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd, 1st Edition 2011,Reprint 2022, ISBN:978-81-265-2179-1.

Unit - II Syllabus

Unit – II	8 Hrs
Cyber Offenses How Criminals Plan Them: Introduction, how criminals plan the attacks, Social Engineering, Cyber Stalking, Cybercaafe & cybercrimes, Botnets: The fuel for cybercrime, Attack Vector. **Attacker Techniques and Motivations:** How Hackers Cover Their Tracks (Anti-forensics), How and Why Attackers Use Proxies, Tunnelling Techniques, Fraud Techniques.	

Learning outcomes

- Understand different types of cyberattacks
- Get an overview of the steps involved in planning cybercrime
- Understand tools used for gathering information about the target.

Introduction

- Technology is a double-edged sword
- Target of offense and false sense of anonymity
- Misuse of information
- Agencies collect information about the individuals
- Cyber criminals use WWW and internet for all illegal activities
- Lack of awareness and about cybercrime and cyber laws.
- People who commit cybercrimes are known as **crackers.**

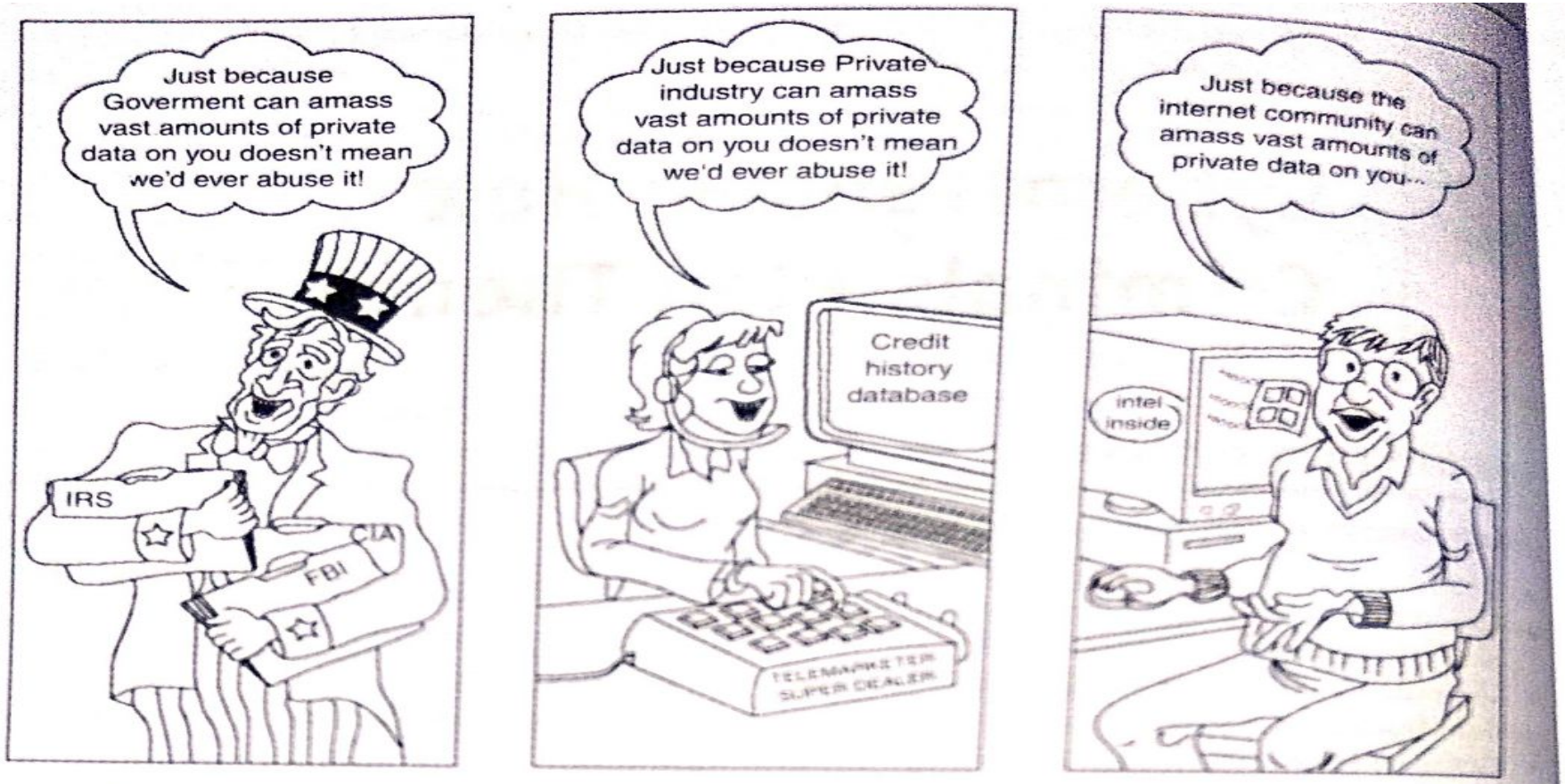
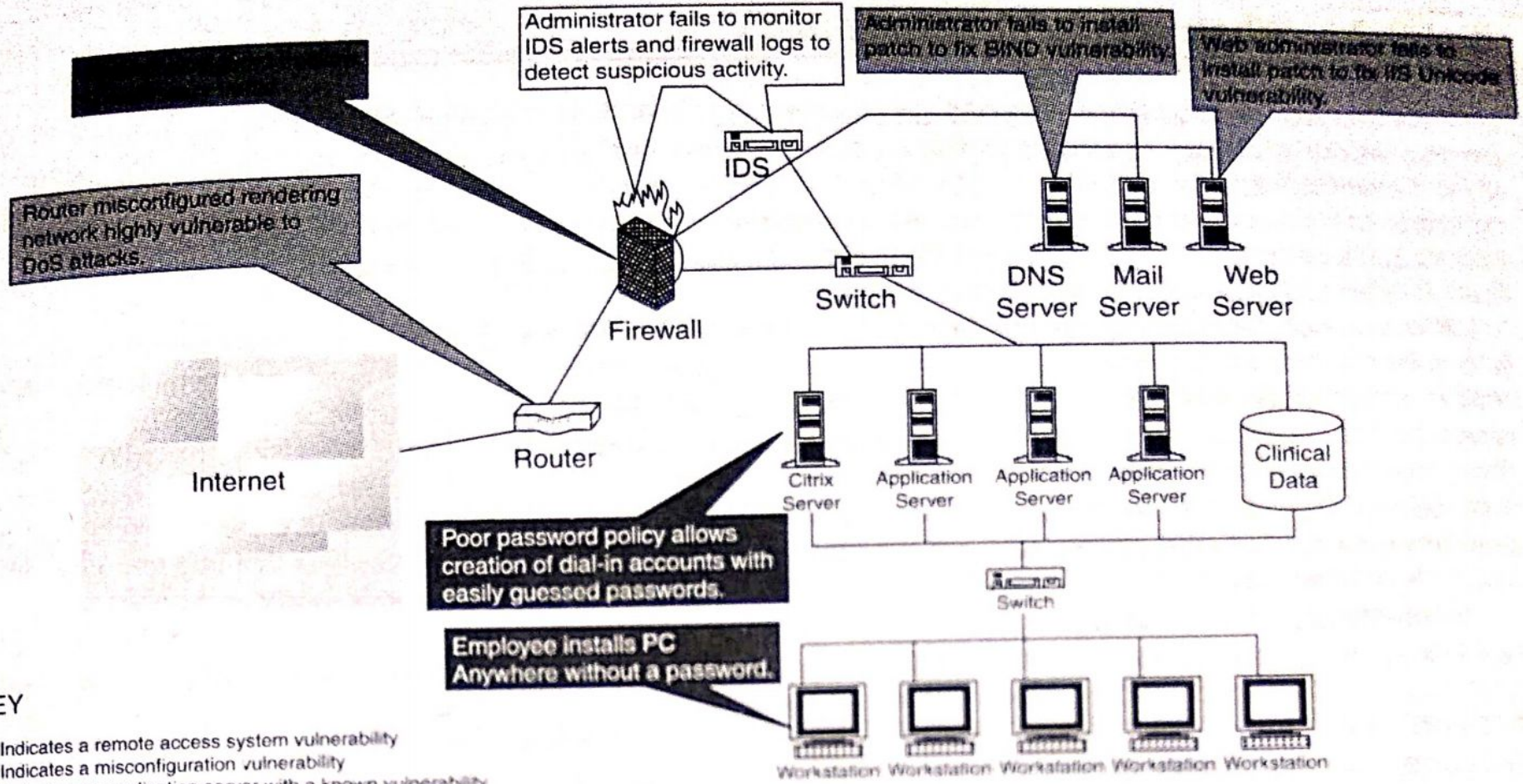


Figure 2.1 | We all vouche for keeping your personal information secret!
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Fig. 29.14), Wiley India.

- An attacker would look to exploit the vulnerabilities in the network.
- **Categories of vulnerabilities**

1. Inadequate border protection (border as in the sense of network periphery);
2. remote access servers (RASs) with weak access controls;
3. application servers with well-known exploits;
4. misconfigured systems and systems with default configurations.


Administrator fails to monitor IDS alerts and firewall logs to detect suspicious activity.
Administrator fails to install patch to fix BIND vulnerability.
Web administrator fails to install patch to fix IIS Unicode vulnerability.
Router misconfigured rendering network highly vulnerable to DoS attacks.
IDS
Firewall
Switch
DNS Server
Mail Server
Web Server
Internet
Router
Citrix Server
Application Server
Application Server
Application Server
Clinical Data
Poor password policy allows creation of dial-in accounts with easily guessed passwords.
Switch
Employee installs PC Anywhere without a password.
Workstation
Workstation
Workstation
Workstation
Workstation
KEY
Indicates a remote access system vulnerability
Indicates a misconfiguration vulnerability
Indicates an application server with a known vulnerability
Indicates a vulnerability resulting from inadequate monitoring of security systems

Hackers and crackers

Hackers:

- Person with strong interest in computers and enjoys learning and experimenting
- Very talented and smart people

Crackers:

- Person who breaks into computer
- Crimes include vandalisms, theft and snooping in unauthorized areas

Categories of cybercrime

Cybercrime can be categorized based on

- The target of the crime
- Whether the crime occurs as a single event or as a series of events

1. Crimes targeted at individuals
2. Crimes targeted at property
3. Crimes targeted at organizations
4. Single event of cybercrime
5. Series of events

1. Crimes targeted at individuals

- Human weakness
- Financial frauds
- Child pornography
- Copy right violations
- Harassment

2. Crimes targeted at property

- Stealing devices
- Transmitting harmful programs to destroy the devices

3. Crimes targeted at organizations

- Cyberterrorism
- Attackers (individual / group)
- Usage of computer tools and usage

4. Single event of cybercrime

- It is the single event from the perspective of victim
- Unknowingly opening attachments contain virus
- This is hacking or fraud

5. Series of events

- Attacker interacting with the victims repetitively
- Series of events / demanding
- Cyberstalking

How criminals plan the attacks

- Criminals use many methods and tools to locate the vulnerabilities of their target
- Target can be individual or / and organizations
- Active attack and passive attack
- Inside attack and outside attack

Inside attack: originating or attempted **within the security perimeter** of an organization.

- Attempted by insider
- Gains access to **more resources** than expected

Outside attack: attempted outside the security perimeter of an organization.

- Attempted through internet or remote access connection.

Phases involved in planning cybercrime

1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
3. Launching an attack (gaining and maintaining the system access).

Reconnaissance

- Is an act of reconnoitering – explore, often with the goal of finding something or somebody.
- Gain information about an enemy or potential enemy.
- Foot printing- gives an overview about the system vulnerability
- Attackers gather the information in two phases
- Passive and active attacks
- The objective- Understand the system, its networking ports and services and other aspects of the security that are needed for launching the attacks.

Reconnaissance- Passive attack

- Gathering the information about the target without his or her knowledge.
- Example: Physically watching a persons behaviour, searching and collecting details using searc engines.

Ways to accumulate the information:

- Using search engines- People search, locate information of person.
- Surfing online community groups.
- Organization's website- Provide a personnel directory about employee- Contact hours/details/mailid/phone no.
- Blogs/newsgroups/press releases- mediums to gain information about the company or employees.
- Going through job posting- Provide information regarding server/infrastructure devices a company maybe using on its network

Reconnaissance- Passive attack

- Network sniffing- To obtain useful information such as IP address range, hidden servers or networks, available services on the system or network.
- Attacker watches the flow of data to see what time certain transactions take place and where the traffic is going

Passive attacks

information with the help [illegible] employees (see Table 2.1):

1. Google or Yahoo search: People search to locate information about employees (see Table 2.1).
2. Surfing online community groups like Orkut/Facebook will prove useful to gain the information about an individual.
3. Organization's website may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc. These can be used in a social engineering attack to reach the target (see Section 2.3).
4. Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.
5. Going through the job postings in particular job profiles for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on it network.

Reconnaissance- Passive attack

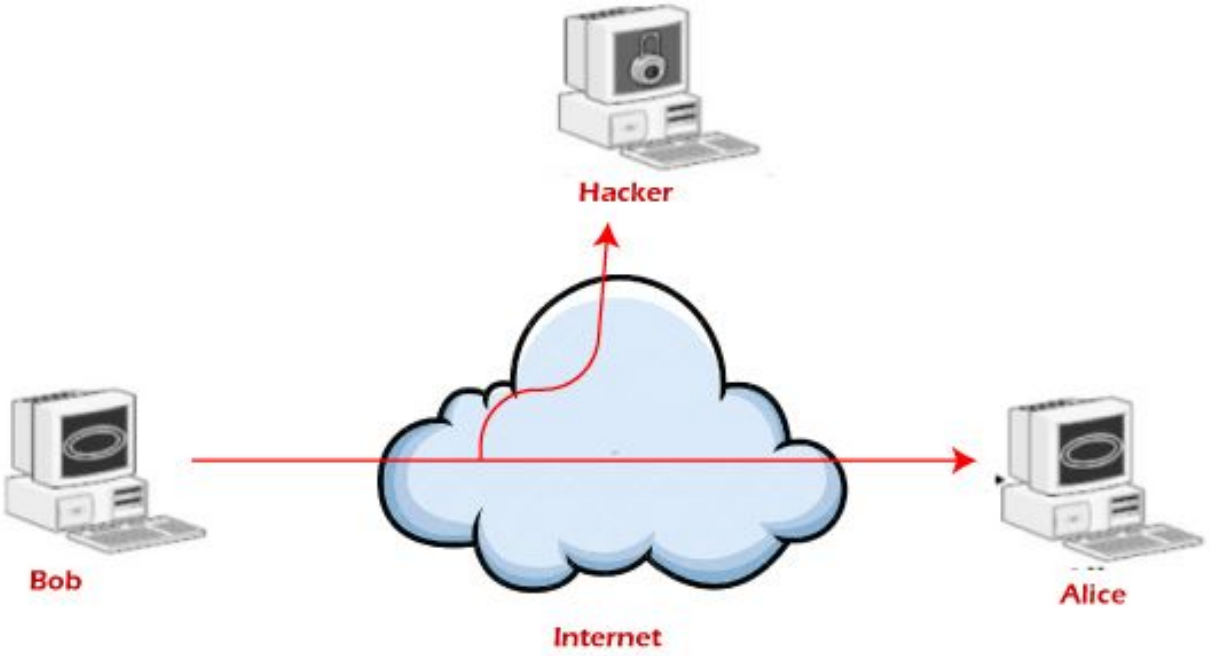
Tools used to perform passive attacks

- Google Earth
- Internet Archive
- Professional community
- People search
- Domain name confirmation
- WHOIS
- NsLookup
- Traceroute
- VisualRoute trace
- eMailTrackerPro
- HTTrack
- Website Watcher
- Competitive Intelligence

Reconnaissance- Active attack

- Probing the network to discover the individual hosts to confirm the information(IP addrersses, OS type, version, services) gathered during the passive attacks.
- It involves the risk of detection and raise a suspicion.
- Also known as “Rattling the doorknobs”.

Passive Attacks (Traffic analysis)



Active attacks

- It involves probing the network to discover individual hosts to confirm the information gathered in the passive attack phase
- **Risk of detection** and is also called rattling the doorknobs or active reconnaissance
- The attacker efforts to change or modify the content of messages.
- Active Attack is danger for **Integrity as well as availability**.
- Due to active attack system is always damaged and System resources can be changed.
- The most important thing is that, In active attack, Victim gets informed about the attack.

Reconnaissance- Active attack

Tools used to perform active attacks

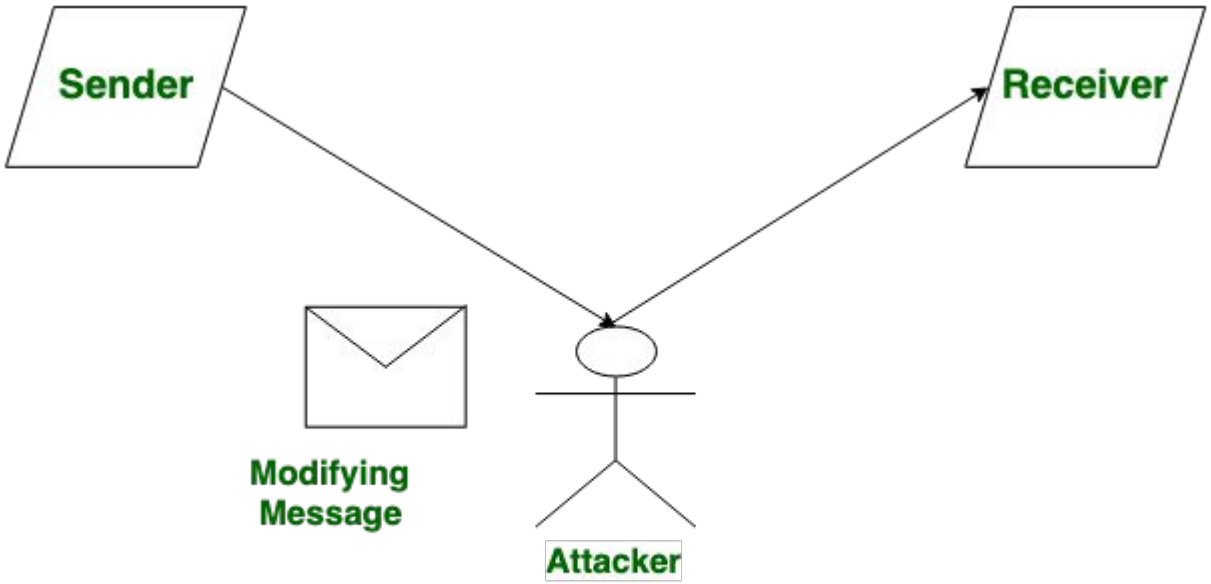
- Arphound
- Arping
- Bing
- DNS tracker
- Hmap
- Hping
- Dsniff
- FindSMB
- Fping
- Httpping
- Hunt
- Mailsnarf
- NBTScan
- Nessus
- Netcat
- Ping
- Nmap
- ScanSSH
- TCPdump
- TCPreplay

Tools used during active attack

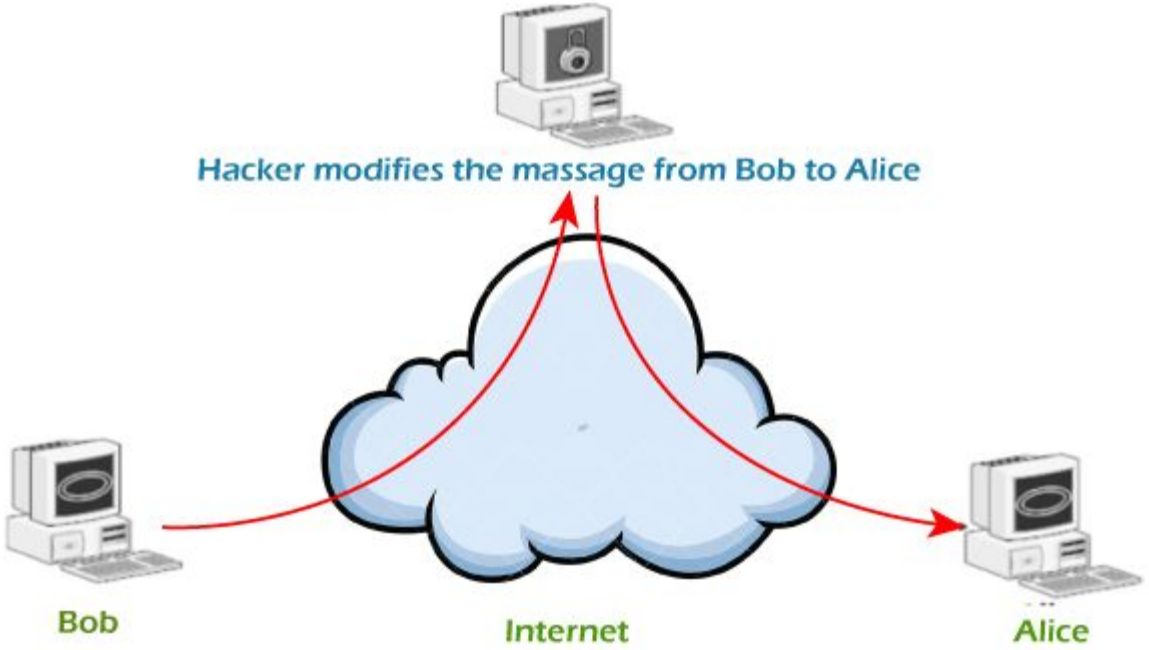
Name of the tool	Brief Description
Arp hound	listens to all traffic on an Ethernet network interface; reports Ip conflict, Ip changes, various ARP spoofing and packets not using expected gateway
Arping	broadcasts ARP Packets and receives
Bing	This is used for Bandwidth Ping. It is point-to-point bandwidth measurement tool based in ping
Bugtrack	This is a database of known vulnerabilities and exploits providing a large quantity of technical information and resources
Dig	perform detailed queries about DNS records and zones, extracting configuration and administrative information about network or domain.
DNStracer	determine the data source for given DNS server and follow the chain of DNS servers back to authoritative sources.
Dsniff	network auditing tool to capture username, password and authentication information
Filesnarf	network auditing toll to capture to capture file transfers and file sharing traffic on a local subnet.
Find SMB	find and describe server message block servers on the local network

Tools used during active attack

Name of the tool	Brief Description
FPing	similar to ping used to perform parallel network discovery.
Fragroute	This intercepts, modifies and rewrites egress traffic destined for a specified host, implementing several IDS evasion techniques
Fragtest	tests IP fragment reassembly behaviour of TCP stack on target.It intercepts, modifies and rewrites egress traffic destined for a specified host, implementing most of the attacks.
Hackbot	host exploration tool, simple vulnerability scanner and banner logger.
Hmap	obtain detailed fingerprinting of web servers to identify vendor, version, patch level, including modules and much more.
Hping	TCP/IP pocket assembler and analyzer.
Httping	similar to ping, but for HTTP requests
Nmap	port scanner, OS fingerprint, service/version identifier.rapidly scans large networks
SMTPscan	determine the type and version of remote SMTP mail server based on active probing and analyzing error codes of the target SMTP server.



Active Attack



Active Attacks (Modifications of messages)

Difference between Active attack and Passive attack

Based on	Active attack	Passive attack
Definition	In active attacks, the attacker intercepts the connection and efforts to **modify the message's content.**	In passive attacks, the attacker **observes the messages, then copy and save** them and can use it for malicious purposes.
Modification	In an active attack, the attacker **modifies the actual information.**	In passive attacks, **information remains unchanged**.
Victim	In active attacks, the **victim gets notified** about the attack.	Unlike active attacks, in passive attacks, **victims do not get informed** about the attack.
System's impact	The damage done with active attacks can be **harmful to the system and its resources**.	The passive attacks **do not harm the system**.
System resources	In active attacks, the **system resources can be changed.**	In passive attacks, the **system resources remain unchanged.**
Dangerous for	They are dangerous for the integrity and availability of the message.	They can be dangerous for confidentiality of the message.
Emphasis on	In active attacks, **attention is on detection.**	In active attacks, **attention is on prevention**.
Types	Active attacks involve Masquerade, Modification of message, Repudiation, Replay, and Denial of service.	It involves traffic analysis, the release of a message.
Prevention	Active attacks are **tough to restrict from entering systems or networks**.	Unlike active attacks, **passive attacks are easy to prohibit.**

Scanning: key step to examine intelligently while gathering the information.

Objectives of scanning are

1. **Port scanning:** Identify open/close ports and services. Refer to Box 2.5.
2. **Network scanning:** Understand IP Addresses and related information about the computer netwo systems.
3. **Vulnerability scanning:** Understand the existing weaknesses in the system.

Scrutinizing phase: called enumeration in the hacking world.

The main objective is to identify

1. The valid user accounts or groups;
2. network resources and/or shared resources;
3. OS and different applications that are running on the OS.

After scanning and enumeration, the attack is launched using the following steps.

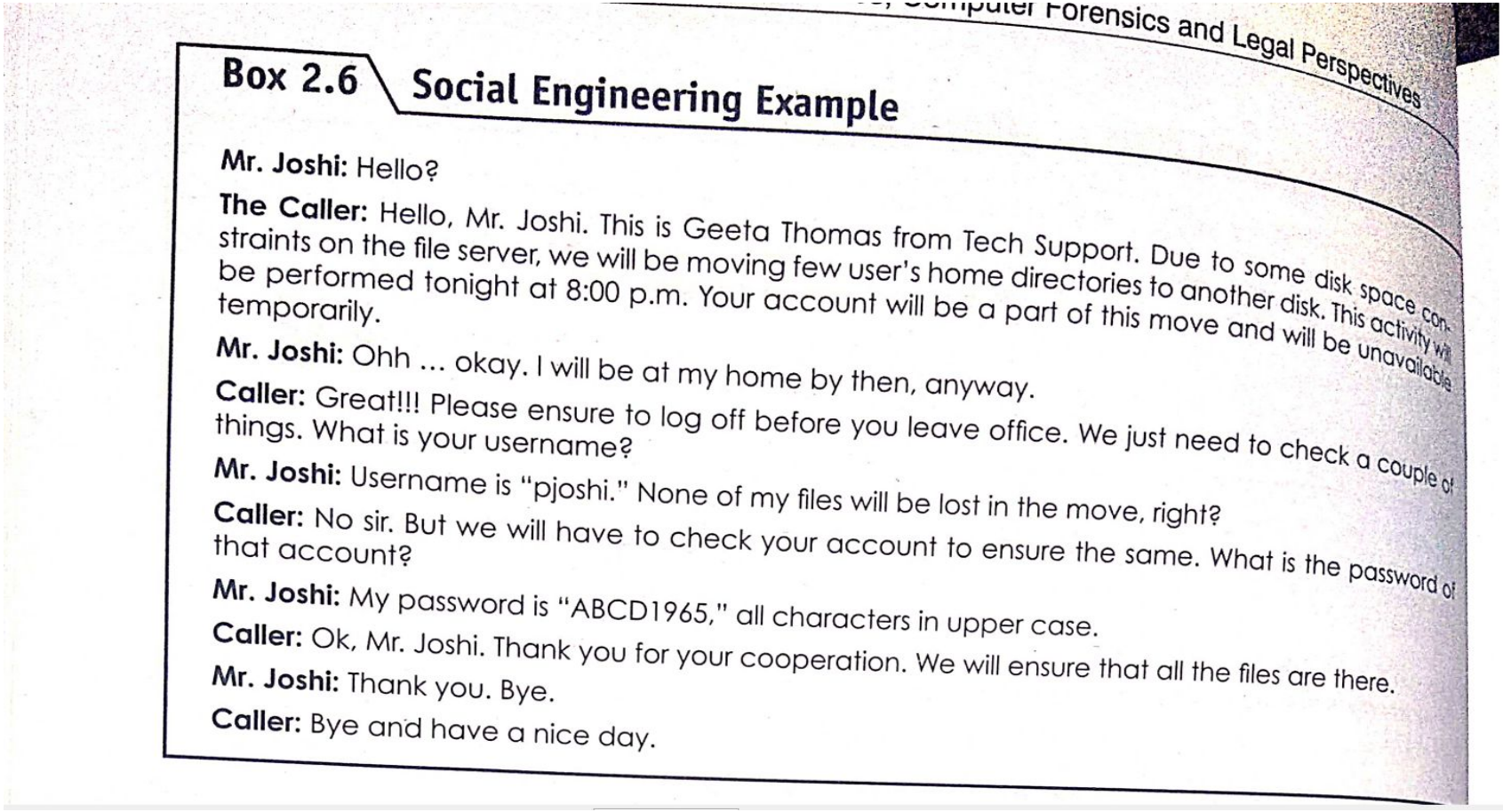
1. Crack the password (we will address it in Chapter 4);
2. exploit the privileges;
3. execute the malicious commands/applications;
4. hide the files (if required);
5. cover the tracks – delete the access logs, so that there is no trail illicit activity.

Social Engineering

- Technique to influence or persuasion to deceive
- It is the tactic of **manipulating, influencing, or deceiving a victim in order to gain control over a computer system**, or to steal personal and financial information.
- Uses telecommunication / internet against the security policy of the organization

Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders. It is an art of exploiting the trust of people, which is not doubted while speaking in a normal manner. The goal of a social engineer is to fool someone into providing valuable information or access to that information. Social engineer studies the human behavior so that

Example



Computer Forensics and Legal Perspectives

Box 2.6 Social Engineering Example

Mr. Joshi: Hello?

The Caller: Hello, Mr. Joshi. This is Geeta Thomas from Tech Support. Due to some disk space constraints on the file server, we will be moving few user's home directories to another disk. This activity will be performed tonight at 8:00 p.m. Your account will be a part of this move and will be unavailable temporarily.

Mr. Joshi: Ohh ... okay. I will be at my home by then, anyway.

Caller: Great!!! Please ensure to log off before you leave office. We just need to check a couple of things. What is your username?

Mr. Joshi: Username is "pjoshi." None of my files will be lost in the move, right?

Caller: No sir. But we will have to check your account to ensure the same. What is the password of that account?

Mr. Joshi: My password is "ABCD1965," all characters in upper case.

Caller: Ok, Mr. Joshi. Thank you for your cooperation. We will ensure that all the files are there.

Mr. Joshi: Thank you. Bye.

Caller: Bye and have a nice day.

Social Engineering – Example

An example of social engineering called phishing:

Scenario:

- Sophia works in a medium-sized company that handles sensitive financial data. She receives an email from what appears to be the company's IT department, stating that there has been a security breach and all employees need to reset their passwords immediately to prevent unauthorized access.

Outcome:

- Sophia, concerned about the security of company data, clicks on the link provided in the email and enters her username and password to reset her password, believing she is following protocol to protect sensitive information.

Social Engineering – Example

Consequences:

- The email was a phishing attempt by a cybercriminal. By entering her credentials on the fake website, she has unwittingly provided her username and password to the attacker. The attacker can now access sensitive company data, potentially leading to financial loss or reputational damage for the company.

Social Engineering – Example

Social Engineering Tactics:

- **Deceptive Email**: The email appears to come from a trusted source (the IT department), creating a sense of urgency and importance.
- **Urgency**: The email emphasizes the urgency of the situation, stating that failure to reset passwords promptly could result in further security breaches.
- **Impersonation**: The sender impersonates the IT department, exploiting trust in the company's internal communications.
- **Fear**: The email instills fear by mentioning a security breach, compelling recipients to act quickly without thoroughly verifying the authenticity of the request.

Social Engineering – Example

Mitigation:

Sophia could have avoided falling victim to this social engineering attack by following these steps:

- **Verification**: Verify the authenticity of the email by contacting the IT department through official channels (phone, in-person, or company portal) to confirm the request before taking any action.
- **Scrutiny**: Examine the email for signs of phishing, such as misspellings, generic greetings, or suspicious links or attachments.
- **Training**: Participate in cybersecurity awareness training provided by the company to recognize and respond appropriately to phishing attempts.

Social Engineering – Classification

Human based Social Engineering

Person to person interaction to get the required/desired information. Following are the ways:

- **Impersonation**: an attacker pretends to be someone else, often a trusted individual or authority figure, to deceive a target into divulging sensitive information, performing actions, or providing access to restricted resources.
- **Posing as an important user**: Pretends as a CEO of a company.
- **Using third person**: Attacker pretends to have permission from an authorized source to use system
- **Calling technical support**: Helpdesk and technical personnel are trained to help which make them good prey.
- **Shoulder Surfing**: Way to gather information – Username and password by watching over person's shoulder when he logs in.
- **Dumpster diving-** Looking in the trash for information written on pieces or computer printouts.

Social Engineering – Example

Social Engineering Tactics:

- **Deceptive Email**: The email appears to come from a trusted source (the IT department), creating a sense of urgency and importance.
- **Urgency**: The email emphasizes the urgency of the situation, stating that failure to reset passwords promptly could result in further security breaches.
- **Impersonation**: The sender impersonates the IT department, exploiting trust in the company's internal communications.
- **Fear**: The email instills fear by mentioning a security breach, compelling recipients to act quickly without thoroughly verifying the authenticity of the request.

Social Engineering – Example

Mitigation:

Sophia could have avoided falling victim to this social engineering attack by following these steps:

- **Verification**: Verify the authenticity of the email by contacting the IT department through official channels (phone, in-person, or company portal) to confirm the request before taking any action.
- **Scrutiny**: Examine the email for signs of phishing, such as misspellings, generic greetings, or suspicious links or attachments.
- **Training**: Participate in cybersecurity awareness training provided by the company to recognize and respond appropriately to phishing attempts.

Classification of social Engineering

1. **Human based social engineering:**

- Person to person interaction
- Ex. Calling to get information

2. **Computer based social engineering:**

- Getting required information by using computer software / internet
- Ex. Fake E-mail

1. Human based social engineering:

- **Impersonating an employee or valid user**
- Posing as an important user
- Using a third person
- Calling technical support
- Shoulder suffering
- Dumpster driving

Shoulder suffering

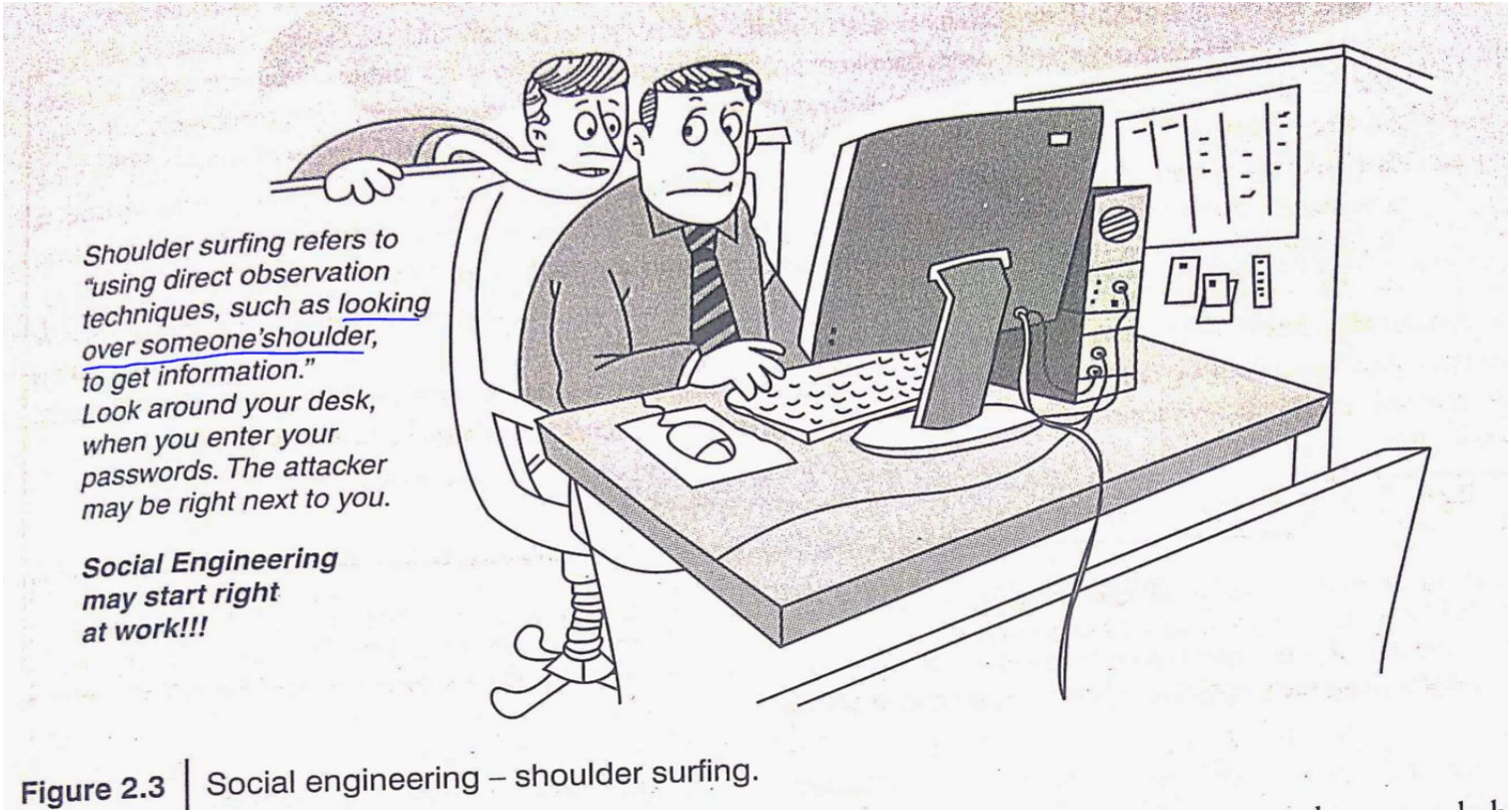


Figure 2.3 | Social engineering – shoulder surfing.

Dumpster driving: looking or getting information

- Trash
- Pieces of paper or computer printouts
- Garbage
- E-waste etc..

2. Computer based social engineering:

- Fake E-mails
- E-mail attachments
- Pop-up windows

Fake E-mails:

Box 2.7 Fake E-Mails

Free websites are available to send fake E-Mails. From Fig. 2.4, one can notice that "To" in the text box is a blank space. Hence, anyone can fill any E-Mail address with the intention of fooling the receiver of the E-Mail. In such a case when the receiver will read the mail, he/she would think that the E-Mail has been received from a legitimate sender.

We will never ever send you junk E-Mail, or give your E-Mail address away to anyone. We hate Spam at least as much as you do- maybe more (and that's why this page can't be used by spammers to send bulk E-Mail or any other funny stuff).

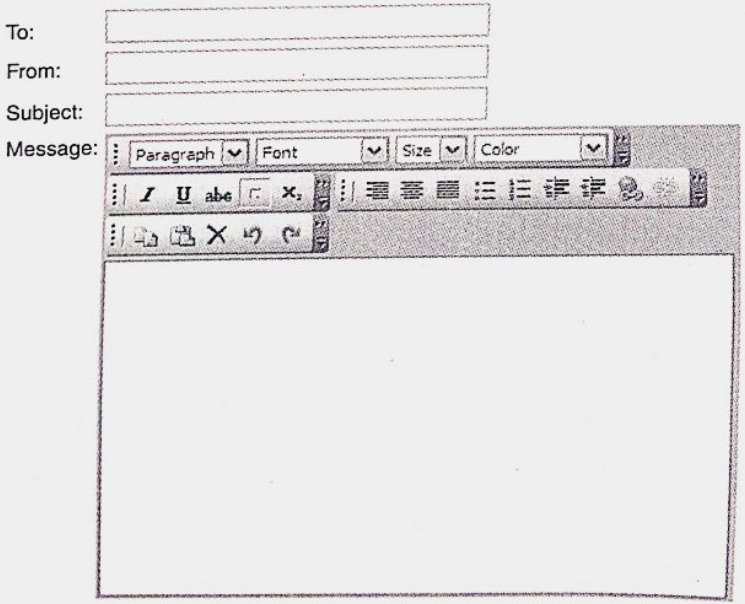


Figure 2.4 Sending fake E-Mails.
Source: http://deadfake.com/Send.aspx (2 April 2009).

E-mail attachments and Pop-up windows:

2. **E-Mail attachments:** E-Mail attachments are used to send malicious code to a victim's system, which will automatically (e.g., keylogger utility to capture passwords) get executed. Viruses, Trojans, and worms can be included cleverly into the attachments to entice a victim to open the attachment. We will address keylogger, viruses, Trojans, and worms in Chapter 4.
3. **Pop-up windows:** Pop-up windows are also used, in a similar manner to E-Mail attachments. Pop-up windows with special offers or free stuff can encourage a user to unintentionally install malicious software.

Past statistics

1. As per Microsoft Corporation recent (October 2007) research, there is an increase in the number of security attacks designed to steal personal information (PI) or the instances of tricking people to provide it through social engineering. According to an FBI survey, on average 41% of security-related losses are the direct result of employees stealing information from their companies. The average cost per internal incident was US$ 1.8 million.
2. The Federal Trade Commission (FTC) report of 2005 shows that "more than one million consumer fraud and ID theft complaints have been filed with federal, state, and local law enforcement agencies and private organizations" (2005, Consumer Fraud and Identity Theft section, para 1; we will discuss ID Theft in Chapter 5).
3. According to a 2003 survey [released on 2 April 2006 by the United States Department of Justice (Identity Theft Hits Three Percent, para 1)], "An estimated 3.6 million – or 3.1% – of American households became victims of ID theft in 2004." This means that now, more than ever, individuals are at a high risk of having their PI stolen and used by criminals for their own personal gain.

Social engineering statistics 2023

- 75% of security professionals say social engineering is the "most dangerous" threat. – CS Hub
- 2,249 social engineering incidents were reported. – Verizon.
- A hacker used social engineering attack on Twilio and gained access to the company's internal systems and the data of 125 customers. – Venturebeat

https://www.getastra.com/blog/security-audit/cyber-security-statistics/#:~:text=Social%20engineering%20statistics%202023,-75%25%20of%20security&text=2%2C249%20social'

https://firewalltimes.com/social-engineering-statistics/

Cyberstalking

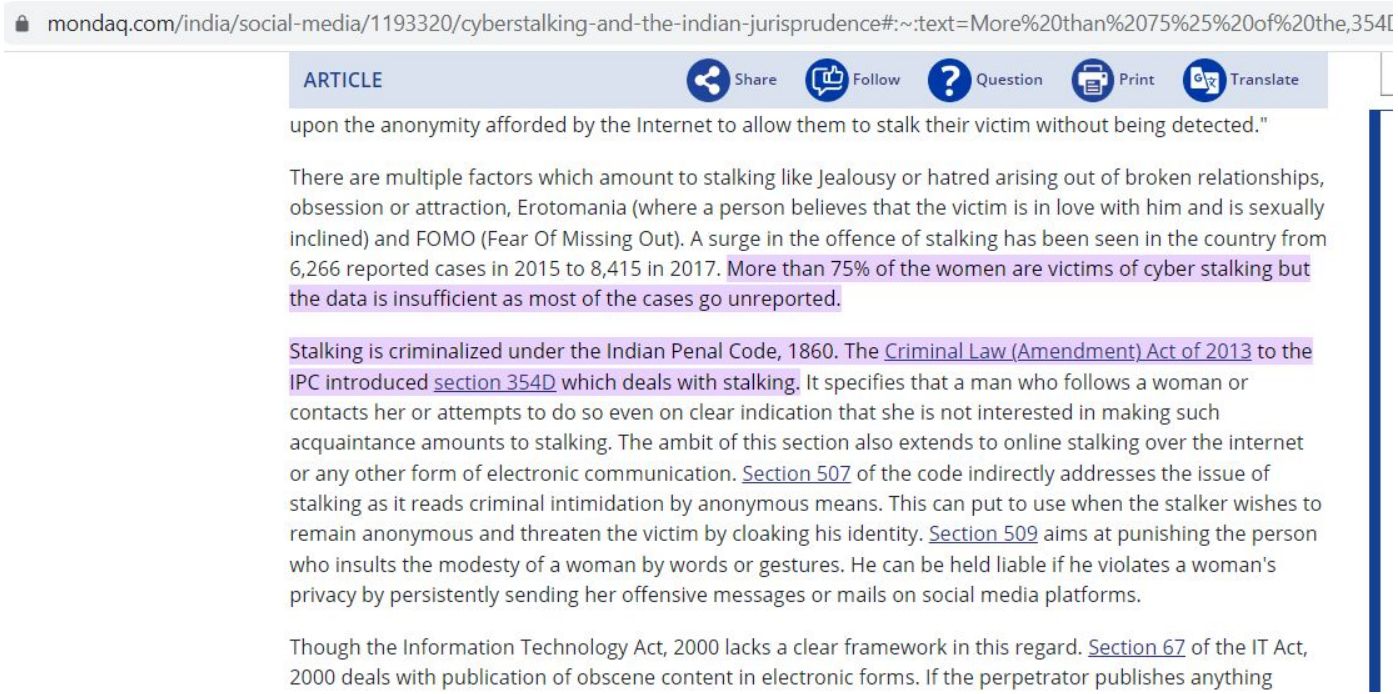
- Cyberstalkers **take advantage of the anonymity afforded by the internet to stalk or harass their victims, sometimes without being caught, punished or even detected**. The terms cyberstalking and cyberbullying are often used interchangeably.
- Trying to approach some-body or something.
- Refers to use of internet / ICT/ electronic communications devices to stalk another person
- Individual or group of individual to harass another individual, group of individual or organization.
- Behaviour includes false accusation, monitoring, transmission of threats, ID theft, damage to data or equipment, and gathering information for harassment purposes.

Types of Cyber stalkers

1. **Online stalkers:** They aim to start the interaction with the victim directly with the help of the Internet. E-Mail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone/cell phone. The stalker makes sure that the victim recognizes the attack attempted on him/her. The stalker can make use of a third party to harass the victim.
2. **Offline stalkers:** The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc. Searching on message boards/newsgroups, personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet (see Table 2.1). The victim is not aware that the Internet has been used to perpetuate an attack against them.

Cases reported on cyber stalking

The majority of cyberstalkers are men and the majority of their victims are women. Some cases also have been reported where women act as cyberstalkers and men as the victims as well as cases of same-sex cyberstalking. In many cases, the cyberstalker and the victim hold a prior relationship, and the cyberstalking begins when the victim attempts to break off the relationship, for example, ex-lover, ex-spouse, boss/subordinate, and neighbor. However, there also have been many instances of cyberstalking by strangers.



https://www.mondaq.com/india/social-media/1193320/cyberstalking-and-the-indian jurisprudence#:~:text=More%20than%2075%25%20of%20the,354D%20which%20deals%20with%20stalking.

How stalking works

[illegible] works in the following ways:

1. Personal information gathering about the victim: Name; family background; contact details such as cell phone and telephone numbers (of residence as well as office); address of residence as well as of the office; E-Mail address; date of birth, etc.
2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
3. Stalkers will almost always establish a contact with the victims through E-Mail. The letters may have the tone of loving, threatening or can be sexually explicit. The stalker may use multiple names while contacting the victim.
4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.

5. The stalker may post the victim's personal information on any website related to illicit services such as sex-workers' services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details (telephone numbers/cell phone numbers/E-Mail address) to have sexual services. The stalker will use bad and/or offensive/attractive language to invite the interested persons.
6. Whosoever comes across the information, start calling the victim on the given contact details (telephone/cell phone nos), asking for sexual services or relationships.
7. Some stalkers subscribe/register the E-Mail account of the victim to innumerable pornographic and sex sites, because of which victim will start receiving such kind of unsolicited E-Mails (refer to Chapter 5).

Real life incident of cyberstalking

Case Study

The Indian police have registered first case of cyberstalking in Delhi[5] – the brief account of the case has been mentioned here. To maintain confidentiality and privacy of the entities involved, we have changed their names.

Mrs. Joshi received almost 40 calls in 3 days mostly at odd hours from as far away as Kuwait, Cochin, Bombay, and Ahmadabad. The said calls created havoc in the personal life destroying mental peace of Mrs. Joshi who decided to register a complaint with Delhi Police.

A person was using her ID to chat over the Internet at the website www.mirc.com, mostly in the Delhi channel for four consecutive days. This person was chatting on the Internet, using her name and giving her address, talking in obscene language. The same person was also deliberately giving her telephone number to other chatters encouraging them to call Mrs. Joshi at odd hours.

This was the first time when a case of cyberstalking was registered. Cyberstalking does not have a standard definition but it can be defined to mean threatening, unwarranted behavior, or advances directed by one person toward another person using Internet and other forms of online communication channels as medium.

Cyberstalking- Case Study

Scenario:

Sarah, a college student, has recently broken up with her boyfriend, Alex, after a tumultuous relationship. Alex has difficulty accepting the breakup and begins to exhibit stalking behaviors towards Sarah.

Cyberstalking Behaviors:

- **Harassing Messages**: Alex starts sending Sarah incessant text messages, emails, and social media messages, despite her repeated requests to stop contacting her. He uses threatening language and tries to guilt-trip Sarah into reconsidering the breakup.
- **Monitoring Online Activity**: Alex creates multiple fake social media accounts to monitor Sarah's online activity. He constantly checks her posts, likes, and comments, even after she blocks him on all her accounts.

Cyberstalking- Case Study

- **Impersonation**: Alex creates a fake online profile pretending to be Sarah and starts posting derogatory comments and false information about her on social media platforms. He also sends friend requests to Sarah's friends and family members, pretending to be her, in an attempt to sabotage her relationships.
- **Doxxing**: In a malicious attempt to intimidate Sarah, Alex publicly shares her personal information, including her phone number, address, and class schedule, on online forums and social media platforms without her consent.
- **Cyberbullying**: Alex enlists the help of his friends to cyberbully Sarah online. They create memes and derogatory posts targeting Sarah and share them widely on social media, causing embarrassment and distress.

Cyberstalking- Case Study

Impact:

- Sarah experiences significant emotional distress as a result of Alex's cyberstalking behaviors. She feels anxious and paranoid, constantly worrying about being watched and harassed online. The invasion of her privacy and the spread of false information tarnish her reputation and make her feel isolated and vulnerable.

Cyberstalking- Case Study

Response and Mitigation:

- **Documenting Evidence**: Sarah keeps records of all the harassing messages, posts, and online interactions with Alex as evidence to support her case.
- **Reporting to Authorities**: Sarah reports Alex's cyberstalking behaviors to the college authorities and local law enforcement, seeking protection and legal recourse against his harassment.
- **Seeking Support**: Sarah reaches out to her friends, family, and a counselor for emotional support and guidance in dealing with the traumatic effects of cyberstalking.

Cyberstalking- Case Study

- **Adjusting Privacy Settings**: Sarah reviews and adjusts her privacy settings on social media platforms to limit access to her personal information and control who can contact or interact with her online.
- **Seeking Legal Assistance**: Sarah consults with a lawyer to explore legal options for obtaining a restraining order or pursuing criminal charges against Alex for his cyberstalking and harassment.

By taking proactive steps to protect herself, seek support, and hold her stalker accountable for his actions, Sarah can begin to reclaim her sense of safety and well-being in the face of cyberstalking.

Cybercafe and cybercrimes

- A cybercafe is **a business which allows people to pay for access to the Internet**. Another name for a cybercafe is an Internet cafe. Such places often look just like cafes or coffee shops, with the addition of computer terminals.

- Cybercrimes such as **stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes**. Cybercafes have also been used regularly for sending obscene mails to harass people.

Cybercafe and cybercrimes

- Risks with public systems:

  - Some keyloggers/spywares might be installed to capture the keystrokes/passwords and other confidential information.
  - Shoulder peeping might be possible.

Cybercafe - Observations

- Use pirated softwares.
- Antivirus softwares are not updated.
- Annual maintenance is not carried out for the machines.
- No filters to block unwanted/phishing websites.
- Cybercafe owners have less awareness about IT security and IT governance.
- Government/ISPs/State police fail to provide IT governance guidelines to cybercafe owners.

Cybercafe – Safety measures

- Always logout after use.
- Stay with the computer when using it.
- Clear history and temporary files.
- Avoid financial transactions.
- Change passwords after using public systems
- Use virtual keyboards instead of physical ones.

1. **Always logout:** While checking E-Mails or logging into chatting services such as instant messaging or using any other service that requires a username and a password, always click "logout" or "sign out" before leaving the system. Simply closing the browser window is not enough, because if somebody uses the same service after you then one can get an easy access to your account. However, do not save your login information through options that allow automatic login. Disable such options before logon.
2. **Stay with the computer:** While surfing/browsing, one should not leave the system unattended for any period of time. If one has to go out, logout and close all browser windows.
3. **Clear history and temporary files:** Internet Explorer saves pages that you have visited in the history folder and in temporary Internet files. Your passwords may also be stored in the browser if that option has been enabled on the computer that you have used. Therefore, before you begin browsing, do the following in case of the browser Internet Explorer:
   - Go to *Tools* → *Internet options* → click the *Content* tab → click *AutoComplete*. If the checkboxes for passwords are selected, deselect them. Click *OK* twice.
   - After you have finished browsing, you should clear the history and temporary Internet files folders. For this, go to *Tools* → *Internet options* again → click the *General* tab → go to *Temporary Internet Files* → click *Delete Files* and then click *Delete Cookies*.
   - Then, under history, click clear history. Wait for the process to finish before leaving the computer.
4. **Be alert:** One should have to stay alert and aware of the surroundings while using a public computer. Snooping over the shoulder is an easy way of getting your username and password.

Cybercafe – Recent trend on its usage

- **Past Growth**: In the early 2000s, cybercafes saw significant growth in India, especially in urban and semi-urban areas.
- **Decline**: Over the years, with the proliferation of affordable smartphones and increasing availability of mobile internet, the relevance of cybercafes has diminished
- **Regulatory Changes**: The Indian government has periodically introduced regulations governing cybercafes to address concerns related to cybercrimes, child safety, and access to objectionable content. These regulations have influenced the operation and viability of cybercafes across the country.
- **Transformation**: Some cybercafes have adapted to changing consumer preferences by diversifying their services, such as offering printing facilities, document scanning, gaming zones, or serving as centers for online form submissions or exam registrations.
- **Survival Challenges**: Despite the decline, cybercafes continue to exist, especially in areas with limited internet infrastructure or among demographics less familiar with digital technologies. However, many face challenges in remaining profitable amidst evolving consumer behaviors and competition from alternative internet access points.

As per survey in india:

eye-opener after going through the following observations:

1. Pirated software(s) such as OS, browser, office automation software(s) (e.g., Microsoft Office) are installed in all the computers.
2. Antivirus software is found to be not updated to the latest patch and/or antivirus signature.
3. Several cybercafes had installed the software called "Deep Freeze" for protecting the computers from prospective malware attacks. Although such intent is noble, this software happens to help cybercriminals hoodwink the investigating agencies. Deep Freeze can wipe out the details of all activities carried out on the computer when one clicks on the "restart" button.[8] Such practices present challenges to the police or crime investigators when they visit the cybercafes to pick up clues after the Interet Service Provider (ISP) points to a particular IP address from where a threat mail was probably sent or an online Phishing attack (Phishing attacks are explained in Chapter 5) was carried out, to retrieve logged files.
4. Annual maintenance contract (AMC) found to be not in a place for servicing the computers; hence, hard disks for all the computers are not formatted unless the computer is down. Not having the AMC is a risk from cybercrime perspective because a cybercriminal can install a Malicious Code on a computer and conduct criminal activities without any interruption.
5. Pornographic websites and other similar websites with indecent contents are not blocked.
6. Cybercafe owners have very less awareness about IT Security and IT Governance.
7. Government/ISPs/State Police (cyber cell wing) do not seem to provide IT Governance guidelines to cybercafe owners.
8. Cybercafe association or State Police (cyber cell wing) do not seem to conduct periodic visits to cybercafes – one of the cybercafe owners whom we interviewed expressed a view that the police will not visit a cybercafe unless criminal activity is registered by filing an First Information Report (FIR). Cybercafe owners feel that police either have a very little knowledge about the technical aspects involved in cybercrimes and/or about conceptual understanding of IT security.

5. **Avoid online financial transactions:** Ideally one should avoid online banking, shopping or other transactions that require one to provide personal, confidential and sensitive information such as credit card or bank account details. In case of urgency one has to do it; however, one should take the precaution of changing all the passwords as soon as possible. One should change the passwords using a more trusted computer, such as at home and/or in office.
6. **Change passwords:** The screenshot displayed in Fig. 2.5 by ICICI Bank about changing the bank account/transaction passwords is the best practice to be followed.[9]
7. **Virtual keyboard:** Nowadays almost every bank has provided the virtual keyboard on their website. The advantages of utilizing virtual keyboard and its functions are displayed in the screenshot shown in Fig. 2.6.[10]
8. **Security warnings:** One should take utmost care while accessing the websites of any banks/financial institution. The screenshot in Fig. 2.7 displays security warnings very clearly (marked in bold rectangle), and should be followed while accessing these financial accounts from cybercafe.

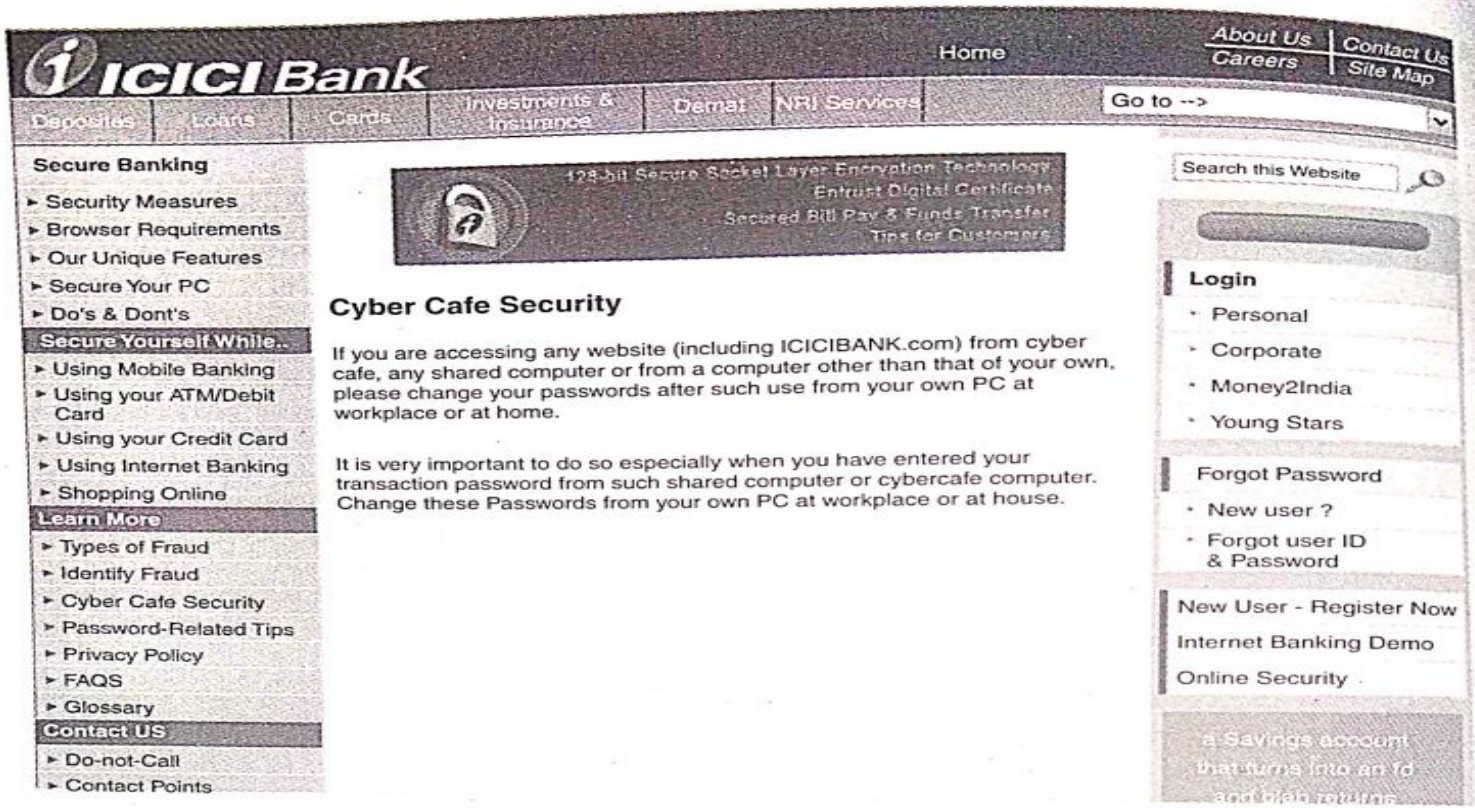
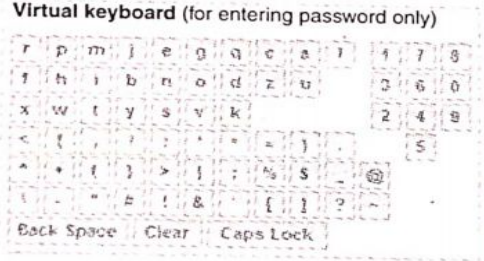


Figure 2.5 | Cybercafe security.
Source: http://www.icicibank.com/pfsuser/temp/cybersec.htm (27 June 2009).



ICICI Bank

Virtual Keyboard for Internet Banking

At ICICI Bank, We are committed to make your banking with us a safe and wonderful experience. We provide you with Virtual Keyboard to Protect your password. Virtual Keyboard is an online application to enter password with the help of a mouse.

Advantage of a Virtual Keyboard

The Virtual Keyboard is designed to protect your password form malicious "Spyware" and "Trojan Programs". Use of Virtual keyboard will reduce the risk of password theft.

Process To Use Virtual Keyboard

Steps to use Virtual keyboard are as follows:

Enter Login ID using Physical Keyboard.

- Select the check box 'Use Virtual Keyboard'.
- Use the Virtual Keyboard to the login password.
- Once you have entered your password, click"Log-in".
-

Functions of different keys on the Virtual Keyboard

Caps Lock: This key can be used to enter upper case if the password consist of capital letters.
Back Space: This key wil clear the last character entered in the password field.
Clear: This key wil clear all characters entered in the password field by Virtual keyboard.
Tab: This key is visible only for change or forced change password. field by Virtual keyboard.This key can be used to ente values in the next field.

Figure 2.6 | Virtual keyboard.
Source: http://www.icicibank.com/pfsuser/webnews/virtualkeyboad.htm (27 June 2009).

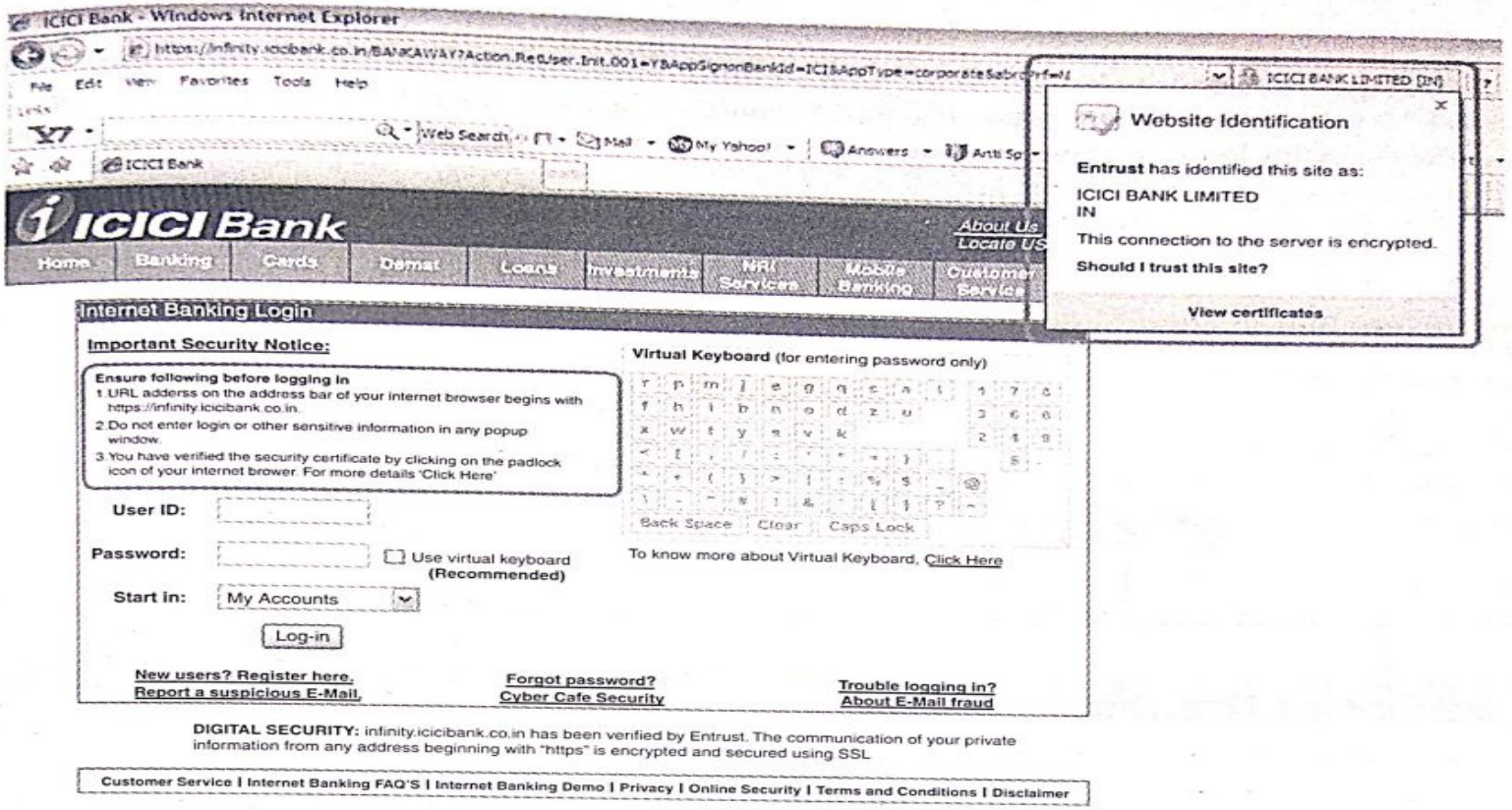


Figure 2.7 | Security warnings.
Source: http://www.icicibank.com/pfsuser/webnews/virtualkeyboad.htm (27 June 2009).

Botnets: The fuel of cyber crime

- Bot- computing
- A botnet (short for “robot network”) is **a network of computers infected by malware that are under the control of a single attacking party, known as the “bot-herder.”**
- Each individual machine under the control of the bot-herder is known as a bot.
- Automated program for doing some particular task

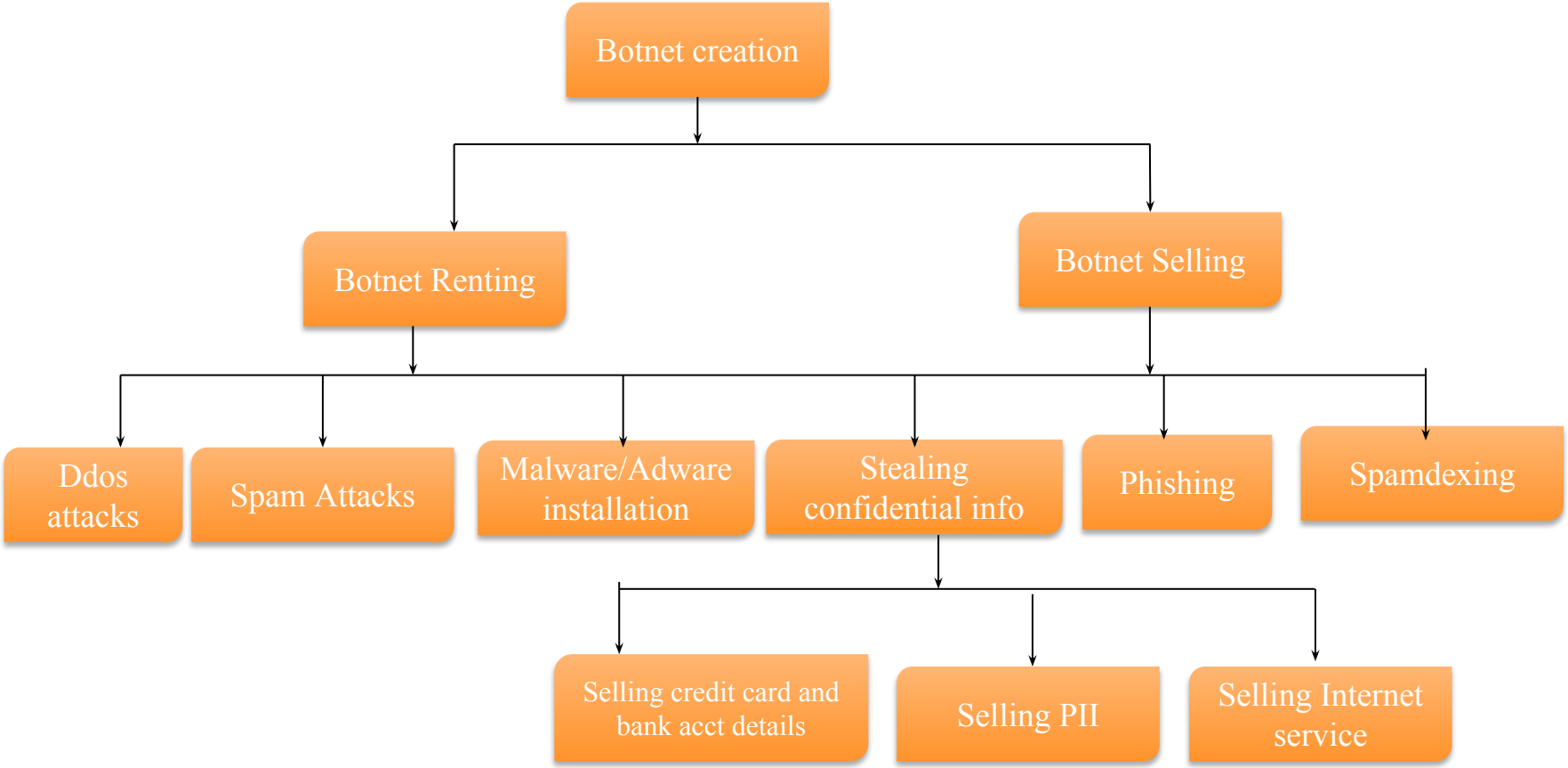
Botnet

In simple terms, a Bot is simply an automated computer program (explained in Box 1.2, Chapter 1). One can gain the control of your computer by infecting them with a virus or other Malicious Code that gives the access. Your computer system maybe a part of a Botnet even though it appears to be operating normally. Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks (the term is discussed in detail in Chapter 4).

A Botnet (also called as zombie network) is a network of computers infected with a malicious progra
that allows cybercriminals to control the infected machines remotely without the users' knowledge. "Zomb
networks" (explained in Chapter 1, Fig. 1.3) have become a source of income for entire groups of cybercrim
nals. The invariably low cost of maintaining a Botnet and the ever diminishing degree of knowledge require
to manage one are conducive to the growth in popularity and, consequently, the number of Botnets.

If someone wants to start a "business" and has no programming skills, there are plenty of "Bot for sale"
offers on forums. Obfuscation and encryption of these programs' code can also be ordered in the same wa
to protect them from detection by antivirus tools. Another option is to steal an existing Botnet. Figure 2.
explains how Botnets create business.

Botnets- Creation and usage



Botnets- The fuel for Cybercrime

- **Malware-** short for malicious software, refers to any software intentionally designed to cause damage, disrupt operations, steal sensitive information, or gain unauthorized access to computer systems, networks, or devices.
- **Adware-**Adware is unwanted software that displays intrusive advertisements or redirects users to malicious websites. While not necessarily harmful, adware can degrade system performance, compromise user privacy, and create security vulnerabilities.
- Spam-spam refers to unsolicited or unwanted emails sent in bulk to a large number of recipients, typically for advertising purposes.

Botnets- The fuel for Cybercrime

- Spamdexing- Known as search engine spamming or search engine manipulation, refers to the practice of manipulating search engine algorithms to achieve higher rankings for web pages in search results, often using deceptive or unethical techniques.
  - Spamdexing can involve keyword stuffing, creating doorway pages, cloaking content, or using link farms to artificially inflate the perceived relevance or popularity of a website.
  - The goal of spamdexing is to increase traffic to a website and improve its visibility in search engine results, ultimately driving more clicks and potential revenue for the site owner.

Botnets- Prevention

- Use of updated antivirus softwares
- Installation and security patches regularly
- Using firewalls to protect the system from hacking while connected to internet.
- Disconnect from internet when not in use
- Download freewares only from trusted websites.
- Constant monitoring of files/folders/mailboxes
- Take immediate response if the system is infected.

One can ensure the following to secure the system

1. **Use antivirus and anti-Spyware software and keep it up-to-date:** It is important to remove and/or quarantine the viruses. The settings of these softwares should be done during the installations so that these softwares get updated automatically on a daily basis.
2. **Set the OS to download and install security patches automatically:** OS companies issue the security patches for flaws that are found in these systems.
3. **Use a firewall to protect the system from hacking attacks while it is connected on the Internet:** A firewall is a software and/or hardware that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria. A firewall is different from antivirus protection. Antivirus software scans incoming communications and files for troublesome viruses vis-à-vis properly configured firewall that helps to block all incoming communications from unauthorized sources.
4. **Disconnect from the Internet when you are away from your computer:** Attackers cannot get into the system when the system is disconnected from the Internet. Firewall, antivirus, and anti-Spyware softwares are not foolproof mechanisms to get access to the system.

5. **Downloading the freeware only from websites that are known and trustworthy:** It is always appealing to download free software(s) such as games, file-sharing programs, customized toolbars, etc. However, one should remember that many free software(s) contain other software, which may include Spyware.
6. **Check regularly the folders in the mail box – "sent items" or "outgoing" – for those messages you did not send:** If you do find such messages in your outbox, it is a sign that your system may have infected with Spyware, and maybe a part of a Botnet. This is not foolproof; many spammers have learned to hide their unauthorized access.
7. **Take an immediate action if your system is infected:** If your system is found to be infected by a virus, disconnect it from the Internet immediately. Then scan the entire system with fully updated antivirus and anti-Spyware software. Report the unauthorized accesses to ISP and to the legal authorities. There is a possibility that your passwords may have been compromised in such cases, so change all the passwords immediately.

Attack vector

An "attack vector" is a path or means by which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome. Attack vectors enable attackers to exploit system vulnerabilities, including the human element. Attack vectors include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception. All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defenses.[14]

To some extent, firewalls and antivirus software can block attack vectors. However, no protection method is totally attack-proof. A defense method that is effective today may not remain so for long because attackers are constantly updating attack vectors, and seeking new ones, in their quest to gain unauthorized access to computers and servers. Refer to Box 2.10.

are now most of them are launched.[16,18]

1. **Attack by E-Mail:** The hostile content is either embedded in the message or linked to by the message. Sometimes attacks combine the two vectors, so that if the message does not get you, the attachment will. Spam is almost always carrier for scams, fraud, dirty tricks, or malicious action of some kind. Any link that offers something "free" or tempting is a suspect.
2. **Attachments (and other files):** Malicious attachments install malicious computer code. The code could be a virus, Trojan Horse, Spyware, or any other kind of malware. Attachments attempt to install their payload as soon as you open them.
3. **Attack by deception:** Deception is aimed at the user/operator as a vulnerable entry point. It is not just malicious computer code that one needs to monitor. Fraud, scams, hoaxes, and to some extent Spam, not to mention viruses, worms and such require the unwitting cooperation of the computer's operator to succeed. Social engineering and hoaxes are other forms of deception that are often an attack vector too.
4. **Hackers:** Hackers/crackers are a formidable attack vector because, unlike ordinary Malicious Code, people are flexible and they can improvise. Hackers/crackers use a variety of hacking tools, heuristics,

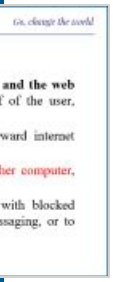
and social engineering to gain access to computers and online accounts. They often install a Trojan Horse to commandeer the computer for their own use.

5. **Heedless guests (attack by webpage):** Counterfeit websites are used to extract personal information. Such websites look very much like the genuine websites they imitate. One may think he/she is doing business with someone you trust. However, he/she is really giving their personal information, like address, credit card number, and expiration date. They are often used in conjunction with Spam, which gets you there in the first place. Pop-up webpages may install Spyware, Adware or Trojans.
6. **Attack of the worms:** Many worms are delivered as E-Mail attachments, but network worms use holes in network protocols directly. Any remote access service, like file sharing, is likely to be vulnerable to this sort of worm. In most cases, a firewall will block system worms. Many of these system worms install Trojan Horses. Next they begin scanning the Internet from the computer they have just infected, and start looking for other computers to infect. If the worm is successful, it propagates rapidly. The worm owner soon has thousands of "zombie" computers to use for more mischief.
7. **Malicious macros:** Microsoft Word and Microsoft Excel are some of the examples that allow macros. A macro does something like automating a spreadsheet, for example. Macros can also be used for malicious purposes. All Internet services like instant messaging, Internet Relay Chart (IRC), and P2P file-sharing networks rely on cozy connections between the computer and the other computers on the Internet. If one is using P2P software then his/her system is more vulnerable to hostile exploits.
8. **Foistware (sneakware):** Foistware is the software that adds hidden components to the system on the sly. Spyware is the most common form of foistware. Foistware is quasi-legal software bundled with some attractive software. Sneak software often hijacks your browser and diverts you to some "revenue opportunity" that the foistware has set up.
9. **Viruses:** These are malicious computer codes that hitch a ride and make the payload. Nowadays, virus vectors include E-Mail attachments, downloaded files, worms, etc.

How Attackers cover their track (Antiforensics)

How Attackers use Proxies:

- A proxy server **acts as an intermediary between the user and the web server**. Proxy servers use a different IP address on behalf of the user, concealing the user's real address from web servers.
- A proxy server uses a specific port to listen for and forward internet requests.



A proxy allows actors to send network traffic through another computer, which satisfies requests and returns the result.

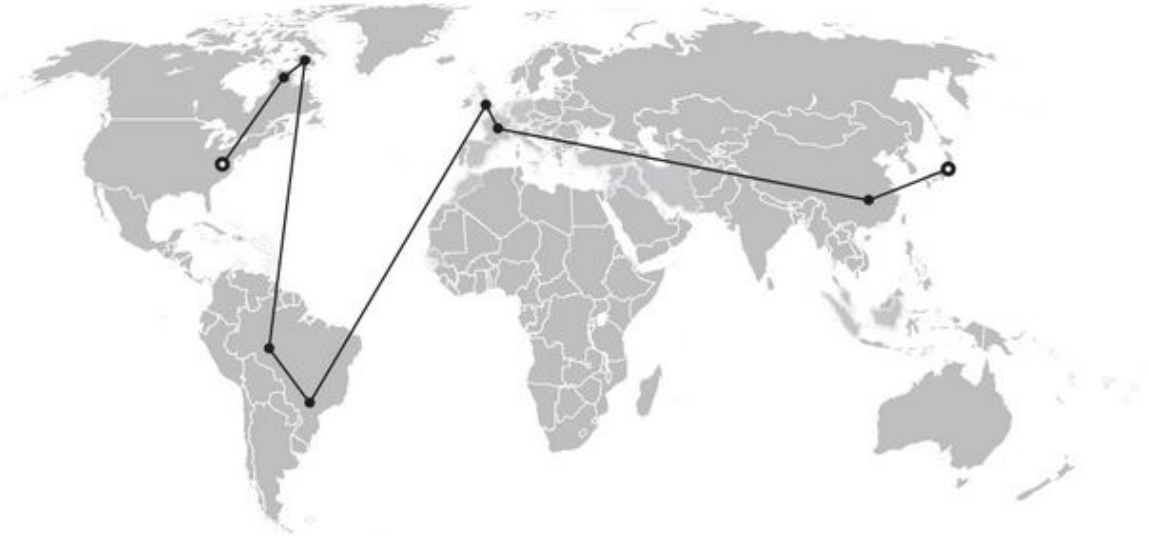
Students or employees can use proxies to communicate with blocked services such as Internet Relay Chat (IRC) and instant messaging, or to browse websites that administrators block.

How Attackers cover their track (Antiforensics)

- Attackers also use proxies because Internet Protocol (IP) addresses are traceable, and they do not want to reveal their true locations.
- As one example, iDefense wrote about the fast-flux architecture (ID# 484463), which uses a proxy infrastructure to satisfy requests.
- Proxies are also a common source of spam e-mail messages, which use open relays (a simple mail transfer protocol [SMTP] proxy).
- Proxies are useful to attackers in many ways. Most attackers use proxies to hide their IP address and, therefore, their true physical location.
- In this way, attackers can conduct fraudulent financial transactions, launch attacks, or perform other actions with little risk.

How Attackers cover their track (Antiforensics)

- While law enforcement can visit a physical location identified by an IP address, attackers that use one (or multiple) proxies across country boundaries are more difficult to locate.
- The endpoint can only view the last proxy with which it is directly communicating and not any of the intermediary proxies or the original location.



How Attackers cover their track (Antiforensics)

- Attackers operate free proxies or alter a victim's proxy settings because proxies can serve as a monitoring tool.
- AnonProxy is one example of a malicious proxy that its authors designed to monitor users and steal information such as social-networking passwords.
- Since a proxy relays traffic, it also has the ability to log and alter sensitive pages or information.
- Attackers must either convince users or install malicious code to modify proxy settings themselves.

How Attackers cover their track (Antiforensics)

- Malicious code authors also install local proxies.
- By altering the host's file or browser configuration to use the proxy, the attacker redirects requests and captures confidential information.
- Some banking Trojans give attackers the ability to proxy requests through the victim's browser because conducting fraud from a legitimate user's IP address is less suspicious.
- Local proxies are more difficult to identify because the local proxy does not open any network ports and scanning the system will reveal no changes.

How Attackers cover their track (Antiforensics)

Types of Proxies

- Proxies are so common that many attackers scan the Internet for common listening proxy ports.
- **The most common proxies listen on TCP port 80 (HTTP proxies), 8000, 8081, 443, 1080 (SOCKS Proxy), and 3128 (Squid Proxy), and some also handle User Datagram Protocol (UDP).**
- Attackers who install custom proxies often do not use standard ports but instead use random high ports.
- Some lightweight proxies are written in scripting languages, which run with an HTTP server and are easier for attackers to modify.

How Attackers cover their track (Antiforensics)

Types of Proxies

- Application proxies require configuration. Some applications either do not operate correctly through proxy services because the proxy server removes necessary information or cannot satisfy the request.
- Some services like The Onion Router (Tor)2 also give users the ability to proxy traffic and hide their original location from victims.
- A virtual private network (VPN) acts as a more versatile proxy and supports more security features. Instead of configuring the application to use a proxy, users can tunnel all traffic through the VPN.
- VPN services usually support strong authentication and are less likely to leak information that could identify the user of a proxy.

How Attackers cover their track (Antiforensics)

Types of Proxies

- Attackers commonly use free or commercial proxies (e.g., SOCKS and VPN) that operators advertise on hacking forums.
- Attackers may prefer these services to public proxies because they advertise anonymity and claim they do not keep logs, unlike Tor, where community operators can monitor traffic going through an exit node that it controls.
- Proxy services that keep logs are a danger to attackers who use these services for conducting fraud and can lead to their arrests.

How Attackers cover their track (Antiforensics)

Types of Proxies

Some commercial VPN and SOCKS proxy services include

- hxxp://secretsline.net
- hxxp://vpn-secure.net
- hxxp://thesafety.us
- hxxp://5socks.net
- hxxp://vpn-service.us
- hxxp://vip72.com
- hxxps://www.cryptovpn.com
- hxxp://www.vipvpn.com
- hxxp://openvpn.ru

How Attackers cover their track (Antiforensics)

Types of Proxies

- Attackers may prefer proxy services advertised on hacking forums because they are less responsive to abuse requests.
- For example, commercial proxy services like FindNot keep logs of their users for a maximum of five days to protect the system from being used for abusive purposes, while many of those services advertised on hacking forums do not keep any logs.
- Operating proxy services is not illegal because it has legitimate purposes related to anonymity for users; however, some commercial proxy services are more willing to respond to abuse than others.

How Attackers cover their track (Antiforensics)

Detecting the Use of Proxies

- Detecting proxies is difficult and not always reliable. Since many malicious code authors install custom proxies and use encrypted or custom protocols, it is very difficult to detect all proxies.
- There are techniques to detect common proxies, but such techniques are unlikely to be effective against attackers who use proxies aggressively.
- Port scanning on corporate networks can identify proxies that listen on default ports. Organizations should also monitor changes to proxy configuration because such changes could indicate that an attacker compromised a host.

Attackers techniques and Motivations

Detecting the use of Proxies

- **IP Geolocation Analysis**: Proxy servers often route traffic through different geographic locations, which can be identified through IP geolocation analysis.
- **Traffic Analysis**: Analyzing network traffic patterns can help identify suspicious or anomalous behavior associated with proxy usage.

Tunneling Techniques

Tunneling

(Source: https://gcore.com/learning/what-is-tunneling/)

Tunneling—also referred to as port forwarding or network tunneling—is the process of transmitting private network data through a public network securely and efficiently.

Tunneling


Neighborhood
Home
Cargo train
Underground tunnel
Store
City dwellers
Bad actor

Attackers techniques and Motivations

Tunneling

- Imagine a protected tunnel, stretching from your house (private network) to your favorite store (destination/local network) amidst a bustling city (public network.)
- Your train (data) carries valuable cargo (your information) that needs to be protected from prying eyes.
- With tunneling, this train enters the protected tunnel from your home, travels securely across the city via a tunnel, and finally arrives at the store, escaping the notice of city residents other than yourself.
- Tunneling keeps your data safe and protected from prying eyes as it travels to its destination.

Attackers techniques and Motivations

Tunneling

- A network is a system of two or more connected devices.
- In networks, devices are connected together so they can share resources and information.
- Tunneling is the part of networking that facilitates secure and efficient data transmission.
- It allows connected systems to communicate and collaborate safely and securely over public networks..

Attackers techniques and Motivations

Tunneling

- One major benefit of tunneling is that it allows remote workers and field teams to safely work offsite without compromising personal or organizational security.
- A remote worker can safely access a private corporate network via the internet.
- For example, they can safely connect to HQ and then access, submit, and download sensitive files by using secure tunnel connections provided by the company.

Attackers techniques and Motivations

Tunneling Techniques

- 2.1.2.1 HTTP
- 2.1.2.2 DNS
- 2.1.2.3 ICMP
- 2.1.2.4 Intermediaries, Steganography, and Other Concepts
- 2.1.2.5 Detection and Prevention

Attackers techniques and Motivations

HTTP

- HTTP has become the de facto high-level protocol on the Internet. As the protocol used for accessing content on the World Wide Web, developers adapted it to carry much more than just the static text and images of Web pages.
- It now carries audio and video streams, can transfer large files, and can even carry application-to-application remote procedure calls (RPCs).
- Its ubiquity and indispensability make it a prime candidate for tunneling operations.

Attackers techniques and Motivations

HTTP

- HTTP has become the de facto high-level protocol on the Internet. As the protocol used for accessing content on the World Wide Web, developers adapted it to carry much more than just the static text and images of Web pages.
- It now carries audio and video streams, can transfer large files, and can even carry application-to-application remote procedure calls (RPCs).
- Its ubiquity and indispensability make it a prime candidate for tunneling operations.

Attackers techniques and Motivations

The HTTP Request Message:

METHOD	/path	?	query	HTTP/VERSION
header				
content				

The HTTP Reply Message:

HTTP/VERSION	STATUS	reason
header		
content		

Attackers techniques and Motivations

HTTP

- The protocol allows, in essence, unlimited space for content (or payload) in the request or reply message in addition to other open areas, such as the headers, whether this content includes arbitrary custom headers or inappropriate data in valid headers.
- This makes it convenient to transfer arbitrary data to and from an HTTP server.
- All one needs to tunnel the traffic is software that can pretend to talk to the protocol but in reality can transfer data for some other (perhaps nefarious) purpose.
- A tunneling Web server or a tunneling Web application running on a legitimate Web server will work

Attackers techniques and Motivations

HTTP

- The protocol allows, in essence, unlimited space for content (or payload) in the request or reply message in addition to other open areas, such as the headers, whether this content includes arbitrary custom headers or inappropriate data in valid headers.
- This makes it convenient to transfer arbitrary data to and from an HTTP server.
- All one needs to tunnel the traffic is software that can pretend to talk to the protocol but in reality can transfer data for some other (perhaps nefarious) purpose.
- A tunneling Web server or a tunneling Web application running on a legitimate Web server will work

Attackers techniques and Motivations

HTTP

- Most malicious code already acts as a simple HTTP tunnel, in practice, it posts sensitive data to malicious Web servers for purposes other than to retrieve a Web-based resource.
- Some common software for the task is GNU httptunnel, JHttpTunnel, and Webtunnel.

Attackers techniques and Motivations

DNS

- The DNS is the core directory service of the Internet.
- Without it, translations between namesand IP addresses, could not happen, and it would be difficult, if not impossible, to manage the daily operations of the Internet.
- Since DNS is a service that an administrator cannot block and must always make available, it is also a good choice for data exfiltration and tunneling.
- The most common delivery mechanism for DNS is the UDP, not TCP, so the specifications do not guarantee communication reliability

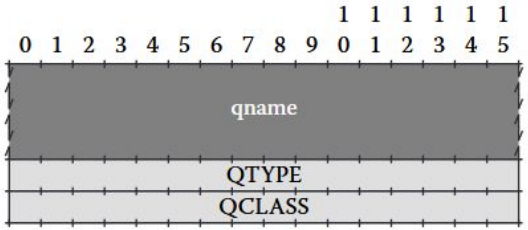
Attackers techniques and Motivations

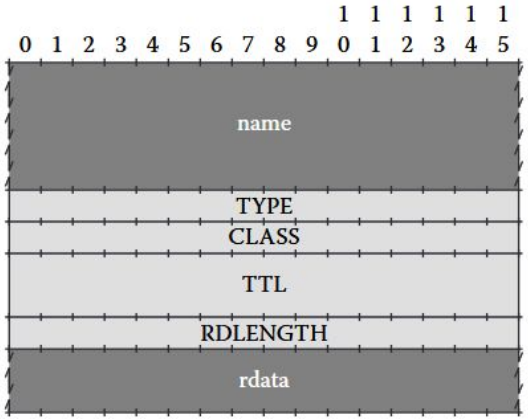
DNS

- It is hierarchically decentralized so clients may not send transmissions directly to a specific end server, but other servers may relay it, and the size of the information contained in each burst of communication is relatively small.
- These features make the deployment of functional tunnels more difficult but not impossible.

Attackers techniques and Motivations

HEADER	
question	The Question for the Name Server
answer	Resource Records (RRs) Answering the Question
authority	RRs Pointing Toward an Authority
additional	RRs Holding Additional Information





Attackers techniques and Motivations

DNS

- In most cases, the tunnel client is simple end user software that makes many requests for non existence hosts.
- The tunnel server is generally a rogue (fake) DNS server where intermediary resolvers eventually route the questions.

Attackers techniques and Motivations

ICMP

- ICMP is a signaling protocol for IP.
- It is used mostly to deliver status and error messages when IP-based communication errors occur or to troubleshoot and test connectivity status.
- Although most enterprise policies already block outbound ICMP packets, some Internet service provider (ISP) solutions may not, and its use as a tunnel is mostly to bypass ISP authentication requirements or as a simple covert channel.

Attackers techniques and Motivations

ICMP

- ICMP echo messages, which users and administrators are used to test the accessibility of a host, are suited for tunneling.
- Ping, as the most common software that implements this ICMP mechanism, sends data to a host and expects a reply.
- ICMP tunneling was one of the earliest methods publicly available to transmit traffic over a protocol.

Attackers techniques and Motivations

Intermediaries, Steganography, and Other Concepts

- Hackers can modify any protocol that filters through a firewall to behave as a tunnel.

Attackers techniques and Motivations

Detection and Prevention

- The potential of covertly extending a network to the outside world is a clearly unacceptable risk.
- While the firewalls and IDS that are in place today have their roles to play, they may not be able to identify or prevent tunneling.
- Tunnels abuse protocols in a way that matches the syntax or the rules of the specifications.
- Any protocol can quickly become a tunnel harbor.
- Packet inspection firewall rules and IDSs can go only so far in identifying and blocking the threats.

Attackers techniques and Motivations

Detection and Prevention

- Tunnels do have a weakness. They almost never adhere to historical or trended traffic patterns.
- While HTTP normally has small transfers outbound with larger transfers inbound, tunneling may cause this to reverse or become nearly equal.
- The duration of connections may also buck the trend, as tunnels need things like keep-alive messages and timeouts.
- In the case of DNS tunnels, the amount of requests per client, or a set of clients, or even across the enterprise may jump significantly.
- In the case of ICMP, packet sizes may not match the expected norms, and with any other tunnels, the ratios of different protocols, frequency, and volume can all be indicators of anomalies.

Attackers techniques and Motivations

Fraud Techniques

- Many phishing attacks against mobile devices use short message service (SMS, or smishing) and voice-over Internet protocol (VoIP) to distribute lures and collect personal information.
- Attackers often send fraudulent SMS messages containing a URL or phone number using traditional phishing themes.
- Responders either enter their personal information into a fraudulent website, as with traditional e-mail phishing, or, if calling phone numbers, may even provide their information directly to other people.

Attackers techniques and Motivations

Prevent falling victim to phishing over mobile devices attacks:

1. Be Skeptical of Unsolicited Messages
2. Verify the Sender
3. Check URLs Carefully
4. Avoid Clicking on Suspicious Links:
5. Don't Provide Personal Information:
6. Enable Security Features
7. Keep Software Updated:
8. Educate Yourself and Others:
9. Use Two-Factor Authentication (2FA):
10. Report Suspicious Messages

Attackers techniques and Motivations

Prevent falling victim to vishing attacks:

1. Be Suspicious of Unsolicited Calls
2. Verify the Caller's Identity
3. Never Give Out Personal Information
4. Beware of Urgency or Threats
5. Don't Trust Caller ID Alone
6. Educate Yourself and Others:
7. Consider Call-blocking Tools:
8. Report Suspicious Calls: I

Attackers techniques and Motivations

Rogue Antivirus

A r**ogue antivirus**, also known as a fake antivirus or scareware, is a type of malicious software that masquerades as legitimate antivirus software.

- **Infection**: You inadvertently download or install the rogue antivirus onto your computer, often through deceptive means such as fake software downloads, misleading advertisements, or malicious email attachments.
- **Fake Security Alerts**: Once installed, the rogue antivirus begins to display fake security alerts and warnings on your computer. These alerts typically claim that your system is infected with numerous viruses, malware, or other security threats.
- **Scare Tactics**: The rogue antivirus uses scare tactics to convince you that your computer is at risk and that immediate action is required to protect your data and privacy. The warnings may appear urgent and alarming, urging you to purchase the full version of the software to remove the supposed threats.

Attackers techniques and Motivations

- **Pressure to Purchase**: The rogue antivirus prompts you to purchase a license or upgrade to the full version of the software to remove the alleged threats and restore your computer's security. It may use aggressive tactics, such as constant pop-up messages or system lockdowns, to pressure you into making a payment.
- **Fake Scan Results**: The rogue antivirus may perform a fake system scan that exaggerates or fabricates the presence of malware on your computer. The scan results are designed to further convince you of the need to purchase the full version of the software.
- **Payment and Installation of Malware**: If you succumb to the pressure and purchase the rogue antivirus, you may unwittingly provide your credit card information to the attackers. In some cases, even after making a payment, the rogue antivirus may fail to remove any threats or may introduce additional malware onto your system.

Attackers techniques and Motivations

- **Financial Loss and Compromised Security**: Not only does the purchase of the rogue antivirus result in financial loss, but it also fails to provide any real protection against security threats. Meanwhile, the rogue software may continue to operate in the background, potentially collecting sensitive information or performing other malicious activities.
- **Removal**: Removing a rogue antivirus can be challenging since it may attempt to resist uninstallation or removal. Specialized antivirus or antimalware software may be required to detect and remove the rogue software effectively.

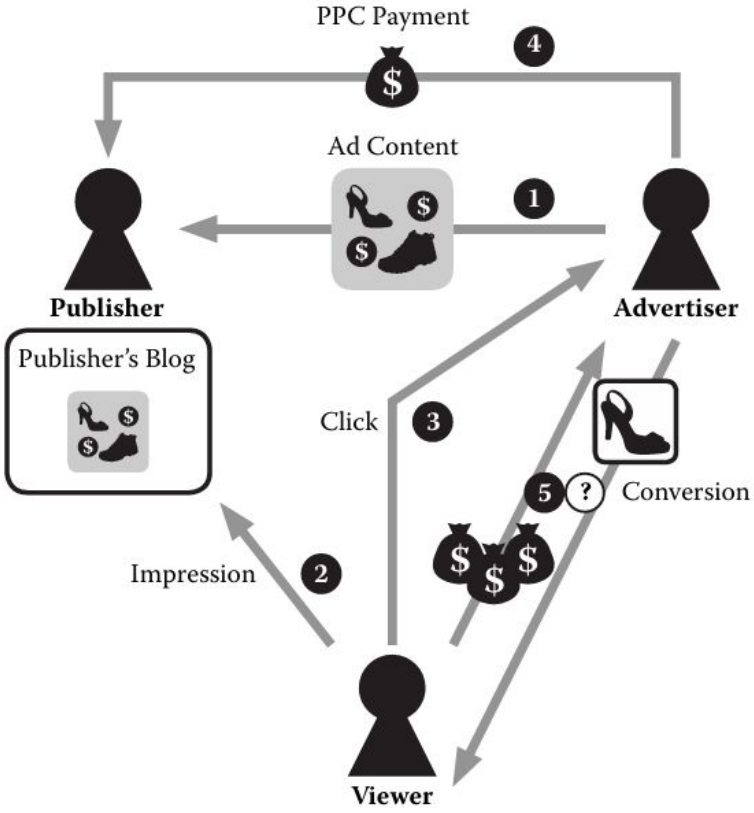
Attackers techniques and Motivations

Pay per click

- Any advertising transaction has three primary parties: the advertiser, the publisher, and the viewer.
- The advertiser is a company that produces content it would like to display to potential customers.
- The publisher is a creative outlet that produces content that will draw visitors to its medium.
- These visitors view the ad and, ideally, purchase the advertised product or service.
- The advertiser pays a fee for a specific number of “impressions,” which is the estimated number of times a viewer will see the ad.
- This model is essentially the same across all forms of media, including print, radio, and television.
- The ultimate goal for the advertiser is to convert ad clicks to actions that generate more revenue than the advertising campaign costs.

Attackers techniques and Motivations

Pay per click business model



Attackers techniques and Motivations

Advantages of the PPC model include:

- **Immediate Results**: PPC advertising can generate immediate traffic and results for advertisers.
- **Targeted Advertising**: Advertisers can target specific audiences based on demographics, interests, and behavior.
- **Measurable Results**: PPC campaigns provide detailed performance metrics, allowing advertisers to track the effectiveness of their ads and make data-driven decisions.

Attackers techniques and Motivations

Click Fraud Motivations

Click fraud refers to the fraudulent clicking on pay-per-click (PPC) ads with the intention of artificially inflating advertising costs or generating revenue for the fraudster.

Motivations:

- **Financial Gain**: One of the primary motivations for click fraud is financial gain. Fraudsters may engage in click fraud to generate revenue through ad networks that pay publishers for clicks on ads displayed on their websites. By clicking on their own ads or collaborating with others to click on ads, fraudsters can earn money dishonestly.
- **Competitive Advantage**: In some cases, competitors may engage in click fraud to sabotage the advertising efforts of their rivals. By repeatedly clicking on their competitors' ads, they can exhaust their advertising budget, drive up their advertising costs, or reduce the effectiveness of their campaigns.

Attackers techniques and Motivations

- **Malicious Intent**: Some individuals or groups engage in click fraud for malicious reasons, such as causing financial harm to businesses, disrupting online operations, or undermining the integrity of online advertising systems. These attackers may have various motivations, including ideological, political, or personal grievances.
- **Revenge or Retaliation**: Click fraud can also be motivated by revenge or retaliation against specific advertisers, publishers, or individuals. In some cases, disgruntled employees, customers, or individuals may engage in click fraud as a form of protest or retaliation for perceived grievances.

Attackers techniques and Motivations

Click Fraud Tactics and Detection

- Click fraud encompasses various tactics employed by fraudsters to artificially inflate clicks on online advertisements.

Click Fraud Tactics:

- **Manual Clicking**: Fraudsters manually click on ads multiple times using different devices or IP addresses to generate invalid clicks.
- **Click Farms**: Click farms consist of individuals or automated bots that are paid to click on ads repeatedly. These farms may be located in countries where labor costs are low.
- **Bot Traffic**: Automated bots are programmed to mimic human behavior and click on ads. These bots can generate large volumes of fraudulent clicks, making them difficult to detect.
- **Competitor Clicks**: Competitors may engage in click fraud by repeatedly clicking on each other's ads to exhaust advertising budgets or reduce ad effectiveness.
- **IP Spoofing**: Fraudsters may use techniques such as IP spoofing to mask their true location and generate clicks from different IP addresses.

Attackers techniques and Motivations

- **Cookie Stuffing**: In cookie stuffing, fraudulent cookies are placed on users' devices without their knowledge. These cookies can trigger clicks on ads even if the user hasn't intentionally clicked on them.
- **Adware and Malware**: Adware and malware programs installed on users' devices can generate fraudulent clicks on ads without the user's consent.

Attackers techniques and Motivations

Click Fraud Detection and Prevention:

- **Monitoring Click Patterns**: Advertisers and ad networks can monitor click patterns and analyze data to identify abnormal click behavior, such as unusually high click volumes or repetitive clicking from the same IP addresses.
- **IP Address Analysis**: Analyzing IP addresses associated with clicks can help detect suspicious activity, such as clicks originating from known click farms or proxy servers.
- **Click Timestamp Analysis**: Examining the timestamps of clicks can reveal patterns indicative of click fraud, such as clicks occurring at regular intervals or during non-peak hours.
- **Device and Browser Analysis**: Identifying clicks from unusual devices or browsers, or those exhibiting erratic behavior, can help flag potentially fraudulent activity.
- **Fraudulent Activity Filters**: Ad networks and platforms can implement filters and algorithms to automatically detect and filter out fraudulent clicks in real-time.

Attackers techniques and Motivations

- **Manual Review**: Conducting manual reviews of click data and investigating suspicious activity can help identify and prevent click fraud.
- **Geolocation Verification**: Verifying the geolocation of clicks and comparing it with the advertiser's target audience can help detect clicks originating from fraudulent sources.
- **Collaboration and Information Sharing**: Advertisers, ad networks, and industry organizations can collaborate and share information about known click fraud tactics and perpetrators to improve detection and prevention efforts.