PCET

Pimpri Chinchwad University

School of Computer Applications

BSc (CS)-II SEM-IV

Unit No. 01 Introduction to Cybercrime

Introduction:

- "Cyber security is the protection of internet-connected systems, including hardware, software and data, from cyber-attacks."
- "Cybersecurity" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Almost everyone is aware of the rapid growth of the Internet.
- Given the unrestricted number of free websites, the Internet has undeniably opened a new way of exploitation known as cybercrime.
- These activities involve the use of computers, the Internet, cyberspace, and the worldwide web (WWW).
- Interestingly, cybercrime is not a new phenomenon; the first recorded cybercrime took place in the year 1820.
- It is one of the most talked about topics in the recent years.
- Based on a 2008 survey in Australia, the below shows the cybercrime trend
- Indian corporate and government sites have been attacked or defaced more than 780 times between February 2000 and December 2002.
- There are also stories/news of other attacks; for example, according to a story posted on 3 December 2009, a total of 3,286 Indian websites were hacked in 5 months – between January and June 2009.
- Various cybercrimes and cases registered under cybercrimes by motives and suspects in States and Union Territories (UTs).

Here are some cyber-attacks on government bodies in India since 2010:

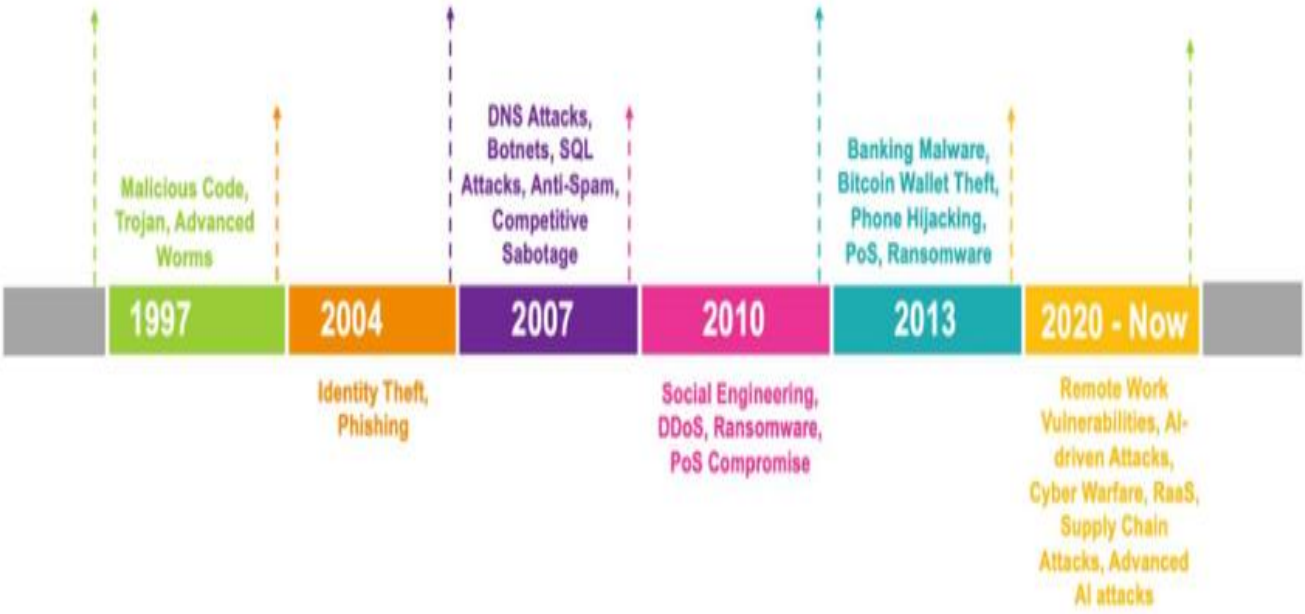
- **Indian Council of Medical Research (ICMR)**: In October 2023, 815 million (8.15 CR.) people's COVID testing data was stolen from the ICMR. The attacker tried to sell the data for $80,000 on hacking forums. Four people have been arrested in connection with the crime.

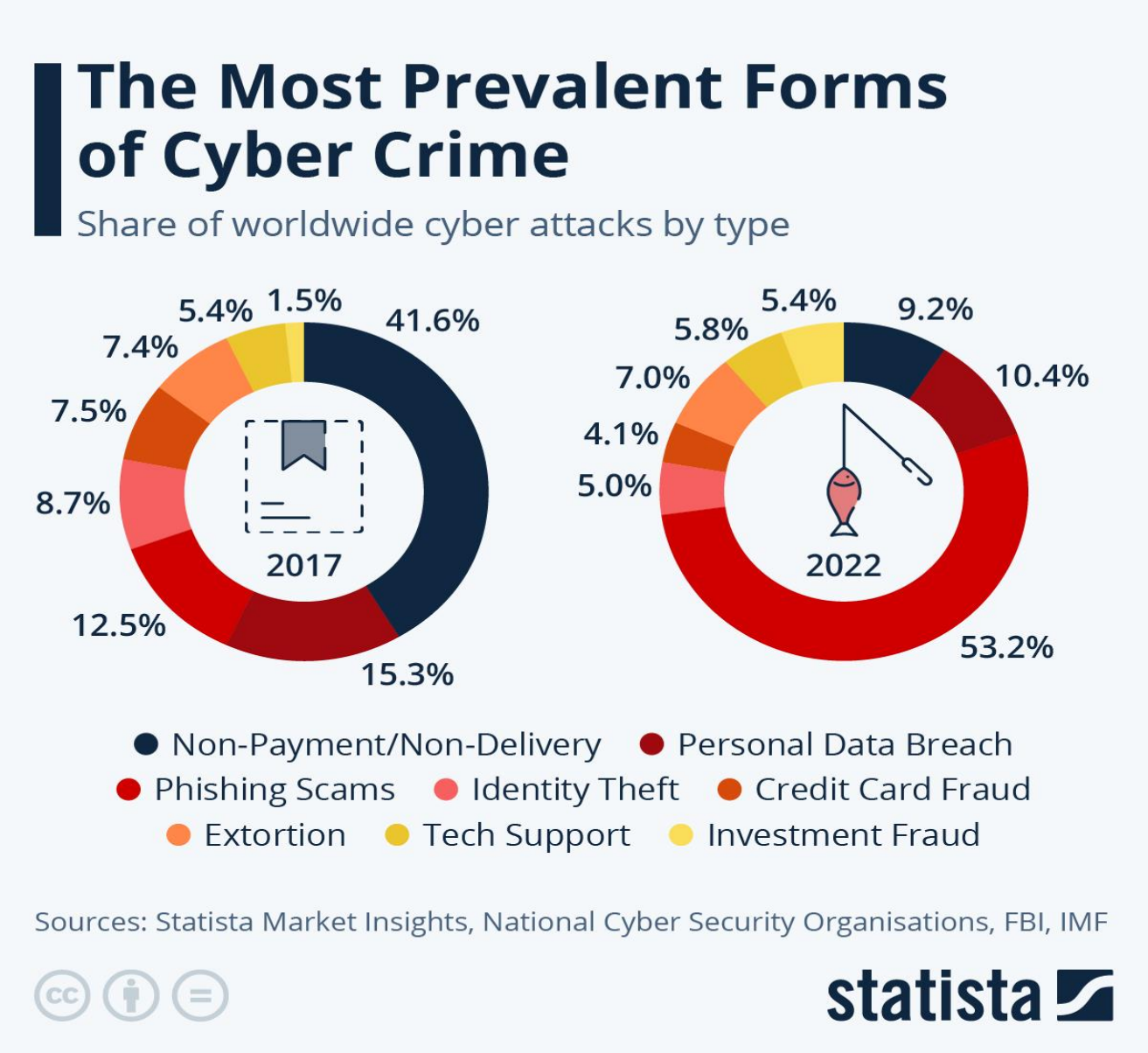
- **Telangana Police, Tamil Nadu labour department, and the National Disaster Management Authority**: These major government bodies were hit by cyber-attacks in 2024.
- **All India Institute of Medical Sciences (AIIMS)**: India's largest hospital was hit by cyber-attacks twice in 2023.

Other cyber-crime statistics in India include:

- The number of cyber-crimes reported in India has increased significantly since 2019.
- In 2022, Telangana had the highest number of reported cyber-crimes in India.
- The Indian Cyber Crime Coordination Centre blocked cyber-crime-related items from March to September 2024.
- The National Cyber Crime Reporting Portal allows the public to report cyber-crimes, especially those against women and children.
- Globally, around 30,000 websites are hacked every day, with 43% of those being small businesses.

Evaluation of Cybercrime





Cybercrime is a broad category of criminal activities that use computers, networks, or networked devices:

- **Purpose**

Cybercriminals use technology to commit a variety of crimes, including:

- Fraud, such as identity theft, email fraud, and internet fraud
- Stealing financial account, credit card, or other payment card information
- Spreading malware, illegal information, images, or other materials
- Disrupting services
- Causing financial or reputational harm
- Trafficking in child pornography and intellectual property

- Violating privacy

Cybercrime: Definition And Origins of The Word

Definition:

"A crime conducted in which a computer was directly and significantly instrumental is called as a Cybercrime."

Alternative definitions of Cybercrime are as follows:

1. Any illegal act where a special knowledge of computer technology is essential for its perpetration (to commit a crime), investigation or prosecution.
2. Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers.
3. Any financial dishonesty that takes place in a computer environment.
4. Any threats to the computer itself, such as theft of hardware or software, damage and demands for money.

Important Definitions related to Cyber Security:

Cyberterrorism:

This term was coined in 1997 by Barry Collin, a senior research fellow at the institute for Security and Intelligence in California. Cyberterrorism seems to be a controversial term. The use of information technology and means by terrorist groups & agents is called as Cyberterrorism.

"The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives."

(or)

Cyberterrorism is defined as "any person, group or organization who, with terrorist intent, utilizes accesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyberterrorism."

Cybernetics:

Cybernetics deals with information and its use. Cybernetics is the science that overlaps the fields of neurophysiology, information theory, computing machinery and automation. Worldwide, including India, cyberterrorists usually use computer as a tool, target for their unlawful act to gain information.

Internet is one of the means by which the offenders can gain priced sensitive information of companies, firms, individuals, banks and can lead to intellectual property (IP) crimes, selling

illegal articles, pornography/child pornography, etc. This is done using methods such as Phishing, Spoofing, Pharming, Internet Phishing, wire transfer, etc. and use it to their own advantage without the consent of the individual.

Phishing:

Phishing is a cyber-attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need a request from their bank, for instance, or a note from someone in their company and to click a link or download an attachment.

Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain & other fraudulent activities.

(or)

Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords, credit card information from users etc.

Cyberspace:

This is a term coined by William Gibson, a science fiction writer in 1984. Cyberspace is where users mentally travel through matrices of data. Conceptually, cyberspace is the nebulous place where humans interact over computer networks. The term “cyberspace” is now used to describe the Internet and other computer networks. In terms of computer science, “cyberspace” is a worldwide network of computer networks that uses the Transmission Control Protocol/Internet Protocol (TCP/IP) for communication to facilitate transmission and exchange of data. Cyberspace is most definitely a place where you chat, explore, research and play.

Cybersquatting:

The term is derived from “squatting” which is the act of occupying an abandoned/unoccupied space/ building that the user does not own, rent or otherwise have permission to use. Cybersquatting, however, is a bit different in that the domain names that are being squatted are (sometimes but not always) being paid for by the cybersquatters through the registration process.

Cybersquatting is the illegal practice of registering or using a domain name that is similar to or identical to a trademark, service mark, personal name, or company name

Cybersquatters usually ask for prices far greater than those at which they purchased it. Some cybersquatters put up derogatory or defamatory remarks about the person or company the domain is meant to represent in an effort to encourage the subject to buy the domain from them.

This term is explained here because, in a way, it relates to cybercrime given the intent of cybersquatting.

Cybersquatting means registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark. In this nature, it can be considered to be a type of cybercrime. Cybersquatting is the practice of buying "domain names" that have existing businesses names.

In India, Cybersquatting is considered to be an Intellectual Property Right (IPR). In India, Cybersquatting is seen to interfere with "Uniform Dispute Resolution Policy" (a contractual obligation to which all domain name registrants are presently subjected to).

Cyberpunk: This is a term coined by Bruce Bethke, published in science fiction stories magazine in November 1983. According to science fiction literature, the words "cyber" and "punk" emphasize the two basic aspects of cyberpunk: "technology" and "individualism." The term "cyberpunk" could mean something like "anarchy
via machines" or "machine/computer rebel movement."

Cyberwarfare: Cyberwarfare means information attacks against an unsuspecting opponent's computer networks, destroying and paralyzing nations. This perception seems to be correct as the terms cyberwarfare and Cyberterrorism have got historical connection in the context of attacks against infrastructure. The term "information infrastructure" refers to information resources, including communication systems that support an industry, institution, or population. These types of Cyber-attacks are often presented as threat to military forces and the Internet has major implications for espionage and warfare.

Cybercrime and Information Security: Lack of information security gives rise to cybercrimes. Let us refer to the amended Indian Information Technology Act 2000 in the context of cybercrime. From an Indian perspective, the new version of the Act 2008 provides a new focus on "Information Security in India". "Cybersecurity" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. The term incorporates both the physical security of devices as well as the information stored therein. It covers protection from unauthorized access, use, disclosure, disruption, modification, and destruction.

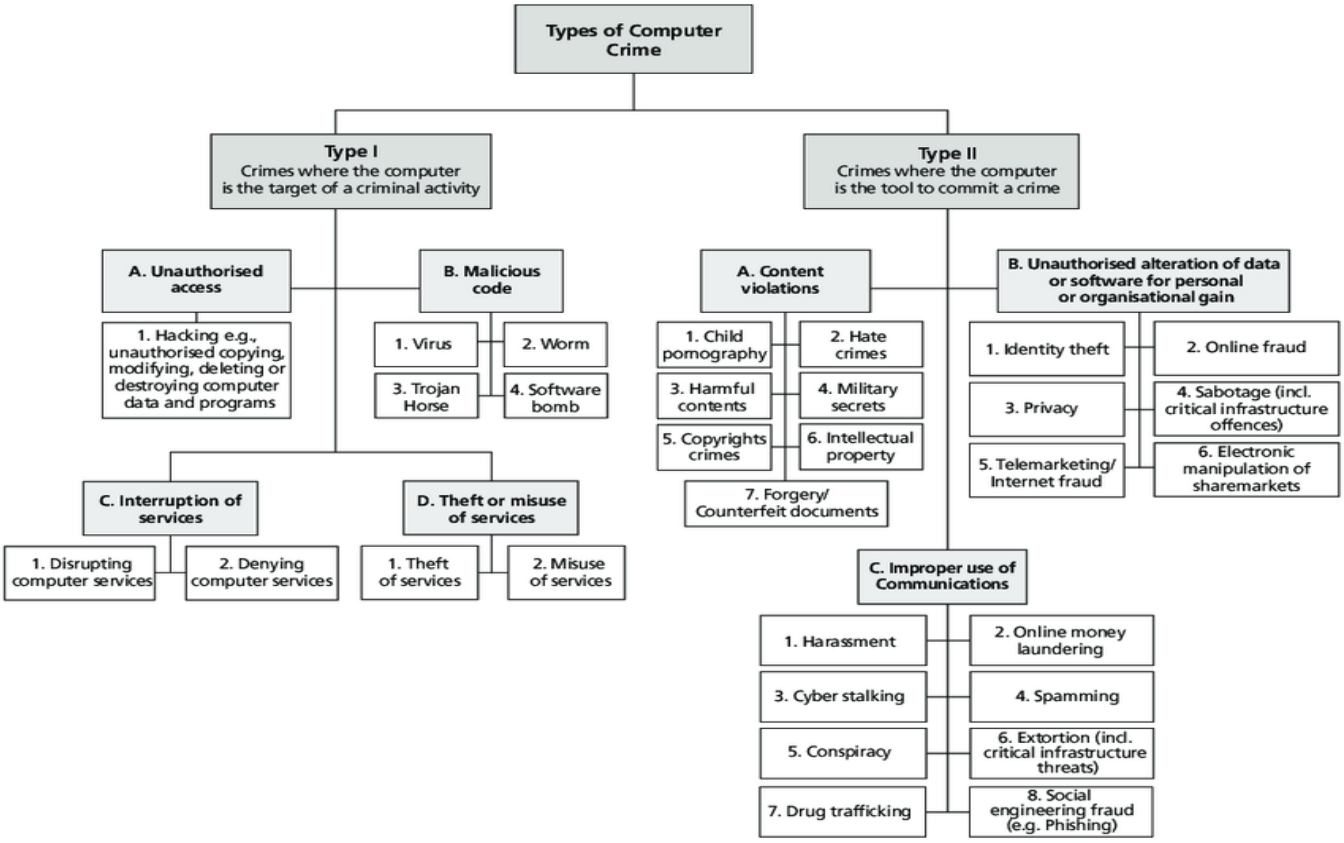
Where financial losses to the organization due to insider crimes are concerned (e.g., leaking customer data), often some difficulty is faced in estimating the losses because the financial impacts may not be detected by the victimized organization and no direct costs may be associated with the data theft. The 2008 CSI Survey on computer crime and security supports

this. Cybercrimes occupy an important space in information security domain because of their impact. The other challenge comes from the difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost (through loss/theft of laptops). Because of these reasons, reporting of financial losses often remains approximate. In an attempt to avoid negative publicity, most organizations abstain from revealing facts and figures about "security incidents" including cybercrime. In general, organizations perception about "insider attacks" seems to be different than that made out by security solution vendor. However, this perception of an organization does not seem to be true as revealed by the 2008 CSI Survey. Awareness about "data privacy" too tends to be low in most organizations. When we speak of financial losses to the organization and significant insider crimes, such as leaking customer data, such "crimes" may not be detected by the victimized organization and no direct costs may be associated with the theft

Cybercrime Trend Over the Years

Types of Cybercrime	*2004 (%)*	*2005 (%)*	*2006 (%)*	*2007 (%)*	*2008 (%)*
Denial of service (DoS)	39	32	25	25	21
Laptop theft	49	48	47	50	42
Telecom fraud	10	10	8	5	5
Unauthorized access	37	32	32	25	29
Viruses (addressed in Chapter 4)	78	74	65	52	50
Financial fraud	8	7	9	12	12
Insider abuse	59	48	42	59	44
System penetration	17	14	15	13	13
Sabotage	5	2	3	4	2
Theft/loss of proprietary information	10	9	9	8	9
• from mobile devices					4
• from all other sources					5
Website defacement (see Figs. 1.6–1.10)	7	5	6	10	6
Abuse of wireless network	15	16	14	17	14
Misuse of web application	10	5	6	9	11

Classification of Cybercrime



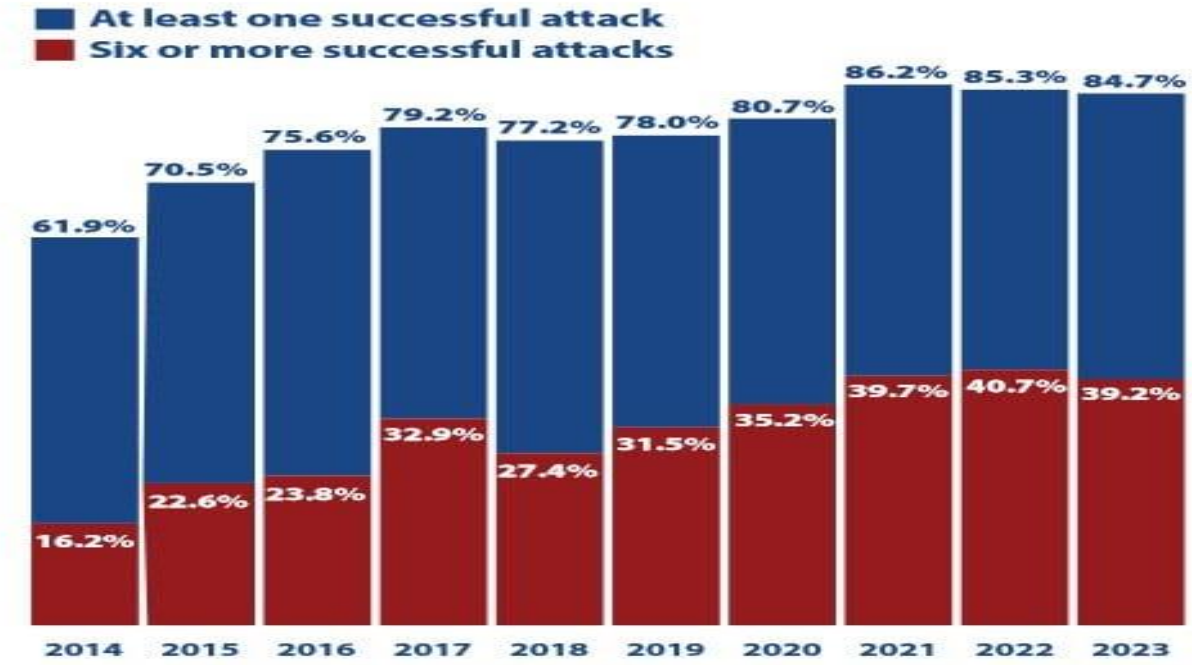


Figure 1: Percentages compromised by at least one successful attack and by six or more successful attacks.

2023 Cyberthreat Defense Report

	Cybercrime in Narrow Sense	*Cybercrime in Broad Sense*	
Role of computer	*Computer as an object* The computer/information stored on the computer is the subject/target of the crime	*Computer as a tool* The computer/or information stored on the computer constitutes an important tool for committing the crime	*Computer as the environment or context* The computer/information stored on the computer plays a non-substantial role in the act of crime, but does contain evidence of the crime
Examples	Hacking, computer sabotage, DDoS-attacks (distributed denial-of-service attacks), virtual child pornography	Computer fraud, forgery distribution of child pornography	Murder using computer techniques, bank robbery and drugs trade

"Crime is defined as an act or the commission of an act that is forbidden, or the omission of a duty that is commanded by a public law and that makes the off ender liable to punishment by that law." Cybercrimes are classified as follows:

- Cybercrime against individual
- Cybercrime against property
- Cybercrime against organization
- Cybercrime against society
- Crimes emanating from Usenet newsgroup

Cybercrime against individual

1. E-Mail Spoofing: A spoofed E-Mail is one that appears to originate from one source but has been sent from another source. For example, let us say, Roopa has an E-Mail address roopa@asianlaws.org. Let us say her boyfriend Suresh and she happen to have a show down. Then Suresh, having become her enemy, spoofed her E-Mail and sent vulgar messages to all her acquaintances. Since the E-Mails appear to have originated from Roopa, her friends could take offense and relationships could be spoiled for life.

2. Online Frauds: The most common types of online fraud are called phishing and spoofing. Phishing is the process of collecting your personal information through e-mails or websites claiming to be legitimate. This information can include usernames, passwords, credit card numbers, social security numbers, etc. Often times the e-mails direct you to a website where you can update your personal information. Because these sites often look "official," they hope you'll be tricked into disclosing valuable information that you normally would not reveal. This often times, results in identity theft and financial loss.

Spyware and viruses are both malicious programs that are loaded onto your computer without your knowledge. The purpose of these programs may be to capture or destroy information, to ruin computer performance or to overload you with advertising. Viruses can spread by infecting computers and then replicating. Spyware disguises itself as a legitimate application and embeds itself into your computer where it then monitors your activity and collects information.

3. Phishing, Spear Phishing and its various other forms such as Vishing and Smishing:

Phishing is the process of collecting your personal information through e-mails or websites claiming to be legitimate. This information can include usernames, passwords, credit card numbers, social security numbers, etc. Often times the e-mails directs you to a website where you can update your personal information. Because these sites often look "official," they hope you'll be tricked into disclosing valuable information that you normally would not reveal. This often times, results in identity theft and financial loss.

Spear Phishing is a method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering. Here is how Spear Phishing scams work; Spear Phishing describes any highly targeted Phishing attack. Spear phishers send E-Mail that appears genuine to all the employees or members within a certain company, government agency, organization or group. The message might look as if it has come from your employer, or from a colleague who might send an E-Mail message to everyone in the company; it could include requests for usernames or passwords. While traditional Phishing scams are designed to steal information from individuals, spear phishing scam works to gain access to a company's entire computer system.

Vishing (voice phishing) is a type of phishing attack that is conducted by phone and often targets users of Voice over IP (VoIP) services like Skype.

It's easy to for scammers to fake caller ID, so they can appear to be calling from a local area code or even from an organization you know. If you don't pick up, then they'll leave a voicemail message asking you to call back. Sometimes these kinds of scams will employ an answering service or even a call center that's unaware of the crime being perpetrated.

Once again, the aim is to get credit card details, birthdates, account sign-ins, or sometimes just to harvest phone numbers from your contacts. If you respond and call back, there may be an automated message prompting you to hand over data and many people won't question this, because they accept automated phone systems as part of daily life now.

Smishing (SMS phishing) is a type of phishing attack conducted using SMS (Short Message Services) on cell phones. Just like email phishing scams, smishing messages typically include a threat or enticement to click a link or call a number and hand over sensitive information.

Sometimes they might suggest you install some security software, which turns out to be malware.

Smishing example: A typical smishing text message might say something along the lines of, "Your ABC Bank account has been suspended. To unlock your account, tap here: https://bit.ly/2LPLdaU" and the link provided will download malware onto your phone. Scammers are also adept at adjusting to the medium they're using, so you might get a text message that says, "Is this really a pic of you? https://bit.ly/2LPLdaU" and if you tap that link to find out, once again you're downloading malware.

4. Spamming: People who create electronic Spam are called spammers. Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unrequested bulk messages indiscriminately. Although the most widely recognized form of Spam is E-Mail Spam, the term is applied to similar abuses in other media: instant messaging Spam, Usenet newsgroup Spam, web search engine Spam, Spam in blogs, wiki Spam, online classified ads Spam, mobile phone messaging Spam, Internet forum Spam, junk fax transmissions, social networking Spam, file sharing network Spam, video sharing sites, etc.

Spamming is difficult to control because it has economic viability – advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Spammers are numerous; the volume of unrequested mail has become very high because the barrier to entry is low.

Therefore, the following web publishing techniques should be avoided:

Repeating keywords;

• use of keywords that do not relate to the content on the site;

• use of fast meta refresh;

• redirection;

• IP Cloaking;

• use of colored text on the same color background;

• tiny text usage;

• duplication of pages with different URLs;

5. Cyber defamation: It is a cognizable (Software) offense. "Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person."

Cyber defamation happens when the above takes place in an electronic form. In other words, cyber defamation occurs when defamation takes place with the help of computers and/or the Internet. For example, someone publishes defamatory matter about someone on a website or sends an E-Mail containing defamatory information to all friends of that person.

6. Cyberstalking and harassment: The dictionary meaning of "stalking" is an "act or process of following prey stealthily – trying to approach somebody or something." Cyberstalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization. The behavior includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.

As the internet has become an integral part of our personal & professional lives, cyberstalkers take advantage of ease of communication & an increased access to personal information available with a few mouse clicks or keystrokes. They are 2 types of stalkers: Online Stalkers: aim to start the interaction with the victim directly with the help of the internet. Offline Stalkers: the stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim.

7. Computer Sabotage: The use of the Internet to stop the normal functioning of a computer system through the introduction of worms, viruses or logic bombs, is referred to as computer sabotage. It can be used to gain economic advantage over a competitor, to promote the illegal activities of terrorists or to steal data or programs for extortion purposes. Logic bombs are event-dependent programs created to do something only when a certain event (known as a trigger event) occurs. Some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date.

8. Pornographic Offenses: Child pornography means any visual depiction, including but not limited to the following:

1. Any photograph that can be considered obscene and/or unsuitable for the age of child viewer;
2. film, video, picture;
3. computer-generated image or picture of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

Child Pornography is considered an offense. The internet is being highly used by its abusers to reach and abuse. children sexually, worldwide. The Internet has become a household commodity in the urban areas of the nation. Its explosion has made the children a viable victim to the cybercrime. As the broad-band connections get into the reach of more and more homes,

larger child population will be using the Internet and therefore greater would be the chances of falling victim to the aggression of pedophiles. Pedophiles are the people who physically or psychologically coerce minors to engage in sexual activities, which the minors would not consciously consent too.

Here is how pedophiles operate:

Step 1: Pedophiles use a false identity to trap the children/teenagers.

Step 2: They seek children/teens in the kids' areas on the services, such as the Games BB or chat areas where the children gather.

Step 3: They befriend children/teens.

Step 4: They extract personal information from the child/teen by winning his/her confidence.

Step 5: Pedophiles get E-Mail address of the child/teen and start making contacts on the victim's E-Mail address as well. Sometimes, these E-Mails contain sexually explicit language.

Step 6: They start sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his/her inhibitions so that a feeling is created in the mind of the victim that what is being fed to him is normal and that everybody does it.

Step 7: At the end of it, the pedophiles set up a meeting with the child/teen out of the house and then drag him/her into the net to further sexually assault him/her or to use him/her as a sex object.

9. Password Sniffing: is a hacking technique that uses a special software application that allows a hacker to steal usernames and passwords simply by observing and passively recording network traffic. This often happens on public WiFi networks where it is relatively easy to spy on weak or unencrypted traffic. And yet, password sniffers aren't always used for malicious intent. They are often used by IT professionals as a tool to identify weak applications that may be passing critical information unencrypted over the Local Area Network (LAN). IT practitioners know that users download and install risky software at times in their environment, running a passive password sniffer on the network of a business to identify leaky applications is one legitimate use of a password sniffer.

Cybercrime against property

1. Credit Card Frauds: Credit card fraud is an inclusive term for fraud committed using a payment card, such as a credit card or debit card. The purpose may be to obtain goods or services, or to make payment to another account which is controlled by a criminal. The Payment Card Industry Data Security Standard (PCI DSS) is the data security standard created to help businesses process card payments securely and reduce card fraud. Credit card fraud can be authorised, where the genuine customer themselves processes a payment to another account

which is controlled by a criminal, or unauthorised, where the account holder does not provide authorisation for the payment to proceed and the transaction is carried out by a third party. Credit cards are more secure than ever, with regulators, card providers and banks taking considerable time and effort to collaborate with investigators worldwide to ensure fraudsters aren't successful. Cardholders' money is usually protected from scammers with regulations that make the card provider and bank accountable. The technology and security measures behind credit cards are becoming increasingly sophisticated making it harder for fraudsters to steal money.

2. Intellectual Property (IP) Crimes: With the growth in the use of internet these days the cyber crimes are also growing. Cyber theft of Intellectual Property (IP) is one of them. Cyber theft of IP means stealing of copyrights, software piracy, trade secrets, patents etc., using internet and computers. Copyrights and trade secrets are the two forms of IP that is frequently stolen. For example, stealing of software, business strategies etc. Generally, the stolen material is sold to the rivals or others for further sale of the product. This may result in the huge loss to the company who originally created it. Another major cyber theft of IP faced by India is piracy. These days one can get pirated version of movies, software etc. The piracy results in a huge loss of revenue to the copyright holder. It is difficult to find the cyber thieves and punish them because everything they do is over internet, so they erase the data immediately and disappear within fraction of a second.

3. Internet time theft: Such a theft occurs when an unauthorized person uses the Internet hours paid for by another person. Basically, Internet time theft comes under hacking because the person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. However, one can identify time theft if the Internet time has to be recharged often, even when one's own use of the Internet is not frequent. The issue of Internet time theft is related to the crimes conducted through identity theft.

Cybercrime against Organization

1. Unauthorized accessing of Computer: Hacking is one method of doing this and hacking is punishable offense. Unauthorized computer access, popularly referred to as hacking, describes a criminal action whereby someone uses a computer to knowingly gain access to data in a system without permission to access that data.

2. Password Sniffing: Password Sniffers are programs that monitor and record the name and password of network users as they login, jeopardizing security at a site. Whoever installs the Sniffer can then impersonate an authorized user and login to access restricted documents. Laws

are not yet set up to adequately prosecute a person for impersonating another person online. Laws designed to prevent unauthorized access to information may be effective in apprehending crackers using Sniffer programs.

3. Denial-of-service Attacks (DoS Attacks): It is an attempt to make a computer resource (i.e.., information systems) unavailable to its intended users. In this type of criminal act, the attacker floods the bandwidth of the victim's network or fills his E-Mail box with spam mail depriving him of the services he is entitled to access or provide. The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e., legitimate users) of a service from using it. A DoS attack may do the following: a. Flood a network with traffic, thereby preventing legitimate network traffic.

b. Disrupt connections between two systems, thereby preventing access to a service.

c. Prevent a particular individual from accessing a service.

d. Disrupt service to a specific system or person.

4. Virus attacks/dissemination of Viruses:

Computer virus is a program that can **"**infect**"** legitimate (valid) programs by modifying them to include a possibly **"**evolved**"** copy of itself. Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines. A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person. Viruses may also contain malicious instructions that may cause damage or annoyance; the combination of possibly Malicious Code with the ability to spread is what makes viruses a considerable concern. Viruses can often spread without any readily visible symptoms. Viruses can take some typical actions:

• Display a message to prompt an action which may set of the virus

• Delete files inside the system into which viruses enter

• Scramble data on a hard disk

• Cause erratic screen behavior

• Halt the system (PC)

• Just replicate themselves to propagate further harm

5. E-Mail bombing/Mail bombs: E-Mail bombing refers to sending a large number of E-Mails to the victim to crash victim**'**s E-Mail account (in the case of an individual) or to make victim**'**s mail servers crash (in the case of a company or an E-Mail service provider). Computer program can be written to instruct a computer to do such tasks on a repeated basis. In recent times, terrorism has hit the Internet in the form of mail bombings. By instructing a computer to repeatedly send E-Mail to a specified person**'**s E-Mail address, the cybercriminal can

overwhelm the recipient's personal account and potentially shut down entire systems. This may or may not be illegal, but it is certainly disruptive.

6. Salami Attack/Salami technique: These attacks are used for committing financial crimes. The idea here is to make the alteration so insignificant that in a single case it would go completely unnoticed; For example a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 2/- or a few cents in a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount every month.

7. Logic Bomb: A Logic Bomb is a piece of often-malicious code that is intentionally inserted into software. It is activated upon the host network only when certain conditions are met. Some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date.

8. Trojan Horse: A Trojan Horse, Trojan for short, is a term used to describe malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.

9. Data Diddling: A data diddling (data cheating) attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties computerize their systems.

10. Newsgroup Spam/Crimes emanating from Usenet newsgroup: This is one form of spamming. The word "Spam" was usually taken to mean Excessive Multiple Posting (EMP). The advent of Google Groups, and its large Usenet archive, has made Usenet more attractive to spammers than ever. Spamming of Usenet newsgroups actually predates E-Mail Spam.

11. Industrial spying/Industrial espionage: Spying is not limited to governments. Corporations, like governments, often spy on the enemy. The Internet and privately networked systems provide new and better opportunities for espionage (spying). "Spies" can get information about product finances, research and development and marketing strategies, an activity known as "industrial spying."

However, cyberspaces rarely leave behind a trail. Industrial spying is not new; in fact, it is as old as industries themselves. The use of the Internet to achieve this is probably as old as the Internet itself.

Traditionally, this has been the reserved hunting field of a few hundreds of highly skilled hackers, contracted by high-profile companies or certain governments via the means of registered organizations (it is said that they get several hundreds of thousands of dollars,

depending on the “assignment”). With the growing public availability of Trojans and Spyware material, even low-skilled individuals are now inclined to generate high volume profit out of industrial spying. This is referred to as “Targeted Attacks” (which includes “Spear Phishing”).

12. Computer network intrusions: “Crackers” who are often misnamed “Hackers can break into computer systems from anywhere in the world and steal data, plant viruses, create backdoors, insert Trojan Horses, or change user names and passwords. Network intrusions are illegal, but detection and enforcement are difficult. Current laws are limited and many intrusions go undetected. The cracker can bypass existing password protection by creating a program to capture logon IDs and passwords. The practice of **“**strong password**”** is therefore important.

13. Software piracy: This is a big challenge area indeed. Cybercrime investigation cell of India defines **“**software piracy**”** as theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

There are many examples of software piracy:

1. end-user copying: friends loaning disks to each other, or organizations under-reporting the number of software installations they have made, or organizations not tracking their software licenses;
2. hard disk loading with illicit means: hard disk vendors load pirated software;
3. counterfeiting: large-scale duplication and distribution of illegally copied software;
4. Illegal downloads from the Internet: by intrusion, by cracking serial numbers, etc.

Beware that those who buy pirated software have a lot to lose:

• getting untested software that may have been copied thousands of times over,
• the software, if pirated, may potentially contain hard-drive-infecting viruses,
• there is no technical support in the case of software failure, that is, lack of technical product support available to properly licensed users,
• there is no warranty protection,
• there is no legal right to use the product, etc.

Cybercrime against Society

1. Forgery: Counterfeit currency notes, postage, and revenue stamps, marksheets, etc. can be forged using sophisticated computers, printers and scanners. Outside many colleges there are miscreants soliciting the sale of fake mark-sheets or even degree certificates. These are made using computers and high-quality scanners and printers. In fact, this is becoming a booming business involving large monetary amount given to student gangs in exchange for these bogus but authentic looking certificates.

2. Cyberterrorism: Cyberterrorism is a controversial term. Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation. It is also sometimes considered an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.

3. Web Jacking: Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it). Thus, the first stage of this crime involves "password sniffing". The actual owner of the website does not have any more control over what appears on that website.

Crimes emanating from Usenet newsgroup:

By its very nature, Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabelled or are deceptive in another way. Therefore, it is expected that you will use caution and common sense and exercise proper judgment when using Usenet, as well as use the service at your own risk.

Usenet is a popular means of sharing and distributing information on the Web with respect to specific topic or subjects. Usenet is a mechanism that allows sharing information in a many-to-many manner. The newsgroups are spread across 30,000 different topics.

Cybercrime: The Legal Perspectives

The topic "Cybercrime: The Legal Perspectives" explores the legal frameworks, challenges, and policies associated with addressing and combating cybercrime. Here is a structured overview:

1. Introduction

Definition of Cybercrime: Unlawful activities carried out using computers or the internet, including hacking, identity theft, online fraud, cyberstalking, and ransomware attacks.

Importance of Legal Perspectives: Understanding the legal dimensions helps develop robust mechanisms to prevent, investigate, and prosecute cybercrime effectively.

2. Types of Cybercrimes

Financial Cybercrimes: Fraud, phishing, credit card scams.

Cyberterrorism: Attacks targeting critical infrastructure.

Identity Theft: Misuse of personal data for illegal purposes.

Intellectual Property Crimes: Piracy, counterfeiting (not genuine, but copied so that it looks like the real thing), and unauthorized use of content.

Cyberbullying and Harassment: Online abuse, stalking (movie slowly and silently towards victom), and defamation.

3. Legal Frameworks to Combat Cybercrime

International Laws:

Budapest Convention (2001): The first international treaty to address internet and computer crime.

UN Guidelines on Cybercrime: Frameworks promoting global cooperation.

National Laws:

Examples:

USA: Computer Fraud and Abuse Act (CFAA).

India: Information Technology Act, 2000.

EU: General Data Protection Regulation (GDPR).

4. Challenges in Cybercrime Laws

Jurisdictional Issues: Cross-border nature of cybercrimes complicates enforcement.

Evolving Technology: Laws struggle to keep pace with technological advancements.

Anonymity and Encryption: Makes identifying perpetrators difficult.

Lack of Global Consensus: Varying definitions and legal frameworks.

Cybersecurity vs. Privacy: Striking a balance between user privacy and law enforcement needs.

5. Legal Procedures for Investigation and Prosecution

Evidence Collection:

Digital forensics and admissibility of electronic evidence.

International Cooperation:

Extradition treaties, mutual legal assistance treaties (MLATs).

Role of Cybersecurity Agencies:

National Computer Emergency Response Teams (CERTs).

Interpol and Europol collaborations.

6. Policy Recommendations

Harmonizing Laws: Establishing uniform international laws.

Public-Private Partnerships: Collaboration between governments and tech companies.

Capacity Building: Training law enforcement in cybercrime detection and prevention.

Awareness Campaigns: Educating the public on cyber hygiene and reporting mechanisms.

7. Ethical and Social Considerations

Data Privacy: Ensuring laws do not infringe on individual freedoms.

Digital Divide: Addressing unequal access to resources that prevent cybercrime.

Victim Support: Mechanisms for assisting victims of cybercrime.

Cybercrimes: An Indian Perspective

1. Introduction

Relevance to India:

- Rapid digitalization through initiatives like Digital India.
- Massive internet user base exceeding 900 million in 2024.
- Growth in e-commerce, online banking, and digital payments.

2. Types of Cybercrimes Prevalent in India

Financial Frauds:

- Online scams (e.g., phishing, vishing, UPI fraud).
- Fake investment schemes and Ponzi apps.

Hacking:

- Website defacements and data breaches.
- Corporate espionage targeting sensitive data.

Identity Theft:

- Misuse of Aadhaar or PAN card information.
- Unauthorized access to bank accounts or online wallets.

Cyberbullying and Harassment:

- Online defamation, trolling, and stalking.
- Cases involving women and children are significant.

Ransomware Attacks:

- Organizations held hostage with encrypted data.
- Demands for payment **in cryptocurrencies.**

Cyberterrorism:

- Attacks on critical infrastructure like power grids and transportation systems.
- Recruitment through online propaganda.

Digital Piracy:

- Unauthorized downloading of software, movies, and music.
- Deepfakes and Misinformation:
- Circulation of fake news and manipulated media.

4. Challenges Specific to India

Lack of Awareness:

- Limited digital literacy among rural and semi-urban populations.
- Low reporting rates due to lack of trust in law enforcement.

Jurisdictional Complexity:

- Many crimes have a cross-border element, complicating enforcement.
- Inadequate Infrastructure:
- Insufficient training for law enforcement and judiciary in handling cybercrime.
- Shortage of forensic labs and experts.

Privacy vs. Security:

- Debates over surveillance laws like Section 69 of the IT Act.
- Dark Web and Cryptocurrency:
- Challenges in tracking anonymous activities.

Emerging Threats:

- IoT device exploitation.
- AI-powered phishing and cyberattacks.

5. Legal Framework in India

Information Technology Act, 2000 (IT Act):

- Governs cybercrime and e-commerce activities.
- Section 66: Addresses hacking and identity theft.
- Section 67: Punishes publication of obscene material.

Indian Penal Code (IPC):

- Relevant sections (e.g., 420 for cheating, 463 for forgery).

Data Protection Laws:

- The Digital Personal Data Protection Act, 2023.
- Aims to safeguard individual privacy.

National Initiatives:

- Indian Cyber Crime Coordination Centre (I4C): Centralized response to cybercrime.
- CERT-In: Tracks and mitigates cybersecurity incidents.
- Cybercrime Reporting Portal: Allows citizens to report crimes online.

6. Initiatives and Best Practices

Government Initiatives:

- Awareness campaigns like Cyber Swachhta Kendra.
- Cybersecurity workshops and school programs.

Public-Private Collaboration:

- Partnerships with tech companies to improve fraud detection.

Capacity Building:

- Training police, judiciary, and forensic experts in handling digital evidence.

Encouraging Research:

- Promoting R&D in indigenous cybersecurity solutions.

7. Way Forward

Strengthening Legal Framework:

- Periodic updates to the IT Act to keep up with technology.

International Cooperation:

- Collaborating with global organizations to combat transnational crimes.

Enhanced Cyber Hygiene:

- Encouraging individuals to use strong passwords, update software, and avoid suspicious links.

Robust Data Protection:

- Enforcing strict data privacy standards for organizations.

Critical Infrastructure Security:

- Focusing on sectors like banking, healthcare, and telecom.

Cybercrimes: Indian Statistics:

Cybercrime in India has seen a significant surge in recent years, reflecting the nation's rapid digital transformation and the accompanying vulnerabilities.

Here's an overview of the latest statistics and trends:

1. Rising Number of Cybercrime Complaints

Daily Complaints: In the first four months of 2024, India registered an average of over 7,000 cybercrime complaints daily. **-Times of India**

Yearly Comparison: This represents a 113.7% increase compared to the period between 2021 and 2023, and a 60.9% rise from 2022 to 2023. -Times of India

2. Financial Impact

Total Losses: Between January and April 2024, Indians lost over ₹1,750 crore to cyber frauds. **Economic Times**

Types of Scams:

Investment Scams: Over 62,687 complaints led to losses of approximately ₹222 crore. Economic Times

Trading Scams: 20,043 cases resulted in losses totaling ₹1,420 crore. **Economic Times**

Digital Arrest Scams: 4,599 incidents caused losses of around ₹120 crore. **Economic Times**

Dating App Scams: 1,725 complaints led to losses amounting to ₹13.23 crore**. Economic Times**

3. Yearly Growth in Cybercrime Reports

2019: 26,049 complaints

2020: 257,777 complaints

2021: 452,414 complaints

2022: 966,790 complaints

2023: 1,556,218 complaints

2024 (Jan-Apr): 740,957 complaints

Economic Times

4. Predominant Motives Behind Cybercrimes (Data Driven News, Analysis, Videos)

Fraud: Accounts for 64.8% of cases, with 42,710 incidents reported in 2022.

Extortion: Comprises 5.5% of cases, totaling 3,648 incidents.

Sexual Exploitation: Makes up 5.2% of cases, with 3,434 incidents reported.

5. State-Wise Distribution of Cybercrime Cases in 2022

Telangana: 15,297 cases

Karnataka: 12,556 cases

Uttar Pradesh: 10,117 cases

6. Government Initiatives

Indian Cyber Crime Coordination Centre (I4C): Established to provide a framework for law enforcement agencies to address cybercrime. Economic Times

National Cybercrime Reporting Portal: Facilitates the reporting of cyber incidents by citizens. Economic Times

Preventive Measures: Blocking fraudulent phone numbers, freezing mule bank accounts, and collaborating with fintech companies to enhance fraud detection.

Cybercrime & The Indian It Act 2000

In India, the ITA 2000 was enacted after the United Nation General Assembly Resolution A/RES/51/162 in January 30, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This was the first step toward the Law relating to E-Commerce at international level to regulate an alternative form of commerce and to give legal status in the area of E-Commerce. It was enacted taking into consideration UNICITRAL model of Law on Electronic Commerce (1996).

Hacking and the Indian Laws:

Section Ref. and Title	Chapter of the Act & Title	Crime	Punishment
Sec.43 (Penalty for damage to computer, computer system etc)	Chapter IX Penalties and Adjudication	Damage to computer system etc.	Compensation for Rs. 1 Crore
Sec.66 (Hacking with computer system)	Chapter XI Offences	Hacking (with intent or knowledge)	Fine of Rs. 2 Lakhs & Imprisonment for 3 years
Sec.67 (Publishing of information which is obscene in electronic form)	Chapter XI Offences	Publication of obscene material in electronic form	Fine of Rs. 1 Lakh & Imprisonment of 5 years and double conviction on second offence
Sec.68 (Power of controller to give directions)	Chapter XI Offences	Not complying with directions of controller	Fine up to Rs. 2 Lakhs & Imprisonment of 3 years
Sec.70 (Protected System)	Chapter XI Offences	Attempting or securing access to computer of another person without his/her knowledge	Imprisonment up to 10 Years
Sec.72 (Penalty for breach of confidentiality and privacy)	Chapter XI Offences	Attempting or securing access to computer for breaking confidentiality	Fine up to Rs. 1 Lakh and Imprisonment up to 2 years
Sec.73 (Penalty for publishing Digital Signature Certificate false in certain particulars)	Chapter XI Offences	Publishing false Digital Signatures, false in certain particulars	Fine of Rs.1 Lakh or imprisonment of 2 years or both
Sec.74 (Publication for fraudulent purpose)	Chapter XI Offences	Publishing of Digital Signatures for fraudulent purpose	Imprisonment for the term of 2 years and fine of Rs. 1 Lakh

Table: The key provisions under the Indian ITA 2000 (before the amendment)

A Global Perspective on Cybercrimes

In Australia, cybercrime has a narrow statutory meaning as used in the Cyber Crime Act 2001, which details offenses against computer data and systems. However, a broad meaning is given to cybercrime at an international level. In the Council of Europe's (CoE's) Cyber Crime Treaty, cybercrime is used as an umbrella term to refer to an array of criminal activity including offenses against computer data and systems, computer-related offenses, content offenses and copyright offenses.

This wide definition of cybercrime overlaps in part with general offense categories that need not be Information & Communication Technology (ICT)-dependent, such as white-collar crime and economic crime.

Although this status is from the International Telecommunication Union (ITU) survey conducted in 2005, we get an idea about the global perspective. ITU activities on countering Spam can be read by visiting the link www.itu.int/spam (8 May 2010). The Spam legislation scenario mentions “none” about India as far as E-Mail legislation in India is concerned.

The linkage of cybersecurity and critical infrastructure protection has become a big issue as a number of countries have begun assessment of threats, vulnerabilities and started exploring mechanisms to redress them. Recently, there have been a number of significant developments such as

1. August 4, 2006 Announcement: The US Senate ratifies CoE Convention on Cyber Crime. The convention targets hackers, those spreading destructive computer viruses, those using the Internet for the sexual exploitation of children or the distribution of racist material, and terrorists attempting to attack infrastructure facilities or financial institutions. The Convention is in full accord with all the US constitutional protections, such as free speech and other civil liberties, and will require no change to the US laws.

2. In August 18, 2006, there was a news article published “ISPs Wary About ‘Drastic Obligations’ on Web Site Blocking.” European Union (EU) officials want to debar suspicious websites as part of a 6-point plan to boost joint antiterrorism activities. They want to block websites that incite terrorist action. Once again it is underlined that monitoring calls, Internet and E-Mail traffic for law enforcement purposes is a task vested in the government, which must reimburse carriers and providers for retaining the data.

3. CoE Cyber Crime Convention (1997–2001) was the first international treaty seeking to address Internet crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. More than 40 countries have ratified the Convention to date.

Cybercrime and the Extended Enterprise:

The concept of the extended enterprise refers to organizations' interconnected networks, including their supply chains, partners, vendors, customers, and even remote employees. While this interconnectedness drives efficiency and innovation, it also creates a broader attack surface, making enterprises increasingly vulnerable to cybercrime.

Key Cybercrime Risks for the Extended Enterprise

1. **Supply Chain Attacks**
    - Cybercriminals exploit weaker security in third-party vendors or partners to infiltrate larger organizations.

- Example: The SolarWinds attack, where a vendor's compromised software led to breaches in numerous organizations.

2. **Ransomware in Partnerships**
   - Attackers target extended networks to spread ransomware through shared systems or data repositories.
3. **Data Breaches and Theft**
   - Sensitive information shared with partners can be stolen if third parties lack robust cybersecurity practices.
   - Cloud-based systems often become prime targets.
4. **Phishing and Social Engineering**
   - Cybercriminals deceive employees or partners to gain unauthorized access to networks or credentials.
5. **IoT and Edge Vulnerabilities**
   - Devices at the edges of the enterprise (IoT sensors, remote systems) are often less secure, making them entry points for attacks.

Challenges in Securing the Extended Enterprise

1. **Diverse Security Standards**
   - Different entities in the extended network may have inconsistent security practices, creating vulnerabilities.
2. **Limited Visibility**
   - Enterprises often lack insight into the security postures of their partners or suppliers.
3. **Increased Attack Surface**
   - Every connected device, partner system, or endpoint adds potential entry points for attackers.
4. **Compliance Complexities**
   - Enterprises must ensure that all entities in the network comply with relevant data protection regulations like GDPR, HIPAA, or CCPA.
5. **Trust Management**
   - Trust between enterprises and third parties can be exploited if proper monitoring and controls are absent.

Best Practices to Mitigate Cybercrime in the Extended Enterprise

1. **Strengthen Vendor Risk Management**
   - Conduct regular audits and risk assessments of third-party vendors.

- Enforce strict contractual obligations for cybersecurity.

2. **Adopt Zero-Trust Architecture**
   - Implement "never trust, always verify" principles for both internal and external network access.
3. **Enhance Endpoint and Edge Security**
   - Deploy endpoint detection and response (EDR) tools and ensure regular updates for IoT and edge devices.
4. **Employee and Partner Training**
   - Educate stakeholders on recognizing phishing and social engineering tactics.
5. **Data Encryption and Secure Communication**
   - Encrypt sensitive data both in transit and at rest.
6. **Cyber Threat Intelligence Sharing**
   - Collaborate with partners, industry groups, and government bodies to share intelligence and improve defenses.
7. **Incident Response Planning**
   - Develop a coordinated response plan that includes third parties to minimize the impact of breaches.

Emerging Solutions for the Extended Enterprise

1. **Blockchain Technology**
   - Offers secure, tamper-proof systems for verifying transactions and communications in supply chains.
2. **AI-Powered Threat Detection**
   - Uses machine learning to identify unusual activities across networks, including those of third parties.
3. **Secure Access Service Edge (SASE)**
   - Integrates networking and security functions to ensure secure, seamless connectivity for remote and third-party users.

Cybercrime Era: Survival Mantra for the Netizens

The term “Netizen” was coined by Michael Hauben. Quite simply, “Netizens” are the Internet users. Therefore, by corollary, “Netizen” is someone who spends considerable time online and also has a considerable presence online (through websites about the person, through his/her active blog contribution and/or also his/her participation in the online chat rooms). The 5P Netizen mantra for online security is:

a. Precaution

b. Prevention

c. Protection

d. Preservation

e. Perseverance

For ensuring cyber safety, the motto for the “Netizen” should be “Stranger is Danger!” If you protect your customer’s data, your employee’s privacy and your own company, then you are doing your job in the grander scheme of things to regulate and enforce rules on the Net through our community. NASSCOM urges that cybercrime awareness is important, and any matter should be reported at once. This is the reason they have established cyberlabs across major cities in India

More importantly, users must try and save any electronic information trail on their computers. That is all one can do until laws become more stringent or technology more advanced. Some agencies have been advocating for the need to address protection of the Rights of Netizens. There are agencies that are trying to provide guidance to innocent victims of cybercrimes. However, these NGO-like efforts cannot provide complete support to the victims of cybercrimes and are unable to get the necessary support from the Police. There are also a few incidents where Police have pursued false cases on innocent IT professionals. The need for a statutorily empowered agency to protect abuse of ITA 2000 in India was, therefore, a felt need for quite some time.

PCET

Pimpri Chinchwad University

School of Computer Applications

BSc (CS)-II SEM-IV

Unit No. 02 Cybercrime

Mobile and Wireless Devices:

Mobile and wireless devices have revolutionized communication and connectivity, playing a critical role in personal and professional lives. However, they also present unique challenges, especially concerning security, efficiency, and management. Below is an overview of their characteristics, applications, benefits, and challenges.

Overview of Mobile and Wireless Devices

1. **Definition**
    - **Mobile Devices**: Portable electronic devices such as smartphones, tablets, laptops, and wearables designed for mobility and communication.
    - **Wireless Devices**: Devices that communicate without physical cables, often relying on technologies like Wi-Fi, Bluetooth, or cellular networks.
2. **Key Features**
    - Portability
    - Wireless connectivity
    - Built-in sensors (GPS, accelerometers, biometric sensors)
    - Compatibility with various applications and services

Wireless Technologies in Use

1. **Wi-Fi**
    - Used for local wireless networking with high-speed internet access.
2. **Bluetooth**
    - Enables short-range communication between devices like headphones, wearables, and IoT gadgets.
3. **Cellular Networks (3G, 4G, 5G)**
    - Provide wide-area network access for calls, messaging, and internet services.
4. **Near Field Communication (NFC)**
    - Used for contactless payments and data sharing.
5. **Zigbee and Z-Wave**
    - Low-power protocols primarily used in IoT devices.

Applications of Mobile and Wireless Devices

1. **Personal Use**
    - Communication (voice, text, video)
    - Entertainment (streaming, gaming)
    - Navigation and fitness tracking
2. **Business and Industry**
    - Remote work and collaboration tools
    - Field service management
    - Customer engagement through apps
3. **Healthcare**
    - Mobile health apps for tracking vitals
    - Remote patient monitoring
4. **Education**
    - E-learning platforms
    - Interactive educational tools
5. **IoT Integration**
    - Smart home devices and industrial automation

Advantages

1. **Mobility and Convenience**
    - Access to information and services anytime, anywhere.
2. **Increased Productivity**
    - Seamless communication and collaboration tools.
3. **Cost-Effective Communication**
    - Reduced costs with internet-based communication (e.g., VoIP, messaging apps).
4. **Enhanced User Experience**
    - Customization through apps and intelligent systems.
5. **Improved Healthcare and Safety**
    - Real-time monitoring and emergency alerts.

Challenges and Risks

1. **Security Issues**
    - Vulnerabilities to cyberattacks such as data breaches, malware, and phishing.
2. **Battery Life**
    - Limited power sources require frequent recharging.
3. **Data Privacy**
    - Increasing concerns over data collection by apps and devices.

4. **Connectivity Dependence**
    - Productivity heavily relies on consistent network access.
5. **Interference and Compatibility**
    - Overlapping frequencies may cause interference; devices from different manufacturers may lack seamless integration.

Future Trends

1. **5G and Beyond**
    - Faster speeds and reduced latency will expand possibilities for AR/VR, IoT, and real-time applications.
2. **Edge Computing**
    - Processing data closer to the source for quicker responses and reduced network load.
3. **AI and Machine Learning**
    - Enhanced capabilities in personal assistants, predictive analytics, and device optimization.
4. **Wearables and Implantable Devices**
    - Increased use of smartwatches, fitness bands, and health-monitoring implants.
5. **Blockchain for Security**
    - Improved device authentication and secure transactions.

Proliferation of Mobile and Wireless Devices

Mobile Technologies – Definition, Types, Uses, Advantages

Mobile technology is a type of technology in which a user utilizes a mobile phone to perform communications-related tasks, such as communicating with friends, relatives, and others. It is used to send data from one system to another. Portable two-way communications systems, computing devices, and accompanying networking equipment make up mobile technology. Mobile technology is largely employed in cellular communication systems and other related areas. It employs a network architecture that allows multiple transmitters to deliver data on a single channel at the same time. Because it reduces the potential of frequency interference from two or more sources, this platform allows multiple users to use single frequencies. The channel has evolved over time.

This is fast expanding; its applications are getting increasingly broad over time, and it is gradually replacing other similar sources of communication on the market, such as post offices and landlines. Mobile technology has progressed from a simple phone and texting device to a multi-tasking system that can be used for GPS navigation, internet browsing, gaming, and

instant messaging, among other things. With the rise, experts claim that the future of computer technology is dependent on wireless networking and mobile computing.

Through tablets and small PCs, mobile technology is becoming increasingly popular. This smartphone system has since been improved to a big multitasking computer that can be used for GPS navigation, gaming, internet browsing, and instant messaging. Tablets and portable laptops have increased the adoption of mobile technology. The mobile networks that connect these devices are referred to as wireless systems. They allow speech, data, and (mobile) apps to be shared between mobile devices.

Mobile technology is becoming increasingly prevalent. Smartphone users have surpassed 3 billion, and the global mobile workforce is expected to reach 1.87 billion by 2022. Any gadget with internet capabilities that can be accessed from anywhere is referred to as mobile technology. Smartphones, tablets, some iPods, and laptops already fall within this category, but this list will undoubtedly grow in the future years.

Types of Mobile Technologies

Followings are the few famous mobile technologies:

1. SMS
2. MMS
3. 4G
4. 3G
5. GSM
6. CDMA
7. Wi-Fi

1. SMS: "SMS" stands for "Short Message Service." It is now the most widely used and oldest text messaging service. SMS are also sent over cellular networks; therefore you'll need a wireless plan and a wireless carrier. SMS is fast gaining popularity in the world as a low-cost messaging medium. Every text message delivered to a cell phone has become known as SMS. Messages can usually be up to 140 characters long. SMS was originally developed for GSM phones, although it is now supported by all major cellular phone networks.

Although SMS is most commonly used for text messaging between friends or coworkers, it also has a variety of additional uses. For example, SMS subscription services can send weather, news, sports updates, and financial quotes to consumers' phones. Employees may also be notified of sales requests, service stops, and other business-related information via SMS.

Fortunately, text messages sent via SMS do not require the receiver's phone to be turned on in order for the message to be delivered. The message will be kept in the SMS service until the receiver switches on his or her phone, at which point it will be transmitted to the recipient's phone. Most cell phone providers enable you to send a specific amount of text messages per month for free.

2. MMS: MMS (Multimedia Messaging Service) messaging is a standard method of delivering multimedia material, including messages. MMS, as opposed to SMS, can send up to forty seconds of video, one picture, a multi-image slideshow, or audio. MMS texting will be supported by the majority of contemporary devices. MMS capability is typically embedded within the text message interface and is turned on automatically when needed. If you enter in a text-only message, for example, it will be transmitted by SMS. If you include a graphic or video, the multimedia part will be sent via MMS. Similarly, if someone sends you a multimedia message, your phone will automatically receive the file via MMS.

An MMS message can convey rich media content to mobile devices at any time and from any location. It is a powerful and effective tool that assists businesses in reinforcing and deepening client loyalty by providing crucial information about their products and services. Because MMS texts are packed with photographs and videos, they are a significant marketing communication tool. As well as other audios. MMS is a cutting-edge method of communicating with others via mobile devices. Text messages are more successful because they deliver valuable information and services to the recipient. The more a corporation approaches its customers, the more probable it is to form a long-term brand partnership.

3. 3G: The third letter in the designation 3G stands for third-generation access technology, which allows mobile phones to connect to the internet. Every new technology introduces new frequency bands and data transmission rates.

The first generation emerged in the 1980s. First-generation uses large phones that had to be mounted on top of cars because they were too heavy to hold. Text messaging was made possible by the second-generation network, which became available in the 1990s. This huge and game-changing advancement also provided a more secure network and laid the path for today's ubiquitous 3G and 4G technology.

The development of 3G connection-based networks in 2001 marked the start of mainstream Internet use on mobile phones. Soon after, smartphones were introduced, bringing all of the capabilities of a device into the palm of your hand. The signals are transmitted by a network of telephone towers, ensuring robust and relatively rapid long-distance communication. The

user's mobile phone is receiving data from the tower nearest to it. Although it may not appear complicated, 3G technology was revolutionary at the time it was introduced.

Upload speeds of up to 3 Mbps are possible on 3G networks. For example, about 15 seconds for uploading a 3-minute MP3 song. The fastest 2G phones, on the other hand, may get up to 144Kbps For example, about 8 minutes to download a 3-minute song. 3G systems are intended for digital phones with a full-screen display and better connectivity.

4. 4G: The fourth generation of mobile networking technology is known as 4G, which comes after the 2G and 3G networks. Although it's commonly referred to as 4G LTE, this isn't exactly right because LTE is just one sort of 4G. Most mobile network service providers use it now since it is the most developed technology.

However, as you may have heard, 5G is becoming operational alongside current 3G and 4G mobile networks. When it initially came out, 4G revolutionized how we use the mobile internet. Despite the fact that 3G networks were relatively limited, 4G network connectivity allowed consumers to browse the internet and watch HD films on their mobile devices, thereby turning smartphones into laptops.

Most tasks that you can do on a laptop or desktop computer can now be done on mobile devices such as smartphones or tablets. No matter how much data you require, 4 G networks allow you to keep consistent speeds practically anywhere. 4G was launched in the United Kingdom in 2012. Currently, the number of mobile subscribers using 3G outnumbers those using 4G. Expect this to alter in the coming years as 4G contracts become more affordable and 4G network coverage increases across the UK.

Premium 4G offers download speeds of around 14 Mbps, which is over five times quicker than the 3G network's predecessor. 4G networks can currently attain speeds of up to 150 Mbps, allowing users to download gigabytes of data in minutes, if not seconds, rather than hours as with 3G networks. Uploading data is also significantly faster with 4G – normal upload speeds are over 8 Mbps, with theoretical rates of up to 50 Mbps, whereas 3G upload speeds are under 0.5 Mbps.

5. Global System for Mobile technology: The (GSM) is an acronym for Global System for Mobile Communication. GSM is a cellular technology that is open and digital and is used for mobile communication. It operates on the 850 MHz, 900 MHz, 1800 MHz, and 1900 MHz frequency ranges. It employs a hybrid of FDMA and TDMA.

6. Code Division Multiple Access: (CDMA) is an acronym for code division multiple access. It is a channel access mechanism that also serves as an example of multiple access. Multiple

access simply means that data from multiple transmitters can be delivered onto a single communication channel at the same time.

7. Wi-Fi (Wireless Fidelity): Wi-Fi is a wireless networking technology that allows us to connect to a network or to other computers or mobile devices across a wireless channel. Data is delivered in a circular region over radio frequencies in Wi-Fi. Wi-Fi (Wireless Fidelity) is a generic acronym for a communication standard for a wireless network that functions as a Local Area Network without the use of cables or other types of cabling.

Use of Mobile technology

- The incorporation of mobile technology into business has aided telecollaboration. Now, people could connect from anywhere using mobile technology, and access the papers and documents they need to complete collaborative work.
- Work is being redefined by mobile technologies. Employees are no longer confined to their desks; they can work from anywhere in the world.
- Mobile technology can help your company save time and money. Employees who work from home save thousands on a regular basis. Mobile phones eliminate the need for costly technology like landline carrier services. Cloud-based services are less expensive than traditional systems. Technology can also help your company become more flexible and productive.
- Mobile technology has the potential to boost productivity significantly. Mobile application integration saves an average of 7.5 hours per week per employee. Workers can also become more productive with the use of smartphones and mobile gadgets.
- The popularity of cloud-based services has skyrocketed in recent years. Cloud-based mobile technology applications have been seen to be more useful than any smartphone, particularly in terms of available storage space.

Advantages of Mobile technology

- Through a variety of applications, we can now stay in touch with our friends and family members anytime we choose. We may now communicate or video visit with anybody we want by just using our cell phone or cell phone. Aside from that, the portable keeps us informed about the rest of the globe.
- Today’s mobile phones have made our day-to-day activities much more natural. Today, one may check the current traffic situation on their phone and make appropriate decisions to arrive on time. The weather is also a factor.

- With the advancement of mobile technology, the entire gaming world is now under one roof. When we are tired of monotonous work or during breaks, we can listen to music, view movies, watch our favorite shows, or simply watch a video of our favorite song.
- Mobile phones are being used for a variety of legitimate tasks, including meeting schedules, sending and receiving documents, providing introductions, warnings, and job applications, among others. Cell phones have become an indispensable tool for all working people.
- These days, mobile phones are also used as a wallet to make payments. Utilities might be used to send money to friends, relatives, and others right now.

Disadvantages of Mobile technology

- The modern family has become reliant on mobile phones. In any case, when we don't have to travel, we surf the internet, play around, and create a genuine junkie.
- Because of the widespread use of mobile technology, people nowadays don't meet in person but rather tweet or comment on social media sites.
- Because of the widespread use of mobile devices, there is a major risk of losing one's protection. By efficiently reading through your web-based social networking account, anyone may now easily obtain data such as where you reside, your loved ones, what you do for a living, where you live, and so on.
- Mobile phone prices have risen in tandem with their worth. People nowadays spend a significant amount of money on cell phones, which could be better spent on more useful things like education or other beneficial items throughout our lives

Trends in Mobility

Mobile device and connection trends: By 2023, there will be 13.1 billion global mobile devices and connections (up from 8.8 billion in 2018). Mobile devices are evolving from lower-generation network connectivity (2G) to higher-generation network connectivity (3G, 3.5G, 4G or LTE, and now 5G).

Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking.

- iPhone. from Apple and Google-led-Android. phones are the best examples of this

trend and there are plenty of other developments that point in this direction.

- This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans.
- It is worth noting the trends in mobile computing; this will help readers to realize the seriousness of cybersecurity issues in the mobile computing domain.

Mobility has expanded the attack surface for cybercriminals, leading to an evolution of cybercrime trends that exploit mobile devices, networks, and applications.

Here are the key trends in mobility within the context of cybercrime:

1. Mobile Malware Surge

- **Types of Malwares**: Adware, ransomware, spyware, and banking Trojans specifically targeting mobile devices.
- **Distribution Channels**:
    - Fake apps in third-party app stores.
    - Phishing campaigns delivering malware via text messages, social media links, or QR codes.
    - Exploiting vulnerabilities in legitimate apps or operating systems.
- Example: Malware like FluBot or Joker, which steal sensitive data such as login credentials or banking details.

2. Smishing (SMS Phishing)

- Cybercriminals increasingly use SMS to trick users into clicking malicious links or sharing sensitive data.
- Exploitation of OTPs (One-Time Passwords) sent via SMS, especially for financial fraud.
- Smishing is often combined with fake delivery notices, promotional messages, or impersonation scams.

3. Mobile Payment Fraud

- **Exploitation of Payment Systems**:
    - Attacks on digital wallets (e.g., Apple Pay, Google Pay).
    - Unauthorized use of NFC (Near Field Communication) and contactless payment systems.
- **Techniques**:
    - SIM swapping to intercept OTPs.
    - Credential stuffing to gain unauthorized access to payment accounts.

4. Vulnerabilities in Mobile Apps

- Poorly secured mobile apps (e.g., banking apps or e-commerce apps) are becoming major attack vectors.
- Common issues include:
    - Weak authentication mechanisms.
    - Hardcoded credentials in the app code.
    - Insecure APIs leaking sensitive user information.

5. Attacks on Mobile Devices in IoT Ecosystems

- Increasing use of mobile devices to control IoT-enabled systems (e.g., smart homes, vehicles).
- Cybercriminals exploit weak security in IoT devices connected via mobile apps or networks.
- Example: Compromising smart car applications to gain control of connected vehicles.

6. Location Data Exploitation

- Location services on mobile devices are a goldmine for cybercriminals.
- Exploits include:
    - Stalking or tracking individuals for extortion.
    - Intercepting location-based app communications for targeted phishing.

7. Mobile Device Hijacking (Cryptojacking)

- Hackers use mobile devices to mine cryptocurrency without the user's knowledge.
- This often happens via malicious apps or browser-based cryptojacking scripts.

8. Mobile Ransomware

- Cybercriminals encrypt or lock mobile devices, demanding ransom to restore access.
- Tactics involve:
    - Exploiting vulnerabilities in Android/iOS.
    - Using fake updates or applications to deliver ransomware.
- Example: Android ransomware strains like "DoubleLocker."

9. Exploitation of Public Wi-Fi Networks

- **Man-in-the-Middle Attacks**: Cybercriminals intercept data transmitted over unsecured public Wi-Fi.
- Common targets: Mobile banking apps, e-commerce sites, or login credentials to services.
- Use of rogue Wi-Fi networks to lure users and steal data.

10. Zero-Day Exploits in Mobile OS

- Increasing sophistication of attackers in exploiting zero-day vulnerabilities in Android and iOS.
- Example: Exploits used by spyware like Pegasus to infiltrate devices for surveillance or theft.

11. Social Engineering via Mobile Devices

- Growth of vishing (voice phishing) attacks.
- Deepfake audio/video used to impersonate trusted contacts for fraud.
- Spear-phishing attacks on high-value targets, often delivered via mobile platforms.

12. Cross-Platform Attacks

- Cybercriminals create malware that can infect both mobile and desktop devices through shared apps or accounts.
- Example: Malware propagating from a compromised mobile device to a corporate network.

13. Attacks on Mobile VPNs

- VPN apps for mobile are increasingly targeted to intercept private communications.
- Fake VPN apps may also harvest user data or serve as spyware.

14. Mobile Device Management (MDM) Exploitation

- In enterprise settings, attackers compromise MDM systems to gain control over mobile devices within an organization.
- This often leads to data breaches or ransomware incidents.

15. QR Code Exploits

- Growth in QR code use (e.g., payments, websites) has led to their exploitation.
- Malicious QR codes redirect users to phishing sites or download malware onto mobile devices.

Combating Mobile Cybercrime Trends

- **Awareness**: User education on identifying phishing attempts and fake apps.
- **Technology**:
    - Improved security in mobile OS with timely patches and updates.
    - AI-driven anomaly detection for mobile apps and transactions.
- **Regulation**: Stronger legal frameworks for mobile app security and data protection.

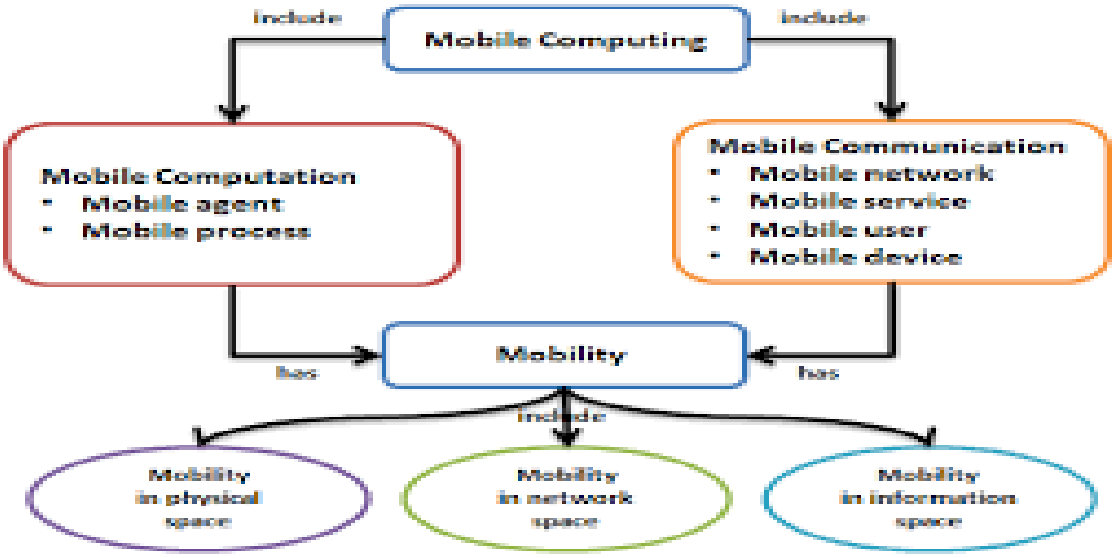
Credit Card Frauds in Mobile and Wireless Computing Era

Today belongs to" Mobile computing" that is anywhere any time computing. In this current period, the rising importance of electronic gadgets – which became an integral part of business, providing connectivity with the internet outside the office – brings many challenges to secure

these devices from being a victim of cyber-crime. These Credit card frauds and all are the new trends in cybercrime that are coming up with mobile computing – mobile commerce (M-COMMERCE) and mobile banking (M-Banking). The developments in wireless technology have fuelled this new mode of working for white collar workers. This is true for credit card processing too. Credit card (or debit card) fraud is a form of identity theft that involves an illegitimate taking of another's credit card information for the purpose of charging purchases to the account or removing funds from it. This paper mainly focuses on the types of credit card frauds, and to help the users against the fraud to prevent both technologies as well as the user level precautions.

Mobile Computing:

Mobile computing is a broad term that refers to a variety of devices that allow people to access data and information from wherever they are. Sometimes referred to as "human-computer interaction," mobile computing transports data, voice, and video over a network via a mobile device.



Wireless Computing

Wireless Computing:

Wireless USB (WUSB) is a form of Universal Serial Bus (USB) technology that uses radio-frequency (RF) links rather than cables to provide the interfaces between a computer and peripherals, such as monitors, printers, external drives, headsets, MP3 players and digital cameras, cordless telephones, mobiles, GPS units, ZigBee technology, wireless computer parts, and satellite television, etc.

Current Wireless Systems

Elements of Credit Card Fraud:

Debit/credit card fraud is thus committed when a person

1) fraudulently obtains, takes, signs, uses, sells, buys, or forges someone else's credit or debit card or card information;

2) Uses his or her own card with the knowledge that it is revoked or expired or that the account lacks enough money to pay for the items charged; and

3) Sells goods or services to someone else with knowledge that the credit or debit card being used was illegally obtained or is being used without authorization.

Theft, the most obvious form of credit card fraud, can happen in a variety of ways, from low tech dumpster diving to high tech hacking. A thief might go through the trash to find discarded billing statements and then use your account information to buy things. A retail or bank website might get hacked, and your card number could be stolen and shared. Perhaps a dishonest clerk or waiter takes a photo of your credit card and uses your account to buy items or create another account. Or maybe you get a call offering a free trip or discounted travel package. But to be eligible, you must join a club and give your account number, say, to guarantee your place. The next thing you know, charges you didn't make are on your bill, and the trip promoters who called you are nowhere to be found.

Types of Credit Card Fraud:

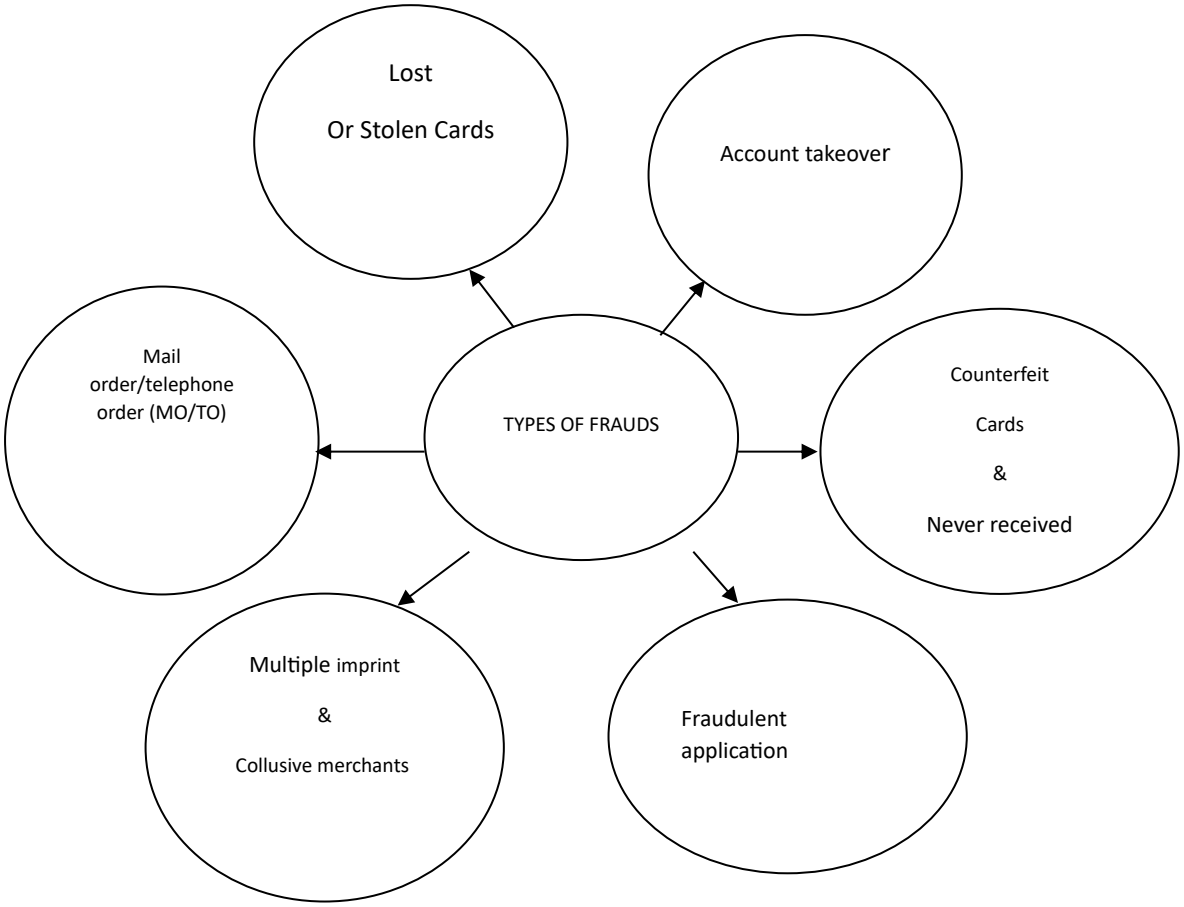


Fig 3: Types of Credit Card Frauds

- The first category, lost or stolen cards, is a relatively common one, and should be reported immediately to minimize any damages.
- The second is called “account takeover” — when a cardholder unwittingly gives personal information (such as home address, mother’s maiden name, etc.) to a fraudster, who then contacts the cardholder’s bank, reports a lost card and change of address, and obtains a new card in the soon-to-be victim’s name.
- The third is counterfeit cards — when a card is “cloned” from another and then used to make purchases. In Asia Pacific, 10% to 15% of fraud results from malpractices such as card skimming but this number has significantly dropped from what it were a couple of years prior, largely due to the many safety features put in place for payment cards, such as EMV chip.
- The fourth is called “never received” — when a new or replacement card is stolen from the mail, never reaching its rightful owner.

- The fifth is fraudulent application— when a fraudster uses another person's name and information to apply for and obtain a credit card.
- The sixth is called "multiple imprint"— when a single transaction is recorded multiple times on old-fashioned credit card imprint machines known as "knuckle busters".
- The seventh is collusive merchants — when merchant employees work with fraudsters to defraud banks.
- The eighth is mail order/telephone order (MO/TO) fraud, which now includes e-commerce, and is the largest category of total payment card fraud in Asia-Pacific, amounting to nearly three-quarters of all fraud cases. The payments industry is working tirelessly to improve card verification and security programs to prevent fraud in so-called "card-not-present" transactions online or via mail order and telephone transactions.

What Can You Do?

Incorporating a few practices into your daily routine can help keep your cards and account numbers safe. For example, keep a record of your account numbers, their expiration dates and the phone number to report fraud for each company in a secure place. Don't lend your card to anyone — even your kids or roommates — and don't leave your cards, receipts, or statements around your home or office. When you no longer need them, shred them before throwing them away.

Other fraud protection practices include:

1. Don't give your account number to anyone on the phone unless you've made the call to a company you know to be reputable. If you've never done business with them before, do an online search first for reviews or complaints.
2. Carry your cards separately from your wallet. It can minimize your losses if someone steals your wallet or purse. And carry only the card you need for that outing.
3. During a transaction, keep your eye on your card. Make sure you get it back before you walk away.
4. Never sign a blank receipt. Draw a line through any blank spaces above the total.
5. Save your receipts to compare with your statement.
6. Open your bills promptly — or check them online often — and reconcile them with the purchases you've made.
7. Report any questionable charges to the card issuer.
8. Notify your card issuer if your address changes or if you will be traveling.

9. Don’t write your account number on the outside of an envelope.

Staying vigilant about protecting your personal information can greatly reduce risk of theft or fraud — an important and necessary step in today’s digital world. While credit and debit cards have built in protections, the first line of defence really starts with the cardholder.

Prevent theft against Technology wise:

1) Use of Credit Card on Public Computer

Public computers are most vulnerable for Credit Card Fraud. Never ever use Credit Card in cybercafé, friends place or even in office. Always trust your own Desktop / Laptop for online transactions. Use reputed Anti-Virus, Anti-Malware & Firewall to avoid any data theft.

2) Credit Card Photocopy as Id Proof / Authorization letter

A Credit Card with Photograph is also accepted as valid Id proof e.g. for bank account opening etc. In case, you booked air ticket for your friend or family member, an authorization letter with Xerox of credit card is required. We tend to give Xerox of both front and back side of credit card. Some unaware users don’t even hide CVV on back side thus vulnerable to credit card fraud. Please note that it is not necessary to give Xerox of back side of credit card. Only front side is sufficient.

3) Fraudulent Calls

Recently, someone was in meeting with their client and suddenly he/she received call. The caller told his/her that bank is going to forfeit all her reward points as they expired day before. Caller also informed that his/her reward points are worth 20,000 and if she would like to retain than he/she need to verify details by sharing credit card details. Basically, the caller created panic situation & linked it to monetary loss. In such situations our brain stops logical thinking. It was fraudulent call and immediately to register FIR. To avoid credit card fraud never ever trust incoming calls. If you receive any such call than call back bank’s helpline to check the truth.

4) Credit Card payment through Mobile / Mobile Apps

These days you might have observed that lot many merchants are promoting online mobile apps. I used RedBus, Flipkart, and BookMyShow etc. These apps allow you to make payment over mobile app through Credit Card. Don’t do any credit card payment through Mobile apps to avoid credit card fraud. In a recent article published in Business Standard, a survey done by Japanese security firm Trend Micro revealed that 39 Payment Gateways, 15 Bank related mobile Apps and other Mobile apps, Shopping apps, Social Networking Apps and Health Care apps used by Indian users are vulnerable to credit card fraud.

5) Prevention is better than Cure

If the situation demands and you carried out any risky/vulnerable transaction than immediately cancel your Credit Card and apply for replacement of credit card. In short, if you foresee or anticipate any Credit Card fraud than apply for replacement of credit card.

Ways to Prevent Credit Card Fraud:

Even as prevalent as fraud has become, there are plenty of methods you can use to help protect yourself. Here are some ways to reduce your risk of falling victim to credit card fraud:

At Home

Use these general best practices for credit card safety, which you should be implementing daily to protect yourself from fraud:

- Sign any new cards immediately. By establishing your signature on the card, you make it much more difficult for someone else to erase or cover your signature and forge it in their own handwriting if the card is ever lost or stolen.
- Carry your cards separately from your cash. Most people carry their cards and cash together in their wallet. But that means if your wallet is stolen, your cards will be stolen as well.
- After you offer your card over to pay, keep it in view when you can.
- Don’t sign a blank receipt. Draw a line through any space above the total amount (including any tip amounts) if you do not intend to authorize additional charges on your card.
- Void all carbon copies and incorrect receipts.
- Save all receipts in a safe place.
- Open your billing statements as soon as you get them, and reconcile your card accounts every month the same way you would reconcile your checking account.
- Report any suspicious activity on your card immediately.
- Never lend your credit card to anyone.
- Always destroy receipts by using a shredder or cutting them into small pieces.
- Never leave receipts lying around.
- Never put your card number on a postcard, the outside of envelopes, or in a photo online.
- Do not give out your card number over the phone unless you initiated the transaction and you know the company is reputable.

Online

Almost everyone is shopping online nowadays, and it's important to understand how you can protect your personal information when doing so. Here are some quick tips:

- Only use your card for purchases on websites you trust.
- Do not click links in emails, especially those from any company or individual you don't recognize.
- Never enter your card information (or social security number, etc.) in response to an email or via an emailed link. Always go directly to the company's site instead by typing the address yourself.
- When entering card information, check the page you're on to make sure it's secure (e.g., starts with https:// or includes a lock symbol in your browser bar).
- Use a credit card (not a debit card) to limit your liability for any fraud that may occur.
- See if your card issuer offers a "disposable" or one-time use card number, which still links to your account but expires after one use (or is only good for use at a single merchant).
- Do not enter personal information (including credit card numbers) if you're on a public computer or public Wi-Fi network.
- Keep your anti-virus software up to date to prevent hacking.
- Watch your transaction history — make sure transactions match the amounts on your receipts, and look out for anything you don't recognize.

Techniques:

Present be numerous algorithms are used to detect card frauds. Some of the Techniques are,

- Artificial Neural Network (ANN)
- Genetic Algorithm (GA)
- Hidden Markov Model (HMM)
- Support Vector Machines (SVM)
- Bayesian Network
- Fuzzy Neural Network
- Expert Systems
- Decision Tree (DT).

Among all the techniques the genetic algorithm works with noisy data and easy to integrate with other systems.GA can combined with other techniques to improve the act of that technique and optimize their parameters.

Security Challenges Posed by Mobile Devices

Believe it or not there are security risks when using a mobile device. We know, it is surprising right, that your phone or tablet could be a possible threat to your safety. When you consider all the potential threats that exist on the Internet and the fact that most of today's mobile devices are connecting to and through the Internet with every function, I think it becomes easier to understand just how vulnerable they are. While more of the threats are the same as those faced by the average laptop or desktop user there are some unique to the mobile world. Mobile phone security threats generally include application based, web-based, network-based and physical threats.

1. Application based threat:

The most of application are downloadable and purposed the most common risk for mobile users; most devices don't do much on their own, and it is the applications that make them so awesome and we all download apps. If it comes to apps the risks run from bugs and basic security risks on the low end of the scale all the way through malicious apps with no other purpose to commit cyber crime.

- Malware
- Spyware
- Privacy
- Zero Day Vulnerabilities

2. Web based threat: According to the nature of mobile use, the fact that we have our devices with us everywhere we go and are connecting to the Internet while doing so, they face the number of unique web-based threats as well as the run-of-the-mill threats of general Internet use.

- Phishing Scams
- Social Engineering
- Drive By Downloads
- Operating System Flaws

3. Network-based threat:

Any mobile devices which typically support a minimum of three network capabilities making them three-times vulnerable to network-based attack. And a network often found on a mobile include cellular, WiFi and Bluetooth.

- Network exploits
- WiFi sniffing
- Cross-Platform Attacks
- BOYD

4. Physical Threats:

It is happened any time, unlikely a desktop sitting at your workstation, or even a laptop in your bag, a mobile device is subject to a number of everyday physical threats.

Loss/Theft: Loss or theft is the most unwanted physical threat to the security of your mobile device. Any devices itself have value and can be sold on the secondary market after all your information is stolen and sold.

Top Mobile Security Threats

Mobile devices can be attacked at different levels. This includes the potential for malicious apps, network-level attacks, and exploitation of vulnerabilities within the devices and the mobile OS.

As mobile devices become increasingly important, they have received additional attention from cybercriminals. As a result, cyber threats against these devices have become more diverse.

1. Malicious Apps and Websites

Like desktop computers, mobile devices have software and Internet access. Mobile malware (i.e. malicious applications) and malicious websites can accomplish the same objectives (stealing data, encrypting data, etc.) on mobile phones as on traditional computers.

Malicious apps come in a variety of different forms. The most common types of malicious mobile apps are trojans that also perform ad and click scams.

2. Mobile Ransomware

Mobile ransomware is a particular type of mobile malware, but the increased usage of mobile devices for business has made it a more common and damaging malware variant. Mobile ransomware encrypts files on a mobile device and then requires a ransom payment for the decryption key to restore access to the encrypted data.

3. Phishing

Phishing is one of the most common attack vectors in existence. Most cyberattacks begin with a phishing email that carries a malicious link or an attachment containing malware. On mobile

devices, phishing attacks have a variety of media for delivering their links and malware, including email, SMS messaging, social media platforms, and other applications.

In fact, while emails are what people most commonly think of when they hear phishing, they are not even close to the most commonly phishing vector on mobile devices. In fact, emails only account for 15% of mobile phishing attacks, placing them behind messaging, social media and "other" apps (not social, messaging, gaming, or productivity).

4. Man-in-the-Middle (MitM) Attacks

Man-in-the-Middle (MitM) attacks involve an attacker intercepting network communications to either eavesdrop on or modify the data being transmitted. While this type of attack may be possible on different systems, mobile devices are especially susceptible to MitM attacks. Unlike web traffic, which commonly uses encrypted HTTPS for communication, SMS messages can be easily intercepted, and mobile applications may use unencrypted HTTP for transfer of potentially sensitive information.

MitM attacks typically require an employee to be connected to an untrusted or compromised network, such as public Wi-Fi or cellular networks. However, the majority of organizations lack policies prohibiting the use of these networks, making this sort of attack entirely feasible if solutions like a virtual private network (VPN) are not used.

5. Advanced Jailbreaking and Rooting Techniques

Jailbreaking and rooting are terms for gaining administrator access to iOS and Android mobile devices. These types of attacks take advantage of vulnerabilities in the mobile OSs to achieve root access on these devices. These increased permissions enable an attacker to gain access to more data and cause more damage than with the limited permissions available by default. Many mobile users will jailbreak/root their own devices to enable them to delete unwanted default apps or install apps from untrusted app stores, making this attack even easier to perform.

6. Device and OS exploits

Often, the focus of cybersecurity is on top-layer software, but lower levels of the software stack can contain vulnerabilities and be attacked as well. With mobile devices – like computers – vulnerabilities in the mobile OS or the device itself can be exploited by an attacker. Often, these exploits are more damaging than higher-level ones because they exist below and outside the visibility of the device's security solutions.

Protecting Against Mobile Threats

With the large and diverse mobile threat landscape, businesses require enterprise mobile security solutions. This is especially true as the shift to remote work makes these mobile devices a more common and critical component of an organization's IT infrastructure.

An effective mobile threat defense solution needs to be able to detect and respond to a variety of different attacks while providing a positive user experience. Accomplishing this requires implementing these guiding principles:

- A 360° view of security across device, apps, and the network
- Full flexibility and scalability
- Full visibility into the risk level of the mobile workforce
- Privacy protection by design
- An optimal user experience

Check Point's Harmony Mobile provides a comprehensive mobile security to keep corporate data safe by securing employees' mobile devices across all attack vectors: apps, network and OS solution. Check To check outsee Harmony Mobile's capabilities for yourself, request a personalized demo with a mobile security expert. You're also welcome to try it out for yourself with a free trial. And for further information about the guiding principles and other important aspects of a mobile security solution, check out this mobile protection buyer's guide.

A cyber-crime is a criminal act in which someone targets a computer or a network of devices in order to gain illegal rights, steal data from them, frauds etc. This type of crime is carried out using technology which primarily takes place online.

Some cyber-crime includes the following −

- Harassment
- Cyber-stalking
- Bullying

Types of Cyber-crimes

The types of cyber-crimes are as follows −

Hacking

It is a type of cyber-crime in which a person tries to identify and exploit weakness in a computer system or a computer network for his own benefits.

Some types of hacking are given below −

- Social Engineering & Phishing
- Malware-Injecting Devices
- Cracking Passwords
- Distributed Denial-of-Service

Virus dissemination

Virus dissemination is a process in which a Malicious software attaches itself to other software (which can be a trojan horse, time bond, virus, worm etc) which has the ability to destroy the victim computer/system.

Cyber Terrorism

Cyber terrorism is a type of attack in which a person uses the Internet to establish violent acts which may result in loss of a life, harm to a person or threaten to life. The main object of this is to gain political advantages by the use of threat.

Computer Vandalism

Computer Vandalism is a type of process in which a program has the ability to perform malicious tasks such as getting someone's passwords or important data. This can even include the removal of user data or deleting one's hard drive.

Security Threats

Now, let us see the Security threats related to mobile devices, which are as follows −

- Data Leakage
- Unsecured Wi-Fi
- Network Spoofing
- Phishing Attacks
- Spyware
- Broken Cryptography
- Improper Session Handling

Let us discuss each threat in detail.

Unsecured Wi-Fi

Free wi-fi is easily attractive to people, if anyone connects to the free wifi, then the hackers might steal your data. Never use the free wifi when accessing confidential services like banking and transactions, there might be a chance of stealing your money.

Phishing Attacks

Phishing attacks are mostly seen in emails and messages. When the user clicks on a suspicious link, there might be a chance of virus files download which can corrupt and hack your devices which results in data loss. In some cases, they will send a form to fill in the confidential information.

Malicious Apps and websites

When you download any app manually from the websites, there might be a chance that the app can accomplish some objectives like stealing data, encrypting the data, etc.

Weak Passwords

If the passwords of the mobile devices are weak there might be a change of others accessing the data. This might result in data leakage and privacy issues. So make sure that the passwords for mobile devices or apps must be strong.

IoT Mobile Security Threats

As we all know most of the things are correcting to the internet and works easily, fast with the internet from wearable tech like smartphones, watches, etc. If these devices are hacked then misuse of these devices might result in huge costs.

Registry Settings for Mobile Devices

A "registry setting for mobile devices" in cybersecurity refers to a configuration option within a mobile device's operating system registry, allowing administrators to control security parameters like password complexity, encryption levels, app installation restrictions, and more, typically managed through Mobile Device Management (MDM) tools to enforce security policies across a fleet of devices.

Key points about registry settings for mobile devices in cybersecurity:

- **Centralized management:**

Administrators can use MDM platforms to push specific registry settings to multiple devices, ensuring consistent security policies across the organization.

- **Fine-grained control:**

Registry settings allow for precise adjustments to various security features, including device lock settings, data encryption, and application permissions.

- **Platform-specific:**

Depending on the mobile operating system (iOS, Android), the location and names of registry keys will differ, requiring tailored configuration knowledge.

Examples of registry settings on mobile devices for cybersecurity:

- **Password complexity:**

Setting minimum password length, character types (uppercase, lowercase, numbers, symbols) to prevent weak passwords.

- **Device encryption:**

Enabling full-disk encryption to protect data in case of device loss or theft.

- **Application installation restrictions:**

Whitelisting approved apps to prevent unauthorized software installation.

- **USB access control:**

Limiting which USB devices can access the mobile device to prevent data exfiltration.

- **Network access control:**

Configuring which networks a device can connect to, including restrictions on public Wi-Fi.

- **Device compatibility:**

Ensure that the registry settings you want to configure are supported by the mobile device operating system and model.

- **User impact:**

Carefully consider the potential impact of restrictive registry settings on user experience and productivity.

- **Regular monitoring and updates:**

Regularly review and update registry settings to reflect evolving security threats and organizational policies.

Authentication Service Security

Authentication service security in cyber security is the process of verifying a user's identity to ensure they have permission to access a resource or service. It helps to protect sensitive information and prevent fraud.

Some authentication service security methods include:

- **Multi-factor authentication**

Uses multiple authentication methods, such as a PIN, biometrics, or password, to reduce the risk of account compromise

- **Biometrics**

Uses unique identifiers, such as fingerprints or facial recognition, to verify a user's identity

- **Single sign-on (SSO)**

Allows users to log in once to access multiple applications or systems without re-entering credentials

- **Token authentication**

Uses a physical token, such as a smart card or smartphone, that contains the user's credentials

- **Password protection**

Uses a user ID and password to verify a user's identity

When designing an authentication service, you can consider things like:

- The technical skills and comfort levels of your users
- The level of security required for the data they access
- Any legal requirements or industry regulations that apply

Attacks on Mobile/Cell Phones

SMiShing: Smishing become common now as smartphones are widely used. SMiShing uses Short Message Service (SMS) to send fraud text messages or links. The criminals cheat the user by calling. Victims may provide sensitive information such as credit card information, account information, etc. Accessing a website might result in the user unknowingly downloading malware that infects the device.

War driving: War driving is a way used by attackers to find access points wherever they can be. With the availability of free Wi-Fi connection, they can drive around and obtain a very huge amount of information over a very short period of time.

WEP attack: Wired Equivalent Privacy (WEP) is a security protocol that attempted to provide a wireless local area network with the same level of security as a wired LAN. Since physical security steps help to protect a wired LAN, WEP attempts to provide similar protection for data transmitted over WLAN with encryption. WEP uses a key for encryption. There is no provision for key management with Wired Equivalent Privacy, so the number of people sharing the key will continually grow. Since everyone is using the same key, the criminal has access to a large amount of traffic for analytic attacks.

WPA attack: Wi-Fi Protected Access (WPA) and then WPA2 came out as improved protocols to replace WEP. WPA2 does not have the same encryption problems because an attacker cannot recover the key by noticing traffic. WPA2 is susceptible to attack because cyber criminals can analyze the packets going between the access point and an authorized user.

Bluejacking: Bluejacking is used for sending unauthorized messages to another Bluetooth device. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers and other devices.

Replay attacks: In a Replay attack an attacker spies on information being sent between a sender and a receiver. Once the attacker has spied on the information, he or she can intercept it and retransmit it again thus leading to some delay in data transmission. It is also known as playback attack.

Bluesnarfing : It occurs when the attacker copies the victim's information from his device. An attacker can access information such as the user's calendar, contact list, e-mail and text messages without leaving any evidence of the attack.

RF Jamming: Wireless signals are susceptible to electromagnetic interference and radio-frequency interference. Radio frequency (RF) jamming distorts the transmission of a satellite station so that the signal does not reach the receiving station.

There are several types of attacks that target these devices, each with its own advantages and disadvantages:

Wi-Fi Spoofing: Wi-Fi spoofing involves setting up a fake wireless access point to trick users into connecting to it instead of the legitimate network. This attack can be used to steal sensitive information such as usernames, passwords, and credit card numbers. One advantage of this attack is that it is relatively easy to carry out, and the attacker does not need sophisticated tools or skills. However, it can be easily detected if users are aware of the legitimate network's name and other details.

Packet Sniffing: Packet sniffing involves intercepting and analyzing the data packets that are transmitted over a wireless network. This attack can be used to capture sensitive information such as email messages, instant messages, and web traffic. One advantage of this attack is that it can be carried out without the user's knowledge. However, the attacker needs to be in close proximity to the victim and must have the technical skills and tools to intercept and analyze the data.

Bluejacking: Bluejacking involves sending unsolicited messages to Bluetooth-enabled devices. This attack can be used to send spam, phishing messages, or malware to the victim's device. One advantage of this attack is that it does not require a network connection, and the attacker can be located anywhere within range of the victim's Bluetooth signal. However, it requires the attacker to have the victim's Bluetooth device's address and is limited to devices that have Bluetooth capabilities.

SMS Spoofing: SMS spoofing involves sending text messages that appear to come from a trusted source, such as a bank or a government agency. This attack can be used to trick users into revealing sensitive information or downloading malware. One advantage of this attack is that it can be carried out without the user's knowledge. However, it requires the attacker to have the victim's phone number, and it can be easily detected if users are aware of the legitimate source of the message.

Malware: Malware is software designed to infect a device and steal or damage data. Malware can be distributed through email attachments, software downloads, or malicious websites. One advantage of this attack is that it can be carried out remotely, without the attacker needing to be physically close to the victim. However, it requires the attacker to have a way to deliver the malware to the victim's device, such as through a phishing email or a fake website.

PCET's

Pimpri Chinchwad University

School of Computer Applications

BSc (CS)-II

Cyber Laws and Security Policies

Unit No. 03 Tools and Methods Used in Cybercrime

Introduction:

Cybercriminals utilize a wide range of tools and methods to carry out attacks, including malware like viruses, worms, and Trojans, social engineering techniques like phishing and vishing, password cracking tools, keyloggers, SQL injection, denial-of-service attacks, proxy servers, anonymizers, and advanced techniques like steganography to infiltrate systems, steal sensitive data, disrupt operations, and cover their tracks; making it crucial for individuals and organizations to implement robust cybersecurity measures to protect against these threats.

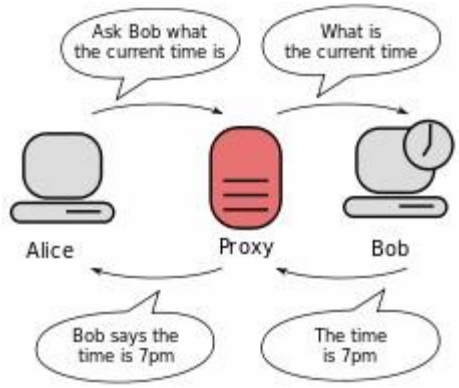
Key points about cybercrime tools and methods:

- **Access Methods:**
  - **Phishing:** Sending deceptive emails or messages to trick users into revealing sensitive information like passwords.
  - **Social Engineering:** Manipulating users through psychological tactics to gain access to systems or data.
  - **Watering Hole Attacks:** Creating malicious websites that target specific user groups to infect them with malware.
- **Malware:**
  - **Viruses:** Self-replicating programs that spread across systems, causing damage.
  - **Worms:** Network-based malware that automatically replicates and spreads without user interaction.
  - **Trojan Horses:** Programs disguised as legitimate software that contain malicious functionality.
  - **Ransomware:** Encrypting a victim's data and demanding a ransom to decrypt it.
- **Exploiting Vulnerabilities:**
  - **SQL Injection:** Inserting malicious SQL queries into a website to gain unauthorized access to databases.

    - **Buffer Overflow:** Overwriting memory buffers to execute malicious code.
    - **Cross-Site Scripting (XSS):** Injecting malicious JavaScript code into a website to steal user data.
- **Network Intrusion Techniques:**
    - **Port Scanning:** Identifying open ports on a system to find potential vulnerabilities.
    - **Packet Sniffing:** Capturing network traffic to monitor data transmission.
    - **Man-in-the-Middle Attacks:** Interception of communication between two parties to steal data.
- **Data Exfiltration and Cover-up:**
    - **Proxy Servers:** Masking the origin of network traffic to hide the attacker's identity.
    - **Anonymizers:** Services that obscure user information to make tracking difficult.
    - **Steganography:** Hiding data within seemingly innocent files to evade detection.

Proxy Server

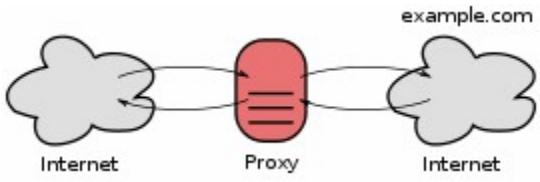
It is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems. Today, most proxies are web proxies, facilitating access to content on the World Wide Web and providing anonymity.



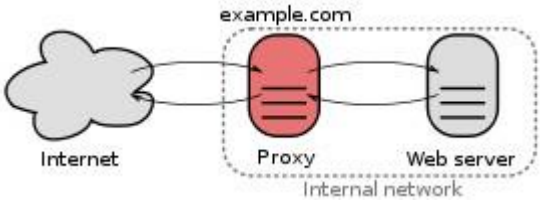
Types of proxy – A proxy server may reside on the user's local computer, or at various points between the user's computer and destination servers on the Internet.

- A proxy server that passes requests and responses unmodified is usually called a gateway or sometimes a tunneling proxy.
- A forward proxy is an Internet-facing proxy used to retrieve from a wide range of sources (in most cases anywhere on the Internet).
- A reverse proxy is usually an Internet-facing proxy used as a front-end to control and protect access to a server on a private network. A reverse proxy commonly also performs tasks such as load-balancing, authentication, decryption or caching.

Open proxies – An open proxy is a forwarding proxy server that is accessible by any Internet user. Gordon Lyon estimates there are "hundreds of thousands" of open proxies on the Internet. An anonymous open proxy allows users to conceal their IP address while browsing the Web or using other Internet services. There are varying degrees of anonymity however, as well as a number of methods of 'tricking' the client into revealing itself regardless of the proxy being used.



Reverse proxies – A reverse proxy (or surrogate) is a proxy server that appears to clients to be an ordinary server. Requests are forwarded to one or more proxy servers which handle the request. The response from the proxy server is returned as if it came directly from the original server, leaving the client no knowledge of the origin servers. Reverse proxies are installed in the neighborhood of one or more web servers. All traffic coming from the Internet and with a destination of one of the neighborhood's web servers goes through the proxy server. The use of "reverse" originates in its counterpart "forward proxy" since the reverse proxy sits closer to the web server and serves only a restricted set of websites.



There are several reasons for installing reverse proxy servers

- Encryption / SSL acceleration: when secure web sites are created, the SSL encryption is often not done by the web server itself, but by a reverse proxy that is equipped with SSL acceleration hardware. See Secure Sockets Layer. Furthermore, a host can provide a single "SSL proxy" to provide SSL encryption for an arbitrary number of hosts;

removing the need for a separate SSL Server Certificate for each host, with the downside that all hosts behind the SSL proxy have to share a common DNS name or IP address for SSL connections. This problem can partly be overcome by using the SubjectAltName feature of X.509 certificates.

- Load balancing: the reverse proxy can distribute the load to several web servers, each web server serving its own application area. In such a case, the reverse proxy may need to rewrite the URLs in each web page (translation from externally known URLs to the internal locations).
- Serve/cache static content: A reverse proxy can offload the web servers by caching static content like pictures and other static graphical content.
- Compression: the proxy server can optimize and compress the content to speed up the load time.
- Spoon feeding: reduces resource usage caused by slow clients on the web servers by caching the content the web server sent and slowly "spoon feeding" it to the client. This especially benefits dynamically generated pages.
- Security: the proxy server is an additional layer of defense and can protect against some OS and Web Server specific attacks. However, it does not provide any protection from attacks against the web application or service itself, which is generally considered the larger threat.
- Extranet Publishing: a reverse proxy server facing the Internet can be used to communicate to a firewall server internal to an organization, providing extranet access to some functions while keeping the servers behind the firewalls. If used in this way, security measures should be considered to protect the rest of your infrastructure in case this server is compromised, as its web application is exposed to attack from the Internet.

If the destination server filters content based on the origin of the request, the use of a proxy can circumvent this filter. For example, a server using IP-based geolocation to restrict its service to a certain country can be accessed using a proxy located in that country to access the service.

Web proxies are the most common means of bypassing government censorship, although no more than 3% of Internet users use any circumvention tools. In some cases users can circumvent proxies which filter using blacklists using services designed to proxy information from a non-blacklisted location.

Proxies can be installed in order to eavesdrop upon the data-flow between client machines and the web. All content sent or accessed – including passwords submitted and cookies used – can be captured and analyzed by the proxy operator. For this reason, passwords to online services

(such as webmail and banking) should always be exchanged over a cryptographically secured connection, such as SSL. By chaining proxies which do not reveal data about the original requester, it is possible to obfuscate activities from the eyes of the user's destination. However, more traces will be left on the intermediate hops, which could be used or offered up to trace the user's activities. If the policies and administrators of these other proxies are unknown, the user may fall victim to a false sense of security just because those details are out of sight and mind. In what is more of an inconvenience than a risk, proxy users may find themselves being blocked from certain Web sites, as numerous forums and Web sites block IP addresses from proxies known to have spammed or trolled the site. Proxy bouncing can be used to maintain your privacy.

Anonymizer

An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information.

There are many reasons for using anonymizers. Anonymizers help minimize risk. They can be used to prevent identity theft, or to protect search histories from public disclosure. Some countries apply heavy censorship on the internet. Anonymizers can help in allowing free access to all of the internet content, but cannot help against persecution for accessing the Anonymizer website itself. Furthermore, as information itself about Anonymizer websites are banned in these countries, users are wary that they may be falling into a government-set trap.

Anonymizers are also used by people who wish to receive objective information with the growing target marketing on the internet and targeted information. For example, large news outlets such as CNN target the viewers according to region and give different information to different populations. Websites such as YouTube obtain information about the last videos viewed on a computer, and propose "recommended" videos accordingly, and most of the online targeted marketing is done by showing advertisements according to that region. Anonymizers are used for avoiding this kind of targeting and getting a more objective view of information.

Types

- Protocol specific anonymizers – Sometimes anonymizers are implemented to work only with one particular protocol. The advantage is that no extra software is needed. The operation occurs in this manner: A connection is made by the user to the anonymizer. Commands to the anonymizer are included inside a typical message. The anonymizer

then makes a connection to the resource specified by the inbound command and relays the message with the command stripped out. An example of a protocol-specific anonymizer is an anonymous remailer for e-mail. Also of note are web proxies, and bouncers for FTP and IRC.

- Protocol independent anonymizers – Protocol independence can be achieved by creating a tunnel to an anonymizer. The technology to do so varies. Protocols used by anonymizer services may include SOCKS, PPTP, or OpenVPN. In this case either the desired application must support the tunneling protocol, or a piece of software must be installed to force all connections through the tunnel. Web browsers, FTP and IRC clients often support SOCKS for example, unlike telnet.

Phishing

Phishing is a cyberattack that uses fraudulent communication to trick people into sharing sensitive information. Phishing attacks can be conducted through email, text messages, phone calls, or websites.

How does phishing work?

- Phishing attacks are a type of social engineering.
- The goal is to steal sensitive data like credit card and login information.
- The attacker may also try to install malware on the victim's device.

Types of phishing attacks

- **Email phishing:** A fraudulent email that appears to come from a reputable source
- **Spear phishing:** A personalized scam that targets a specific individual, group, or organization
- **Smishing:** A fake mobile text message that tricks people into sharing sensitive information
- **Vishing:** A fraudulent phone call or voice message that tricks people into sharing sensitive information

Virus and Worms

In cybercrime, "viruses" and "worms" are considered types of malicious software (malware) used by attackers to infiltrate and damage computer systems, with the key difference being that a virus requires a host file to spread, while a worm can replicate and spread independently across networks without needing a host file; both are commonly used as tools to steal data, disrupt operations, or gain unauthorized access to systems.

Key points about viruses and worms:

1. **Virus:**

- **Spreading mechanism:** Attaches itself to executable files and spreads when the infected file is opened or executed.
- **Example scenarios:** A virus might be embedded in a malicious email attachment, infecting a user's computer when they open it.
- **Impact:** Can modify or delete data on the infected system, disrupt system functionality, or install other malware.

2. **Worm:**

- **Spreading mechanism:** Self-replicates and spreads across networks automatically, exploiting vulnerabilities in systems to move from one computer to another without user interaction.
- **Example scenarios:** A worm might scan for open network shares and copy itself to other computers on the network, rapidly infecting multiple devices.
- **Impact:** Can overload networks with traffic due to rapid replication, consuming system resources and causing performance issues.

How cybercriminals use viruses and worms:

- **Data theft:** By infiltrating systems with a virus or worm, attackers can steal sensitive information like login credentials, financial details, or personal data.
- **Ransomware attacks:** Some viruses are designed to encrypt a victim's data and demand a ransom payment to decrypt it.
- **Botnet creation:** Worms can be used to create large networks of compromised computers (botnets) that can be controlled remotely to launch distributed denial-of-service (DDoS) attacks.

Protection against viruses and worms:

- **Antivirus software:** Regularly updated antivirus programs can detect and remove viruses and worms from a system.
- **Network security:** Firewalls and intrusion detection systems can monitor network traffic and block malicious attempts to spread malware.
- **User education:** Educating users about the dangers of opening suspicious emails, downloading unknown files, and keeping software updated can help prevent infections.

Trojan Horses and Backdoors

A "Trojan Horse" in cybercrime refers to a malicious program disguised as a legitimate application, allowing attackers to gain unauthorized access to a system while a "backdoor" is a hidden entry point within a system that bypasses security measures, enabling attackers to access and control a computer remotely, essentially creating a secret way to gain access without detection; both are commonly used tools in cybercrime to steal data, spy on users, or launch further attacks.

Key points about Trojan Horses and Backdoors:

Functionality:

- **Trojan Horse:** A seemingly harmless program that, once executed, performs malicious actions like installing malware, stealing sensitive data, or taking control of the system.
- **Backdoor:** A hidden code or mechanism within a system that allows an attacker to access the system without going through normal authentication processes.

How they are used:

- **Trojan Horse Distribution:** Often delivered through phishing emails, malicious links, or disguised as legitimate software updates, tricking users into downloading and running them.
- **Backdoor Implementation:** Can be intentionally built into software by a developer (sometimes for legitimate troubleshooting purposes) or inserted by a hacker through malware.

Types of Trojan Horses:

- **Remote Access Trojan (RAT):** Provides complete control over a victim's computer, allowing attackers to monitor activity, steal data, and execute commands remotely.
- **Banking Trojan:** Specifically targets online banking credentials by capturing login information entered by the user.
- **Downloader Trojan:** Downloads and installs additional malware onto a compromised system.
- **Spyware Trojan:** Monitors user activity by logging keystrokes, capturing screenshots, and tracking browsing history.

Impact of Backdoors:

- **Data Exfiltration:** Allows attackers to steal sensitive information like login credentials, financial details, or intellectual property.
- **Persistent Access:** Enables attackers to maintain access to a system even after the initial infection, allowing them to launch further attacks.
- **Botnet Creation:** Can be used to turn compromised computers into part of a larger network (botnet) to launch distributed denial-of-service (DDoS) attacks.

Important Considerations:

- **Detection and Prevention:** Antivirus software, firewalls, and user awareness training are crucial to identify and prevent Trojan Horse and backdoor threats.
- **Software Updates:** Regularly updating software to patch known vulnerabilities is essential.
- **Email Security:** Be cautious when opening email attachments and links, especially from unknown senders.

Steganography

In cybercrime, steganography refers to the practice of hiding sensitive information within seemingly normal digital media like images, audio files, or documents, allowing malicious actors to covertly transmit stolen data or malicious code without raising suspicion by embedding it within seemingly innocent files; essentially, it's a way to "hide in plain sight" by concealing secret messages within other data streams.

How steganography works

Steganography works by concealing information in a way that avoids suspicion. One of the most prevalent techniques is called ‘least significant bit’ (LSB) steganography. This involves embedding the secret information in the least significant bits of a media file.

For example:

- In an image file, each pixel is made up of three bytes of data corresponding to the colors red, green, and blue. Some image formats allocate an additional fourth byte to transparency, or ‘alpha’.
- LSB steganography alters the last bit of each of those bytes to hide one bit of data. So, to hide one megabyte of data using this method, you would need an eight-megabyte image file.
- Modifying the last bit of the pixel value doesn’t result in a visually perceptible change to the picture, which means that anyone viewing the original and the steganographically-modified images won’t be able to tell the difference.

The same method can be applied to other digital media, such as audio and video, where data is hidden in parts of the file that result in the least change to the audible or visual output.

Types of steganography

From a digital perspective, there are five main types of steganography. These are:

1. Text steganography
2. Image steganography
3. Video steganography
4. Audio steganography
5. Network steganography

Text steganography

Text steganography involves hiding information inside text files. This includes changing the format of existing text, changing words within a text, using context-free grammars to generate readable texts, or generating random character sequences.

Image steganography

This involves hiding information within image files. In digital steganography, images are often used to conceal information because there are a large number of elements within the digital representation of an image, and there are various ways to hide information inside an image.

Audio steganography

Audio steganography involves secret messages being embedded into an audio signal which alters the binary sequence of the corresponding audio file. Hiding secret messages in digital sound is a more difficult process compared to others.

Video steganography

This is where data is concealed within digital video formats. Video steganography allows large amounts of data to be hidden within a moving stream of images and sounds. Two types of video steganography are:

- Embedding data in uncompressed raw video and then compressing it later
- Embedding data directly into the compressed data stream

Network steganography

Network steganography, sometimes known as protocol steganography, is the technique of embedding information within network control protocols used in data transmission such TCP, UDP, ICMP, etc.

DoS and DDoS Attacks

In cyber security, a "DoS" (Denial-of-Service) attack involves flooding a target system with traffic from a single source, while a "DDoS" (Distributed Denial-of-Service) attack uses

multiple compromised devices to overwhelm the target with traffic from various locations, making it significantly harder to defend against; common tools used to launch these attacks include Low Orbit Ion Cannon (LOIC), High Orbit Ion Cannon (HOIC), Slowloris, and various botnet controllers which can command large networks of infected devices to participate in a DDoS attack.

Key points about DoS and DDoS attacks and related tools:

- **DoS attacks:**
    - Use a single source to send a large volume of traffic to a target server, aiming to overload its resources and make it unavailable to legitimate users.
    - Tools like LOIC or a simple script can be used to launch a DoS attack.
    - May exploit specific vulnerabilities in the target system to amplify the attack.
- **DDoS attacks:**
    - Utilize multiple compromised devices (often part of a botnet) to launch a coordinated attack against a target, generating significantly more traffic than a DoS attack.
    - Tools like HOIC, which can manage multiple attack vectors, are often used for DDoS attacks.
    - Can be more difficult to mitigate due to the distributed nature of the attack.

Some other commonly cited DoS/DDoS attack tools:

- **HTTP Flood:** Sends a large number of HTTP requests to a web server, overwhelming its processing capabilities.
- **SYN Flood:** Exploits the TCP handshake process by sending numerous SYN packets without completing the connection, causing the server to exhaust resources.
- **UDP Flood:** Sends large volumes of UDP packets to the target server, which can overload its network interface.
- **Slowloris:** A "low and slow" attack that sends partial HTTP requests at a slow rate to keep the server busy processing incomplete connections.

Important considerations:

- **Ethical use:** It is crucial to only use these tools for legitimate penetration testing purposes with proper authorization and to never target systems you do not have permission to access.
- **Defense mechanisms:** Organizations can implement various mitigation strategies against DoS/DDoS attacks, including traffic filtering, rate limiting, scaling infrastructure, and utilizing cloud-based DDoS protection services.

SQL Injection (SQLi)

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. This can allow an attacker to view data that they are not normally able to retrieve. This might include data that belongs to other users, or any other data that the application can access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

In some situations, an attacker can escalate a SQL injection attack to compromise the underlying server or other back-end infrastructure. It can also enable them to perform denial-of-service attacks.

How SQL Injection Works

1. **User Input is Not Properly Sanitized:**
    - If a web application directly incorporates user input into an SQL query **without validation**, it becomes vulnerable.
2. **Attacker Injects Malicious SQL Code:**
    - Instead of expected input, an attacker submits **SQL commands** that alter the intended query behavior.
3. **Database Executes the Malicious Query:**
    - If the application does not properly escape or filter inputs, the SQL code runs with **unexpected effects**, such as **dumping sensitive data**.

Example of SQL Injection

Vulnerable Query

sql

CopyEdit

```
SELECT * FROM users WHERE username = 'user123' AND password = 'pass123';
```

- A legitimate login request might send user123 and pass123.

SQL Injection Attack

If the attacker inputs **' OR '1'='1** as the password:

sql

CopyEdit

```
SELECT * FROM users WHERE username = 'user123' AND password = '' OR '1'='1';
```

- Since **'1'='1'** always evaluates **TRUE**, the query returns **all users**, potentially bypassing authentication.

Types of SQL Injection

1. **Classic SQLi (Error-Based)**

- The attacker manipulates the query and uses **database error messages** to extract data.

2. **Blind SQLi**
   - No error messages are displayed; the attacker tests queries based on **true/false responses**.
3. **Time-Based SQLi**
   - The attacker uses database **delays (SLEEP commands)** to infer query success or failure.
4. **Union-Based SQLi**
   - The attacker appends UNION SELECT statements to extract **additional data**.

What is the impact of a successful SQL injection attack?

A successful SQL injection attack can result in unauthorized access to sensitive data, such as:

- Passwords.
- Credit card details.
- Personal user information.

Buffer Overflow

What is Buffer Overflow?

Buffer overflow is a software coding error or vulnerability that can be exploited by hackers to gain unauthorized access to corporate systems. It is one of the best-known software security vulnerabilities yet remains common. This is partly because buffer overflows can occur in various ways and the techniques used to prevent them are often error-prone.

The software error focuses on buffers, which are sequential sections of computing memory that hold data temporarily as it is transferred between locations. Also known as a buffer overrun, buffer overflow occurs when the amount of data in the buffer exceeds its storage capacity. That extra data overflows into adjacent memory locations and corrupts or overwrites the data in those locations.

What is a Buffer Overflow Attack?

A buffer overflow attack takes place when an attacker manipulates the coding error to carry out malicious actions and compromise the affected system. The attacker alters the application's execution path and overwrites elements of its memory, which amends the program's execution path to damage existing files or expose data.

A buffer overflow attack typically involves violating programming languages and overwriting the bounds of the buffers they exist on. Most buffer overflows are caused by the combination of manipulating memory and mistaken assumptions around the composition or size of data.

A buffer overflow vulnerability will typically occur when code:

1. Is reliant on external data to control its behavior
2. Is dependent on data properties that are enforced beyond its immediate scope
3. Is so complex that programmers are not able to predict its behavior accurately

Buffer overflow consequences

Common consequences of a buffer overflow attack include the following:

1. **System crashes**: A buffer overflow attack will typically lead to the system crashing. It may also result in a lack of availability and programs being put into an infinite loop.
2. **Access control loss**: A buffer overflow attack will often involve the use of arbitrary code, which is often outside the scope of programs' security policies.
3. **Further security issues**: When a buffer overflow attack results in arbitrary code execution, the attacker may use it to exploit other vulnerabilities and subvert other security services.

Types Of Buffer Overflow Attacks

There are several types of buffer overflow attacks that attackers use to exploit organizations' systems. The most common are:

1. **Stack-based buffer overflows**: This is the most common form of buffer overflow attack. The stack-based approach occurs when an attacker sends data containing malicious code to an application, which stores the data in a stack buffer. This overwrites the data on the stack, including its return pointer, which hands control of transfers to the attacker.
2. **Heap-based buffer overflows**: A heap-based attack is more difficult to carry out than the stack-based approach. It involves the attack flooding a program's memory space beyond the memory it uses for current runtime operations.
3. **Format string attack**: A format string exploit takes place when an application processes input data as a command or does not validate input data effectively. This enables the attacker to execute code, read data in the stack, or cause segmentation faults in the application. This could trigger new actions that threaten the security and stability of the system.

Attacks on Wireless Network

Wireless network attacks refer to malicious activities or strategies aimed at exploiting the vulnerabilities of wireless communication systems, including Wi-Fi networks, mobile data networks, and Bluetooth connections. The goal of these attacks can range from unauthorized data interception and tampering to network disruption and device control. As wireless networks

broadcast data through the air, they inherently present more accessibility points for potential attackers compared to wired networks. Consequently, without robust security measures in place, these networks can be susceptible to unauthorized access and misuse, jeopardizing both personal and business data.

Common Types of Wireless Network Attacks

1. Eavesdropping

Eavesdropping, often referred to as "sniffing", is a passive attack where an unauthorized individual intercepts and reads the traffic over a wireless network. Essentially, the attacker "listens in" on the wireless signals being transmitted between devices and the network access points.

How does it work?

Capturing airborne data: Since wireless networks operate by transmitting data using electromagnetic waves, these signals can be captured by any device within range that's equipped with the appropriate receiving antenna and software.

Decoding: If the data is unencrypted, an eavesdropper can easily read the captured data directly. However, if the data is encrypted, the attacker would need additional tools or techniques to decode and understand the intercepted information.

Use of sniffing tools: There are software tools specifically designed to facilitate sniffing, allowing attackers to analyze and sort the captured data packets. Examples include Wireshark and Aircrack-ng.

2. Man-In-The-Middle Attacks (MITM)

A Man-In-The-Middle Attack, often abbreviated as MITM, is a form of wireless network attack where an attacker secretly intercepts and relays communication between two parties. The attacker makes independent connections with the victims and relays messages between them, making them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

How does it work?

Interception: The attacker first needs to insert themselves between the victim and the entity they are communicating with (e.g., between a user and a Wi-Fi network).

Decryption (if necessary): If the intercepted data is encrypted, the attacker would need to decrypt it. This can be done using various techniques, one common method being the use of rogue Wi-Fi access points in wireless network scenarios.

Relay and capture: The attacker captures the outgoing messages from a source, potentially alters them, and then sends them to the intended recipient. The recipient, believing the communication is secure, responds, which the attacker can again capture, alter, and relay.

Termination: Once the attacker has gained the desired information or caused sufficient disruption, they can end the session, and the victims might remain unaware of the breach.

3. Evil twin attack

An Evil Twin Attack involves an attacker setting up a rogue wireless access point that mimics or impersonates a legitimate one. This malicious access point is the "evil twin" of the legitimate network. Unsuspecting users, thinking they are connecting to a trusted or known network, instead connect to the rogue access point set up by the attacker.

How does it work?

Setup: The attacker configures a device to act as a wireless access point, often using a common network name (SSID) that potential victims might recognize, such as "Free Airport Wi-Fi" or duplicating the name of a nearby legitimate network.

Broadcasting: The evil twin access point broadcasts its SSID, waiting for devices to connect to it. In some scenarios, an attacker might also deploy a jamming attack on the legitimate access point to make users more likely to connect to the stronger-signal evil twin.

Interception: Once a user connects to the evil twin, they may be presented with a fake login page to capture credentials, or the attacker can simply monitor their online activity, capturing any unencrypted data that is transmitted.

Manipulation: In advanced scenarios, the attacker might alter the data being sent or received by the victim or redirect them to malicious websites.

4. **WEP/WPA key cracking**

WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) are encryption protocols designed to secure wireless networks. Cracking these keys refers to the process of deciphering or obtaining the encryption keys used by these protocols without authorization. The goal is typically to gain unauthorized access to the network and potentially eavesdrop on or alter transmitted data. While WEP has been largely deprecated due to its known vulnerabilities, WPA and its successor, WPA2, remain widely used. It's essential to be aware of the vulnerabilities in older encryption methods and always opt for the most robust and updated security protocols available, such as WPA3.

Common tools:

Aircrack-ng: Perhaps the most popular suite of tools for cracking wireless encryption. It can crack WEP keys and retrieve the passphrase from WPA/WPA2-protected networks given enough data packets.

Airsnort: Another tool for decrypting WEP encryption on Wi-Fi networks. It passively monitors transmissions and computes encryption keys once it gathers enough packets.

Wireshark: A network protocol analyzer, not exclusively for wireless cracking but can be used in tandem with other tools to capture packets and analyze traffic.

Reaver: This tool specifically targets WPS (Wi-Fi Protected Setup) vulnerabilities in routers, which can indirectly compromise WPA/WPA2 security.

Kismet: A wireless network detector, sniffer, and intrusion detection system. It can be used to detect networks and capture data packets, which can later be used to crack encryption keys.

5. Deauthentication attacks

A Deauthentication Attack involves an attacker sending deauthentication frames in a Wi-Fi network with the intention of forcibly disconnecting a wireless client from an access point. By masquerading as the target device or the access point, the attacker can convince the other party to drop the connection. This type of attack targets the communication rather than the encryption, rendering even well-protected networks vulnerable.

How do deauthentication attacks work?

Frame spoofing: The attacker sends fraudulent deauthentication frames (packets) to either the client or the access point. These frames are crafted to appear as if they come from the other party.

Disconnection: Upon receiving these frames, the targeted device (either the client or the access point) terminates the connection, believing it to be a legitimate request.

Network disruption: The attack can be continuous, sending deauthentication frames at intervals to keep the device disconnected or prevent reconnection, causing persistent disruptions.

PCET's

Pimpri Chinchwad University

School of Computer Applications

BSc (CS)-II SEM-IV

Cyber Laws and Security Policies

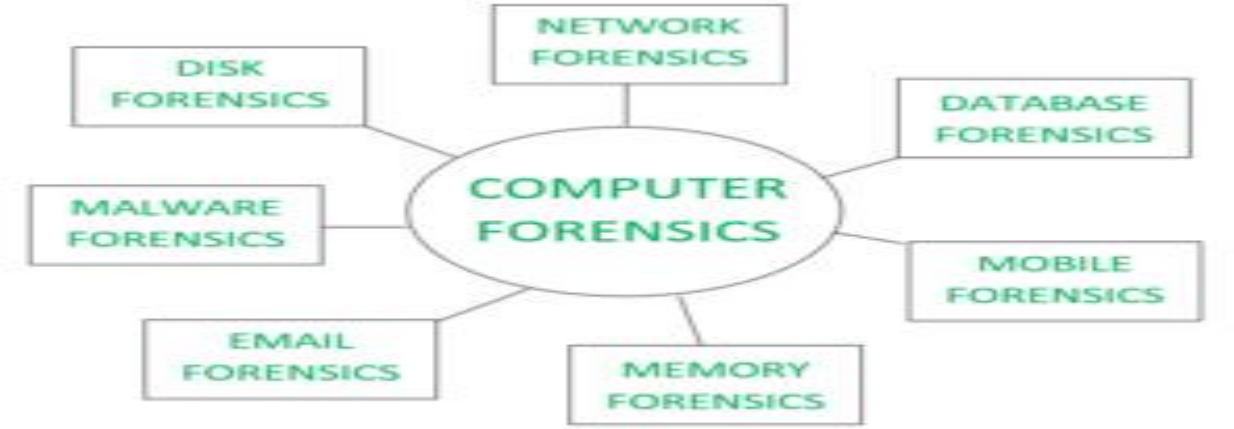
Unit No. 04 Understanding Computer Forensics

Introduction:

Computer Forensics is a scientific method of investigation and analysis in order to gather evidence from digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

TYPES

- **Disk Forensics:** It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.
- **Network Forensics:** It is a sub-branch of Computer Forensics that involves monitoring and analyzing the computer network traffic.
- **Database Forensics:** It deals with the study and examination of databases and their related metadata.
- **Malware Forensics:** It deals with the identification of suspicious code and studying viruses, worms, etc.
- **Email Forensics:** It deals with emails and their recovery and analysis, including deleted emails, calendars, and contacts.
- **Memory Forensics:** Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analyzing it for further investigation.
- **Mobile Phone Forensics:** It mainly deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc., and other data present in it.



CHARACTERISTICS

- **Identification:** Identifying what evidence is present, where it is stored, and how it is stored (in which format). Electronic devices can be personal computers, Mobile phones, PDAs, etc.
- **Preservation:** Data is isolated, secured, and preserved. It includes prohibiting unauthorized personnel from using the digital device so that digital evidence, mistakenly or purposely, is not tampered with and making a copy of the original evidence.
- **Analysis:** Forensic lab personnel reconstruct fragments of data and draw conclusions based on evidence.
- **Documentation:** A record of all the visible data is created. It helps in recreating and reviewing the crime scene. All the findings from the investigations are documented.
- **Presentation:** All the documented findings are produced in a court of law for further investigations.

Historical Background of Cyberforensics:

1970s – Emergence of Digital Data: The earliest forms of digital forensics can be traced back to the 1970s, when digital data started becoming more prevalent. Computers were primarily mainframes and minicomputers at this time.

1980s – Growth of Personal Computers: With the rise of personal computers in the 1980s, there was an increased need for methods to investigate computer-related crimes. Early digital forensics efforts focused on analyzing computer systems to recover evidence.

1990s – Establishment of Techniques: The 1990s saw the establishment of foundational techniques and tools for digital forensics. Law enforcement agencies and cybersecurity experts began developing protocols and methodologies for investigating digital crimes.

Late 1990s – Internet and Cybercrimes: As the internet became more accessible and widespread, cybercrimes emerged as a major concern. Digital forensics had to adapt to the challenges posed by crimes committed online, such as hacking, identity theft, and online fraud.

Early 2000s – Formalization and Standardization: The early 2000s brought about greater formalization and standardization of digital forensics processes. Organizations like the International Association of Computer Investigative Specialists (IACIS) and the National Institute of Standards and Technology (NIST) started providing guidelines and best practices for digital investigations.

Mid 2000s – Mobile Devices and Digital Media: The increase of mobile devices and digital media storage expanded the scope of digital forensics. Analysts had to develop techniques for extracting evidence from a variety of devices, including cell phones, USB drives, and memory cards.

Late 2000s – Cloud Computing and Virtualization: The advent of cloud computing and virtualization presented new challenges for digital forensics. Investigators had to adapt to the decentralized nature of data storage and the complexities of virtual environments.

2010s – Big Data and Advanced Techniques: The explosion of big data and the use of advanced technologies like machine learning and artificial intelligence started influencing digital forensics. These technologies allowed for more efficient analysis of large volumes of data to uncover patterns and insights.

Present and Beyond – Evolving Landscape: Digital forensics continues to evolve as technology advances. The increasing use of encryption, the Internet of Things (IoT), blockchain, and other emerging technologies presents both new opportunities and challenges for digital investigators.

Throughout its history, digital forensics has become an integral part of law enforcement, cybersecurity, and legal proceedings. Its creation and growth have benefited the community at large.

Digital Forensics Science

It is a branch of cyber security which mainly focus on investigation of cyber crime cases. Digital forensics recover and store the collected data securely to analyze and find the evidences from digital devices. Digital forensics can be used in wide range cases which includes cybercrime, criminal investigation, frauds etc. Digital forensic investigations can bring out very

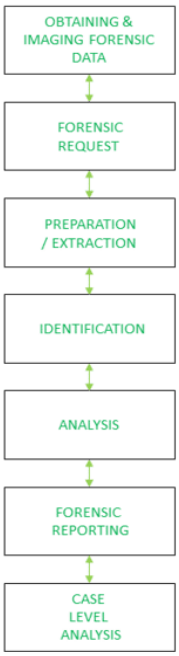
crucial information after cyberattacks which can be very helpful during the hearing process in the court of law.

Where Digital Forensics in Cyber Security is Used?

Digital forensics is used to gather electronic evidence, assets, and data from digital devices, systems, or the internet. It is also used to retrieve and analyze this information by following proper steps. Digital forensics is used to investigate cyberattacks, data breaches, intellectual property theft, fraud, and other criminal activities. It can be used as:

- To Identify the cause and reason behind the cyberattacks
- Containing and rectifying the attacks
- Protecting digital evidence before its vulnerability gets exploits
- Tracking back the hacker's footprints and discovering the tools used by the hackers
- Determining if data was read or stole
- Determining the period during which the network was illegally accessed
- Tracing the login activities of the hacker to trace their origin

How Is Digital Forensics Used in an Investigation?



- **Obtaining & imaging forensic data:** Imaging is a very important and crucial step whenever a forensic examiner investigates a case. The purpose of imaging is to copy and create a replica of every single bit of original data to use it for analysis while ensuring that the original data remains untouched. This ensures the integrity and preservation of the data throughout the analysis process.
- **Forensic Request:** A forensic request is a request to investigate a case within a given outline, including the purpose, scope, authority, methodology, expected deliverables, and confidentiality measures. This outline provides a clear understanding of the case.
- **Preparation/Extraction:** The preparation in digital forensic is very important phase in which the forensic environment is prepared and selection and testing of necessary tools is done and ensuring the legal requirements met or not. The proper documentation is maintained to show step-by-step process and steps taken by examiners to have better understanding about the investigation for any new examiner. After that the extraction of data which contains system files, deleted files, system logs, network data and application data.
- **Identification:** Identification of relevant data from the extracted data which includes files, logs, mails and other data. the identification is important because it helps you to not mislead or stuck in the case and can help you to speed up to solve the case.
- **Analysis:** Analysis of identified data to find the hidden evidence and patterns. In the analysis process we can analyze about who created, and modified files and application

also where it is found and when it is created and where it is sent. The analysis tells what happened with the system when the specific file is transmitted.

- **Forensic reporting:** Creating a detailed report about the case findings, proper chain of custody, tools used, methodologies used, conclusion and proper documentation which is presentable in legal contexts.
- **Case level analysis:** The final analysis by studying and reviewing the case again with all findings and evidence to made understanding and to find out the final conclusion.

The Need for Computer Forensics

The increasing reliance on digital devices and the rise of cybercrime necessitates computer forensics, a field that identifies, collects, preserves, and analyses digital evidence to solve crimes, recover data, and ensure justice.

Here's a more detailed explanation of why computer forensics is so important:

1. Solving Cybercrimes and Digital Offenses:

Recovering Data: Computer forensics helps recover lost, damaged, or deleted data from computers, mobile devices, and other digital storage media.

Identifying Perpetrators: By analyzing digital evidence, investigators can trace the origin of cyberattacks, identify suspects, and gather evidence for legal proceedings.

Investigating Cybercrimes: Computer forensics plays a crucial role in investigating a wide range of cybercrimes, including data breaches, hacking, fraud, intellectual property theft, and cyberstalking.

Supporting Legal Cases: The findings of computer forensics investigations can be used as evidence in court to secure convictions and ensure justice for victims.

2. Protecting Intellectual Property and Corporate Security:

Intellectual Property Theft: Computer forensics can help identify and recover stolen intellectual property, such as trade secrets, confidential information, and copyrighted material.

Corporate Security: Organizations use computer forensics to investigate cyberattacks, identify vulnerabilities, and improve their security posture.

Incident Response: Computer forensics is a key component of incident response, helping organizations detect, analyze, and remediate security incidents.

3. National Security and Law Enforcement:

Cyber Espionage: Computer forensics can help identify and investigate cyber espionage, where foreign governments or actors attempt to steal sensitive information.

National Security: As cybercrimes continue to escalate, computer forensics has become an important tool for national security agencies.

Law Enforcement: Law enforcement agencies rely on computer forensics to investigate a wide range of crimes, including cybercrimes and traditional crimes where digital evidence is involved.

4. Regulatory Compliance and Auditing:

Compliance: Computer forensics can help organizations ensure compliance with industry regulations and legal requirements related to data privacy and security.

Auditing: Computer forensics can be used to audit computer systems and networks to identify vulnerabilities and ensure that security policies are being followed.

Cyber Forensics and Digital Evidences

Cyber forensics, also known as digital forensics, involves identifying, preserving, collecting, and analyzing digital evidence like text messages, emails, and browsing history, used in legal proceedings or investigations.

What is Cyber Forensics?

- Cyber forensics (or digital forensics) is the process of examining digital data to uncover evidence related to a crime, incident, or other event.
- It involves using specialized tools and techniques to extract, analyze, and preserve digital evidence from various sources, including computers, mobile devices, networks, and the cloud.
- The goal is to reconstruct events, identify perpetrators, and gather evidence that can be used in legal proceedings or internal investigations.

What is Digital Evidence?

- Digital evidence encompasses any electronically stored or transmitted information that can be used as proof in a legal proceeding or investigation.
- Examples of digital evidence include:
    - Emails and text messages
    - Internet browsing history
    - Social media posts
    - Documents, images, and videos
    - Metadata (data about data)
    - Network traffic
- Digital evidence can be found on a variety of devices, including computers, mobile phones, servers, and network devices.

Key Characteristics of Digital Evidence:

- **Volatility:** Digital evidence can be easily altered or deleted, so it's crucial to preserve it as quickly as possible.
- **Interconnectivity:** Digital evidence is often interconnected with other evidence, so it's important to consider the context in which it was created.
- **Complexity:** Digital evidence can be complex and require specialized knowledge and tools to analyze.
- **Preservation:** Digital evidence must be preserved in a way that maintains its integrity and admissibility in court.

Stages of a Digital Forensics Investigation:

1. **Identification:** Identifying the resources and devices involved in the investigation.
2. **Preservation:** Preserving the necessary data to ensure its integrity.
3. **Analysis:** Analysing the collected data to identify relevant information.
4. **Documentation:** Documenting all steps taken during the investigation.
5. **Presentation:** Presenting the findings in a clear and concise manner.

Forensic Analysis of E-Mail

What are Email Forensics?

Email forensics is dedicated to investigating, extracting, and analysing emails to collect digital evidence as findings in order to crack crimes and certain incidents, in a forensically sound manner.

The process of email forensics, it's conducted across various aspects of emails, which mainly includes

- Email messages
- Email addresses (sender and recipient)
- IP addresses
- Date and time
- User information
- Attachments
- Passwords
- logs (Cloud, server, and local computer)

How Email Works?

Just like other digital forensics technology, it's not easy to conduct forensics without understanding the basis of the underlying technologies.
Emails are probably generated from various mediums and approaches and thus different technologies are applied accordingly.

Commonly speaking, a man writes an email on his digital device, maybe a phone or computer, and then sends it to the one he wants to. Though it's seemingly the man has finished his work, the upon email processing work just starts in order to successfully and correctly be delivered to the recipient.

When an email is sent out, countless servers are actually undertaken the whole information of the email before it can really arrive in the recipient's inbox, which is said that we have to understand what's proceeding after we click the "send" button.

Email Programs and Protocols

During the process, there are 3 protocols and 3 email programs tightly related and are vital to be known.

- Simple Mail Transfer Protocol (SMTP): it is the standard Protocol used to transmit and send emails.
- Internet Message Access Protocol (IMAP): it is one of the standard protocols used for receiving emails.
- POP3 (Post Office Protocol 3): it is one of the standard protocols used to receive mail.
- Mail Transfer Agent (MTA): sends and forwards emails through SMTP. e.g. Sendmail, postfix.
- Mail User Agent (MUA): mail client used to receive emails, which uses IMAP or POP3 protocol to communicate with the server. e.g. Outlook, Apple Mail, Gmail.
- Mail Delivery Agent (MDA): saves the mails received by MTA to local, cloud disk or designated location, meanwhile it usually scans for spam mails and viruses. e.g. Promail, Dropmail.
- Mail Receive Agent (MRA): implements IMAP and POP3 protocol, and interacts with MUA. e.g. dovecot

How to Conduct Email Forensics Investigation?

With the increasing popularity of the use of email based on the boom of the internet, some typical crimes are tied to email. For instance, financial crime, cyber security, and extortion software, to name a few.

To bring email criminals to justice, it's crucial to look into email investigation in cyber security. Before we can dive into the major investigative extraction working directions of email forensics, be noted:

1. **Local Computer-based emails:** For local computer-based email data files, such as Outlook .pst or .ost files, it's recommended to follow our following techniques directly.

2. **(Cloud）Server-based emails:** For （Cloud）Server based email data files, it's not possible to conduct complete forensic work until you obtain the electronic copies in the (Cloud)server database under the consent of the service providers.
3. **Web-based emails:** For Web-based e-mail (e.g. Gmail,) investigations, it's more likely possible to just filter specific keywords to extract email address-related information instead of the overall email data and information compared to local computer-based emails.

Viewing and Analysing E-mail Headers

The primary evidence in email investigations is the email header where massive and valuable information could be found.

When carrying out the analysis, you'd be advised to get started from the bottom to the top, since the most crucial information from the sender would be on the bottom while information about the receiver would be on the topmost.

Since we already talked about MTAs where you could find out the route of the email transferred, it should be good for you to give it a detailed scan of the email header.

Email Server Investigation

To locate the source of an email, it's required to investigate the email's servers. Since it's not surprising criminals tend to delete their emails in case of being caught or accused of sensitive emails.

However, there is still a chance to get them back.

In extreme cases, even though both emails have been deleted from both sides between senders and recipients, a copy might be still on the server, since there is always retention on the server after the email is successfully delivered each time due to specific government regulations for email.

Whereas, you don't want to miss out on investigating the log before it is archived after a certain period.

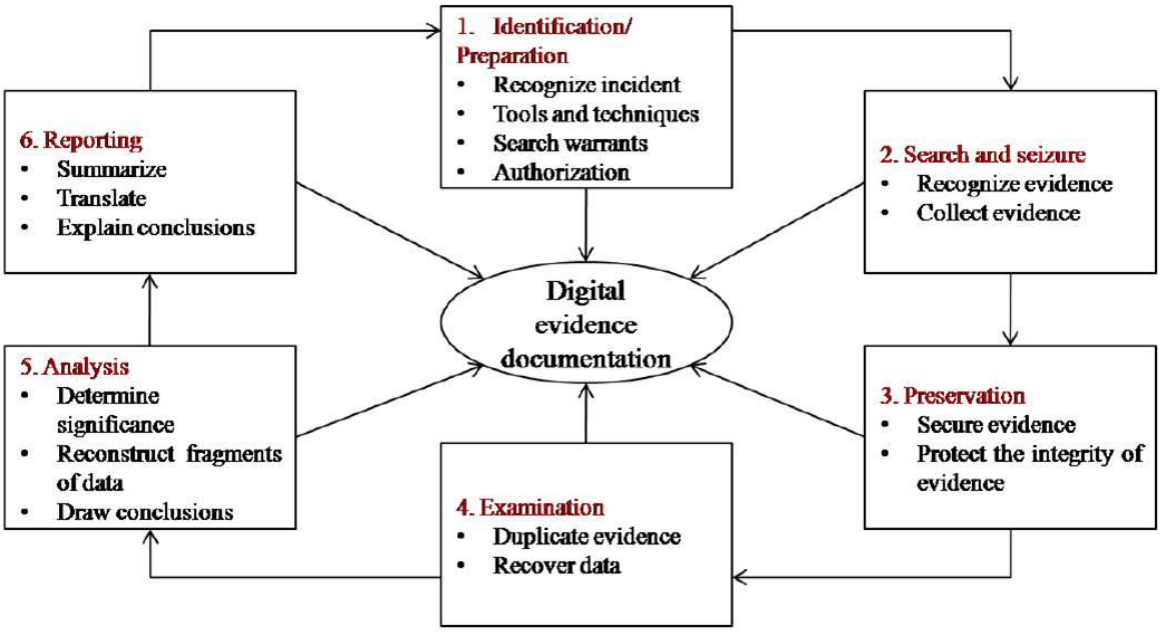
Digital Forensics Life Cycle

The digital forensics process is shown in the following figure. Forensic life cycle phases are:

1. Preparation and identification
2. Collection and recording
3. Storing and transporting
4. Examination/investigation
5. Analysis, interpretation, and attribution

6. Reporting

7. Testifying



1. Preparing for the Evidence and Identifying the Evidence

In order to be processed and analysed, evidence must first be identified. It might be possible that the evidence may be overlooked and not identified at all. A sequence of events in a computer might include interactions between:

- Different files
- Files and file systems
- Processes and files
- Log files

In case of a network, the interactions can be between devices in the organization or across the globe (Internet). If the evidence is never identified as relevant, it may never be collected and processed.

2. Collecting and Recording Digital Evidence

Digital evidence can be collected from many sources. The obvious sources can be:

- Mobile phone
- Digital cameras
- Hard drives
- CDs
- USB memory devices

Non-obvious sources can be:

- Digital thermometer settings
- Black boxes inside automobiles
- RFID tags

Proper care should be taken while handling digital evidence as it can be changed easily. Once changed, the evidence cannot be analysed further. A cryptographic hash can be calculated for the evidence file and later checked if there were any changes made to the file or not. Sometimes important evidence might reside in the volatile memory. Gathering volatile data requires special technical skills.

3. Storing and Transporting Digital Evidence

Some guidelines for handling of digital evidence:

- Image computer-media using a write-blocking tool to ensure that no data is added to the suspect device
- Establish and maintain the chain of custody
- Document everything that has been done
- Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability

Care should be taken that evidence does not go anywhere without properly being traced. Things that can go wrong in storage include:

- Decay over time (natural or unnatural)
- Environmental changes (direct or indirect)
- Fires
- Floods
- Loss of power to batteries and other media preserving mechanisms

Sometimes evidence must be transported from place to place either physically or through a network. Care should be taken that the evidence is not changed while in transit. Analysis is generally done on the copy of real evidence. If there is any dispute over the copy, the real can be produced in court.

4. Examining/Investigating Digital Evidence

Forensics specialist should ensure that he/she has proper legal authority to seize, copy and examine the data. As a general rule, one should not examine digital information unless one has the legal authority to do so. Forensic investigation performed on data at rest (hard disk) is called dead analysis.

Many current attacks leave no trace on the computer's hard drive. The attacker only exploits the information in the computer's main memory. Performing forensic investigation on main memory is called live analysis. Sometimes the decryption key might be available only in RAM. Turning off the system will erase the decryption key. The process of creating and exact duplicate of the original evidence is called imaging. Some tools which can create entire hard drive images are:

- DCFLdd
- Iximager
- Guymager

The original drive is moved to secure storage to prevent tampering. The imaging process is verified by using the SHA-1 or any other hashing algorithms.

5. Analysis, Interpretation and Attribution

In digital forensics, only a few sequences of events might produce evidence. But the possible number of sequences is very huge. The digital evidence must be analyzed to determine the type of information stored on it. Examples of forensics tools:

- Forensics Tool Kit (FTK)
- EnCase
- Scalpel (file carving tool)
- The Sleuth Kit (TSK)
- Autopsy

Forensic analysis includes the following activities:

- Manual review of data on the media
- Windows registry inspection
- Discovering and cracking passwords
- Performing keyword searches related to crime
- Extracting emails and images

Types of digital analysis:

- Media analysis
- Media management analysis
- File system analysis
- Application analysis
- Network analysis
- Image analysis
- Video analysis

6. Reporting

After the analysis is done, a report is generated. The report may be in oral form or in written form or both. The report contains all the details about the evidence in analysis, interpretation, and attribution steps. As a result of the findings in this phase, it should be possible to confirm or discard the allegations. Some of the general elements in the report are:

- Identity of the report agency
- Case identifier or submission number
- Case investigator
- Identity of the submitter
- Date of receipt
- Date of report
- Descriptive list of items submitted for examination
- Identity and signature of the examiner
- Brief description of steps taken during examination
- Results / conclusions

7. Testifying

This phase involves presentation and cross-examination of expert witnesses. An expert witness can testify in the form of:

- Testimony is based on sufficient facts or data
- Testimony is the product of reliable principles and methods
- Witness has applied principles and methods reliably to the facts of the case

Experts with inadequate knowledge are sometimes chastised by the court. Precautions to be taken when collecting digital evidence are:

- No action taken by law enforcement agencies or their agents should change the evidence
- When a person to access the original data held on a computer, the person must be competent to do so
- An audit trial or other record of all processes applied to digital evidence should be created and preserved
- The person in-charge of the investigation has overall responsibility for ensuring that the law and these are adhered to

Chain of Custody

A chain of custody is the process of validating how evidences have been gathered, tracked, and protected on the way to the court of law. Forensic professionals know that if you do not have a chain of custody, the evidence is worthless.

The chain of custody is a chronological written record of those individuals who have had custody of the evidence from its initial acquisition to its final disposition. A chain of custody begins when evidence is collected and the chain is maintained until it is disposed off. The chain of custody assumes continuous accountability.

Network Forensics

Today's networks are mainly wireless networks. Most of the Wi-Fi communications are unprotected. Wireless forensics is a part of network forensics, which in turn is a part of computer forensics.

Wireless forensics is the methodology and tools required to collect, analyze the network traffic that can be presented as valid digital evidence in the court of law. The evidence collected can include plain data, or VoIP information (voice calls).

Wireless forensics process involves:

- Capturing all data moving over the Wi-Fi network
- Analysing network events to uncover anomalies
- Discovering source of security attacks
- Investigating breaches on computers and wireless networks

Challenges in Computer Forensics

Although there are well-developed forensic techniques, cybercrime investigation is not easy. Huge amount of data is available and searching for evidence in that enormous data is not easy. Most of the existing tools allow anyone to change the attribute associated with digital data.

Encryption is a commonly used ant forensics technique and keyword search can be defeated by renaming file names. Cybercrime investigators often face a problem of collecting evidence from very large groups of files. They need to use techniques like link analysis and visualization. To find leads they need to use machine learning techniques (patterns).

- Networks span multiple time zones and multiple jurisdictions
- Network data will be available offline and online (real-time)
- Real-time data requires ability to capture and analyze data on the fly
- The data may involve different protocols
- The data may be huge due to increasing bandwidth
- A protocol might also involve multiple layers of signal (VoIP, HTTP tunneling)
- Current forensic tools will not be able to handle real-time data and huge amount of data

Technical Challenges

The two challenges faced in a digital forensic investigation are complexity and quantity. The complexity problem refers to the data collected being at the lowest level or in raw format. Non-technical people will find it difficult to understand such data.

Tools can be used to transform the data from low level format to readable format. The quantity problem refers to the amount of data that needs to be analyzed. Data reduction techniques can be used to group data or remove known data. Data reduction techniques include:

- Identifying known network packets using IDS signatures
- Identifying unknown entries during log processing
- Identifying known files using hash databases
- Sorting files by their types

Legal challenges

Digital evidence can be tampered easily, sometimes, even without any traces. It is common for modern computers to have multiple gigabyte sized disks. Seizing and freezing of digital evidence can no longer be accomplished just by burning a CD-ROM. Failure to freeze the evidence prior to opening files has invalidated critical evidence.

There is also the problem of finding relevant evidence within massive amounts of data which is a daunting task. The real legal challenges involve the artificial limitations imposed by constitutional, statutory and procedural issues. There are many types of personnel involved in digital/computer forensics like technicians, policy makers, and professionals.

Technicians have sound knowledge and skills to gather information from digital devices, understand software and hardware as well as networks. Policy makes establish forensics policies that reflect broad considerations. Professionals are the link between policy and execution who have extensive technical skills as well as good understanding of the legal procedures.

Special Tools and Techniques

Digital forensics tools are software applications or hardware devices specifically designed to aid in the investigation and analysis of digital evidence. These tools assist digital forensic examiners in tasks such as data acquisition, data recovery, data analysis, and reporting.

Common digital forensics tools include:

Digital forensics tools are software applications or hardware devices specifically designed to aid in the investigation and analysis of digital evidence. These tools assist digital forensic examiners in tasks such as data acquisition, data recovery, data analysis, and reporting.

Common digital forensics tools include:

EnCase

EnCase is a popular commercial digital forensics tool that offers comprehensive capabilities for data acquisition, analysis, and reporting. It offers a comprehensive software package, from triage to final reports, streamlining the investigative process.

The recipient of SC Magazine's "Best Computer Forensic Solution" award for ten years in a row is a renowned software used in forensic cybersecurity investigations. Since 1998, EnCase has been instrumental in recovering evidence and analyzing files on hard drives and mobile phones, assisting professionals in criminal investigation cases.

Forensic Toolkit Imager (FTK)

FTK Imager, a free tool, ensures the integrity of digital evidence by analysing drive images without modifying their original state. It supports all operating systems, recovers deleted files, parses XFS files, and generates file hashes for data integrity checks. Therefore, it is a crucial tool for forensic investigations.

Autopsy

Autopsy is a modular and user-friendly digital forensics platform used by investigators to assess computer and phone data. It offers timeline analysis, hash filtering, keyword search, web artifact extraction, file recovery, and rapid identification of indicators of compromise. Background jobs run in parallel, providing quick results for targeted keywords. Autopsy also

allows for creating a centralized repository and is an open-source solution. It is currently available for Windows only.

X-Ways Forensics

It is a highly efficient work environment designed for computer forensic examiners. It is renowned for its speed and low resource consumption. Built on the WinHex hex and disk editor, X-Ways Forensics provides a range of advanced features, including disk and data capture software, cloning, imaging, and various other tools. It offers a comprehensive solution for digital forensic investigations.

Cellebrite UFED

Founded in Israel in 1999, Cellebrite specializes in mobile device forensics for law enforcement and enterprises. Their expertise lies in collecting, reviewing, analyzing, and managing data from mobile devices. The Digital Intelligence Investigative Platform offered by Cellebrite facilitates the unification of the investigative life cycle and the preservation of digital evidence.

Volatility

It is a popular open-source memory forensics tool used for analyzing volatile memory dumps to extract valuable information.

Their open-source framework enables incident response and malware detection through volatile memory forensics, preserving crucial evidence during system shutdowns. Written in Python and compatible with various machines, it analyzes cached sectors, crash dumps, DLLs, network connections, process lists, and registry files. The tool is freely available, with its code hosted on GitHub.

Wireshark

Wireshark is the world's most-used network protocol analysis tool, trusted by governments, corporations, and academic institutions worldwide. It provides microscopic-level visibility into network activity by capturing and analyzing network traffic. With a user-friendly interface available on multiple operating systems, Wireshark aids in detecting and investigating malicious activity. It supports various data sources and allows exporting of output in multiple formats.

Exterro

Founded in 2004 in Portland, Oregon, Exterro specializes in workflow-driven software and governance, risk, and compliance (GRC) solutions. With a focus on assisting in-house legal teams, streamlining compliance processes, and managing risks, Exterro offers a range of products covering e-discovery, privacy, risk management, and digital forensics. Notably, their

forensics-focused tools include capabilities for remote endpoint collection, scalable data processing, automated processes, and Mac and mobile data inquiries.

Digital Forensic Techniques

Digital forensics employs various techniques and tools to examine compromised devices. These techniques aid in uncovering hidden information, analyzing digital activity, detecting anomalies, and recovering deleted files. Here are some common techniques utilized in digital forensics.

Reverse Steganography: This involves uncovering hidden data within files by analysing data hashing, which reveals changes in the underlying data structure.

Stochastic Forensics: It helps in investigating digital activity without digital artefacts, which is particularly useful for detecting insider threats and data breaches.

Cross-drive Analysis: Professionals use this technique for correlating information across multiple drives to establish baselines and identify suspicious events.

Live Analysis: Live analysis helps in examining volatile data stored in RAM or cache while the device is running, typically conducted in a forensic lab to preserve evidence.

Deleted File Recovery: Recovering partially deleted files by searching for fragments spread across the system and memory.

Forensics Auditing

Forensics auditing is also known as forensics accounting. Forensics auditing includes the steps needed to detect and deter fraud. Forensics auditor makes use of the latest technology to examine financial documents and investigate crimes like frauds, identity theft, securities fraud, insider trading, etc.

Forensics auditors are responsible for detecting fraud, identifying individuals involved, collecting evidence, presenting the evidence, etc. Government departments or agencies can possibly use the techniques of forensics auditing to assess compliance with regulations governing payments of grants/subsidies.

PCET's

Pimpri Chinchwad University

School of Computer Applications

BSc (CS)-II SEM-IV

Cyber Laws and Security Policies

Unit No. 05 Introduction to Security Policies and Cyber Laws

Introduction:

Security Policies: Security policies are a set of rules and practices designed to protect an organization's information, assets, and technologies. These policies encompass guidelines, procedures, and protocols established to ensure the confidentiality, integrity, and availability of data. They dictate how data should be accessed, stored, transmitted, and protected within an organization. Security policies often cover areas such as data encryption, password management, network security, incident response, and employee training on security practices.

Cyber Laws: Cyber laws are legal regulations enacted to govern and control activities conducted in the cyberspace. They address various aspects of digital interactions, including online behavior, data protection, intellectual property rights, cybersecurity, and electronic transactions. Cyber laws aim to prevent cybercrimes, regulate online activities, safeguard individual privacy, and establish legal frameworks for resolving disputes arising in the digital realm. Examples of cyber laws include the General Data Protection Regulation (GDPR) in Europe, the Computer Fraud and Abuse Act (CFAA) in the United States, and various other regional or national regulations globally.

Need for an Information Security Policy

Security threats are constantly evolving, and compliance requirements are becoming increasingly complex. Organizations must create a comprehensive information security policy to cover both challenges. An information security policy makes it possible to coordinate and enforce a security program and communicate security measures to third parties and external auditors.

The importance of an information security policy

Information security policies can have the following benefits for an organization:

- **Facilitates data integrity, availability, and confidentiality** – Effective information security policies standardize rules and processes that protect against vectors threatening data integrity, availability, and confidentiality.

- **Protects sensitive data** – Information security policies prioritize the protection of intellectual property and sensitive data such as personally identifiable information (PII).
- **Minimizes the risk of security incidents** – An information security policy helps organizations define procedures for identifying and mitigating vulnerabilities and risks. It also details quick responses to minimize damage during a security incident.
- **Executes security programs across the organization** – Information security policies provide the framework for operationalizing procedures.
- **Provides a clear security statement to third parties** – Information security policies summarize the organization's security posture and explain how the organization protects IT resources and assets. They facilitate quick response to third-party requests for information by customers, partners, and auditors.
- **Helps comply with regulatory requirements** – Creating an information security policy can help organizations identify security gaps related to regulatory requirements and address them.

Information Security Practices

There are several steps that organizations can take to improve their information security:

1. **Risk assessment**: Organizations should conduct regular risk assessments to identify potential vulnerabilities and threats to their sensitive information. This allows them to prioritize their security efforts and focus on the most critical risks.
2. **Access control**: Organizations should implement strict access controls to ensure that only authorized individuals are able to access sensitive information. This can include measures such as secure authentication, multi-factor authentication, and role-based access controls.
3. **Data encryption**: Organizations should encrypt sensitive information to protect it from unauthorized access and disclosure. This can include encrypting data at rest and in transit, as well as using secure protocols for communication.
4. **Network security**: Organizations should secure their networks to prevent unauthorized access and protect against malware and other cyber threats. This can include using firewalls, intrusion detection and prevention systems, and virtual private networks (VPNs).
5. **Incident management**: Organizations should have an incident management plan in place to respond quickly and effectively to security breaches. This should include procedures for incident response, incident management, and incident reporting.

6. **Compliance**: Organizations should comply with relevant laws and regulations related to information security, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).
7. **Employee training**: Organizations should provide regular training to employees on information security best practices, policies, and procedures. This can help to ensure that employees understand the importance of protecting sensitive information and know how to do so.
8. **Regularly monitoring and testing**: Organizations should regularly monitor and test their security systems to ensure they are working properly and to identify potential vulnerabilities. This can include regular vulnerability scans, penetration testing, and security audits.

Information Security Standards

Information security standards are guidelines and best practices designed to protect information systems and data from unauthorized access, use, disclosure, disruption, modification, or destruction. These standards help organizations manage and mitigate risks related to information security.

Some of the most widely recognized information security standards include:

1. **ISO/IEC 27000 Series**: This family of standards provides a framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). The most well-known standard in this series is ISO/IEC 27001, which specifies the requirements for an ISMS2.
2. **NIST Cybersecurity Framework**: Developed by the National Institute of Standards and Technology (NIST), this framework provides a policy framework of computer security guidance for how private sector organizations in the US can assess and improve their ability to prevent, detect, and respond to cyber-attacks.
3. **Common Criteria (ISO/IEC 15408)**: This standard focuses on the certification of IT products and ensures their evaluation based on a set of approved standards widely followed by industry and governments.
4. **CIS Controls:** The Center for Internet Security (CIS) publishes security benchmarks for various devices and systems, which are widely accepted by governments and industries.

5. **ISO 22301:** This standard contains requirements for Business Continuity Management Systems, ensuring that organizations can continue operating during and after a disruptive incident.

Introducing Various Security Policies and Their Review Process

Security policies are critical frameworks that organizations use to protect sensitive data, ensure regulatory compliance, and minimize the risks of cyber threats. These policies provide guidelines for employees, contractors, and third parties on how to handle, manage, and protect information systems. Effective security policies help an organization define its security posture and manage its vulnerabilities proactively.

What is a Security Policy in Cybersecurity?

A security policy is a formal document that describes how an organization will manage and protect its information assets. It establishes guidelines regarding the handling of sensitive data, how access is granted, and implemented measures that protect it from unauthorized access and data breaches, among other cyber perils.

In other words, it gives direction on the cybersecurity strategy of the organization. It clarifies the role each employee plays in security.

Types of Security Policies

a) **Access Control Policy:** Defines who can access what resources and how, ensuring only authorized users have access.
b) **Acceptable Use Policy (AUP):** Outlines acceptable and unacceptable usage of company IT resources, including email, internet, and software.
c) **Incident Response Policy:** Establishes procedures for handling security incidents, including data breaches and cyberattacks.
d) **Data Security Policy:** Addresses the protection of sensitive data, including storage, transmission, and disposal.
e) **Physical Security Policy:** Covers the security of physical assets, such as buildings, equipment, and access points.
f) **Bring Your Own Device (BYOD) Policy:** Establishes guidelines for employees using their personal devices for work purposes
g) **Employee Training and Awareness Policy:** Ensures employees are trained on security best practices and are aware of potential threats.
h) **Remote Access Policy:** Defines how and when employees can remotely access company resources.

i) **Data Backup and Recovery Policy:** Establishes procedures for backing up and recovering data in case of a disaster or loss.

Review Process for Security Policies

A robust security policy review process is necessary to ensure that policies remain relevant, effective, and aligned with changing organizational needs and security threats.

a. Initial Policy Development:

- Involves collaboration between key stakeholders, such as IT, legal, HR, compliance, and senior management, to define the objectives and contents of the security policies.
- Initial policies should be based on industry standards and regulatory requirements, such as ISO 27001, NIST, or GDPR.

b. Periodic Review and Updates:

- **Frequency:** Security policies should be reviewed periodically (e.g., annually or biannually) to account for new security threats, regulatory changes, or business process updates.
- **Procedure:** Reviews should be conducted by a team of cross-functional stakeholders, including security experts, legal advisors, and business leaders.
- **Criteria for Review:** The review process should consider changes in the threat landscape, the effectiveness of existing controls, incidents or breaches, new compliance requirements, and advancements in technology.

c. Gap Analysis:

- **Purpose:** Identify gaps between existing security policies and current organizational practices or industry standards.
- **Method:** Compare the organization's current security posture against best practices, audit results, and new emerging threats.

d. Testing and Simulations:

- Conduct regular testing of security policies, including simulated cyberattacks (penetration tests) or breach response drills (e.g., tabletop exercises).
- This ensures that the policies are practical and can be executed effectively during an actual security incident.

e. Stakeholder Feedback:

- Engage employees and relevant stakeholders to provide feedback on the security policies. This feedback can help identify weaknesses or areas that are difficult to implement.

f. Audit and Compliance Checks:

- Security policies should be subjected to internal and external audits to ensure that they comply with relevant laws, regulations, and industry standards.
- Regular audits help assess the effectiveness of the policy and its alignment with compliance mandates.

g. Approval and Sign-off:

- Once updates or new policies are proposed, they must be reviewed and approved by senior management, legal, and compliance departments before implementation.
- Approval ensures that the organization is committed to the policies and that they have the necessary resources for execution.

h. Communication and Training:

- Once a policy is reviewed and updated, it's crucial to communicate changes to all relevant parties. Training sessions should be conducted to ensure employees understand their responsibilities under the updated policies.
- Awareness campaigns, security briefings, or hands-on workshops can be effective in ensuring that the policy is implemented successfully.

Challenges in Policy Review and Implementation

- **Changing Threat Landscape:** Cybersecurity threats are constantly evolving, making it challenging to keep security policies updated. The organization needs to stay ahead of potential risks.
- **Employee Compliance:** Ensuring that all employees follow security policies can be difficult, especially if the policies are overly complex or not enforced through proper monitoring and auditing.
- **Resource Constraints:** Sometimes, the budget or technical resources needed to implement certain security measures might not be available, leading to delays in policy enforcement.