||Jai Sri Gurudev ||

BGSKH Education Trust (R.) – A unit of Sri Adichunchanagiri Shikshana Trust(R.)

BGS College of Engineering and Technology (BGSCET)

Mahalakshmipuram, West of Chord Road, Bengaluru-560086

(Approved by AICTE, New Delhi and Affiliated to VTU, Belagavi)

INTRODUCTION TO CYBER SECURITY (BETCK105/205 I) NOTES

For First/Second Semester B.E[VTU/CBCS, 2023-2024] Syllabus

Syllabus

Course Title: Introduction to Cyber Security **Course Code: :** BETCK105I/205

MODULE-I	**Teaching Hours**
Introduction to Cybercrime: Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes, An Indian Perspective, Hacking and Indian Laws., Global PerspectivesTextbook:1 Chapter 1 (1.1 to 1.5, 1.7-1.9)	**8**
Blooms Taxonomy: L1 – Remembering, L2 – Understanding	
MODULE-II	**Teaching Hours**
Cyber Offenses: How Criminals Plan Them: Introduction, How criminals plan the attacks, Social Engineering, Cyber Stalking, Cybercafe & cybercrimes. Botnets: The fuel for cybercrime, Attack Vector. Textbook:1 Chapter 2 (2.1 to 2.7)	**8**
Blooms Taxonomy: L1 – Remembering, L2 – Understanding	
MODULE-III	**Teaching Hours**
Tools and Methods used in Cybercrime: Introduction, Proxy Servers, Anonymizers, Phishing, Password Cracking, Key Loggers and Spyways, Virus and Worms, Trozen Horses and Backdoors, Steganography, DoS and DDOS Attackes, Attacks on Wireless networks. Textbook:1 Chapter 4 (4.1 to 4.9, 4.12)	**8**
Blooms Taxonomy: L1 – Remembering, L2 – Understanding	
MODULE-IV	**Teaching Hours**
Phishing and Identity Theft: Introduction, methods of phishing, phishing, phising techniques, spear phishing, types of phishing scams, phishing toolkits and spy phishing, counter measures, Identity Theft Textbook:1 Chapter 5 (5.1. to 5.3)	**8**
Blooms Taxonomy: L1 – Remembering , L2 – Understanding	
MODULE-V	**Teaching Hours**
Understanding Computer Forensics: Introdcution, Historical Background of Cyberforensics, Digital Foresics Science, Need for Computer Foresics, Cyber Forensics and Digital Evidence, Digital Forensic Life cycle, Chain of Custody Concepts, network forensics. Textbook:1 Chapter 7 (7.1. to 7.5, 7.7 to 7.9)	**8**
Blooms Taxonomy: L1 – Remembering, L2 – Understanding	

SL No	**Title Of The Book**	**Name Of the Author/s**	**Name Of the Publisher**	**Edition and Year**	**ISBN**
1	, “Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives”	Sunit Belapure and Nina Godbole	Wiley India Pvt Ltd	First Edition (Reprinted 2018)	978-81- 265-21791, 2011,

MODULE 1. INTRODUCTION TO CYBERCRIME

List of Topics:

- Introduction
- Cybercrime: Definition and Origins of the Word
- Cybercrime and Information Security
- Who are Cybercriminals?
- Classifications of Cybercrimes
- Cybercrime: The Legal Perspectives
- Cybercrimes: An Indian Perspective
- Cybercrime and the Indian ITA 2000
- A Global Perspective on Cybercrimes
- Cybercrime Era: Survival Mantra for the Netizens

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 phenomena; 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

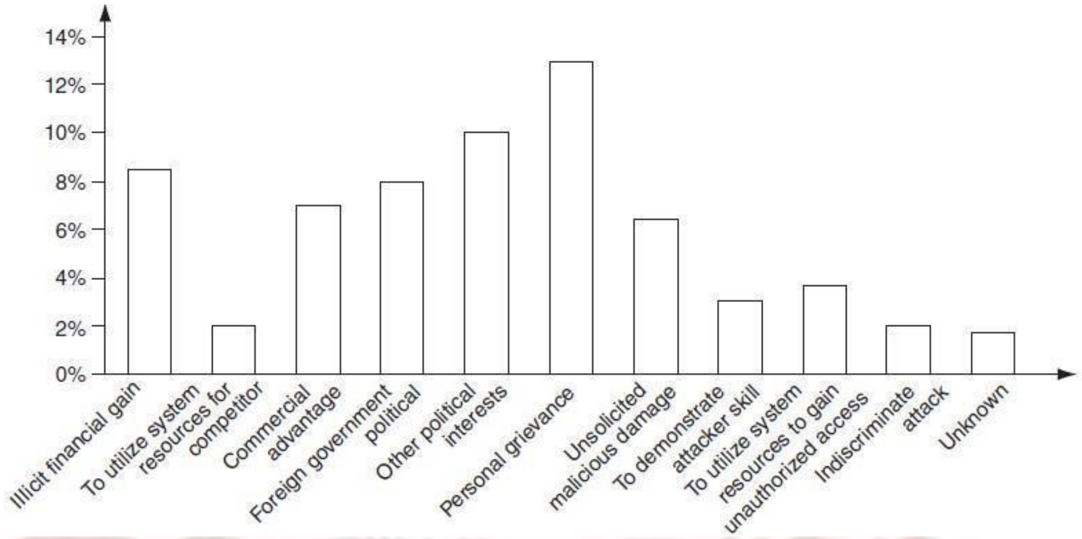


Figure: Cybercrime Trend

- 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).

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.
5. "Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them."

Note that in a wider sense, "computer-related crime" can be any illegal behavior committed by means of, or in relation to, a computer system or network; however, this is not cybercrime. The term "cybercrime" relates to a number of other terms that may sometimes be used to describe crimes committed using computers.

- Computer-related crime
- Computer crime
- Internet crime
- E-crime
- High-tech crime, etc. are the other synonymous terms.

Cybercrime specifically can be defined in a number of ways; a few definitions are:

1. A crime committed using a computer and the Internet to steal a person's identity (identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs.
2. Crimes completed either on or with a computer.
3. Any illegal activity done through the Internet or on the computer.
4. All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW.

According to one information security, cybercrime is any criminal activity which uses network access to commit a criminal act. Cybercrime may be internal or external, with the former easier to perpetrate. The term "cybercrime" has evolved over the past few years since the adoption of Internet connection on a global scale with hundreds of millions of users. Cybercrime refers to the act of performing a criminal act using cyberspaceas the communications vehicle.

Some people argue that a cybercrime is not a crime as it is a crime against software & not against a person (or) property. However, while the legal systems around the world scramble to introduce laws to combat cyber criminals, 2 types of attacks are prevalent:

1. Techno-crime: A premeditated act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system. The 24X7 connection to the internet makes this type of cybercrime a real possibility to engineer from anywhere in the world, leaving

few, if any, “finger prints”.

2. Techno-vandalism: These acts of “brainless” defacement of websites and/or other activities, such as copying files and publicizing their contents publicly, are usually opportunistic in nature. Tight internal security, allied to strong technical safeguards should prevent the vast majority of such incidents.

There is a very thin line between the two terms “computer crime” and “computer fraud”; both are punishable. Cybercrimes (harmful acts committed from or against a computer or network) differ from most terrestrial crimes in four ways:

a. how to commit them is easier to learn,
b. they require few resources relative to the potential damage caused,
c. they can be committed in a jurisdiction without being physically present in it &
d. they are often not clearly illegal.

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, utilizesaccesses 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 &amp; 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 computernetworks. 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.

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 herebecause, 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:

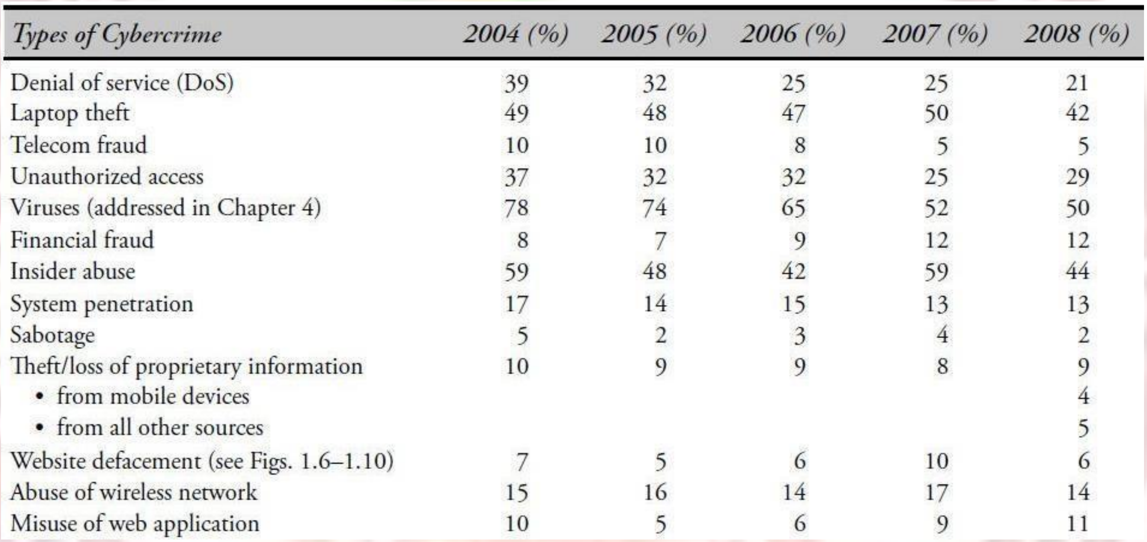
Cyberwarfare means information attacks against an unsuspecting opponent's computer networks, destroying and paralyzing nations. This perception seems to be correct as the terms cyberwarfare and Cyberterrorism have got historical connection in the context of attacks against infrastructure. The term "information infrastructure" refers to information resources, including communication systems that support an industry, institution or population. These type of Cyber attacks are often presented as threat to military forcesand 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 (ITA) 2000 in the context of cybercrime. From an Indian perspective, the new version of the Act (referred to as ITA 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.

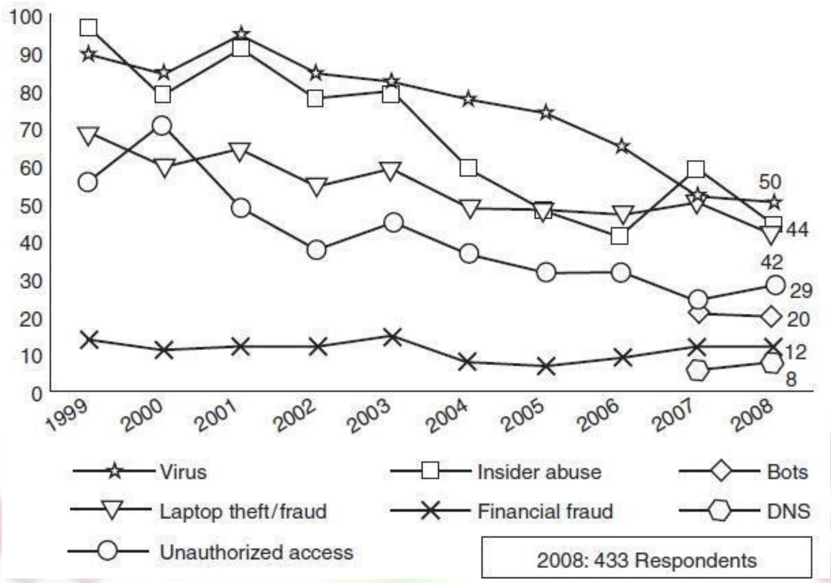
Where financial losses to the organization due to insider crimes are concerned (e.g., leaking customer data), often some difficulty is faced in estimating the losses because the financial impacts may not be detectedby the victimized organization and no direct costs may be associated with the data theft. The 2008 CSI Surveyon 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 thanthat made out by security solution vendor. However, this perception of an organization does not seem to be trueas 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



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

Figure: Cybercrime trend over the years



<u>Figure</u>: shows several categories of incidences – viruses, insider abuse, laptop theft and unauthorized access to systems

<u>The Botnet Menace</u>:

A group of computers that are controlled by software containing harmful programs, without their users' knowledge is called as **<u>Botnet</u>**. The term "Botnet" is used to refer to a group of compromised computers (zombie computers, i.e., personal computers secretly under the control of hackers) running malwares under a common command and control infrastructure. Below figure shows how a "zombie" works.

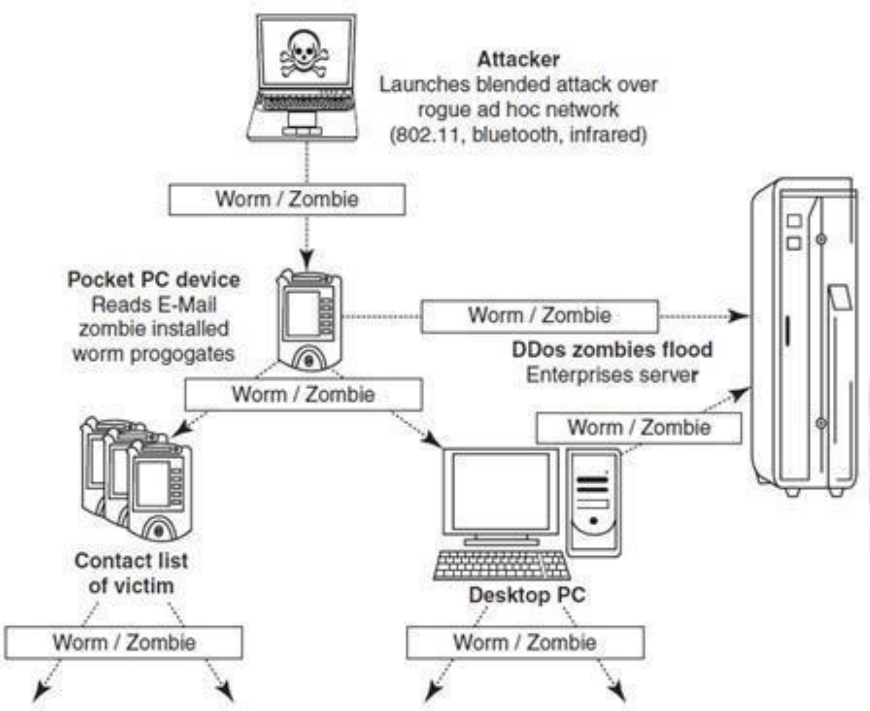


Figure: How a Zombie works

- A Botnet maker can control the group remotely for illegal purposes, the most common being
  - denial-of-service attack (DoS attack),
  - Adware,
  - Spyware,
  - E-Mail Spam,
  - Click Fraud
  - theft of application serial numbers,
  - login IDs
  - financial information such as credit card numbers, etc.
- An attacker usually gains control by infecting the computers with a virus or other Malicious Code. The computer may continue to operate normally without the owner's knowledge that his computer has been compromised.
- The problem of Botnet is global in nature and India is also facing the same.
  - India has an average of 374 new Bot attacks per day and had more than 38,000 distinct Bot-infected computers in the first half of the year 2009.
  - Small and medium businesses in the country are at greater risk, as they are highly vulnerable to

Bots, Phishing, Spam and Malicious Code attacks.

- Mumbai with 33% incidences tops the Bot-infected city list,
- followed by New Delhi at 25%,
- Chennai at 17% and
- Bangalore at 13%.

- Tier-II locations are now also a target of Bot-networks with Bhopal at 4% and Hyderabad, Surat, Pune and Noida at 1% each.
- The Internet is a network of interconnected computers. If the computers, computer systems, computer resources, etc. are unsecured and vulnerable to security threats, it can be detrimental to the critical infrastructure of the country.

WHO ARE CYBERCRIMINALS?

Cybercrime involves such activities

- credit card fraud;
- cyberstalking;
- defaming another online;
- gaining unauthorized access to computer systems;
- ignoring copyright, software licensing and trademark protection;
- overriding encryption to make illegal copies;
- software piracy and stealing another’s identity (known as identity theft) to perform criminal acts

Types of Cybercriminals:

1. Type I: Cybercriminals – hungry for recognition

- Hobby hackers;
- IT professionals (social engineering is one of the biggest threat);
- Politically motivated hackers;
- Terrorist organizations.

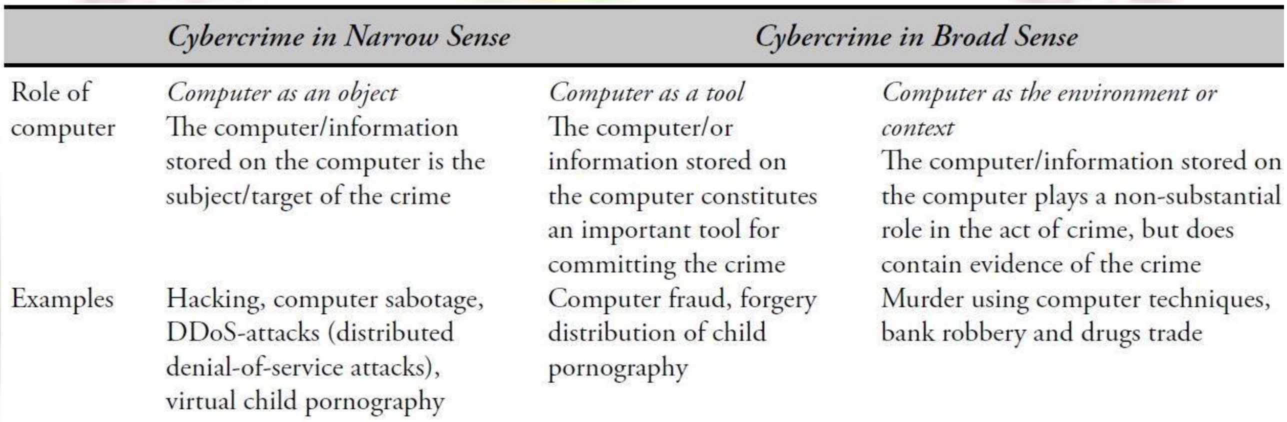
2. Type II: Cybercriminals – not interested in recognition

- Psychological perverts;
- financially motivated hackers (corporate espionage);
- state-sponsored hacking (national espionage, sabotage)
- organized criminals

3. Type III: Cybercriminals – the insiders

- Disgruntled or former employees seeking revenge;
- Competing companies using employees to gain economic advantage through damage and/or theft.

CLASSIFICATIONS OF CYBERCRIMES



	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

Table: Classifying Cybercrimes

"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". Cyber crimes 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 actually 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, spoofs her E-Mail and sends 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 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.

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 Phishingscams are designed to steal information from individuals, spear phishing scam works to gain access to acompany'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 thelink 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.1y/2LPLdaU" and if you tap that link to find out, once again you're downloading malware.

4. <u>Spamming</u>: People who create electronic Spam are called spammers. Spam is the abuse of electronicmessaging 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;
- hidden links;
- use of different pages that bridge to the same URL (gateway pages).

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 ofsuch 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 individualsto 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 dormantall 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 intothe reach of more and more homes, larger child population will be using the Internet and therefore greaterwould 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 ifthe 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 toaccess 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. "Spies" can get information about product finances, research and development and marketing strategies, an activity known as "industrial spying."

However, cyberspies 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 inclinedto 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 givento 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 ofInternet 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 mislabeled 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

- Cybercrime poses a biggest challenge.
- Computer Crime: As per "Criminal Justice Resource Manual (1979)", computer-related crime was defined in the broader meaning as: "any illegal act for which knowledge of computer technology is essential for a successful prosecution".
- International legal aspects of computer crimes were studied in 1983.
- In that study, computer crime was consequently defined as: "encompasses any illegal act for which knowledge of computer technology is essential for its commit".
- Cybercrime, in a way, is the outcome of "globalization." However, globalization does not mean globalized welfare at all.
- Globalized information systems accommodate an increasing number of transnational offenses.
- The network context of cybercrime makes it one of the most globalized offenses of the present and the most modernized threats of the future.
- This problem can be resolved in two ways.
  a) One is to divide information systems into segments bordered by state boundaries (cross-border flow of information).
  b) The other is to incorporate the legal system into an integrated entity obliterating these state boundaries.
- Apparently, the first way is unrealistic. Although all ancient empires including Rome, Greece and Mongolia became historical remnants, and giant empires are not prevalent in current world, the partitionof information systems cannot be an imagined practice.
- In a globally connected world, information systems become the unique empire without tangible territory.

CYBERCRIMES: AN INDIAN PERSPECTIVE

India has the fourth highest number of Internet users in the world. According to the statistics posted on the site (http://www.iamai.in/), there are 45 million Internet users in India, 37% of all Internet accesses happen from cybercafés and 57% of Indian Internet users are between 18 and 35 years. The population of educatedyouth is high in India. It is reported that compared to the year 2006, cybercrime under the Information Technology (IT) Act recorded a whopping 50% increase in the year 2007. A point to note is that the majority of offenders were under 30 years. The maximum cybercrime cases, about 46%, were related to incidents of cyberpornography, followed by hacking. In over 60% of these cases, offenders were between 18 and 30 years, according to the "Crime in 2007" report of the National Crime Record Bureau (NCRB).

Cybercrimes: Indian Statistics:

Cybercrimes: Cases of various categories under ITA 2000: 217 cases were registered under IT Act during the year 2007 as compared to 142 cases during the previous year 2006, with an increase of 52.8%. 99 cases of the total 217 cases registered under ITA 2000 were related to obscene publication/transmission in electronic form known as cyberpornography. There were 76 cases of hacking with computer system which is related to loss/damage of computer resource/utility. India is said to be "youth country" given the population age distribution. However from cybercrime perspective, this youth aspect does not seem good as revealed by cybercrime statistics in India.

Cybercrimes: Cases of various categories under IPC Section: A total of 339 cases were registered under IPC sections during the year 2007 as compared to 311 such cases during 2006, thereby reporting an increase of 9%.Majority of the crimes out of total 339 cases registered under IPC fall under 2 categories i.e.., Forgery & Criminal breach of Trust or Fraud.

Incidence of Cybercrimes in cities: 17 out of 35 mega cities did not report any case of cybercrime (neither under the IT Act nor under IPC Sections) during the year 2007. A total of 17 mega cities have reported 118 cases under IT Act and 7 mega cities reported 180 cases under various sections of IPC.

The Indian Government is doing its best to control cybercrimes. For example, Delhi Police have now trained 100 of its officers in handling cybercrime and placed them in its Economic Offences Wing. As at the time of writing this, the officers were trained for 6 weeks in computer hardware and software, computer

networks comprising data communication networks, network protocols, wireless networks and network security.

CYBERCRIME & THE INDIAN ITA 2000

In India, the ITA 2000 was enacted after the United Nation General Assembly ResolutionA/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 areaof 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 And Title**	**Crime**	**Punishment**
Sec.43 (Penalty for damage to computer, computer system etc)	Chapter IX Penalties and Adjudication	Damage to computer system etc.	Compensation forRs. 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 upto 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 to10 Years
Sec.72 (Penalty for breach of confidentiality and privacy)	Chapter XI Offences	Attempting or securing access to computer for breaking confidentiality of the information of computer	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 began 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:

It is a continuing problem that the average user is not adequately educated to understand the threats and how to protect oneself. Actually, it is the responsibility of each user to become aware of the threats as well asthe opportunities that "connectivity" and "mobility" presents them with. In this context, it is important to understand the concept of "extended enterprise." This term represents the concept that a company is made upnot just of its employees, its board members and executives, but also its business partners, its suppliers and even its customers.

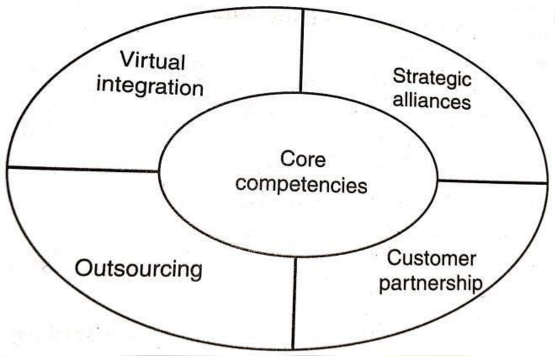


Figure: Extended Enterprise

The extended enterprise can only be successful if all of the component groups and individuals have the information they need in order to do business effectively. An extended enterprise is a **"**loosely coupled, self-organizing network**"** of firms that combine their economic output to provide **"**products and services**"** offerings to the market. Firms in the extended enterprise may operate independently. Seamless flow of "information" to support instantaneous "decision-making ability" is crucial for the "external enterprise". This becomes possible through the "interconnectedness". Due to the interconnected features of information & communication technologies, security overall can only be fully promoted when the users have full awareness of existing threats & dangers.

Given the promises and challenges in the extended enterprise scenario, organizations in the international community have a special role in sharing information on good practices and creating open and accessible enterprise information flow channels for exchanging of ideas in a collaborative manner.

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 alsoa 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.

||Jai Sri Gurudev ||
BGSKH Education Trust (R.) – A unit of Sri Adichunchanagiri Shikshana Trust(R.)
BGS College of Engineering and Technology (BGSCET)
Mahalakshmipuram, West of Chord Road, Bengaluru-560086
(Approved by AICTE, New Delhi and Affiliated to VTU, Belagavi)

Question Bank

Subject: Introduction to Cyber Security **Class:** CSE/ISE

Subject code: BETCK105I/205I **Faculty:** Mrs. Jyothi R

Course Outcomes

CO1: Interpret the cybercrime terminologies
CO2: Analyze Cyber offenses and Botnets
CO3: Illustrate Tools and Methods used on Cybercrime
CO4: Analyze Phishing and Identity Theft
CO5: Justify the need of computer forensics

Module-1 Introduction to Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes, An Indian Perspective, Hacking and IndianLaws., Global Perspectives
Textbook:1 Chapter 1 (1.1 to 1.5, 1.7-1.9)

Sl. No.	Questions	Marks	CO	BT
Topic:	**Introduction**			
1.	Explain the following • Cyberspace • Cyberpunk • Cyberwarfare • Cyber squatting • Cyber terrorism	08M	CO1	L2
Topic:	**Definition and Origins of the Word,**			
2.	Define cybercrime, discuss the origin of Cybercrime.	06M	CO1	L2
3.	Explain the two types of Attacks in Cyber security.	06M	CO1	L2
Topic:	**Cybercrime and Information Security,**			
4.	Write a short note on cybercrime and information security	06M	CO1	L2
5.	Explain the Botnet Menace with diagram	06M	CO2	L2
6.	What are the major types of Incidents occurring inthe computer environment	06M	CO1	L2
Topic:	**Who are Cybercriminals?**			
7.	Who are cybercriminals? explain in detail.	06M	C01	L3
Topic:	**Classifications of Cybercrimes,**			

8.	Explain the classification of cybercrime in a narrow sense and broad sense with examples.	06M	CO1	L2
9.	Explain the classification of cybercrime Against Individual, property, organization, society and crimes emanating from Usenet newsgroups.	06M	CO1	L2
10.	Discuss about the classification of cybercrime. What are the different types of cybercrime towards an individual?	08M	CO1	L2
11.	Explain the following crimes with examples a) Email Spoofing b) Phishing c) Spamming d) Cyberdefamation e) Cyber Stalking and Harassment. f) Computer Sabotage g) Pornographic offenses h) Password Sniffing Identity Theft	06M	CO1	L2
12.	Discuss the following crimes with examples a) Hacking b) Industrial Espionage c) DoS attack d) Email Bomb e) Virus attack and dissemination of viruses f) Salami Attack g) Logic Bomb h) Industrial Espionage (Trojan Horse) i) Data Diddling j) Crimes Emanating from Usenet Newsgroups	10M	CO1	L2
13.	Explain the following crimes against property with examples • Software Piracy • Computer Network Intrusion Online • Fraud • Internet Time Theft IP crimes	06M	CO1	L2
14.	Explain the following crimes against Society • Forgery • Cyberterrorism Web Jacking	06M	CO1	L2
15.	Discuss the concept of pornography offences andchild pornography and explain the steps involved in pedophiles operations.	08M	CO2	L2
16.	What is the main purpose of hacking, explain hacking with examples	09M	CO1	L2
17.	Explain Spamming, mention its types,	08M	CO1	L2
Topic:	**An Indian Perspective, Hacking and IndianLaws., Global Perspectives**			

18.		Explain the Indian perspective of Cybercrime.	08M	C01	L2
19.		What are the hacking and Indian laws present on cyber crimes	08M	C01	L2
20.		Explain cybercrime and the Indian ITA 2000	08M	C01	L2
21.		Discuss a global perspective on cyber crime	08M	CO1	L2
22.		Write a short note on cybercrime and the extended Enterprise	08M	CO1	L2
23.		Write the difference between Crime and Fraud	08M	CO1	L2

Module II: Cyber Offenses

How Criminals Plan Them – Introduction, How Criminals Plan The Attacks, Social Engineering, and Cyber Stalking, Cyber Cafe And Cybercrimes, Botnets: The Fuel For Cybercrime, Attack Vector Cloud Computing.

Learning Objectives

- Understand different types of cyber attacks.
- Get an overview of the steps involved in planning cybercrime.
- Understand tools used for gathering information about the target.
- Get an overview on social engineering – what and how.
- Learn about the role of cybercafés in cybercrime.
- Understand what cyber stalking is.
- Learn about Botnets and attack vector.
- Get an overview on cloud computing – what and how.

How Criminals Plan Them –Introduction

- Technology is a “double-edged sword” as it can be used for both good and bad purposes
- People with the tendency to cause damages or carrying out illegal activities will use it for bad purpose.
- Computers and tools available in IT are also used as either target of offense.
- In today’s world of Internet and computer networks, a criminal activity can be carried out across national borders.
- Chapter 1 provided an overview of hacking, cyber terrorism, network intrusions, password sniffing, computer viruses, etc. They are the most commonly occurring crimes that target the computer.
- Cybercriminal use the World Wide Web and Internet to an optimum level for all illegal activities to store data, contacts, account information, etc.
- The criminals take advantage of the widespread lack of awareness about cybercrimes and cyber laws among the people who are constantly using the IT infrastructure for official and personal purposes.
- People who commit cybercrimes are known as “Crackers” (Box 2.1).

Box 2.1 | Hackers, Crackers and Phreakers
Hacker: A hacker is a person with a strong interest in computers who enjoys learning and experimenting with them. Hackers are usually very talented, smart people who understand computers better than others. The term is often confused with cracker that defines someone who breaks into computers (refer to Box 2.2).
Brute force hacking: It is a technique used to find passwords or encryption keys. Brute force hacking involves trying every possible combination of letters, numbers, etc., until the code is broken.

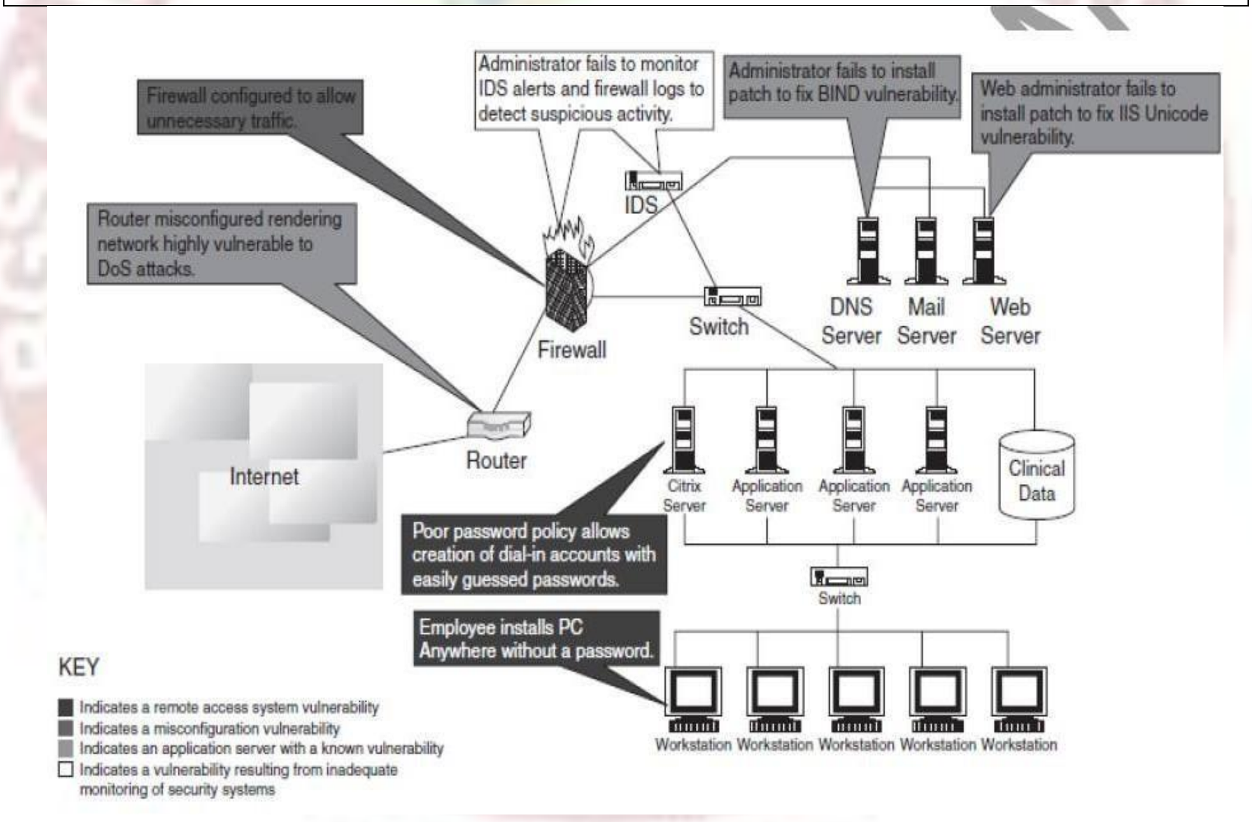
Cracker: A cracker is a person who breaks into computers. Crackers should not be confused with hackers. The term “cracker” is usually connected to computer criminals. Some of their crimes include vandalism, theft and snooping in unauthorized areas.

Cracking: It is the act of breaking into computers. Cracking is a popular, growing subject on the Internet. Many sites are devoted to supplying crackers with programs that allow them to crack computers. Some of these programs contain dictionaries for guessing passwords. Others are used to break into phone lines (called “phreaking”). These sites usually display warnings such as “These files are illegal; we are not responsible for what you do with them.”

Cracker tools: These are programs used to break into computers. Cracker tools are widely distributed on the Internet. They include password crackers, Trojans, viruses, war dialers and worms.

Phreaking: This is the notorious art of breaking into phone or other communication systems. Phreaking sites on the Internet are popular among crackers and other criminals.

War dialer: Program automatically dials phone numbers looking for computers on the other end. It catalogs numbers so that the hackers can call back and try to break in. An attacker would look to exploit the vulnerabilities in the networks, most often so because the networks are not adequately protected.


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

- The categories of vulnerabilities that hackers typically search for are the following:
  - Inadequate border protection (border as in the sense of network periphery);
  - remote access servers (RASs) with weak access controls;

    - application servers with well-known exploits;
    - misconfigured systems and systems with default configurations.
- To help the reader understand the network attack scenario, Fig. 2.2 illustrates a small network highlighting specific occurrences of several vulnerabilities described above.

Box 2.2 | What Color is Your Hat in the Security World?

A **black hat** is also called a “cracker” or “dark side hacker.” Such a person is a malicious or **criminal hacker**. Typically, the term “cracker” is used within the security industry. However, the general public uses the term hacker to refer to the same thing. In computer terminology, the meaning of “hacker” can be much broader. The name comes from the opposite of “white hat hackers.”

A **white hat hacker** is considered an **ethical hacker**. In the realm of IT, a “white hat hacker” is a person who is ethically opposed to the abuse of computer systems. It is said that the term is derived from American western movies, where the protagonist typically wore a white cowboy hat and the antagonist typically wore a black one. As a simplified explanation, a “white hat” generally focuses on securing IT systems, whereas a “black hat” (the opposite) would like to break into them, so this sounds like an age-old game of a thief and a police.

A **brown hat hacker** is one who thinks before acting or committing a malice or non-malice deed. A grey hat commonly refers to a hacker who releases information about any exploits or security holes he/she finds openly to the public. He/she does so without concern for how the information is used in the end (whether for patching or exploiting).

2.1.1 Categories of Cybercrime

Cybercrime can be categorized based on the following:

1. The target of the crime and
2. whether the crime occurs as a single event or as a series of events.

Cybercrime can be targeted against individuals (**persons**), assets (**property**) and/or **organizations** (government, business and social).

1. **Crimes targeted at individuals:** The goal is to exploit human weakness such as greed and naivety. These crimes include financial frauds, sale of non-existent or stolen items, child pornography (explained in Section 1.5.13, Chapter 1), copyright violation, harassment, etc. with the development in the IT and the Internet; thus, criminals have a new tool that allows them to expand the pool of potential victims. However, this also makes difficult to trace and apprehend the criminals.
2. **Crimes targeted at property:** This includes stealing mobile devices such as cell phone, laptops, personal digital assistant (PDAs), and removable medias (CDs and pen drives); transmitting harmful programs that can disrupt functions of the systems and/or can wipe out data from hard disk, and can create the malfunctioning of the attached devices in the system such as modem, CD drive, etc.

3. **Crimes targeted at organizations:** Cyber terrorism is one of the distinct crimes against organizations/ governments. Attackers (individuals or groups of individuals) use computer tools and the Internet to usually terrorize the citizens of a particular country by stealing the private information, and also to damage the programs and files or plant programs to get control of the network and/or system (see Box 2.3).
4. **Single event of cybercrime:** It is the single event from the perspective of the victim. For example, unknowingly open an attachment that may contain virus that will infect the system (PC/laptop). This is known as hacking or fraud.
5. **Series of events:** This involves attacker interacting with the victims repetitively. For example, attacker interacts with the victim on the phone and/or via chat rooms to establish relationship first and then they exploit that relationship to commit the sexual assault.

Box 2.3 | Patriot Hacking

Patriot hacking[1] also known as **Digital Warfare**, is a form of vigilante computer systems' cracking done by individuals or groups (usually citizens or supports of a country) against a real or perceived threat. Traditionally, Western countries, that is, developing countries, attempts to launch attacks on their perceived enemies.

Although patriot hacking is declared as illegal in the US, however, it is reserved only for government agencies [i.e., Central Intelligence Agency (CIA) and National Security Agency (NSA)] as a legitimate form of attack and defense. Federal Bureau of Investigation (FBI) raised the concern about rise in cyber attacks like website defacements (explained in Box 1.4, Chapter1) and denial-of-service attacks (DoS – refer to Section 4.9, Chapter 4), which adds as fuel into increase in international tension and gets mirrored it into the online world.

After the war in Iraq in 2003, it is getting popular in the North America, Western Europe and Israel. These are countries that have the greatest threat to Islamic terrorism and its aforementioned digital version.

The People's Republic of China is allegedly making attacks upon the computer networks of the US and the UK. Refer to Box 5.15 in Chapter 5. For detailed information visit www.patriothacking.com

2.2 How Criminals Plan the Attacks

- Criminals use many methods and tools to locate the vulnerabilities of their target.
- The target can be an individual and/or an organization.
- Criminals plan passive and active attacks
- **Active attacks** are usually used to alter the system (i.e., computer network) whereas **passive attacks** attempt to gain information about the target.
- **Active attacks** may affect the availability, integrity and authenticity of data whereas **passive attacks** lead to violation of confidentiality.

The following phases are involved in planning cybercrime:

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

2.2.1 Reconnaissance (reconnaissance= 9ఘుa)

- The literal meaning of “Reconnaissance” is an act of **finding something or somebody** (especially to gain information about an enemy or potential enemy).
- In the world of “hacking,” reconnaissance phase begins with “Footprinting” – this is the preparation toward pre-attack phase, and involves accumulating data about the target’s environment and computer architecture to find ways to intrude into that environment.
- Footprinting gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities.
- The objective of this preparatory phase is to understand the system, its networking ports and services, and any other aspects of its security that are needful for launching the attack.
- Thus, an attacker attempts to gather information in two phases: passive and active attacks. Let us understand these two phases.

2.2.2 Passive Attacks

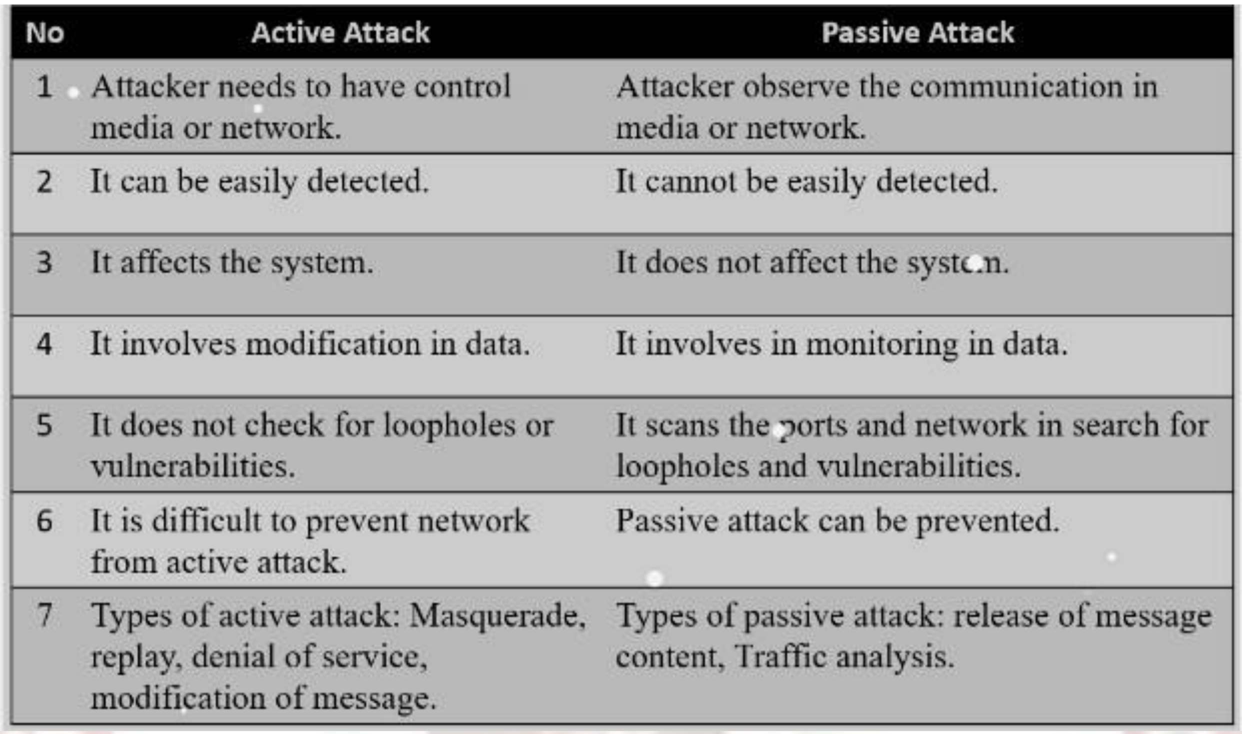
A passive attack involves gathering information about a target without his/her (individual’s or company’s) knowledge. It can be as simple as watching a building to identify what time employees enter the building premises. However, it is usually done using Internet searches or by Googling (i.e., searching the required information with the help of search engine Google) an individual or company to gain information.

1. Google or Yahoo search: People search to locate information about employees.
2. Surfing online community groups like Orkut/Facebook will prove useful to gain the information about an individual.
3. Organization’s website may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc. These can be used in a social engineering attack to reach the target (see Section 2.3).
4. Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.

5. Going through the job postings in particular job profiles for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on its network.

2.2.3 Active Attacks

An active attack involves probing the network to discover individual hosts to confirm the information (IP addresses, operating system type and version, and services on the network) gathered in the passive attack phase. It involves the risk of detection and is also called “Rattling the doorknobs” or “Active reconnaissance.” Active reconnaissance can provide confirmation to an attacker about security measures in place (e.g., whether the front door is locked?), but the process can also increase the chance of being caught or raise a suspicion.



No	Active Attack	Passive Attack
1	Attacker needs to have control media or network.	Attacker observe the communication in media or network.
2	It can be easily detected.	It cannot be easily detected.
3	It affects the system.	It does not affect the system.
4	It involves modification in data.	It involves in monitoring in data.
5	It does not check for loopholes or vulnerabilities.	It scans the ports and network in search for loopholes and vulnerabilities.
6	It is difficult to prevent network from active attack.	Passive attack can be prevented.
7	Types of active attack: Masquerade, replay, denial of service, modification of message.	Types of passive attack: release of message content, Traffic analysis.

2.2.4 Scanning and Scrutinizing Gathered Information

Scanning is a key step to examine intelligently while gathering information about the target.

The objectives of scanning are as follows:

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

2.2.5 Attack (Gaining and Maintaining the System Access)

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

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

2.3 Social Engineering

- Social engineering is the “technique to influence” and “persuasion to deceive” people to obtain the information or perform some action.
- Social engineers exploit the natural tendency of a person to trust social engineers’ word, rather than exploiting computer security holes.
- It is generally agreed that people are the weak link in security and this principle makes social engineering possible.
- A social engineer usually uses telecommunication (i.e., telephone and/or cell phone) or Internet to get them to do something that is against the security practices and/or policies of the organization.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- It is an art of exploiting the trust of people, which is not doubted while speaking in a normal manner.
- The goal of a social engineer is to fool someone into providing valuable information or access to that information.
- Social engineer studies the human behavior so that people will help because of the desire to be helpful, the attitude to trust people, and the fear of getting into trouble.
- The sign of truly successful social engineers is that they receive information without any suspicion.
- A simple example is calling a user and pretending to be someone from the service desk working on a network issue; the attacker then proceeds to ask questions about what the user is working on, what file shares he/she uses, what his/her password is, and so on… (see Box 2.6).

Box 2.6 | Social Engineering Example
Mr. Joshi: Hello?
The Caller: Hello, Mr. Joshi. This is Geeta Thomas from Tech Support. Due to some disk space constraints on the file server, we will be moving few user’s home directories to another disk. This activity will be performed tonight at 8:00 p.m. Your account will be a part of this move and will be unavailable temporarily.
Mr. Joshi: Ohh … okay. I will be at my home by then, anyway.
Caller: Great!!! Please ensure to log off before you leave office. We just need to check a couple of things. What is your username?
Mr. Joshi: Username is “pjoshi.” None of my files will be lost in the move, right?
Caller: No sir. But we will have to check your account to ensure the same. What is the password of that account?
Mr. Joshi: My password is “ABCD1965,” all characters in upper case.
Caller: Ok, Mr. Joshi. Thank you for your cooperation. We will ensure that all the files are there.
Mr. Joshi: Thank you. Bye.

Caller: Bye and have a nice day.

2.3.1 Classification of Social Engineering

Human-Based Social Engineering

- Human-based social engineering refers to person-to-person interaction to get the required/desired information.
- An example is calling the help desk and trying to find out a password.

1. Impersonating an employee or valid user:

- “Impersonation” is perhaps the greatest technique used by social engineers to deceive people.
- Social engineers “take advantage” of the fact that most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or to let someone into the building who “forgot” his/her badge, etc., or pretending to be an employee or valid user on the system.

2. Posing as an important user:

- The attacker pretends to be an important user – for example, a Chief Executive Officer (CEO) or high-level manager who needs immediate assistance to gain access to a system.
- The attacker uses intimidation so that a lower-level employee such as a help-desk worker will help him/her in gaining access to the system. Most of the low-level employees will not ask any question to someone who appears to be in a position of authority.

3. Using a third person:

- An attacker pretends to have permission from an authorized source to use a system. This trick is useful when the supposed authorized personnel is on vacation or cannot be contacted for verification.

4. Calling technical support:

- Calling the technical support for assistance is a classic social engineering example.
- Help-desk and technical support personnel are trained to help users, which makes them good prey for social engineering attacks.

5. Shoulder surfing:

- It is a technique of gathering information such as usernames and passwords by watching over a person’s shoulder while he/she logs into the system, thereby helping an attacker to gain access to the system.

6. Dumpster diving:

- It involves **looking in the trash for information written on pieces of paper or computer printouts**.
- This is a typical North American term; it is used to describe the practice of rummaging through commercial or residential trash to find useful free items that have been discarded.
- It is also called dumpstering, binning, trashing, garbing or garbage gleaning.
- “Scavenging” is another term to describe these habits.
- In the UK, the practice is referred to as “ binning” or “skipping” and the person doing it is a “binner” or a “skipper.”

Computer-Based Social Engineering

- Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet.
- For example, sending a **fake E-Mail to the user** and asking him/her to re-enter a password in a webpage to confirm it.

1. Fake E-Mails:

- The attacker sends fake E-Mails (see Box 2.7) to users in such that the user finds it as a real e-mail.
- This activity is also called "Phishing".
- It is an attempt to attract the Internet users (netizens) to reveal their personal information, such as **usernames, passwords** and **credit card details** by impersonating as a trustworthy and legitimate organization or an individual.
- Banks, financial institutes and payment gateways are the common targets.
- Phishing is typically carried out through E-Mails or instant messaging and often directs users to enter details at a website, usually designed by the attacker with abiding the look and feel of the original website.
- Thus, Phishing is also an example of social engineering techniques used to fool netizens.
- The term "Phishing" has been evolved from the analogy that Internet scammers are using E-Mails attract to fish for passwords and financial data from the sea of Internet users (i.e., netizens).
- The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords without the knowledge of AOL users.
- As hackers have a tendency of replacing "f" with "ph," the term "Phishing" came into being.

2. E-Mail attachments:

- E-Mail attachments are used to send malicious code to a victim's system, which will automatically (e.g., keylogger utility to capture passwords) get executed.
- Viruses, Trojans, and worms can be included cleverly into the attachments to entice a victim to open the attachment.

3. Pop-up windows:

- Pop-up windows are also used, in a similar manner to E-Mail attachments. Pop-up windows with special offers or free stuff can encourage a user to unintentionally install malicious software.

2.4 Cyberstalking

- 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.

- Cyberstalking refers to the use of Internet and/or other electronic communications devices to stalk another person.

- **It involves harassing or threatening behavior that an individual will conduct repeatedly**, for example, following a person, visiting a person's home and/or at business place, making phone calls, leaving written messages, or vandalizing against the person's property. As the Internet has become an integral part of our personal and professional lives, cyberstalkers take advantage of ease of communication and an increased access topersonal information available with a few mouse clicks or keystrokes.

2.4.1 Types of Stalkers

There are primarily two types of stalkers.

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

2.4.2 Cases Reported on Cyberstalking

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

2.4.3 How Stalking Works?

It is seen that stalking works in the following ways:

1. Personal information gathering about the victim: Name; family background; contact details such as cell phone and telephone numbers (of residence as well as office); address

of residence as well as of the office; E-Mail address; date of birth, etc.

2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
3. Stalkers will almost always establish a contact with the victims through E-Mail. The letters may have the tone of loving, threatening or can be sexually explicit. The stalker may use multiple names while contacting the victim.
4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.
5. The stalker may post the victim's personal information on any website related to illicit services such as sex-workers' services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details (telephone numbers/cell phone numbers/E-Mail address) to have sexual services. The stalker will use bad and/or offensive/attractive language to invite the interested persons.
6. Whosoever comes across the information, start calling the victim on the given contact details (telephone/cell phone nos), asking for sexual services or relationships.
7. Some stalkers subscribe/register the E-Mail account of the victim to innumerable pornographic and sex sites, because of which victim will start receiving such kind of unsolicited E-Mails.

2.4.4 Real-Life Incident of Cyberstalking

Case Study

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

- Mrs. Joshi received almost 40 calls in 3 days mostly at odd hours from as far away as Kuwait, Cochin, Bombay, and Ahmadabad.
- The said calls created havoc in the personal life destroying mental peace of Mrs. Joshi who decided to register a complaint with Delhi Police.
- A person was using her ID to chat over the Internet at the website www.mirc.com, mostly in the Delhi channel for four consecutive days.
- This person was chatting on the Internet, using her name and giving her address, talking in obscene language.
- The same person was also deliberately giving her telephone number to other chatters encouraging them to call Mrs. Joshi at odd hours.
- This was the first time when a case of cyberstalking was registered.
- Cyberstalking does not have a standard definition but it can be defined to mean threatening, unwarranted behavior, or advances directed by one person toward another person using Internet and other forms of online communication channels as medium.

Box 2.8 | Cyberbullying

The National Crime Prevention Council defines Cyberbullying as "when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person.”

www.StopCyberbullying.org, an expert organization dedicated to Internet safety, security, and privacy defines cyberbullying as “a situation when a child, tween, or teen is repeatedly ‘tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted’ by another child, tween, or teen using text messaging, E-Mail, instant messaging, or any other type of digital technology.”

The practice of cyberbullying is not limited to children and, while the behavior is identified by the same definition in adults, the distinction in age groups is referred to as cyberstalking or cyberharassment when perpetrated by adults toward adults.
Source: http://en.wikipedia.org/wiki/Cyber-bullying (2 April 2009).

2.5 Cybercafe and Cybercrimes

- In February 2009, Nielsen survey on the profile of cybercafes users in India, it was found that 90% of the audience, across eight cities and 3,500 cafes, were male and in the age group of 15–35 years; 52% were graduates and postgraduates, though almost over 50% were students.
- Hence, it is extremely important to understand the IT security and governance practiced in the cybercafes.
- In the past several years, many instances have been reported in India, where cybercafes are known to be used for either real or false terrorist communication.
- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes.
- Cybercafes have also been used regularly for sending obscene mails to harass people.
- Public computers, usually referred to the systems, available in cybercafes, hold two types of risks.
- **First**, we do not know what programs are installed on the computer – that is, risk of malicious programs such as keyloggers or Spyware, which maybe running at the background that can capture the keystrokes to know the passwords and other confidential information and/or monitor the browsing behavior.
- **Second**, over-the-shoulder surfing can enable others to find out your passwords. Therefore, one has to be extremely careful about protecting his/her privacy on such systems, as one does not know who will use the computer after him/her.
- **Indian Information Technology Act (ITA) 2000,** does not define cybercafes and interprets cybercafes as “network service providers” referred to under the Section 79, which imposed on them a responsibility for “due diligence” failing which they would be liable for the offenses committed in their network.
- Cybercriminals prefer cybercafes to carry out their activities.
- The criminals tend to identify one particular personal computer (PC) to prepare it for their use.
- Cybercriminals can either install malicious programs such as keyloggers and/or Spyware or launch an attack on the target.
- Cybercriminals will visit these cafes at a particular time and on the prescribed frequency,

maybe alternate day or twice a week.

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

In the event that a central agency takes up the responsibility for monitoring cybercafes, an individual should take care while visiting and/or operating from cybercafe. Here are a few tips for safety and security while using the computer in a cybercafe:

1. **Always logout:**
2. **Stay with the computer:**
3. **Clear history and temporary files:**
4. **Be alert:**
5. **Avoid online financial transactions:**
6. **Change passwords:**
7. **Use Virtual keyboard:**
8. **Security warnings:**

2.6 Botnets: The Fuel for Cybercrime

2.6.1 Botnet

- The dictionary meaning of Bot is "(computing) an automated program for doing some particular task, often over a network."
- Botnet is a term used for collection of software robots, or Bots, that run autonomously and automatically.
- The term is often associated with malicious software but can also refer to the network of computers using distributed computing software.
- In simple terms, a Bot is simply an automated computer program One can gain the control of computer by infecting them with a virus or other Malicious Code that gives the access.
- Computer system maybe a part of a Botnet even though it appears to be operating normally.
- Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks.
- A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.
- "Zombie networks" have become a source of income for entire groups of cybercriminals. The invariably low cost of maintaining a Botnet and the ever diminishing degree of knowledge required to manage one are conducive to the growth in popularity and, consequently, the number of Botnets.
- If someone wants to start a "business" and has no programming skills, there are plenty of "Bot for sale" offers on forums.
- 'encryption of these programs' code can also be ordered in the same way to protect them from detection by antivirus tools.
- Another option is to steal an existing Botnet. Figure 2.8 explains how Botnets create business.
- One can reduce the chances of becoming part of a Bot by limiting access into the system.
- Leaving your Internet connection ON and unprotected is just like leaving the front door of the house wide open.

One can ensure following to secure the system:

1. Use antivirus and anti-Spyware software and keep it up-to-date:
2. Set the OS to download and install security patches automatically:
3. Use a firewall to protect the system from hacking attacks while it is connected on the Internet: A firewall is a software and/or hardware that is designed to block unauthorized access while permitting authorized communications.
4. Disconnect from the Internet when you are away from your computer:
5. Downloading the freeware only from websites that are known and trustworthy:
6. Check regularly the folders in the mail box – "sent items" or "outgoing" – for those

messages you did not send:

7. Take an immediate action if your system is infected:

Box 2.9 | Technical Terms
Malware: It is malicious software, designed to damage a computer system without the owner's informed consent. Viruses and worms are the examples of malware.
Adware: It is advertising-supported software, which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Few Spywares are classified as Adware.
Spam: It means unsolicited or undesired E-Mail messages
Spamdexing: It is also known as search Spam or search engine Spam. It involves a number of methods, such as repeating unrelated phrases, to manipulate the relevancy or prominence of resources indexed by a search engine in a manner inconsistent with the purpose of the indexing system.
DDoS: Distributed denial-of-service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods.

2.7 Attack Vector

- **An "attack vector" is a path**, which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome.
- **Attack vectors** enable attackers to exploit system vulnerabilities, including the human element.
- **Attack vectors** include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception. All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defenses.
- To some extent, firewalls and antivirus software can block attack vectors.
- However, no protection method is totally attack-proof.
- A defense method that is effective today may not remain so for long because attackers are constantly updating attack vectors, and seeking new ones, in their quest to gain unauthorized access to computers and servers. Refer to Box 2.10.
- The most common malicious payloads are viruses (which can function as their own attack vectors), Trojan Horses, worms, and Spyware.
- If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.
- In the technical terms, payload is the necessary data being carried within a packet or other transmission unit – in this scenario (i.e., attack vector) payload means the malicious activity that the attack performs.
- From the technical perspective, payload does not include the "overhead" data required to get the packet to its destination. Payload may depend on the following point of view:

"What constitutes it?" To a communications layer that needs some of the overhead data to do its job, the payload is sometimes considered to include that part of the overhead data that this layer handles. The attack vectors described here are how most of them are launched.

1. **Attack by E-Mail:** The content is either embedded in the message or linked to by the message. Sometimes attacks combine the two vectors, so that if the message does not get you, the attachment will. Spam is almost always carrier for scams, fraud, dirty tricks, or malicious action of some kind. Any link that offers something "free" or tempting is a suspect.
2. **Attachments (and other files):** Malicious attachments install malicious computer code. The code could be a virus, Trojan Horse, Spyware, or any other kind of malware. Attachments attempt to install their payload as soon as you open them.
3. **Attack by deception:** Deception is aimed at the user/operator as a vulnerable entry point. It is not just malicious computer code that one needs to monitor. Fraud, scams, and to some extent Spam, not to mention viruses, worms and such require the unwitting cooperation of the computer's operator to succeed. Social engineering are other forms of deception that are often an attack vector too.
4. **Hackers:** Hackers/crackers are a formidable attack vector because, unlike ordinary Malicious Code, people are flexible and they can improvise. Hackers/crackers use variety of hacking tools, heuristics, Cyberoffenses: How and social engineering to gain access to computers and online accounts. They often install a Trojan Horse to commandeer the computer for their own use.
5. **Heedless guests (attack by webpage):** Counterfeit websites are used to extract personal information. Such websites look very much like the genuine websites they imitate. One may think he/she is doing business with someone you trust. However, he/she is really giving their personal information, like address, credit card number, and expiration date. They are often used in conjunction with Spam, which gets you there in the first place. Pop-up webpages may install Spyware, Adware or Trojans.

6. **Attack of the worms:** Many worms are delivered as E-Mail attachments, but network worms use holes in network protocols directly. Any remote access service, like file sharing, is likely to be vulnerable to this sort of worm. In most cases, a firewall will block system worms. Many of these system worms install Trojan Horses.

7. **Malicious macros:** Microsoft Word and Microsoft Excel are some of the examples that allow macros. A macro does something like automating a spreadsheet, for example. Macros can also be used for malicious purposes. All Internet services like instant messaging, Internet Relay Chart(IRC), and P2P file-sharing networks rely on cozy connections between the computer and the other computers on the Internet. If one is using P2P software then his/her system is more vulnerable to hostile exploits.
8. **Foistware (sneakware):** Foistware is the software that **adds hidden components** to the system with cunning nature. Spyware is the most common form of foistware. Foistware is partial- legal software bundled with some attractive software. Sneak software often

hijacks your browser and diverts you to some “revenue opportunity” that the foistware has set up.

9. **Viruses:** These are malicious computer codes that hitch a ride and make the payload. Nowadays, virus vectors include E-Mail attachments, downloaded files, worms, etc.

Box 2.10 | Zero-Day Attack

A zero-day (or zero-hour) attack[17] is a computer threat which attempts to exploit computer application vulnerabilities that are unknown to anybody in the world (i.e., undisclosed to the software vendor and software users) and/or for which no patch (i.e., security fix) is available. Zero-day exploits are used or shared by attackers before the software vendor knows about the vulnerability.

Sometimes software vendors discover the vulnerability but developing a patch can take time. Alternatively, software vendors can also hold releasing the patch reason to avoid the flooding the customers with numerous individual updates. A “zero-day” attack is launched just on or before the first or “zeroth” day of vendor awareness, reason being the vendor should not get any opportunity to communicate/distribute a security fix to users of such software. If the vulnerability is not particularly dangerous, software vendors prefer to hold until multiple updates (i.e., security fixes commonly known as patches) are collected and then release them together as a package. Malware writers are able to exploit zero-day vulnerabilities through several different attack vectors.

Zero-day emergency response team (ZERT): This is a group of software engineers who work to release non-vendor patches for zero-day exploits. Nevada is attempting to provide support with the Zeroday Project at www.zerodayproject.com, which purports to provide information on upcoming attacks and provide support to vulnerable systems. Also, visit the weblink http://www.isotf.org/zert to get more information about it.

2.8 Cloud Computing

- The growing popularity of cloud computing and virtualization among organizations have made it possible, the next target of cybercriminals.
- Cloud computing services, while offering considerable benefits and cost savings, move servers outside the organizations security perimeter, which make it easier for cybercriminals to attack these systems.
- Cloud computing is Internet (“cloud”)-based development and use of computer technology (“computing”).
- The term cloud is used as a metaphor for the Internet, based on the cloud drawing used to depict the Internet in computer networks.
- Cloud computing is a term used for hosted services delivered over the Internet.
- A cloud service has three distinct characteristics which differentiate it from traditional hosting:
    1. It is sold on demand – typically by the minute or the hour;
    2. It is elastic in terms of usage – a user can have as much or as little of a service as he/she wants at any given time;

3. The service is fully managed by the provider – a user just needs PC and Internet connection.

Significant innovations into distributed computing and virtualization as well as improved access speed over the Internet have generated a great demand for cloud computing.

2.8.1 Why Cloud Computing?

The cloud computing has following advantages.

1. Applications and data can be accessed from anywhere at any time. Data may not be held on a hard drive on one user's computer.
2. It could bring hardware costs down. One would need the Internet connection.
3. Organizations do not have to buy a set of software or software licenses for every employee and the organizations could pay a metered fee to a cloud computing company.
4. Organizations do not have to rent a physical space to store servers and databases. Servers and digital storage devices take up space. Cloud computing gives the option of storing data on someone else's hardware, thereby removing the need for physical space on the front end.
5. Organizations would be able to save money on IT support because organizations will have to ensure about the desktop (i.e., a client) and continuous Internet connectivity instead of servers and other hardware. The cloud computing services can be either private or public.

2.8.2 Types of Services

Services provided by cloud computing are as follows:

1. **Infrastructure-as-a-service (IaaS):** It is like Amazon Web Services that provide **virtual servers** with unique IP addresses and **blocks of storage** on demand. Customers benefit from an Application Programmable Interface (API) from which they can control their servers. As customers can pay for exactly the amount of service they use, like for electricity or water, this service is also called utility computing.
2. **Platform-as-a-service (PaaS):** It is a set of software and development tools hosted on the provider's servers. Developers can create applications using the provider's APIs. **Google Apps** is one of the most famous PaaS providers. Developers should take notice that there are not any interoperability standards; therefore, some providers may not allow you to take your application and put it on another platform.
3. **Software-as-a-service (SaaS):** It is the broadest market. In this case, the provider allows the customer only to use its applications. The **software interacts with the user through a user interface**. These applications can be anything from Web-based E-Mail to applications such as Twitter or Last.fm.

2.8.3 Cybercrime and Cloud Computing

- Nowadays, prime area of the risk in cloud computing is protection of user data. Although cloud computing is an emerging field, the idea has been evolved over few years.
- Risks associated with cloud computing environment are as follows

1. Elevated user access-Any data processed outside the organization brings with it an inherent level of risk
2. Regulatory compliance-Cloud computing service providers are not able and/or not willing to undergo external assessments.
3. Location of the data-User doesn’t know where the data is stored or in which country it is hosted.
4. Segregation of data-Data of one organization is scattered in different locations
5. Recovery of the data-In case of any disaster, availability of the services and data is critical.
6. Information security- violation reports Due to complex IT environment and several customers logging in and logging out of the hosts, it becomes difficult to trace inappropriate and/or illegal activity
7. Long-term viability- In case of any major change in the cloud computing service provider (e.g., acquisition and merger, partnership breakage), the service provided is at the stake.

||Jai Sri Gurudev ||
BGSKH Education Trust (R.) – A unit of Sri Adichunchanagiri Shikshana Trust(R.)
BGS College of Engineering and Technology (BGSCET)
Mahalakshmipuram, West of Chord Road, Bengaluru-560086
(Approved by AICTE, New Delhi and Affiliated to VTU, Belagavi)

Question Bank

Subject: Introduction to Cyber Security **Class:** AI and ML/AIDS/CSD

Subject code: BETCK105I/205I **Faculty:** Mrs. Jyothi R

Course Outcomes

CO1: Interpret the cybercrime terminologies
CO2: Analyze Cyber offenses and Botnets
CO3: Illustrate Tools and Methods used on Cybercrime
CO4: Analyze Phishing and Identity Theft
CO5: Justify the need of computer forensics

Module 2: Cyber Offenses: How Criminals Plan them Introduction, How criminals plan the attacks, Social Engineering, Cyber Stalking, Cybercafe & cybercrimes, Botnets: The fuel for cybercrime, Attack Vector. Chapter 2 (2.1 to 2.7)

Sl. No.	**Questions**	**CO**	**BT**
Topic:	**Introduction**		
1.	Explain the following • Hacker • Brute Force Hacking • Cracker • Cracker tools • Phreaking • War dialer	CO2	L2
2.	How are cybercrimes classified? Explain with examples. OR Explain the categories of cybercrime?	CO2	L2
3.	Explain the difference between passive and active attacks provide tools as example.	CO2	L2
4.	List and explain the Phases of Cybercrime Planning	CO2	L2
5.	What is Social Engineering Explain the classification of social engineering withexamples	CO2	L2
6	How are cybercrimes classified? Explain with examples.**OR** Explain the categories of cybercrime?	CO2	
7	Explain in details Ports and Ports scanning in cyber offenses.	CO2	
8	What is cyberstalking? As per your understanding is it a crime under the Indian IT act?	CO2	
9	Explain types of Stalkers	CO2	
10	Explain the steps of how stalking works?	CO2	L3
11	Explain the Real-life Incident of Cyberstalking?	CO2	

12	How cyber cafes are creating the paths for cybercrimes?	CO2	L2
13	Discuss the safety and security measures while using the computer in a cybercafe?	CO2	L2
14	Explain how Botnets canbe used as fuel to cybercrime.	CO2	L2
15	Explain with neat diagram how Botnets createbusiness and used for gainful purpose.	CO2	L2
16	What are the different attacks launched with attack vector. Explain	CO2	L2
17	Explain the Zero-Day Attack?	CO2	L2

Module 3
Tools and Methods Used in Cybercrime

Introduction

Different forms of attacks through which attackers target the computer systems are as follows:

1. Initial uncovering:
    - Two steps are involved here.
        i. In the first step called as reconnaissance, the attacker gathers information about the target on the Internet websites.
        ii. In the second step, the attacker finds the company's internal network, such as, Internet domain, machine names and the company's Internet Protocol (IP) address ranges to steal the data.
2. Network probe (investigation):
    - At the network probe stage, the attacker scans the organization information through a "ping sweep" of the network IP addresses.
    - Then a "port scanning" tool is used to discover exactly which services are running on the target system.
    - At this point, the attacker has still not done anything that would be considered as an abnormal activity on the network or anything that can be classified as an intrusion.
3. Crossing the line toward electronic crime (E-crime):
    - Once the attackers are able to access a user account, then they will attempt further exploits to get an administrator or "root" access.
    - Root access is a UNIX term and is associated with the system privileges required to run all services and access all files on the system (readers are expected to have a basic familiarity with Unix-based systems).
    - "Root" is an administrator or super-user access and grants them the privileges to do anything on the system.
4. Capturing the network:
    - At this stage, the attacker attempts to "own" the network. The attacker gains the internal network quickly and easily by target systems.

- The next step is to remove any evidence of the attack. The attacker will usually install a set of tools that replace existing files and services with Trojan files and services that have a backdoor password.

5. Grab the data:
    - Now that the attacker has "captured the network," he/she takes advantage of his/her position to steal confidential data
6. Covering tracks:
    - This is the last step in any cyber attack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected.
    - The attacker can remain undetected for long periods.
    - During this entire process, the attacker takes optimum care to hide his/her identity (ID) from the first step itself.

Proxy Servers and Anonymizers

Proxy server is a computer on a network which acts as an intermediary for connection with other computers on that network.

- The attacker first connects to a proxy server and establishes a connection with the target system through existing connection with proxy.
- This enables an attacker to surf on the Web anonymously and/or hide the attack.
- A client connects to the proxy server and requests some services (such as a file, webpage) available from a different server.
- The proxy server evaluates the request and provides the resource by establishing the connection to the respective server and/or requests the required service on behalf of the client.
- Using a proxy server can allow an attacker to hide ID (i.e., become anonymous on the network).

A proxy server has following purposes:

1. Keep the systems behind the curtain (mainly for security reasons).
2. Speed up access to a resource (through "caching"). It is usually used to cache the web pages from a web server.
3. Specialized proxy servers are used to filter unwanted content such as advertisements.
4. Proxy server can be used as IP address multiplexer to enable to connect number of

computers on the Internet, whenever one has only one IP address

- One of the advantages of a proxy server is that its cache memory can serve all users.
- If one or more websites are requested frequently, may be by different users, it is likely to be in the proxy's cache memory, which will improve user response time.
- An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information.
- Anonymizers are services used to make Web surfing anonymous by utilizing a website that acts as a proxy server for the web client.

Phishing

"Phishing" refers to an attack using mail programs to deceive Internet users into disclosing confidential information that can be then exploited for illegal purposes.

- While checking electronic mail (E-Mail) one day a user finds a message from the bank threatening to close the bank account if he/she does not reply immediately.
- Although the message seems to be suspicious from the contents of the message, it is difficult to conclude that it is a fake/false E-Mail.
- This message and other such messages are examples of Phishing – in addition to stealing personal and financial data – and can infect systems with viruses and also a method of online ID theft in various cases.
- These messages look authentic and attempt to get users to reveal their personal information.
- It is believed that Phishing is an alternative spelling of "fishing," as in "to fish for information."
- The first documented use of the word "Phishing" was in 1996.

How Phishing Works?

Phishers work in the following ways:

1. Planning: Criminals, usually called as phishers, decide the target.
2. Setup: Once phishers know which business/business house to spoof and who their victims.
3. Attack: the phisher sends a phony message that appears to be from a reputable source.
4. Collection: Phishers record the information of victims entering into webpages or pop-

up windows.

5. Identity theft and fraud: Phishers use the information that they have gathered to make illegal purchases or commit fraud.

Nowadays, more and more organizations/institutes provide greater online access for their customers and hence criminals are successfully using Phishing techniques to steal personal information and conduct ID theft at a global level.

Password Cracking

- Password is like a key to get an entry into computerized systems like a lock.
- Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.
- Usually, an attacker follows a common approach – repeatedly making guesses for the password.

The purpose of password cracking is as follows:

1. To recover a forgotten password.
2. As a preventive measure by system administrators to check for easily crackable passwords.
3. To gain unauthorized access to a system.

Manual password cracking is to attempt to logon with different passwords. The attacker follows the following steps:

1. Find a valid user account such as an Administrator or Guest;
2. create a list of possible passwords;
3. rank the passwords from high to low probability;
4. key-in each password;
5. try again until a successful password is found.

Passwords can be guessed sometimes with knowledge of the user's personal information. Examples of guessable passwords include:

1. Blank (none);
2. the words like "password," "passcode" and "admin";
3. series of letters from the "QWERTY" keyboard, for example, qwerty, asdf or qwertyuiop;
4. user's name or login name;

5. name of user's friend/relative/pet;
6. user's birthplace or date of birth, or a relative's or a friend's;
7. user's vehicle number, office number, residence number or mobile number;
8. name of a celebrity who is considered to be an idol (e.g., actors, actress, spiritual gurus) by the user;

- An attacker can also create a script file (i.e., automated program) which will be executed to try each password in a list.
- This is still considered manual cracking, is time-consuming and not usually effective.
- Passwords are stored in a database and password verification process is established into the system when a user attempts to login or access a restricted resource.
- To ensure confidentiality of passwords, the password verification data is usually not stored in a clear text format.
- For example, one-way function (which may be either an encryption function or a cryptographic hash) is applied to the password, possibly in combination with other data, and the resulting value is stored.
- When a user attempts to login to the system by entering the password, the same function is applied to the entered value and the result is compared with the stored value. If they match, user gains the access; this process is called authentication.

The most commonly used hash functions can be computed rapidly and the attacker can test these hashes with the help of passwords cracking tools (see Table 4.3) to get the plain text password.

Password cracking attacks can be classified under three categories as follows:

1. Online attacks;
2. offline attacks;
3. non-electronic attacks (e.g., social engineering, shoulder surfing and dumpster diving).

Online Attacks

- An attacker can create a script file that will be executed to try each password in a list and when matches, an attacker can gain the access to the system.
- The most popular online attack is man-in-the middle (MITM) attack, also termed as "bucket- brigade attack" or sometimes "Janus attack."
- It is a form of active stealing in which the attacker establishes a connection between a

victim and the server to which a victim is connected.

- When a victim client connects to the fraudulent server, the MITM server intercepts the call, hashes the password and passes the connection to the victim server (e.g., an attacker within reception range of an unencrypted Wi-Fi wireless access point can insert himself as a man-in- the-middle).
- This type of attack is used to obtain the passwords for E-Mail accounts on public websites such as Yahoo, Hotmail and Gmail and can also used to get the passwords for financial websites that would like to gain the access to banking websites.

Offline Attacks

- Mostly offline attacks are performed from a location other than the target (i.e., either a computer system or while on the network) where these passwords reside or are used.
- Offline attacks usually require physical access to the computer and copying the password file from the system onto removable media.

Password guidelines.

1. Passwords used for business E-Mail accounts, personal E-Mail accounts and banking/financial user accounts should be kept separate.
2. Passwords should be of minimum eight alphanumeric characters (common names or phrases should be phrased).
3. Passwords should be changed every 30/45 days.
4. Passwords should not be shared with relatives and/or friends.
5. Password used previously should not be used while renewing the password.
6. Passwords of personal E-Mail accounts and banking/financial user accounts should be changed from a secured system, within couple of days, if these E-Mail accounts has been accessed from public Internet facilities such as cybercafes/hotels/libraries.
7. Passwords should not be stored under mobile phones/PDAs, as these devices are also prone to cyberattacks.
8. In case E-Mail accounts/user accounts have been hacked, respective agencies/institutes should be contacted immediately.

Keyloggers and Spywares

- Keystroke logging, often called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored.
- Keystroke logger or keylogger is quicker and easier way of capturing the passwords and monitoring the victims' IT savvy behavior. It can be classified as software keylogger and hardware keylogger.

Software Keyloggers

- Software keyloggers are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded.
- Software keyloggers are installed on a computer system by Trojans or viruses without the knowledge of the user.
- Cybercriminals always install such tools on the insecure computer systems available in public places (i.e., cybercafés, etc) and can obtain the required information about the victim very easily.
- A keylogger usually consists of two files that get installed in the same directory: a dynamic link library (DLL) file and an EXEcutable (EXE) file that installs the DLL file and triggers it to work. DLL does all the recording of keystrokes.

Some Important Keyloggers are as follows

All In One Keylogger	Stealth Keylogger	Perfect Keylogger
KGB Spy	Spy Buddy	Elite Keylogger
CyberSpy	Powered Keylogger	

Hardware Keyloggers

- Hardware keyloggers are small hardware devices.
- These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device.
- Cybercriminals install such devices on ATM machines to capture ATM Cards' PINs.
- Each keypress on the keyboard of the ATM gets registered by these keyloggers.
- These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

Antikeylogger

- Antikeylogger is a tool that can detect the keylogger installed on the computer system and can remove the tool. (Visit http://www.anti-keyloggers.com for more information)

Advantages of using antikeylogger are as follows:

1. Firewalls cannot detect the installations of keyloggers on the systems; hence, antikeyloggers can detect installations of keylogger.
2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs; if not updated, it does not serve the purpose, which makes the users at risk.
3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
4. It prevents ID theft (we will discuss it more in Chapter 5).
5. It secures E-Mail and instant messaging/chatting.

Spywares

- Spyware is a type of malware (i.e., malicious software) that is installed on computers which collects information about users without their knowledge.
- The presence of Spyware is typically hidden from the user; it is secretly installed on the user’s personal computer.
- Sometimes, however, Spywares such as keyloggers are installed by the owner of a shared, corporate or public computer on purpose to secretly monitor other users.

Some Important Spywares are as follows:

Spy.	Spector Pro.	Spector Pro.
eBlaster.	Remotespy .	Stealth Recorder Pro.
Stealth Website Logger.	Flexispy.	Wiretap Professional.
PC PhoneHome.	SpyArsenal Print Monitor Pro.	

Box 4.3 | Malwares

Malware, short for malicious software, is a software designed to infiltrate a computer system without the owner’s informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive or annoying software or program code. Malware can be classified as follows:

1. Viruses and worms: These are known as *infectious malware*. They spread from one computer system to another with a particular behavior.

2. Trojan Horses: A Trojan Horse,[14] 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

3. Rootkits: Rootkits is a software system that consists of one or more programs designed to obscurethe fact that a system has been compromised.

4. Backdoors: Backdoor[16] in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plain text and so on while attempting to remain undetected.

5. Spyware:

6. Botnets:

7. Keystroke loggers:

Virus and Worms

- Computer virus is a program that can "infect" legitimate 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.
- A virus can start on event-driven effects (e.g., triggered after a specific number of executions), time-driven effects (e.g., triggered on a specific date, such as Friday the 13th) or can occur at random.

Viruses can take some typical actions:

1. Display a message to prompt an action which may set of the virus;

2. delete files inside the system into which viruses enter;
3. scramble data on a hard disk;
4. cause erratic screen behavior;
5. halt the system (PC);
6. just replicate themselves to propagate further harm.

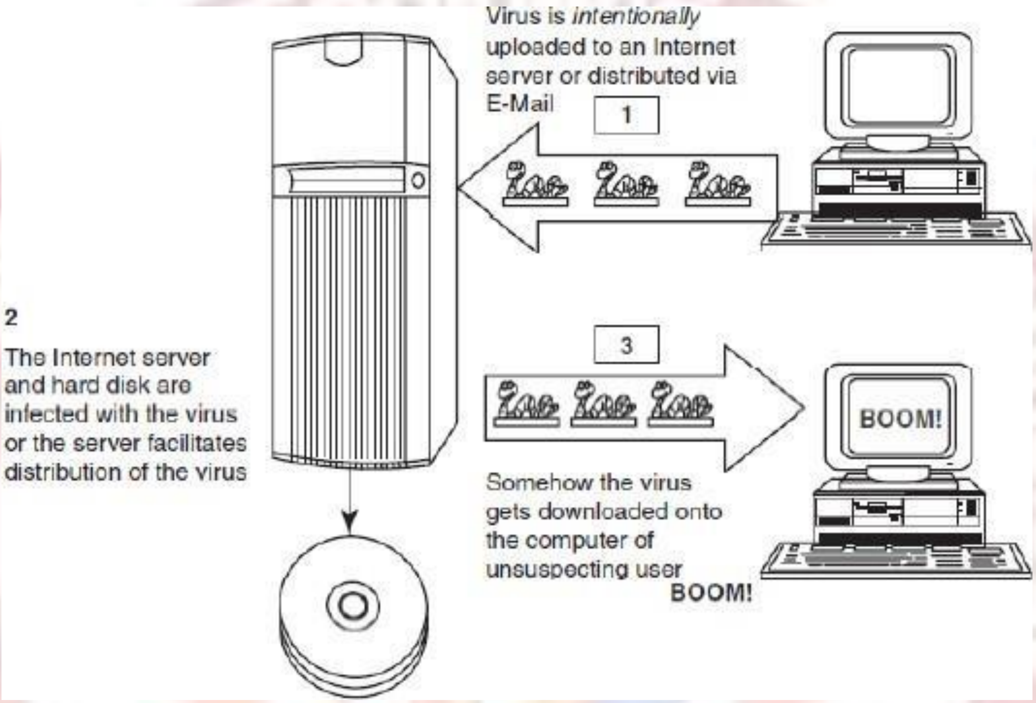

Virus is *intentionally* uploaded to an Internet server or distributed via E-Mail
1
2
The Internet server and hard disk are infected with the virus or the server facilitates distribution of the virus
3
BOOM!
Somehow the virus gets downloaded onto the computer of unsuspecting user
BOOM!

Figure: Virus Spread Through Internet

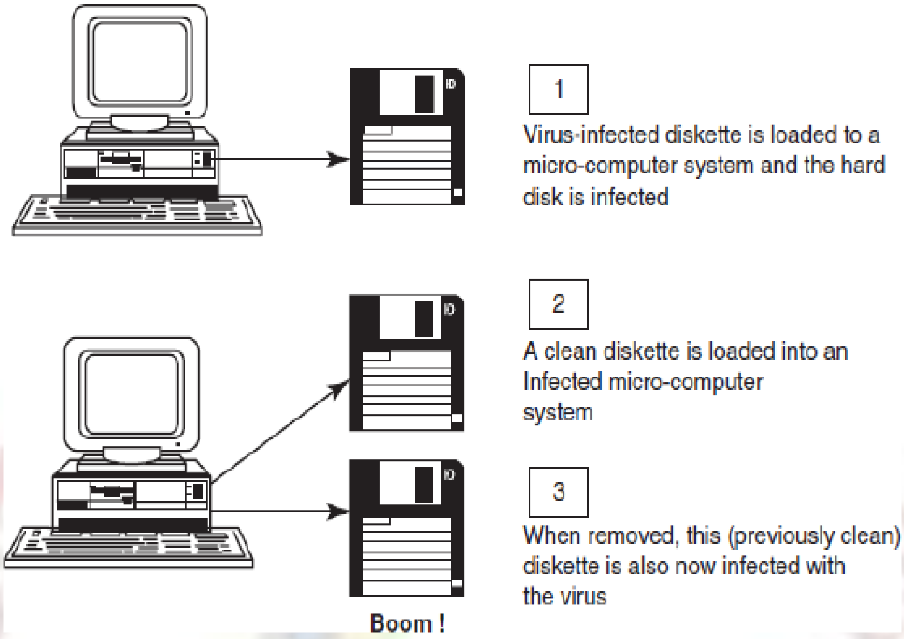

1
Virus-infected diskette is loaded to a micro-computer system and the hard disk is infected
2
A clean diskette is loaded into an Infected micro-computer system
3
When removed, this (previously clean) diskette is also now infected with the virus
Boom !

Figure: Virus Spread Through stand alone System

- **Computer virus** has the ability to copy itself and infect the system.
- The term *virus* is also commonly but erroneously used to refer to other types of malware, Adware and Spyware programs that do not have reproductive ability.
- A true virus can only spread from one system to another (in some form of executable code) when its host is taken to the target computer; for instance, when a user sent it over the Internet or a network, or carried it on a removable media such as CD, DVD or USB drives.
- Viruses can increase their chances of spreading to other systems by infecting files on a network file system or a file system that is accessed by another system.
- Malware includes computer viruses, worms, Trojans, most Rootkits, Spyware, dishonest Adware, crimeware and other malicious and unwanted software as well as true viruses.
- Viruses are sometimes confused with computer worms and Trojan Horses, which are technically different (see Table 4.7 to understand the difference between computer virus and worm).
- A worm spreads itself automatically to other computers through networks by exploiting security vulnerabilities, whereas a Trojan is a code/program that appears to be harmless but hides malicious functions.

- Worms and Trojans, such as viruses, may harm the system's data or performance.
- Some viruses and other malware have noticeable symptoms that enable computer user to take necessary corrective actions, but many viruses are surreptitious or simply do nothing for user's to take note of them.
- Some viruses do nothing beyond reproducing themselves.

Types of Viruses

1. **Boot sector viruses:** It infects the storage media on which OS is stored (e.g., hard drives) and which is used to start the computer system.
2. **Program viruses:** These viruses become active when the program file (usually with extensions .bin, .com,.exe, .ovl, .drv) is excuted
3. **Multipartite viruses:** It is a hybrid of a boot sector and program viruses. It infects program files along with the boot record when the infected program is active.
4. **Stealth viruses:** It hides itself and so detecting this type of virus is very difficult. It can hiding itself such a way that antivirus software also cannot detect it. Example for Stealth virus is "Brain Virus".
5. **Polymorphic viruses:** It acts like a "chameleon" that changes its virus signature (i.e., binary pattern) every time it spreads through the system (i.e., multiplies and infects a new file). Hence, it is always difficult to detect polymorphic virus with the help of an antivirus program.
6. **Macro viruses:** Many applications, such as Microsoft Word and Microsoft Excel, support MACROs (i.e., macrolanguages). These macros are programmed as a macro embedded in a document. Once macrovirus gets onto a victim's computer then every document he/she produces will become infected.
7. **Active X and Java Control:** All the web browsers have settings about Active X and Java Controls.

World's worst worm attacks.

Conficker	INF/AutoRun	Win32 PSW	Win32/Agent
Win32/FlyStudio	Win32/Pacex.Gen	Win32/Qhost	WMA/ TrojanDownloader

The world's worst virus and worm attacks!!!

Morris Worm	ILOVEYOU	Nimda	Jerusalem
Code Red	Melissa	Melissa	
Sobig	Storm Worm	Michelangelo	

Trojan Horses and Backdoors

- Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, ruining the file allocation table on the hard disk.
- A Trojan Horse may get widely redistributed as part of a computer virus.
- The term Trojan Horse comes from Greek mythology about the Trojan War.
- Like Spyware and Adware, Trojans can get into the system in a number of ways, including from a web browser, via E-Mail.
- It is possible that one could be forced to reformat USB flash drive or other portable device to eliminate infection and avoid transferring it to other machines.
- Unlike viruses or worms, Trojans do not replicate themselves but they can be equally destructive.
- On the surface, Trojans appear benign and harmless, but once the infected code is executed, Trojans kick in and perform malicious functions to harm the computer system without the user's knowledge.
- For example, waterfalls.scr is a waterfall screen saver as originally claimed by the author; however, it can be associated with malware and become a Trojan to unload hidden programs and allow unauthorized access to the user's PC.

Some typical examples of threats by Trojans are as follows:

1. They erase, overwrite or corrupt data on a computer.
2. They help to spread other malware such as viruses (by a dropper Trojan).
3. They deactivate or interfere with antivirus and firewall programs.
4. They allow remote access to your computer (by a remote access Trojan).
5. They upload and download files without your knowledge.
6. They gather E-Mail addresses and use them for Spam.

7. They log keystrokes to steal information such as passwords and credit card numbers.
8. They copy fake links to false websites, display porno sites, play sounds/videos and display images.
9. They slow down, restart or shutdown the system.
10. They reinstall themselves after being disabled.
11. They disable the task manager.
12. They disable the control panel.

Backdoor

- A backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes.
- However, attackers often use backdoors that they detect or install themselves as part of an exploit.
- In some cases, a worm is designed to take advantage of a backdoor created by an earlier attack.
- A backdoor works in background and hides from the user.
- It is very similar to a virus and, therefore, is quite difficult to detect and completely disable.
- A backdoor is one of the most dangerous parasite, as it allows a malicious person to perform any possible action on a compromised system.

Following are some functions of backdoor:

1. It allows an attacker to create, delete, rename, copy or edit any file, execute various commands; change any system settings; alter the Windows registry; run, control and terminate applications; install arbitrary software and parasites.
2. It allows an attacker to control computer hardware devices, modify related settings, shutdown or restart a computer without asking for user permission.
3. It steals sensitive personal information, valuable documents, passwords, login names, ID details; logs user activity and tracks web browsing habits.

4. It records keystrokes that a user types on a computer's keyboard and captures screenshots.
5. It sends all gathered data to a predefined E-Mail address, uploads it to a predetermined FTP server or transfers it through a background Internet connection to a remote host.
6. It infects files, corrupts installed applications and damages the entire system.

Following are a few examples of backdoor Trojans:

1. Back Orifice
2. Bifrost:
3. SAP backdoors
4. Onapsis Bizploit:

Follow the following steps to protect your systems from Trojan Horses and backdoors:

1. Stay away from suspect websites/weblinks:
2. Surf on the Web cautiously:
3. Install antivirus/Trojan remover software:

Steganography

- Steganography is the practice of concealing (hiding) a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos , meaning "covered, concealed, or protected", and graphein meaning "writing".
- It is a method that attempts to hide the existence of a message or communication.
- Steganography is always misunderstood with cryptography
- The different names for steganography are data hiding, information hiding and digital watermarking.
- Steganography can be used to make a digital watermark to detect illegal copying of digital images. Thus, it aids confidentiality and integrity of the data.
- *Digital watermarking* is the process of possibly irreversibly embedding information into a digital signal.
- The Digital signal may be, for example, audio, pictures or video.

- If the signal is copied then the information is also carried in the copy.
- In other words, when steganography is used to place a hidden "trademark" in images, music and software, the result is a technique referred to as "watermarking"

Steganalysis

- Steganalysis is the art and science of detecting messages that are hidden in images, audio/video files using steganography.
- The goal of steganalysis is to identify suspected packages and to determine whether or not they have a payload encoded into them, and if possible recover it.
- Automated tools are used to detect such steganographed data/information hidden in the image and audio and/or video files.

Box 4.7 | Difference between Steganography and Cryptography

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message; this is in contrast to cryptography, of the message itself is not disguised, but the content is obscured. It is said that terrorists use where the existence steganography techniques to hide their communication in images on the Internet; most popular images are used such as those of film actresses or other celebrities. In its basic form, steganography is simple.

DoS and DDoS Attacks

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource (i.e., information systems) unavailable to its intended users.

DoS Attacks

- 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 attackers typically target sites or services hosted on high-profile web servers** such as banks, credit card payment gateways, mobile phone networks and even root name servers.

- Buffer overflow technique is employed to commit such kind of criminal attack known as *Spoofing*.
- The term IP address Spoofing refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of concealing the ID of the sender or impersonating another computing system.
- A packet is a formatted unit of data carried by a packet mode computer network.
- The attacker spoofs the IP address and floods the network of the victim with repeated requests.
- As the IP address is fake, the victim machine keeps waiting for response from the attacker's machine for each request.
- This consumes the bandwidth of the network which then fails to serve the legitimate requests and ultimately breaks down.
- The United States Computer Emergency Response Team defines symptoms of DoS attacks to include:
    1. Unusually slow network performance (opening files or accessing websites);
    2. unavailability of a particular website;
    3. inability to access any website;
    4. dramatic increase in the number of Spam E-Mails received (this type of DoS attack is termed as an E-Mail bomb).

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:

1. Flood a network with traffic, thereby preventing legitimate network traffic.
2. Disrupt connections between two systems, thereby preventing access to a service.
3. Prevent a particular individual from accessing a service.
4. Disrupt service to a specific system or person.

Classification of DoS Attacks

1. **Bandwidth attacks:** Loading any website takes certain time. Loading means complete webpage appearing on the screen and system is awaiting user's input.

2. **Logic attacks:** These kind of attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack.
3. **Protocol attacks**: Protocols here are rules that are to be followed to send data over network.
4. **Unintentional DoS attack :** This is a scenario where a website ends up denied not due to a attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity.

Types or Levels of DoS Attacks

There are several types or levels of DoS attacks as follows:

1. **Flood attack:** This is the earliest form of DoS attack and is also known as *ping food*. It is based on an attacker simply sending the victim overwhelming number of ping packets, usually by using the "ping" command, which result into more traffic than the victim can handle.
2. **Ping of death attack:** The ping of death attack **sends oversized Internet Control Message Protocol (ICMP) packets,** and it is one of the core protocols of the IP Suite. It is mainly used by networked computers' OSs to send error messages indicating (e.g., that a requested service is not available or that a host or router could not be reached) datagrams (encapsulated in IP packets) to the victim.
3. **SYN attack:** It is also termed as ***TCP SYN Flooding***. In the TCP, handshaking of network connections is done with SYN and ACK messages.
   - An attacker initiates a TCP connection to the server with an SYN.
   - The server replies with an SYN-ACK.
   - The client then does not send back an ACK, causing the server to allocate memory for the pending connection and wait.
   - This fills up the buffer space for SYN messages on the target system, preventing other systems on the network from communicating with the target system.
4. **Teardrop attack:** The teardrop attack is an attack where **fragmented packets are forged to overlap each other when the receiving host tries to reassemble them**. IP's packet fragmentation algorithm is used to send corrupted packets to confuse the victim

and may hang the system. This attack can crash various OSs due to a bug in their TCP/IP fragmentation reassembly code.

5. **Smurf attack:** This is a type of DoS attack that **floods a target system via spoofed broadcast ping messages.** This attack consists of a host sending an echo request (ping) to a network broadcast address.
6. **Nuke:** Nuke is an old DoS attack against computer networks consisting of **fragmented or invalid packets sent to the target.**

Tools Used to Launch DoS Attack

1. **Jolt2 :** The vulnerability allows remote attackers to cause a DoS attack against Windows-based machines – the attack causes the target machine to consume of the CPU time on processing of illegal packets.
2. **Nemesy :** This program generates random packets of spoofed source IP to enable the attacker to launch DoS attack.
3. **Targa :** It is a program that can be used to run eight different DoS attacks. The attacker has the option to launch either individual attacks or try all the attacks until one is successful.
4. **Crazy Pinger :** This tool could send large packets of ICMP(Internet Control Message Protocol) to a remote target network.
5. **SomeTrouble:** It is a remote flooder and bomber. It is developed in Delphi.

DDoS Attacks

- In a DDoS attack, an attacker may use your computer to attack another computer.
- By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer.
- He/she could then force your computer to send huge amounts of data to a website or send Spam to particular E-Mail addresses.
- The attack is “distributed” because the attacker is using multiple computers, including yours, to launch the DoS attack.
- A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system.

- The zombie systems are called “secondary victims” and the main target is called “primary victim.”
- Malware can carry DDoS attack mechanisms – one of the better-known examples of this is MyDoom.
- Botnet is the popular medium to launch DoS/DDoS attacks.
- Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts.

How to Protect from DoS/DDoS Attacks

Computer Emergency Response Team Coordination Center (CERT/CC) offers many preventive measures from being a victim of DoS attack.

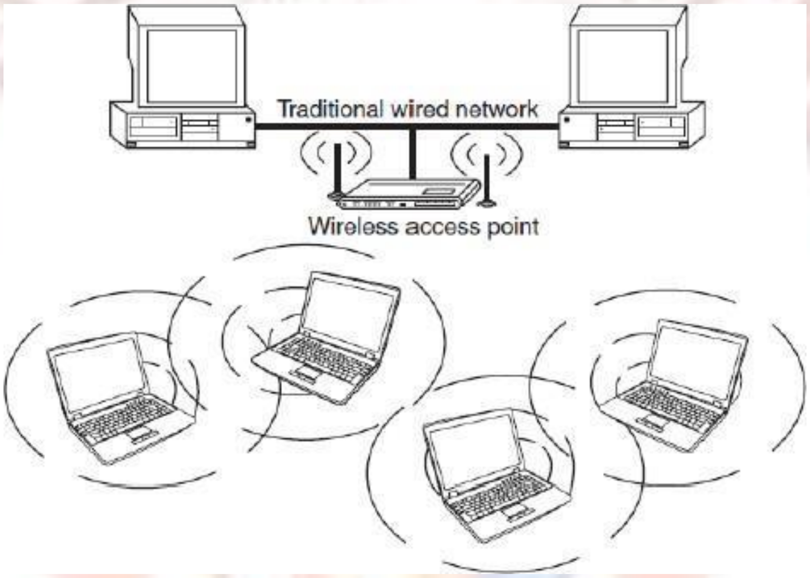
1. Implement router **filters**. This will lessen your exposure to certain DoS attacks.
2. If such filters are available for your system, **install patches** to guard against TCP SYN flooding.
3. Disable any unused or inessential network service.
4. Enable quota systems on your OS if they are available.
5. Observe your system’s performance and establish baselines for ordinary activity.
6. Routinely examine your physical security with regard to your current needs.
7. Use Tripwire or a similar tool to detect changes in configuration information or other files.
8. Invest in and maintain “hot spares” – machines that can be placed into service quickly if a similar machine is disabled.
9. Invest in redundant and fault-tolerant network configurations.
10. Establish and maintain regular backup schedules
11. Establish and maintain appropriate password policies

Attacks on Wireless Networks

- Wireless technologies have become increasingly popular in day-to-day business and personal lives.
- Hand-held devices such as the PDAs allow individuals to access calendars, E-Mail addresses, phone number lists and the Internet.
- Wireless networks extend the range of traditional wired networks by using radio waves to

transmit data to wireless-enabled devices such as laptops and PDAs.

- Wireless networks are generally composed of two basic elements
  - access points (APs) and
  - other wireless-enabled devices, such as laptops radio transmitters and receivers to communicate or "connect" with each other.
- APs are connected through physical wiring to a conventional network, and they broadcast signals with which a wireless device can connect.
- Wireless access to networks has become very common by now in India – for organizations and for individuals.



Wireless Networks

The following are different types of "mobile workers":

1. **Tethered/remote worker:** This is considered to be an employee who generally remains at a single point of work, but is remote to the central company systems.
2. **Roaming user:** This is either an employee who works in an environment (e.g., warehousing, shop floor, etc.) or in multiple areas (e.g., meeting rooms).
3. **Nomad:** This category covers employees requiring solutions in semi-tethered (connected) environments where modem use frequently.
4. **Road warrior:** This is the ultimate mobile user and spends little time in the office;

Important components of wireless network

1. **802.11 networking standards:** Institute of Electrical and Electronics Engineers (IEEE)-

802.11 is a family of standards for wireless local area network (WLAN), stating the specifications and/or requirements for computer communication.

2. **Access points:** It is also termed as AP. It is a hardware device and/or software that act as a central transmitter and receiver of WLAN radio signals. Users of wireless device, such as laptop/PDAs, get connected with these APs, which in turn get connected with the wired LAN. An AP acts as a communication hub for users to connect with the wired LAN.
3. **Wi-Fi hotspots:** A hotspot is a site that offers the Internet access by using Wi-Fi technology over a WLAN. Hotspots are found in public areas (such as coffee shops, public libraries, hotels and restaurants) and are commonly offered facility throughout much of North America and Europe.
   - *Free Wi-Fi hotspots:* Wireless Internet service is offered in public areas, free of cost and that to without any authentication.
   - *Commercial hotspots:* The users are redirected to authentication and online payment to avail the wireless Internet service in public areas.
4. **Service Set IDentifier (SSID):** It is the name of 802.11i WLAN and all wireless devices on a WLAN must use the same SSID to communicate with each other. While setting up WLAN, the user (or WLAN administrator) sets the SSID, which can be up to 32 characters long so that only the users who knew the SSID will be able to connect the WLAN. It is always advised to turn OFF the broadcast of the SSID.
5. **Wired equivalence privacy (WEP):** Wireless transmission is susceptible to eavesdropping and to provide confidentiality, WEP was introduced as part of the original 802.11i Protocol in 1997. It is always termed as deprecated security algorithm for IEEE 802.11i WLANs. SSID along with WEP delivers fair amount of secured wireless network.
6. **Wi-Fi protected access (WPA and WPA2):** WPA was introduced as an interim standard to replace WEP to improve upon the security features of WEP. WPA2 provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some corporate and government agencies.
7. **Media access control (MAC):** It is a unique identifier of each node (i.e., each network interfaces) of the network and it is assigned by the manufacturer of a network interface card (NIC) stored in its hardware. MAC address filtering allows only the devices with specific MAC addresses to access the network.

Tools used for hacking wireless networks
NetStumbler: This tool is based on Windows OS and easily identifies wireless signals being broadcast within range.
Kismet: This tool detects and displays SSIDs that are not being broadcast which 0is very critical in finding wireless networks.

Airsnort: This tool is very easy and is usually used to sniff and crack WEP keys
CowPatty: This tool is used as a brute force tool for cracking WPA-PSK and is considered to be the "New WEP" for home wireless security.
Wireshark (formerly ethereal): Ethereal can scan wireless and Ethernet data and comes with some robust filtering capabilities. It can also be used to sniff out 802.11 management Beacons and probes, and subsequently could be used as a tool to sniff out non-broadcast SSIDs.

Traditional Techniques of Attacks on Wireless Networks

In security breaches, penetration of a wireless network through unauthorized access is termed as *wireless cracking*. There are various methods that demand high level of technological skill and knowledge, and availability of numerous software tools made it less sophisticated with minimal technological skill to crack WLANs.

1. **Sniffing:** The attacker usually installs the sniffers remotely on the victim's system and conducts activities such as
   - Passive scanning of wireless network;
   - detection of SSID;
   - colleting the MAC address;
   - collecting the frames to crack WEP.
2. **Spoofing:** The attacker often launches an attack on a wireless network by simply creating a new network with a stronger wireless signal and a copied SSID in the same area as a original network. Different types of Spoofing are as follows.
   - *MAC address Spoofing*
   - *IP Spoofing:*
   - *Frame Spoofing:*
3. **Denial of service (DoS):** We have explained this attack in detail in UNIT-2.
4. **Man-in-the-middle attack (MITM):** It refers to the scenario wherein an attacker on host *A* inserts *A* between all communications – between hosts *X* and *Y* without knowledge of *X* and *Y*. All messages sent by *X* do reach *Y* but through *A* and vice versa. The objective behind this attack is to merely observe the communication or modify it before sending it out.
5. **Encryption cracking:** It is always advised that the first step to protect wireless networks

is to use WPA encryption. The attackers always devise new tools and techniques to deconstruct the older encryption technology, which is quite easy for attackers due to continuous research in this field. Hence, the second step is to use a long and highly randomized encryption key; this is very important. It is a little pain to remember long random encryption; however, at the same time these keys are much harder to crack.

How to Secure the Wireless Networks

Nowadays, security features of Wi-Fi networking products are not that time-consuming and nonintuitive; however, they are still ignored, especially, by home users. Although following summarized steps will help to improve and strengthen the security of wireless network, to know the available tools to monitor and protect the wireless networks:

1. Change the default settings of all the equipments/components of wireless network (e.g., IP address/ user IDs/administrator passwords, etc.).
2. Enable WPA/WEP encryption.
3. Change the default SSID.
4. Enable MAC address filtering.
5. Disable remote login.
6. Disable SSID broadcast.
7. Disable the features that are not used in the AP (e.g., printing/music support).
8. Avoid providing the network a name which can be easily identified (e.g., My_Home_Wifi).
9. Connect only to secured wireless network (i.e., do not autoconnect to open Wi-Fi hotspots).
10. Upgrade router's firmware periodically.
11. Assign static IP addresses to devices.
12. Enable firewalls on each computer and the router.
13. Position the router or AP safely.
14. Turn off the network during extended periods when not in use.
15. Periodic and regular monitor wireless network security.

Box 4.11 | The New "Wars" in the Internet Era!

1. Warwalking:

2. Warbiking:

3. Warkitting:

4. WAPKitting:

5. WAPjacking:

Phishing and Identity Theft: Introduction , Phishing

Identity theft can be done thorough the following ways.

1. **Spam E-Mails**
   - Also known as "junk E-Mails" they involve nearly identical messages sent to numerous recipients. Spam E-Mails have steadily grown since the early 1990s. Botnets, networks of virus-infected computers, are used to send about 80% of Spam.
   - Types of Spam E-Mails are as follows:
2. **Unsolicited bulk E-Mail (UBE):** It is *synonym for SPAM* unsolicited E-Mail sent in large quantities.
3. **Unsolicited commercial E-Mail (UCE):** Unsolicited E-Mails are sent in large quantities from commercial perspective, for example, advertising. See Box 5.3 to know more about US Act on Spam mails.

Examples:

1. **HSBC, Santander, CommonWealth Bank:** International Banks having large customer base, phishers always dive deep in such ocean to attempt to hook the fish.
2. **eBay:** It is a popular auction site, often mimicked to gain personal information.
3. **Amazon:** It was the top brand to be exploited by phishers till July 2009.
4. **Facebook:** Netizens, who liked to be on the most popular social networking sites such as Facebook, are always subject to threats within Facebook as well as through E-Mail. One can reduce chances of being victim of Phising attack by using the services – security settings to enable contact and E-Mail details as private.

   The E-Mail will usually ask the user to provide valuable information about himself /herself or to "verify" information that the user may have provided in the past while registering for online account. To maximize the chances that a recipient will respond, the phisher might employ any or all of the following tactics:

1. **Names of legitimate organizations:** Instead of creating a phony company from scratch, the phisher might use a legitimate company's name and incorporate the look and feel of its website (i.e., including the color scheme and graphics) into the Spam E-Mail.
2. **"From" a real employee:** Real name of an official, who actually works for the organization. This way, if a user contacts the organization to confirm whether "Rajeev Arora" truly is "Vice President of Marketing" then the user gets a positive response and feels assured.
3. **URLs that "look right":** The E-Mail might contain a URL (i.e., weblink) which seems to be original website wherein user can enter the information the phisher would like to steal.
4. **Urgent messages:** Creating a fear to trigger a response is very common in Phishing attacks – the E-Mails warn that failure to respond will result in no longer having access to the account or E-Mails might claim that organization has detected suspicious activity in the users' account or that organization is implementing new privacy software for ID theft solutions.

Here are a few examples of phrases used to entice the user to take the action.

1. "Verify your account":

2. "You have won the lottery":

3. "If you don't respond within 48 hours, your account will be closed":

Let us understand the ways to reduce the amount of Spam E-Mails we receive.

1. Share personal E-Mail address with limited people and/or on public websites – the more it is exposed to the public, the more Spam E-Mails will be received.
2. Never reply or open any Spam E-Mails.
3. Disguise the E-Mail address on public website or groups by spelling out the sign "@" and the DOT (.); for example, Rajeev**AT**gmail**DOT**com. This usually prohibits phishers to catch valid E-Mail addresses while gathering E-Mail addresses through programs.

4. Use alternate E-Mail addresses to register for any personal or shopping website. Never ever use business E-Mail addresses.
5. Do not forward any E-Mails from unknown recipients.
6. Make a habit to preview an E-Mail before opening it.
7. Never use E-Mail address as the screen name in chat groups or rooms.
8. Never respond to a Spam E-Mail asking to remove your E-Mail address from the mailing distribution list. More often it confirms to the phishers that your E-Mail address is active.

B. Hoax E-Mails (deceive or trick E-Mail)

- These are deliberate attempt to deceive or trick a user into believing or accepting that something is real, when the hoaxer (the person or group creating the hoax) knows it is false.
- Hoax E-Mails may or may not be Spam E-Mails.
- It is difficult sometimes to recognize whether an E-Mail is a “Spam” or a “hoax.”
- **The websites mentioned below** can be used to check the validity of such “hoax” E- Mails.

1. **www.breakthechain.org: T**his website contains a huge database of chain E-Mails, like we discussed, the phisher sends to entice the netizens to respond to such E-Mails.
2. **www.hoaxbusters.org:** This is an excellent website containing a large database of common Internet hoaxes. It is maintained by the Computer Incident Advisory Capability, which is a division of the US Department of Energy.

Identity Theft (ID Theft)

- This term is used to refer to fraud that involves someone pretending to be someone else to steal money or get other benefits.
- ID theft is a punishable offense under the Indian IT Act (Section 66C and Section 66D).
- The statistics on ID theft proves the severity of this fraud and hence a non-profit organization was found in the US, named as **Identity Theft Resource Center (ITRC)**, with the objective to extend the support to the society to spread awareness about this fraud.

- Federal Trade Commission (FTC) has provided the statistics about each one of the identity fraud mentioning prime frauds presented below.

1. **Credit card fraud (26%):**
2. **Bank fraud (17%):** Besides credit card fraud, cheque theft and Automatic Teller Machines (ATM) pass code theft have been reported that are possible with ID theft
3. **Employment fraud (12%):** In this fraud, the attacker borrows the victim’s valid SSN to obtain a job.
4. **Government fraud (9%):** This type of fraud includes SSN, driver license and income tax fraud.
5. **Loan fraud (5%):** It occurs when the attacker applies for a loan on the victim’s name and this can occur even if the SSN does not match the name exactly.

It is important to note the various usage of ID theft information.

1. 66% of victims’ personal information is used **to open a new credit account** in their name.
2. 28% of victims’ personal information is used **to purchase cell phone service**.
3. 12% of victims end up having **warrants issued in their name** for financial crimes committed by the identity thief.

Personally Identifiable Information (PII)

The fraudsters attempts to steal the elements mentioned below, which can express the purpose of distinguishing individual identity:

1. Full name;
2. national identification number (e.g., SSN);
3. telephone number and mobile phone number;
4. driver’s license number;
5. credit card numbers;
6. digital identity (e.g., E-Mail address, online account ID and password);
7. birth date/birth day;
8. birthplace;
9. face and fingerprints.

The information can be further classified as

a. non-classified and
b. classified.

1. **Non-classified information**
   - **Public information:**
   - **Personal information:**
   - **Routine business information:**
   - **Private information:**
2. **Classified information**
   - **Confidential:** Information that requires protection and unauthorized disclosure could damage national security (e.g., information about strength of armed forces and technical information about weapons).
   - **Secret:** Information that requires substantial protection and unauthorized disclosure could seriously damage national security (e.g., national security policy, military plans or intelligence operations).
   - **Top secret:** Information that requires the highest degree of protection and unauthorized disclosure could severely damage national security (e.g., vital defense plans and cryptologic intelligence systems).

ID theft fraudsters and/or industrial/international spies target to gain the access to private, confidential, secret and top secret information.

Types of Identity Theft

1. Financial identity theft;
2. criminal identity theft;
3. identity cloning;
4. business identity theft;
5. medical identity theft;
6. synthetic identity theft;
7. child identity theft.

Techniques of ID Theft

1. **Human-based methods:**
   - *Direct access to information:*
   - *Dumpster diving:*
   - *Theft of a purse or wallet:*
   - *Mail theft and rerouting:*
   - *Shoulder surfing:*
   - *Dishonest or mistreated employees:*
   - *Telemarketing and fake telephone calls:*
2. **Computer-based technique:**
   - *Backup theft:*
   - *Hacking, unauthorized access to systems and database theft:*
   - *Phishing:*
   - *Pharming:*
   - *Hardware:*

||Jai Sri Gurudev ||

BGSKH Education Trust (R.) – A unit of Sri Adichunchanagiri Shikshana Trust(R.)

BGS College of Engineering and Technology (BGSCET)

Mahalakshmipuram, West of Chord Road, Bengaluru-560086

(Approved by AICTE, New Delhi and Affiliated to VTU, Belagavi)

Question Bank

Subject: Introduction to Cyber Security **Class:** AI and ML/AIDS/CSD

Subject code: BETCK105I/205I **Faculty:** Mrs. Jyothi R

Course Outcomes

CO1: Interpret the cybercrime terminologies
CO2: Analyze Cyber offenses and Botnets
CO3: Illustrate Tools and Methods used on Cybercrime
CO4: Analyze Phishing and Identity Theft
CO5: Justify the need of computer forensics

Module 3: Tools and Methods used in Cybercrime: Introduction, Proxy Servers, Anonymizers, Phishing, Password Cracking, Key Loggers and Spy wares, Virus and Worms, Trozen Horses and Backdoors, Steganography, DoS and DDOS Attacks, Attacks on Wireless networks.

Sl. No.	**Questions**	**CO**	**BT**
1	Discuss the different forms of attacks through which attacker target the computer system	CO3	L2
2	Discuss the proxy server and Anonymizers in the cyber security	CO3	L2
3	List the difference between proxy server and anonymizer?	CO3	L2
4	Discuss the following: Google Cookie, Cookie, DoubleClick and G-Zapper.	CO3	L2
5	Explain the Phishing, with examples and discuss the step how it works?	CO3	L2
6	What are the different ways of password cracking?	CO3	L2
7	How can keyloggers can be used to commit a cybercrime? OR Explain the following i) Software keyloggers, ii) Hardware keyloggers, iii) Antikeylogger and Spywares	CO3	L2
8	Discuss the concept of Virus and worms. How criminals use these tools for the attack.	CO3	L2
9	Discuss the difference between virus and a worm	CO3	L2
10	Discuss the difference between Trozen Horses and Backdoors?	CO3	L2
11	Elaborate the steganography and Steganalysis? How criminals use these methods? Discuss the steganography and Cryptography	CO3	L3
12	Discuss the difference between DoS and DDoS attack	CO3	L2
13	Explain and list the classification of DoS attacks	CO3	L2
14	Discuss Types or levels of DoS attacks	CO3	L2
15	Discuss the tools used to launch DoS attack.	CO3	L2
16	Discuss the different types of mobile workers?	CO3	L2
17	what is the difference between WEP and WPA2?	CO3	L2

18	Discuss the traditional techniques of attacks on Wireless network? **	CO3	L2
19	What is the difference between WAPkitting and WAPjacking?	CO3	L2
20	How to secure the Wireless network?	CO3	L2
21	Discuss the theft Internet hours and Wi-Fi based Frauds and Misuses	CO3	L2

Module 4: Phishing and Identity Theft

Phishing and Identity Theft: Introduction, methods of phishing, phishing, phishing techniques, spear phishing, types of phishing scams, phishing toolkits and spy phishing, counter measures, Identity Theft Textbook:1 Chapter 5 (5.1. to 5.3)

Learning Objectives

- 1. Learn about Phishing and its related techniques
- 2. Understand different methods of Phishing
- 3. Get an overview about 3P's of Cybercrime
- Phishing, Pharming, Phoraging
- 4. What is spear phishing? How to avoid being victim of this ?
- 5. Overview of whaling
- 6. Learn about identity (ID) theft and understand ID theft as a major threat to businesses.
- 7. Understand "Myths and Facts" about ID theft.
- 8. Understand different types of ID thefts
- 9. Learn about different techniques of ID theft.
- 10. Understand about countermeasures for ID theft.

4.1. Introduction

- Phishing is a one of the methods towards enticing netizens to reveal their personal information that can be used for identity theft.
- ID theft involves unauthorized access to personal data.
- Section 66C of the IT Act states that "whosoever fraudulently dishonestly make use of the electronics signature, password or any unique identification features of any other person→ shall be punished with imprisonment of three years. And shall also be liable for fine which extend to one lakh rupees."
- Section 66D of the IT Act states that "whoever, by means for any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend up to three years and also liable for fine up to which extend to one lakh rupees."
- Phishing is a social engineering tactics to trick users into revealing confidential information.

Statistics about Phishing

- Phishing map available on www.avira.com
- Virtual lab monitors the evolution of E-mail Phishing across the globe.
- The graphical illustrations available on www.m86security.com

→ Monitors origin from where Phishing E-mail are sent.

→Facebook, HSBC *(Holdings plc is a British multinational universal bank and financial services holding company),* PayPal and Bank of America →targeted organization.

→US, India and China are → Targeted Countries.

3. Phishing attacks are monitored on a daily basis and displayed on www.phishtank.com

4. According to May 2009 Phishing Monthly Report compiled by Symantec Security Response Anti -Fraud Team

→ Total 3,650 non-English Phishing websites were recorded in the month of May 2009.

→ Phishing URLs are categorized based on the top-level domains (TLDs). The most used TLD in Phishing websites during the month of May 2009 were ".com, ".net and ".org" comprising 50%, 9% and 5%, respectively.

Phishing Activity Trends Report of Q4-2009 published by Anti-Phishing Working Group (APWG,) states the Phishing attack trends and statistics for the quarter. It is important to note that:

Financial organizations, payment services and auction websites are ranked as the most targeted industry.

Port 80 [HTTP] is found to be the most popular port in use followed by Port 443 [S-HTTP] and Port 8080 (WEB SERVER) among all the phishing attacks.

APWG (Anti-Phishing Working Group)

1. Explain the functions of Anti-phishing Working Group (04M)

- www. antiphishing.org, is an international consortium, founded in 2003 by David Jevans
- to bring security products and services companies, law enforcement agencies, government agencies, trade association, regional international treaty organizations and communications companies together, who are affected by Phishing attacks.
- APWG has more than 3,200+ members from more than 1,700 organizations and agencies across the globe.
- To name a few, member organizations are leading security companies such as BitDefender, Symantec, McAfee, VeriSign and IronKey.
- ING Group, VISA, Mastercard and the American Bankers Association are the members from financial industry.
- APWG is focused on eliminating identity theft that results from the growing attacks/scams of Phishing and E-Mail Spoofing.
- APWG provides a platform to discuss Phishing issues, define the scope Phishing problem in terms of costs and share information about best practices to these attacks/scams.

a).What is Phishing? Explain with examples.
b). Define the term Phishing with respect to Wikipedia, Webopedia and TechEncyclopedia.

4.2 Phishing

Wikipedia:

- It is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication

Webopedia:

- It is an act of sending an E-Mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for ID theft.
- The E-Mail directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security and bank account numbers that the legitimate organization already has.
- The website, however, is bogus and set up only to steal the user's information

Tech Encyclopedia: It is a scam to steal valuable information such as credit card and social security numbers (SSN), user IDs and passwords.

- It is also known as "brand Spoofing."
- An official-looking E-Mail is sent to potential victims pretending to be from their bank or retail establishment.
- E-Mails can be sent to people on selected lists or any list, expecting that some percentage of recipients will actually have an account with the organization.
- Is a type of deception designed to steal your identity.
- Here the phisher tries to get the user to disclose the personal information→ such as credit card numbers, passwords, account data or other information's.
- Email is the popular medium of Phishing attack and such E-Mails are also called as Spams; however not all E-mails are spam E-Mails.
- Types of E-Mails → Spam E-Mails and hoax E-Mails

Spam E-Mails and hoax E-Mails

- Spam E-Mails → Junk E-Mails
- Identical messages sent to numerous recipients.
- Grown since 1990, → Botnet network of virus infected computers are used to send 80% of spam emails.
- Types→ 1. **Unsolicited bulk E-Mails (UBE)**→ email sent to large quantities

  2. **Unsolicited Commercial E-Mail (UCE)**→ for commercial purpose such as advertising.

SPAMBOTS (UBE)

- Automated computer program and/or a script developed, mostly into "C" programing language to send Spam mails.

- SPAMBOTS gather the E-Mail addresses from the internet to build mailing list to send UE.
- These are called as web crawlers, as they gather E-mail addresses from numerous websites, chatroom conversations, newsgroups and special interest group (SIG) postings.
- → It scans for two things a) hyperlinks b) E-Mail addresses.
- The term SPAMBOT is also sometimes Used with reference to a program designed to prevent spam to reach the subscribers of an Internet service provider (ISP).
- Such programs are called E-Mail blockers and/or filters.

CAN-SPAM Act

- The CAN-SPAM Act of 2003 (15 U.S.C. 7701, et seq., Public Law No. 108-187, was S.877 of the 108th US Congress).
- United States' first national standards for the sending of commercial E-Mail and requires the Federal Trade Commission (FTC) to enforce its provisions.
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003.
- The CAN-SPAM Act is commonly referred to as the "You-Can-Spam" Act because the bill explicitly legalizes most E-Mail Spam.
- In particular, it does not require E-Mailers to get permission before they send marketing messages.
- It also prevents states from enacting stronger anti-Spam protections, and prohibits individuals who receive Spam from suing spammers.

a). Differentiate between Spam and Hoax mails

Spam E-Mails popular medium of Phishers to scam users

- 1. **HSBC, Santander, Common Wealth Bank**→ International bank having large customer base, phishers dive deep in such ocean to attempt to hook the fish.
- 2. **eBay**→ auction site often mimicked to gain personal information
- 3. **Amazon** →I t was the top brand to be exploited by phishers till July 2009.
- 4. **Facebook** → Netizens, who liked to be on the most popular social networking sites such as Facebook, are always subject to threats within Facebook as well as through E-Mails.

Tactics used by Phishers to attack the common people using E-Mails asking for valuable information about himself/herself or to verify the details

- 1. **Names of legitimate organizations:**

Instead of creating a phony company from scratch, the phisher micht use a legitimate company's name and incorporate the look and feel of its website (i.e., including the color scheme and graphics) into the Spam E-Mail.

2. **From a real employee:**
   Real name of an official, who actually works for the organization, will appear in the "from" line or the text of the message (or both). This way, if a user contacts the organization to confirm whether "Rajeev Arora" truly is "Vice President of Marketing" then the user gets a positive response and feels assured.

-

- **3. URLs that look right:**
- The E-Mail might contain a URL (i.e., weblink) which seems to be legitimate website wherein user can enter the information the phisher would like to steal.
- However, in reality the website will be a quickly cobbled copycat -a spoofed" website that looks like the real thing, that is, legitimate website. In some cases, the link might lead to selected pages of a legitimate website- such as the real company's actual privacy policy or legal disclaimer.
- **4. Urgent messages:**
- Creating a fear to trigger a response is very common in Phishing attacks – the E-Mails warn that failure to respond will result in no longer having access to the account or E-Mails might claim that organization has detected suspicious activity in the users' account or that organization is implementing new privacy software for ID theft solutions.

<u>Here are a few examples of phrases used to entice the user to take the action.</u>

- **1. Verity your account:**
- The organization will never ask the user to send passwords, login names, permanent account numbers (PANs) or SSNs and other personal information through E-Mail.
- For example, if you receive an E-Mail message from Microsoft asking you to update your credit card Information, do not respond without any confirmation with Microsoft authorities- this is a perfect example of Phishing attack.
- **2. You have won the lottery:**
- The lottery scam is a common Phishing scam known as advanced fee fraud. One of the most common forms of advanced fee fraud is a message that claims that you have won a large sum of money, or that a person will pay you a large sum of money for little or no work your part.
- The lottery scam often includes references to big companies, for example, Microsoft.
- There is no Microsoft lottery. It is observed that most of the phished E-Mails display the agencies/companies situated in Great Britain and hence it is extremely important for netizens to confirm/verify the authenticity of such E-Mails before sending any response.
  If " any-Mail is received displaying "You have won the lottery in Great Britain," confirm it on www.gamblingcommission.gov.uk
- If any E-Mail is received displaying your selection for any job into Great Britain, confirm/verify the details of the organization on www.companieshouse.gov.uk or on http://www.upmystreet. com/local/uk.html

- **3. If you don't respond within 48 hours, your account will be closed**
- These messages convey a sense of urgency so that you will respond immediately without thinking. A Phishing E-Mail message might even claim that your response is required because your account might have been compromised

Let us understand the ways to reduce the amount of Spam E-Mails we receive

- 1. Share personal Email address with limited people and/or on public websites-the more exposed to the public, the more Spam E-Mails will be received.
- 2. Never reply or open any Spam E-Mails. Any spam E-Mails that are opened or replied to inform the phishers not only about your existence but also about validity of your E-Mail address.
- 3. Disguise the E-Mail address on public website or groups by spelling out the sign "@" and the DOT for example, RajeevATgmailDOTcom. This usually prohibits

phishers to catch valid E-Mail addresses while gathering E-Mail addresses through programs.

- 4Use alternate E-Mail addresses to register for any personal or shopping website. Never ever use business E-Mail addresses for these sites but rather use E-mail addresses that are free from Yahoo, Hotmail or Gmail.
- 5. Do not forward any E-Mails from unknown recipients.
- 6.Make a habit to preview an E-Mail (an option available in an E-Mail program) before opening it.
- 7. Never use E-Mail address as the screen name in chat groups or rooms.
- 8. Never respond to a Spam E-Mail asking to remove your E-Mail address from the mailing distribution list. More often it confirms to the phishers that your E-Mail address is active.

Hoax Mails

- These are deliberate attempt to deceive or trick a user into believing or accepting that something 1s real. when the hoaxer (the person or group creating the hoax) knows it is false.
- Hoax E-Mails may or may not be Spam E-Mails.
- www.breakthechain.org: This website contains a huge database of chain E-Mails.
- www.hoaxbusters.org: excellent website containing a large database of common Internet hoaxes.
- It contains information about all the scams.
- I maintained by Computer Incident Advisory Capability, Which is the division of US department of energy. Eg., "Breaking news"→ Info→" Barack Obama refused to be the president of the US → E-mail Signature as CNN

4.2.1 Methods of Phishing,

Explain four types of methods used by the phishers to reveal personal information on Internet

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

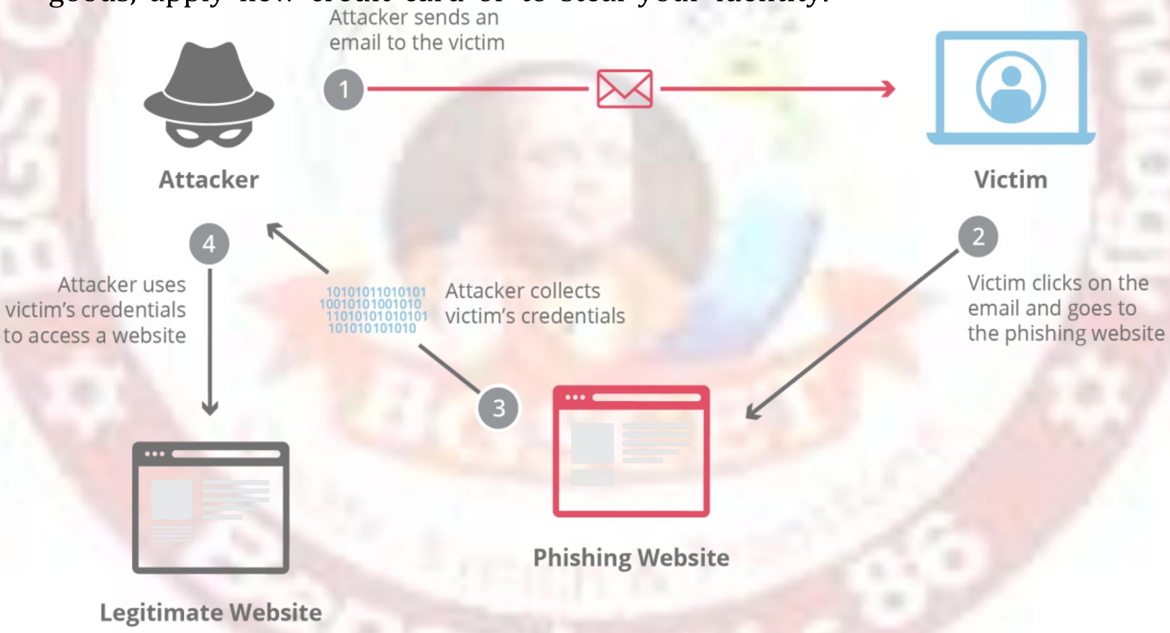
1. Dragnet

- A method involves the use of spammed E-Mails, bearing falsified corporate identification (ne.., corporate names, logos and Customers of trademarks), which are addressed to a large group of people (a particular financial institution or members of a particular auction site) to web- sites or pop-up windows with Similarly falsified identification.
- Dragnet phishers do not identify specific prospective victims in advance.
- Instead, they rely on false information included in an E-Mail to trigger an immediate response by victims-typically, clicking on links in the body of the E-Mail to take the victims to the websites or pop- up windows where they are requested to enter bank or credit card account data or other personal data.

2. Road-and-reel

- In this method, phishers identify specific prospective victims in advance, and convey false information to them to prompt their disclosure of personal and financial data.
- For example, on the phony webpage, availability of similar item for a better price (i.e., cheaper price) is displayed which the victims may be searching for and upon visiting the webpage, victims were asked for personal information such as name, bank account numbers and passwords, before confirming that the "sale" and the information is available to the phisher easily.

- **3. Lobsterpot**
- This method focuses upon use of spoofed websites.
- It consists of creating of bogus/ phony websites, similar to legitimate corporate ones, targeting a narrowly defined class of victims, which is likely to seek out.
- These attacks are also known as "content injection Phishing."
- Here the phisher places a weblink into an E-Mail message to make it look more legitimate and actually takes the victim to a phony scam site, which appears as legitimate website similar to official site. These fake sites are spoofed websites.
- Ones the netizens is into the one of these spoofed sites, he/she might willingly send personal information to the con artist. Then they use your information to purchase goods, apply new credit card or to steal your identity.


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
101010110101010 1001010101001010 11010101010101 1010101010 10
Attacker collects victim's credentials
3
Phishing Website
Legitimate Website

4. Gillnet

- This technique relies far less on social engineering techniques and phishers introduce Malicious Code into E-Mails and websites.
- They can, for example, misuse browser functionality by injecting hostile content into another site's pop-up window.
- Merely by opening a particular E-Mail or browsing a particular website, netizens may have a Trojan Horse introduced into their systems.
- In some cases, the Malicious Code will change settings in user's systems so that users who want to visit legitimate banking websites will be redirected to a look-alike Phishing site.

- In other cases, the malicious code will record user's keystrokes and passwords when they visit legitimate banking sites, then they transmit those data to phisher for later illegal access to user's financial accounts.

Box 1:

Explain the following attack against the legitimate website.
a) Website Spoofing
b) XSS-Cross site Scripting
c) XSRF- Cross scripting Request Forgery

Website Spoofing (attack launched on legitimate Webpage)

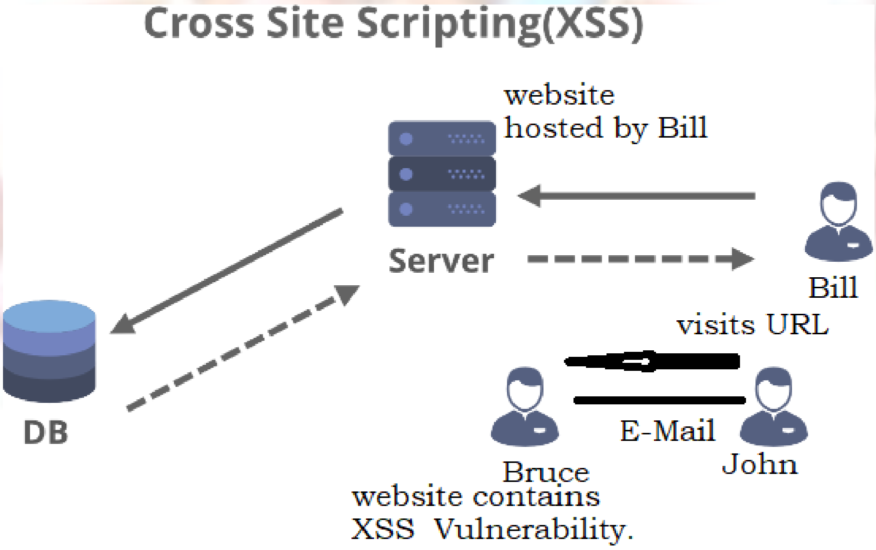
It is an act of creating a website, as a hoax, with the intention of misleading readers that the website has been created by a different person or organization.

Normally, the website will adopt the design of the target website and it sometimes has a similar URL.

XSS (Cross Site Scripting) (attack launched on legitimate Webpage)

Cross-site scripting (XSS): XSS is a type of computer security vulnerability typically found in web applications that enable malicious attacker to inject client-side script into webpage viewed by other users.

An exploited cross-site scripting vulnerability can be Used by attackers to bypass access controls Such as the same origin policy.



XSRF Cross-site request forgery (attack launched on legitimate Webpage)

CSRF is also known as a one-click attack or session riding (abbreviated as CSRF or XSRF) and is a type of malicious exploit of a website where by unauthorized commands are transmitted from a user that the website trusts.

Unlike cross-site scripting (XSS), which exploits the trust a user has on a particular site, CSRF exploits the trust that a site has in a user's browser.

Phishing vis-à-vis Spoofing

- 1. Phishing is used to get the victim to reveal valuable (or at times invaluable) information about him/her. Phishers would use Spoofing to create a fake E-Mail.
- 2. Spoofing is not intended to steal information but to actually make the victim do something for phishers.
- 3. Phishing may, at times, require Spoofing to entice the victim into revealing the information about Spoofing does not always necessarily result in Phishing someone else's account

The Combined Attack - Phishing and Spoofing

- Phisher sends an E-Mail, during Income Tax return fling period, from an official looking IT (Income Tax) account which is spoofed.
- The E-Mail would contain URL to download a new tax form that was recently issued.
- Once the victim clicks the URL a "virus cum Trojan Horse" is downloaded to the victim's system.
- The IT Form may seem official, but like a Trojan Horse, the payload has already been delivered.
- The virus lies in wait, logging the actions of the victim.
- Once the victim inputs certain keywords, like bank names, credit card names, social networking websites and so forth, it logs the site and the passwords used.
- Those results are flagged and sent to the phisher.
- The virus could then gather the user's E-Mail contacts and send a fake E-Mail to them as well, containing the virus.
- The phisher now has gained the required personal information as well as virus was sent, downloaded and spread to entice other netizens.

4.2.2. Phishing Techniques [UFWFSP]

Discuss the various techniques used by Phishers to launch Phishing attacks
OR
Discuss the different Phishing techniques?

- 1. URL (weblink) Manipulation
- 2. Filter Evasion
- 3. Website Forgery
- 4. Flash Phishing
- 5. Social Phishing
- 6. Phone Phishing

1. URL (weblink) manipulation

- URLs are the weblinks (i.e., Internet addresses) that direct the netizens/users to a specific website.
- In Phishing attack, these URLs are usually supplied as misspelled, for example, instead of www.abcbank.com, URL is provided as www.abcbank1.com.
- Phishers use Lobsterpot method of Phishing and make the difference of one or two letters in the URLs, which is ignored by netizens.
- This makes a big difference and it directs users to a fake/bogus website or a webpage.

Homograph Attack

- It is used by Phisher to attack on Internationalized Domain Name (IDN) to deceive the netizens by redirecting them on the phony website which look like the original website.
- ASCII has several characters and/or pairs of characters which look alike,
- Eg. 0 and “O”. “l” (L lower case) and I(“i” alphabet in uppercase) [GOOGLE.COM can be registered as G00GLE.COM]
- Microsoft.com or/rnicrosoft.com
- Phisher could create and register a domain name which appears almost identical to an existing domain and takes netizens to the Phony websites.
- Phisher could easily record password or account details though spoofed websites, while passing traffic through the original websites.

2. Filter Evasion

- This technique use graphics (i.e., images) instead of text to obviate from netting such E-Mails by anti-Phishing filters. Normally, these filters are inbuilt into the web browsers. For example,
- Internet Explorer version 7 has inbuilt "Microsoft phishing filter." One can enable it during the installation or it can be enabled post-installation. It is important to note that it is not enabled by default.
- Firefox 2.0 and above has inbuilt "Google Phishing filter." duly licensed from Google. It is enabled by default.
- The Opera Phishing filter is dubbed Opera Fraud Protection and is included in version 9.5+.

3. Website forgery

- In this technique the phisher directs the netizens to the website designed and developed by him, to login into the website, by altering the browser address bar through JavaScript commands.
- As the netizen logs into the fake/bogus website, phisher gets the confidential information very easily.
- Another technique used is known as "cloaked" URL-domain forwarding and/or inserting control characters into the URL while concealing the weblink address of the real website.

4. Flash Phishing

- Anti-Phishing toolbars are installed/enabled to help checking the webpage content for signs of Phishing, but have limitations that they do not analyse flash objects at all.
- Phishers use it to emulate the legitimate website.
- Netizens believe that the website is "clean" and is a real website because anti-Phishing toolbar is unable to detect it.

5. Social Phishing

- Phishers entice the netizens to reveal sensitive data by other means and it works in a systematic manner.
- Phisher sends a mail as if it is sent by a bank asking to call them back because there was a security breach.
- The victim calls the bank on the phone numbers displayed in the mail.
- The phone number provided in the mail is a false number and the victim gets redirected to the phisher.
- Phisher speaks with the victim in the similar fashion/style as a bank employee, asking to verify that the victim is the customer of the bank. For example, "Sir, we need to make sure that you are indeed our customer. Could you please supply your credit card information so that I can verify your identity".
- Phisher gets the required details swimmingly.

6. Phone Phishing

- Phisher can use a fake caller ID data to make it appear that the call is received from a trusted organization to entice the users to reveal their personal information such as account numbers and passwords.
- Mishing- Mobile Phishing attacks (Vishing and Smishing)

Innovative Phishing Attack Launched through Android Market

- Android: It is an open-source operating system (OS) for mobile phones and is based on Linux Kernel.
- Its popular due to the release of Google's Nexus One Phone.
- Its Market is as popular as iPhone App Store. →22,000 applications available
- https://news.spoftpedia.co → a malware writer succeeded to list a rogue Phishing application called 09Droid on the Android Market website.
- It found shell for mobile application, but later came to know that its being used to steal Online Banking credentials.
- Travsi Credit Union (TCU) issued an alert to all consumers regarding this malware injection through 09Droid.→Application was stealing financial information of consumers.

4.2.3 Spear Phishing

What is spear Phishing? Explain with examples.
OR
What is Whaling? Explain the difference between Whaling and Spear Phishing.

- It is method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering.

- 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 like 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.
- Unfortunately, through the modus operandi of the Spear phishers, the E-Mail sender information has been faked or spoofed.
- While traditional Phishing scams are designed to steal information from individuals, Spear Phishing scams work to gain access to a company's entire computer system.
- It you respond with a username or password, or if you click on the links or open the attachments in a Spear Phishing E-Mail, pop-up window or website, then you might become a victim of ID theft and you might put your employer or group at risk.
- Spear Phishing also describes scams that target people who use a certain product or website.
- Scam artists use any information they can to personalize a Phishing scam to as specific a group as possible.
- Thus, "Spear Phishing is a targeted E-Mail attack that a scammer sends only to people within a small group, such as a company".
- The E-Mail message might appear to be genuine, but if you respond to it, you might put yourself and your employer at risk.
- You can help avoiding Spear Phishing scams by using some of the same techniques you have already used to help avoid standard Phishing scams

Whaling

- It is a Specific from of Phishing and/or Spear Phishing.
- Targeting executives from the top management in the organizations, in private companies.
- The objective is to swindle the executive into revealing confidential information.
- E-Mails sent here are designed to masquerade as a critical business E-Mail sent from a legitimate business authority.
- It has falsified industry wide concern and is meant to be tailored for executives.
- Whaling Phisher have forged official looking FBI subpoena E-mails. And claimed that manager needs to click a link and install special software to view subpoena.
- In 2008 FBI 20,000 corporate CEO were attacked. More than 2000 people clicked on the whaling link. Linked software was a keylogger that secretly recorded the CEO passwords and forwarded those passwords to the Phisher men.

Avoiding Spear Phishing Scams

1. Never reveal personal or financial information in a response to an E-Mail request, no matter who appears to have sent it.
2. If you receive an E-Mail message that appears suspicious, call the person or organization listed in the From line before you respond or open any attached files.
3. Never click links in an E-Mail message that requests personal or financial information. Enter the web address into your browser window instead
4. Report any E-Mail that you suspect might be a Spear Phishing campaign within your company.
5. You can use the phisher filter-it scans and helps identify suspicious websites, and provides up-to the hour updates and report about known phishing sites.

4.2.4. Types of Phishing Scams

Explain the different types of Phishing scams.
OR
Discuss various types of Phishing Scams. (10M)

1. **Deceptive Phishing→**
    - Phishing scams started by broadcasting deceptive E-Mail messages with objective of ID theft.
    - E-Mails are broadcasted to a wide group of netizens asking about the need to verify banking account information/system failure requiring users to re-enter their personal information.
    - The netizens easily get enticed and reveal their information by responding to these E-Mails and/or clicking on weblinks or signing onto a fake website designed by the phisher.
2. **Malware-based Phishing→**
    - It refers to scams that involve running Malicious Code on the netizens system.
    - Malware can be launched as an E-Mail attachment or as a downloadable file from a website or by exploiting known security vulnerabilities.
    - For example, small and medium businesses are always found to be ignorant to keep their operating systems (OS) antivirus software up to date with latest patch updates released by vendors.
3. **Keyloggers→**
    - A small integrity program to steal information sends to phisher, keylogger log, to the phisher through the Internet.
    - The keyloggers can also be embedded into netizen's browser as a small utility program which can start automatically when the browser is opened or can be embedded into system holes as device drivers.
4. **Session hijacking →**
    - It is an attack in which netizens' activities are monitored until they establish their bonafide credentials by signing into their account or begin the transaction and at that point the Malicious Code takes over and comport unauthorized actions such as *transferring funds without netizen's knowledge*.
5. **In-session Phishing→** another parallel session in the same browser.:
    - It is a Phishing attack based upon one web browsing session being able to detect the presence of another session (such as visit to an online banking website) on the same web browser and then a pop-up window is launched that pretends to be opened from the targeted session
6. **Web Trojans→**
    - Pops up to collect netizen's credentials and transmit them to the phisher while netizens are attempting to log in. Such pop-ups are usually invisible
7. **Pharming→** I
    - It is a new threat evolved with a goal to steal online identity of the netizens and Pharming
    - Is known as one of the "P" in cybercrime
    - In Pharming, following two techniques are used:
    - **Hosts file poisoning:**
    - The most popular operating system (OS) in the world is Windows and It has "host names" in their "hosts" file.

- A simple text file was used in web address during early days of the Internet. (before DNS)
- Phisher used to "poison" the host file to redirect the netizen to a fake/bogus Website, designed and developed by the phisher, which will "look alike the original website, to Steal the netizen's personal information easily.
- **DNS-based Phishing:**
- Phisher tampers with a DNS so that requests for URLs or name service return a fake address and subsequently netizens are directed to a fake site.
- Netizens usually are unaware that they are entering their personal confidential information in a website controlled by phishers and probably not even in the same country as the legitimate website.
- DNS-based Phishing is also known as DNS hijacking.
- Along with this attack Click Fraud is an advanced form of technique evolved to conduct Phishing scams.

8. **System configuration attacks:**
    - Phisher intrude into netizens system to modify settings for malicious purposes.
    - For example, URLs saved under favourites in the browser De modified to redirect the netizen to a fake/bogus "look alike" websites (i.e., URL for a of a bank can be changed from "www.xyzbank.com to www.xyzbanc.com.).
9. **Data theft →**
    - Critical and confidential data getting stolen is one of the biggest concerns in the modern times.
    - As more information resides on the corporate a servers and the web attackers have a boom time because taking away/copying information in electronic form is easy.
    - Unsecured systems are often found to be inappropriately maintained from cybersecurity perspective.
    - When such system is connected, the web servers can launch an attack with numerous methods and techniques. Data theft is used in business espionage.

10. **Content injection Phishing**:

    - In these types of scams, phisher replaces the part of the content of a legitimate website with false content.

11. **Man-in-the middle Phishing:**

    - Phisher is positioned himself in between the netizens and legitimate website or system.
    - Phisher records the input being provided by the netizen but continues to pass it on to the web server so that netizens transactions are nor affected.

12. **Search engine Phishing:**
    - It occurs when phishers create websites with attractive sounding offers (often found too good to be true) and have them indexed legitimately with search engines.
    - Netizens find websites during their normal course of search for products or services and are trapped to reveal their personal information.
    - For example, phishers set up fake/ bogus banking websites displaying an offer of lower credit costs or better interest rates than other banks offer of lower credit costs or better interest rates than other banks.

13. SSL certificate Phishing:

- Phishing is an advanced type of scam. Phishers target web servers with SSL certificates to create a duplicitous website with fraudulent webpages displaying familiar "lock" icon.
- It is important to note that, in such types of scams, SSL certificates are always found to be legitimate as they match the URL of the fake pages that are mimicking the target brands but in reality, had no connection to these brands displayed.
- It is difficult to recognize such websites; however, smart netizens can detect such deception after reviewing the certificate and/or whether the website has been secured with an extended validation SSL certificate.

Three P's of Cybercrime -Phishing, Pharming & Phoraging

- **Pharming:** It is an attack aiming to redirect a website traffic to another bogus websites.
- Pharming is a neologism based on farming + Phishing.
- Concern for businesses hosting E-Commerce and Online banking websites.
- Here attacker cracks vulnerability in an ISP, DNS server and hijacks the domain name of a commercial site.
- **Phoraging:** It is defined as a process of collecting data from many different online sources to build up the identity of someone with the ultimate aim of committing the identity theft.
- It is information diving-searching for information.
- Now a days looking for matrimonial sites, social networking sites for professional to reveal personal information.
- **Advanced Form of Phishing- Tabnapping or Tabjacking**
- Tabs are web browser tabs.
- Browser Tabs that are not in use are called as napping.
- Most often netizens work with multiple tabs, open with multiple web browsing sessions on each one. Its takes hour together time.
- Phishers have identified a way to invade the browser tabs and change it to a page designed to steal information.
- If a page is ideal for a particular time period, and then phisher redirects the victim to a phished webpage.
- Phisher judge the idle webpages based on mouse movement, scroll bar movement and keystrokes.
- Websites from banking/financial institutes as well as popular sites like Gmail, Facebook, Instagram, WhatsApp are the primary targets.

DNS Hijacking (session hijacking)

- **DNS Hijacking:** It is also known as DNS redirection and it is the practice of redirecting the resolution of Domain Name Server (DNS) names to rogue DNS servers.
- An illegal change to a DNS server directs URL to a different website.
- In some cases, new websites URL may have done one different letter in the name that might go unnoticed. The bogus website might offer similar and/or competing products for sale.
- DNS is used to interpret domain names such as www. <domainname>.com into an IP address. The IP address consists of numbers such as xxx.xx.xxx.x (192.60.168.1) that give a domain a unique identification

- It is used by attacker with malicious intent who redirect or hijack the DNS addresses to bogus DNS servers for the purpose of injecting malware into your PC, Promoting Phishing scams, advertising on high traffic website and other criminal related activity.
- DNS hijacker use Trojan to exchange the legitimate DNS server assignment by the ISP with a manual DNS server assignment from a bogus DNS server.
- When netizens visit the reputable websites with legitimate domain names, they are automatically hijacked to a malicious website that is disguised as the legitimate one.
- Switch from the legitimate DNS server to bogus DNS server goes unnoticed by both the netizens and the legitimate website owner.
- This opens up the malicious website to perform any criminal act that the phisher wishes because the netizens thinks that they are in the real website.

Click Fraud (session hijacking)

- It is a type of Internet crime that occurs in pay-per-click online advertising when a person automated script or computer program imitates a legitimate user of a web browser clicking on an advertisement (ad) for the purpose of generating a charge per click without having actual interest in the target of the ad's link.
- Click Fraud is the subject of some controversy and increasing litigation because of the advertising networks being a key beneficiary of the fraud.
- It is an illegal practice that occurs when individuals click on a website click through advertisements to increase the payable number of clicks.
- Illegal click can be performed by clicking the Advertising hyperlinks or by using automated software or online Bots that are programmed to click these banner ads and pay per click text ad links.
- Research has indicated that Click Fraud is perpetrated by individuals who use Click Fraud to increase their own personal banner ad revenues and also by companies who use Click Fraud as a way to deplete a competitor's advertising budget.
- Visit the weblinks mentioned below to explore more on Click Fraud:
- 1. Exposing Click Fraud: http://news.cnet.com/Exposing-click-fraud/2100-1024_3-5273078
- 2.The dark side of online advertising. http://www.businessweek.com/magazine/content/06_40/b4003001.html

SEO (Search Engine Optimization) Attacks Beware While Searching through Search Engines

- SEO is the practice of maximizing the volume or quality of traffic to a website from search engines Techniques used for Black hat SEO attacks
- Techniques used for Black hat SEO attacks

1. Fake antivirus
2. SEO page
3. SEO poisoning
4. Black hat SEO kits

Distributed Phishing Attack (DPA)

- It is an advanced form of Phishing attack that works as per victim's personalization of the location of sites collecting credentials and a covert transmission of credential to a hidden coordination centre run by the phisher.
- Here a large number of fraudulent web hosts are used for each set of lured E-Mails.

4.2.5 Phishing toolkits and Spy phishing

Explain Phishing Toolkits with examples.

A Phishing toolkit is a set of scripts/programs that allows a phisher to automatically set up Phishing websites that spoof the legitimate websites of different brands including the graphics displayed on these websites.

These developed by individual or groups and sold for money.

Phisher use hypertext pre-processor (PHP) to develop the phishing kits.

These are Do-It Yourself Phishing kits-information sent to recipients other than the authors of Phishing kits) other than the intended users.

Distributed Phishing Attack (DPA)

- It is an advanced form of Phishing attack that works as per victim's personalization of the location of sites collecting credentials and a covert transmission of credential to a hidden coordination centre run by the phisher.
- Here a large number of fraudulent web hosts are used for each set of lured E-Mails.

4.2.5 Phishing toolkits and Spy phishing

- A Phishing toolkit is a set of scripts/programs that allows a phisher to automatically set up Phishing websites that spoof the legitimate websites of different brands including the graphics displayed on these websites.
- These developed by individual or groups and sold for money.
- Phisher use hypertext pre-processor (PHP) to develop the phishing kits.
- These are Do-It Yourself Phishing kits-information sent to recipients other than the authors of Phishing kits) other than the intended users.
- Rock Phish: It is a Phishing toolkit popular in the hacking community since 2005. It allows non-techies to launch Phishing attacks.
- The kit allows a single website with multiple DNS name to host a variety of phished webpages, covering numerous organizations and institutes
- Xrenoder Traojan Spyware: It resets the homepage and/or the search settings to point to other websites usually for commercial purposes or porn traffic.
- Cpanel Google: It is a Trojan Spyware that modifies the DNS entry in the host's file to point to its own website.
- If Google gets redirected to its website, a netizen may end up having a version of a website prepared by the phisher.

4.2.6 Phishing countermeasures

What are countermeasures to prevent malicious attacks. (06M)

1. The countermeasures will prevent malicious attacks that phisher may target to gain the unauthorized access to the system to steal the relevant personal information about the victim, from the system.
2. It is always challenging to recognize/Judge the legitimacy of a website while Googling (i.e., surfing on the Internet) and find it more intriguing while downloading any attachment from that particular website.

3. explained in Table 4.1
4. Table 4.1 How to avoid being victim of Phishing attack

SL. NO.	Security Measures
1	Keep antivirus up to date
2	Do not click on hyperlinks in E-Mails
3	Take advantage of anti-Spam software
4	Verify https (SSL)[secure Socket layer]
	Use anti-Spyware software
6	Get educated
7	Use the Microsoft Baseline Security Analyzer (MBSA)
8	Firewall
9	Use backup system images
10	Do not enter sensitive or financial information into pop-up windows
11	Secure the hosts file
12	Protect against DNS Pharming attacks

How to Judge/Recognize Legitimate Websites

- ScanSafe (www.scansafe.com) was the first company in the world to after web security. Scandoo (www.Scandoo.com) scans all search results’ to protect the user from visiting false websites (i.e., websites that spread malicious viruses or Spyware as well as protecting the user from viewing offensive content).
- Presently this Site is nor available as improvements for add-on features based on users' feedback is underway.
- MCAfee Site Advisor software (www.siteddvisor.com) is a free web security plug-in that provides the user with red, yellow and green website security ratings based on the search results.
- These ratings are based on tests conducted by McAfee after looking for all kinds of threats such as to name a few Phishing sites, E-Commerce vulnerabilities, browser exploits, etc.

SPS (Sanitizing Proxy System) Algorithm to Thwart Phishing Attacks

- Phishing attack comprised two phases: a) attraction and b) acquisition
- Characteristics of SPS:

1. Two-level filtering
2. Flexibility of the rule set

3. Simplicity of the filtering algorithm
4. Accountability of HTTP response sanitizing
5. Robustness against both misbehavior of novice users and evasion techniques

Explain the flowchart of Phishing attacks.

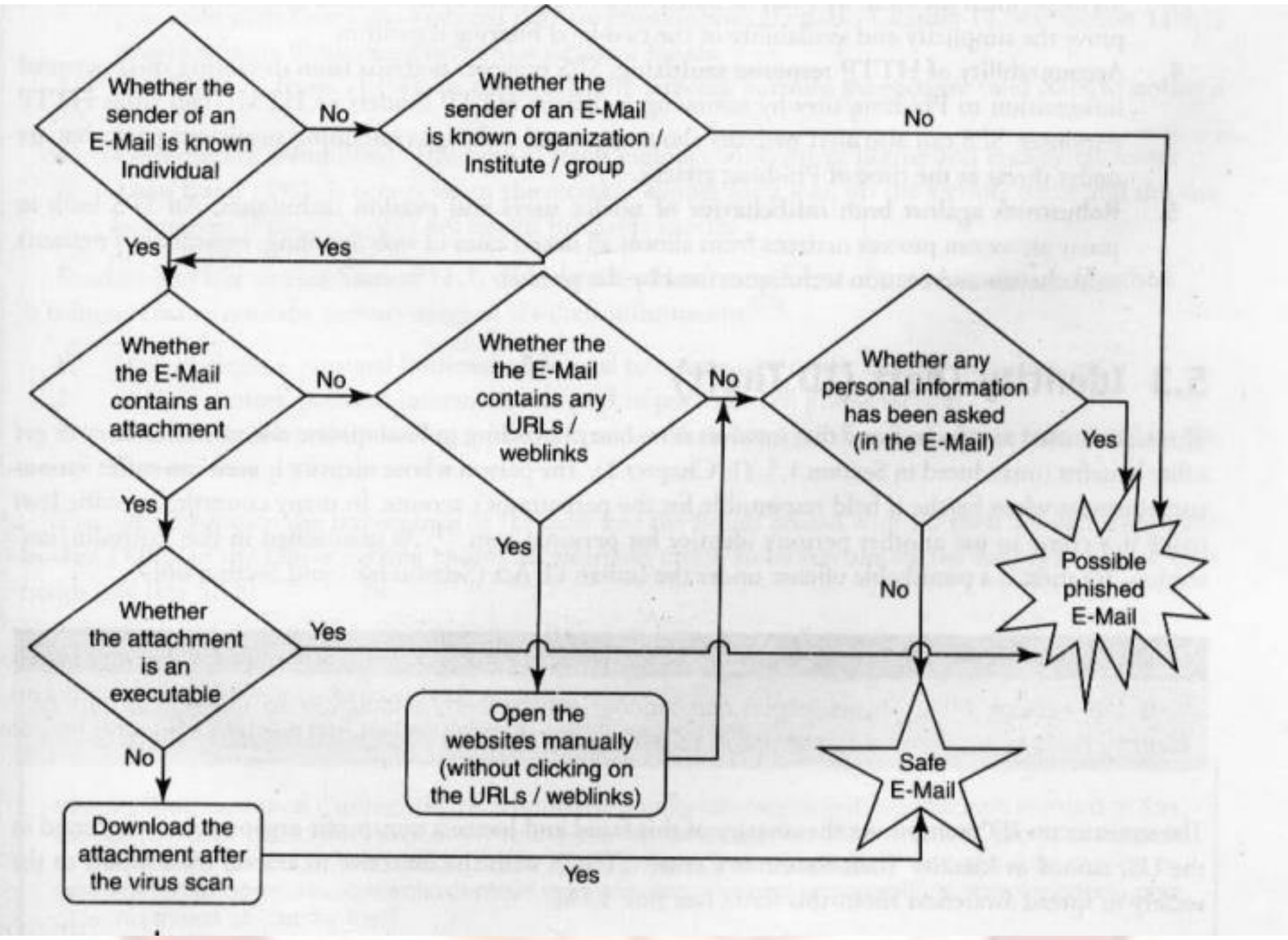

Whether the sender of an E-Mail is known Individual
No
Whether the sender of an E-Mail is known organization / Institute / group
No
Yes
Yes
Whether the E-Mail contains an attachment
No
Whether the the E-Mail contains any URLs / weblinks
No
Whether any personal information has been asked (in the E-Mail)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

Fig: Phishing Attack flow chart

4.3 Identity Theft

What is identity theft? Explain with examples. (08M)
How can information be classified? (06M)
What are the different techniques of Identity theft?(08M)

- It happens when someone uses your personally identifying information. Like your name, social security number, or credit card number, without your permission to commit fraud or other crimes.

- OR
- This term is used to refer to fraud that involves someone pretending to be someone else to steal money or get other benefits.
- ID theft is a punishable offense under the Indian IT Act (Section 66C and Section 60D)
- The statistics on ID theft proves the severity of this fraud and hence a non-profit organization was found in the US, named as Identity Theft Resource Center (ITRC), with the objective to extend the society to spread awareness about this fraud

FTC→ Mentioned the Prime Frauds

- Credit card fraud (26%): The highest rated fraud that can occur is when someone acquires the victims credit card number and uses it to make a purchase.
- Bank fraud (17%): Besides credit card fraud, cheque theft and Automatic Teller Machines (ATM) pass code theft have been reported that are possible with ID theft.
- Employment fraud (12%): In this fraud, the attacker borrows the victim's valid SSN to obtain a
- job.
- Government fraud (9%): This type of fraud includes SSN, driver license and income tax fraud.
- Loan fraud (5%): It occurs when the attacker applies for a loan on the victim's name and this can
- Occur even if the SSN does not match the name exactly.

Identity Theft Information

- 66% of victim's personal information is used to open a new credit account in their name.
- 28% of victim's personal information is used to purchase cell phone service.
- 12% of victims end up having warrants issued in their name for financial crimes committed by the identity thief.

Identity Theft Resource Center (ITRC)

- Identity Theft Resource Center (ITRC) is a non-profit, nationally respected organization situated at San Diego, CA USA dedicated exclusively to the prevention of identity theft.
- The ITRC provides support to the society for public education about identity theft.
- The organization also provides advice to governmental agencies, law enforcement agencies and business organizations about evolving and growing threat of identity theft.

Myth	Fact
There's no way to protect yourself from identity theft	The risk of identity theft can be minimized by taking preventive measures.
Identity theft is only a financial crime	Other identity theft also available and are dangerous, medical ID theft of Personal medical record, for false insurance claims.
It's my bank's fault if I become a victim of identity theft	Majority identity theft begins elsewhere, PI may be stolen from lost or stolen wallet, check book, credit or debit card (low tech tool) High tech tool, hacking, Phishing, skimming)
It is safe to give your personal information over the phone if your caller ID confirms that it is your bank	Caller ID Spoofing can be done, don't give any information to any one.
Checking your credit report periodically or using a credit monitoring service is all you need to do to protect yourself from identity theft.	One can get free credit report in the US from each of the credit bureaus from www.AnnualCreditReport.com
My personal contact information (mailing address, telephone number, E-Mail address, etc.) is not valuable to an identity thief.	Any information that could be used by a thief to impersonate you should be protected.
Shredding my mail and other personal documents will keep me safe.	Shredding documents that contain personal information before you throw them away is a great way to protect yourself from "dumpster diving," which occurs when attackers search the trash for personal information.
I don't use the Internet, so my personal information is not exposed online.	Your personal information appears in more places than you might realize whether its your medical records, a job application or a school emergency contact form. Many of these records are kept in electronic databases and transmitted online.
Social networking is safe.	They can be dangerous when it comes to your identity..

	privacy controls offered by most of these sites, and use common sense.
It is not safe to shop or bank online	Like social networking, shopping and banking online are safe as long as you use common sense and make good choices about where and how you do it. Observe the webpage is legitimate.

4.3.1. Personally Identifiable Information (PII)

The fraudster always has an eye on the information which can be used to uniquely identify, contact or locate a single person or can be used with other sources to uniquely identity a single individual. PII has four common variants based on personal, personally, identifiable and identifying.

The fraudsters attempts to steal the elements mentioned below, which can express the purpose of distinguishing individual identity :

1. Full name,
2. National identification number (e.g., SSN
3. Telephone num
4. driver's license number;
5. credit card numbers;
6. digital identity (e.g., E-Mail address, online account ID and password);
7. birth date/birth day;
8. birthplace;
9. face and fingerprints.

Identify an Individual.

- 1. First or last name;
- 2. age;
- 3. country, state or city of residence;
- 4. gender;
- 5. name of the school/college/workplace
- 6. job position, grades and/or salary;
- 7. criminal record.

Classification of Information can be of two types namely:

Non-classified information

1. Public information (public record)
2. Personal information (addresses, telephone numbers, E-mail addresses)
3. Routine business information
4. Private Information (SSN, credit card numbers and other financial information.

5. Confidential business information (sales plans, patentable innovation, new product plans)

Classified information

- **Confidential→** Information about strength of armed forces and Technical Information about weapons
- **Secret** →National security policy, military plans or Intelligence operations
- **Top Secret→** Damage national security, vital defence plans and cryptographic Intelligence system

4.3.2 Types of Identity Theft

What are the different types of Identity theft?

- 1. Financial Identity Theft
- 2. Criminal Identity Theft
- 3. Identity Cloning
- 4. Business Identity Theft
- 5. Medical Identity Theft
- 6. Synthetic Identity Theft
- 7. Child Identity Theft

Financial Identity Theft

- In total, 25 types of financial ID thefts are investigated by the US Secret Service.
- Financial identity occurs when a fraudster makes a use of someone else's identifying details, such as name, SSN and bank account details, to commit fraud that is detrimental to a victims finances.

Criminal Identity Theft

- It involves taking over someone else's identity to commit a crime such as enter into a country, get special Permits, hide one's own identity or commit acts of terrorism. These criminal activities can include:
- 1 Computer and cybercrimes;
- 2. organized crime;
- 3. drug traffickings
- alien smugglings
- 5. money laundering.

Identity Cloning

- Identity cloning may be the scariest variation of all ID theft.

- Instead of stealing the personal information for financial gain or committing crimes in the victims name, identity clones compromise the victims life by actually living and working as the victim.
- ID clones may even pay bills regularly, get engaged and married, and start a family.
- In summary, identity cloning is the act of a fraudster living a natural and usual life similar to a victim's life, may be at a different location.

Business Identity Theft

- Bust-out" is one of the schemes fraudsters use to steal business identity; it is paid less importance n
- parison with individual's ID theft
- A fraudster rents a space in the same building as victims office
- A fraudster rents a space in the same building as victims office
- Hence, it is extremely important to protect business sensitive information (BSI) to avoid any further scams.

Medical Identity Theft

- India is known for medical tourism.
- Thousands of tourists visit India every year, getting their medical problems attended (surgeries, total health check-up Kerala massage etc.,)
- Because of Good Quality and Reasonable in Price in medical services.
- protected health information (PHI).
- The stolen information can be used by the fraudster or sold in the black market to people who "need them.

Synthetic Identity Theft

- This is an advanced form of ID theft in the ID theft world.
- The fraudster will take parts of personal information from many victims and combine them.
- The new identity is not any specific person, but all the victims can be affected when it is used.

Child Identity Theft

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

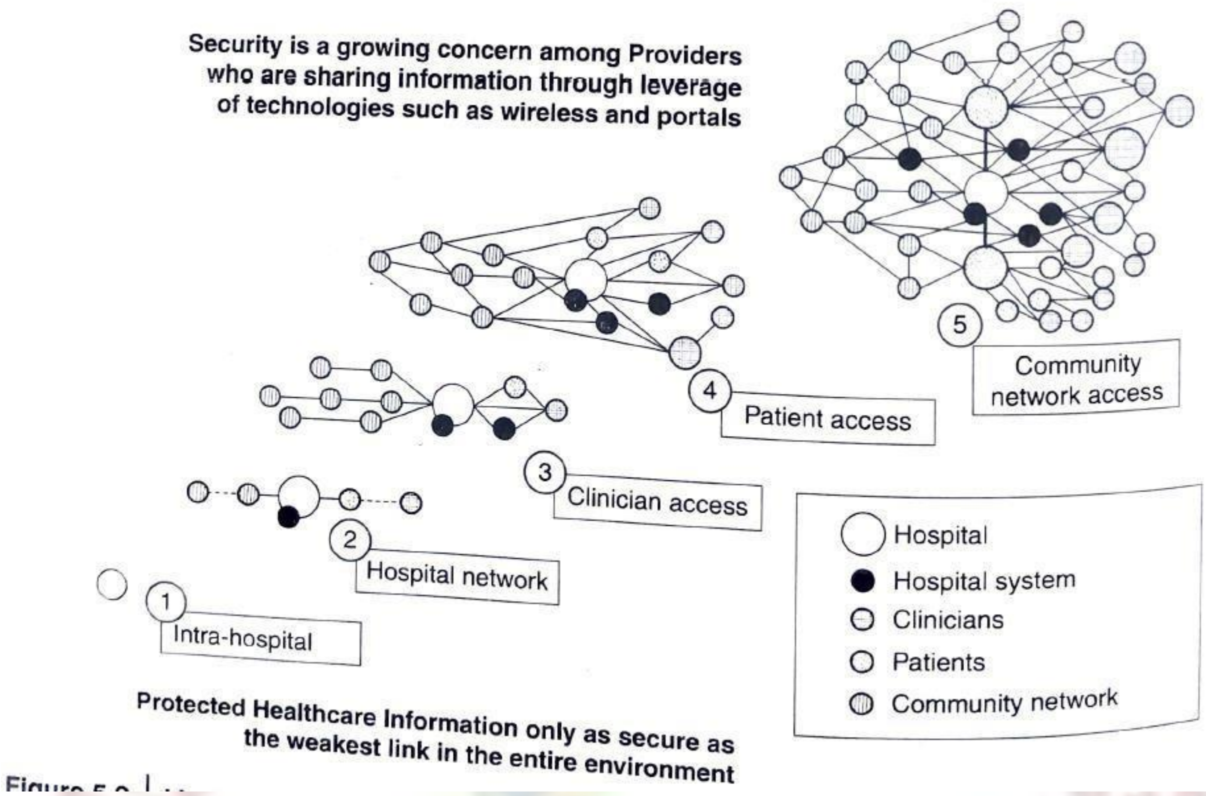

Security is a growing concern among Providers who are sharing information through leverage of technologies such as wireless and portals
1 Intra-hospital
2 Hospital network
3 Clinician access
4 Patient access
5 Community network access
Hospital
Hospital system
Clinicians
Patients
Community network
Protected Healthcare Information only as secure as the weakest link in the entire environment

Fig. Medical domain interconnected entities

4.3.3 Techniques of ID Theft

Human-based methods

- **Direct access to information:** People who have earned a certain degree of trust (ex., house cleaners, babysitters, nurse, friends or roommates) can obtain legitimate access to a business or residence to steal information.
- **Dumpster diving:**
- Retrieving documents from trash bins is very common and is called dumpster diving.
- **Theft of a purse or wallet:** Wallet often contains bank credit cards, debit cards, driving licence medical insurance identity card and what not.
- Pickpockets work on the street as well as in public transport and exercise rooms to steal the wallets and in turn sell the personal information.
- **Mail theft and rerouting:**
- It is easy to steal the postal mails from mailboxes, which has poor security mechanism and all the documents available to the fraudster are free of charge, for example, Bank Mail (credit cards and account statements), administrative forms or partially completed credit offers.
- The fraudster can use your name and other information that may prove to be harmful for an individual in the near future.
- Therefore, return items to the sender or request a change of address.

- **Shoulder surfing:** People who loiter around in the public facilities such as in the cybercafes, near ATMs and telephone booths can keep an eye to grab the personal details.
- **False or disguised ATM (skimming"):** Just as it is possible to imitate a bank ATM, it is also possible to install miniaturized equipment on a valid ATM.
- This equipment (a copier) captures the card information, using which, duplicate card can be made and personal identification number (PIN) can be obtained by stealing the camera films.
- **Dishonest or mistreated employees:** An employee or partner with access to the personal files, salary information, insurance files or bank information can gather all sorts of confidential information and can use it to provide sufficient damage.
- **Telemarketing and fake telephone calls:** This is an effective method for collecting information from unsuspecting people. The caller who makes a "cold call" (supposedly from a bank) asks the victim to verify account information immediately on the phone, often without m explanation or verification. This attack is known as Vishing.

<u>Computer-based technique</u>

These techniques are attempts made by the attacker to exploit the vulnerabilities within existing processes and/or systems.

- **Backup theft:** In addition to stealing equipment from private buildings, attackers also strike public facilities such as transport areas, hotels and recreation centres. They carefully analyse stolen equipment or backups to recover the data.

- **Hacking unauthorized access to systems and database theft:** Besides stealing the equipment and/or hardware criminals attempt to compromise information systems with various tools, techniques and methods to gain unauthorized access to download the required information.
- **Phishing:** It is an attack that attempts to steal money or identity by getting victim to reveal personal information.
- **Pharming:** It is a scamming practice in which malicious code is installed on a personal computer or server misdirecting users to fraudulent websites without their knowledge or consent. User will input information unknowingly.

4.3.4 Identity Theft: Countermeasures

How to prevent being a victim of Identity theft?

- Identity Theft is growing day-by-day
- We need to keep the credit card and PIN safely
- Always Vigilant and take optimum care towards protecting the self-identity

SL. NO	Security Measures
1	Monitor your credit closely
2	Keep records of your financial data and transactions
3	Install security software
4	Use an updated Web browser
5	Be wary of E-Mail attachments and links in both E-Mail and instant messages.
6	Store sensitive data securely
7	Shred documents
8	Protect your PII
9	Stay alert to the latest scams

4.3.5 How to Efface Your Online Identity

- Protect identity is important for netizens, by erasing the footprint on the internet.

SL.NO	How to protect/efface your online identity
1	www.giantmatrix.com
2	www.privacyeraser.com
3	www.reputationdetender.com
4	www.suicidemachine.org
5	www.seppukoo.comm

||Jai Sri Gurudev ||
BGSKH Education Trust (R.) – A unit of Sri Adichunchanagiri Shikshana Trust(R.)
BGS College of Engineering and Technology (BGSCET)
Mahalakshmipuram, West of Chord Road, Bengaluru-560086
(Approved by AICTE, New Delhi and Affiliated to VTU, Belagavi)

Question Bank

Subject: Introduction to Cyber Security **Class:** AI and ML/AIDS/CSD

Subject code: BETCK105I/205I **Faculty:** Mrs. Jyothi R

Course Outcomes

CO1: Interpret the cybercrime terminologies
CO2: Analyze Cyber offenses and Botnets
CO3: Illustrate Tools and Methods used on Cybercrime
CO4: Analyze Phishing and Identity Theft
CO5: Justify the need of computer forensics

Module 4: Phishing and Identity Theft: Introduction, methods of phishing, phishing, phishing techniques, spear phishing, types of phishing scams, phishing toolkits and spy phishing, counter measures, Identity Theft Textbook:1 Chapter 5 (5.1. to 5.3)

Sl. No.	**Questions**	**CO**	**BT**
1	Explain the functions of Anti-phishing Working Group	CO4	L2
2	Explain the statistics that prove phishing is a dangerous enemy among all the methods/techniques.	CO4	L2
3	What is Phishing? Explain with examples.	CO4	L2
4	a). Define the term Phishing with respect to Wikipedia, Webopedia and TechEncyclopedia. b). Differentiate between Spam and Hoax mails	CO4	L2
5	i). What are the different methods of Phishing attacks? Explain in details. OR Explain four types of methods used by the phishers to reveal personal information on Internet ii) Explain the following attack against the legitimate website. a) Website Spoofing b) XSS-Cross site Scripting c) XSRF- Cross scripting Request Forgery	CO4	L2
6	Discuss the different Phishing techniques? OR Discuss the various techniques used by Phishers to launch Phishing attacks	CO4	L2
7	What is spear Phishing? Explain with examples.	CO4	L2
8	What is Whaling? Explain the difference between Whaling and Spear Phishing	CO4	L2
9	Explain the different types of Phishing scams. OR Discuss various types of Phishing Scams.	CO4	L2
10	Explain Phishing Toolkits with examples.	CO4	L2
11	What are countermeasures to prevent malicious attacks	CO4	L3
12	Explain the flowchart of Phishing attacks.	CO4	L2
13	What is identity theft? Explain with examples.	CO4	L2

14	How can information be classified	CO4	L2
15	What are the different techniques of Identity theft?	CO4	L2
16	What are the different types of Identity theft?	CO4	L2
17	How to prevent being a victim of Identity theft?	CO4	L2

Module 5

Understanding Computer Forensics

Understanding Computer Forensics: Introduction, Historical Background of Cyberforensics, Digital Forensics Science, Need for Computer Forensics, Cyber Forensics and Digital Evidence, Digital Forensic Life cycle, Chain of Custody Concepts, network forensics.

5.1 Introduction,

- Cyber forensics plays role in investigation of cybercrime.
- Evidence in the case of Cyber offenses is extremely important from legal perspective.
- There are legal aspects involved in the investigation as well as handling of the digital forensics evidence.
- Technically trained and experienced experts are involved in the forensics activities.
- Use of hand-held devices are incensing now a days. [PDA (Personal Digital Assistance), mobile Phones, iPods]
- Use of data mining in cyber forensics, forensics auditing and anti-forensics.

5.2 Historical Background of Cyberforensics,

- The Florida Computer Crimes Act was the first computer crime law to address computer fraud and intrusion. It was enacted in Florida in 1978.
- The application of computer for investigating computer-based crime has led to development of a new field called computer forensics. Sometimes, computer forensics is also referred to as "digital forensics.

"Forensics evidence" is important in the investigation of Cyber-crimes.

- Computer Forensics needs DIGITAL EVIDENCE, in cases involving data acquisition, preservation, recovery, analysis and reporting, intellectual property theft, computer misuses corporate policy violation, mobile device (PDA, cell phone) data acquisition and analysis, malicious software/application, system intrusion and compromise, encrypted, deleted and hidden files recovery pornography, confidential information leakage etc.,
- The focus of Computer Forensics is to find out digital evidence.
- DE is required to establish whether or a fraud or crime has been conducted.

Computer forensics

- Computer forensics is primarily concerned with the systematic identification, acquisition preservation and analysis of digital evidence, typically after an unauthorized access to computer or unauthorized use of computer has taken place:

- while the main focus of "computer security is to computer systems as well as maintaining "confidentiality, integrity and availability of computer systems.

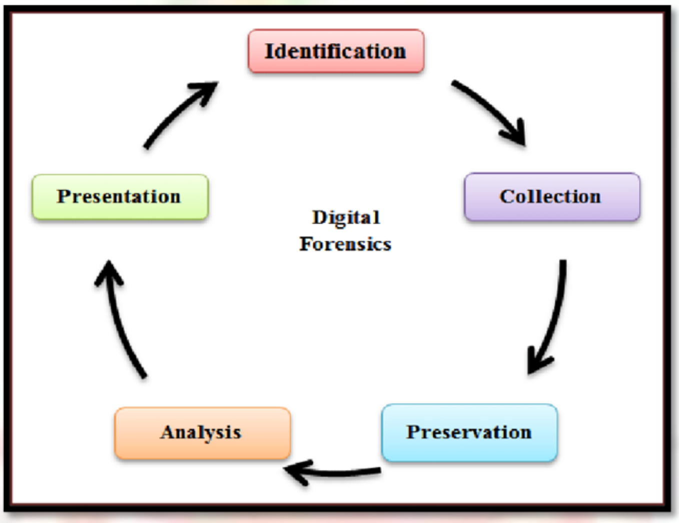
Two Categories of Computer Crime

- 1). Criminal Activity that involves using a Computer to commit a crime
- 2). Criminal activity that has a computer as a target.
- Typical types of data requested for a digital forensics examination by the law enforcement agencies include.
- 1) Investigation into electronic mail (E-Mail) usage, website history, cell phone usage, cellular and Voice over Internet Protocol (VolP) phone usage, file activity history, file creation or deletion, chat history, account login/logout records and more.

Q1: Discuss the Historical Background of Cyberforensics

Historical Background of Cyberforensics.

- Forensics means a "characteristic of evidence that satisfies its suitability for admission as fact and it persuade based upon proof.
- "Forensics science" is the application of science to law and it is ultimately defined by use in court.



5.3 Digital Forensics Science,

Digital forensics is the application of analyses techniques to the reliable and unbiased collection, analysis interpretation and presentation of digital evidence. There is a number of slightly varying definitions/The term computer forensics, however, is generally considered to be related to the use of analytical and investigative techniques to identify, collect, examine and preserve evidence/information which is magnetically stored or encoded

The objective of "Cyberforensics" is to provide digital evidence of a specific or general activity. Following are two more definitions worth considering:

1. **Computer forensics:** It is the lawful and ethical seizure, acquisition, analysis, reporting and safeguarding of data and metadata derived from digital devices which may contain information that is notable and perhaps of evidentiary value to the trier of fact in managerial, administrative, civil and criminals' investigations. In other words, it is the collection of techniques and tools used to find evidence in a computer.

2. **Digital forensics:** It is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation

and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

It is difficult to provide a precise definition of "digital evidence" because the evidence is recovered from devices that are not traditionally considered to be computers. (Some researchers prefer to expand the definition by including the "collection" and "examination" of all forms of digital data, including the data found in cell phones, PDAs, iPods and other electronic devices. In general, the role of digital forensics is to:

.

1. Uncover and document evidence and leads.
2. Corroborate evidence discovered in other ways (E-Discovery)
3. Assist in showing a pattern of events (data mining has an application here).
4. Connect attack and victim computers (Locard's Exchange Principle)
5. Reveal an end-to-end path of events leading to a compromise attempt, successful or not.
6. Extract data that may be hidden, deleted or otherwise not directly available.

.

The typical scenarios involved are:

1. Employee Internet abuse
2. Data leak/ data breach - unauthorized disclosure of corporate information and data (accidental and intentional);
3. Industrial espionage (corporate "spying" activities);
4. damage assessment (following an incident);
5. criminal fraud and deception cases;
6. criminals Cases (many criminals simply store information on computers, intentionally or unwittingly) and countess others;

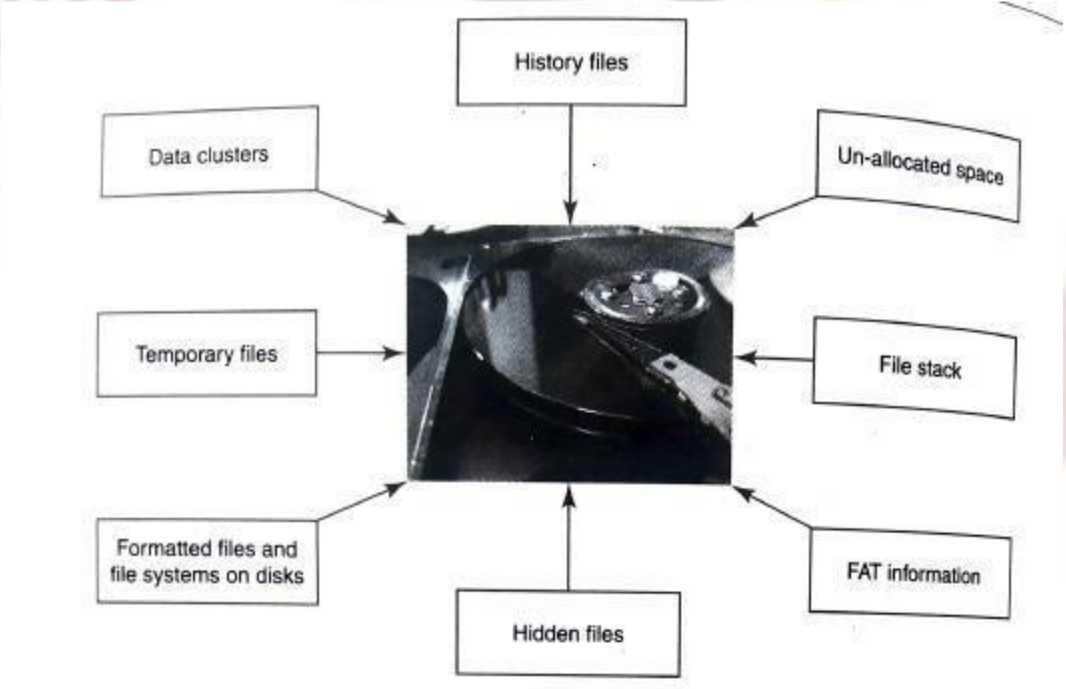


Figure 5.1 shows the kind of data you "see" using forensics tools.

Using digital forensics techniques, one can:

1. Corroborate and clarify evidence otherwise discovered.
2. Generate investigative leads for follow-up and verification in óther ways.
3. Provide help to verify an intrusion hypothesis.
4. Eliminate incorrect assumptions.

Box 5.1: COFEE Time:

- **Computer Online Forensics Evidence Extractor (COFEE)** is a USB thumb drive-gadget onto which Microsoft have loaded 150+ commands that can, among other things, decrypt passwords, display internet activity and uncover all a data stored on the computer.
- The tool was developed by Anthony Fung, a former Hong Kong police office and now an employee who works for Microsoft.
- Microsoft collected the problem faced by law enforcement agencies around the world to develop solution to the problem.
- Law enforcement professional need to capture critical evidence on a computer at the scene of an investigation before the evidence is powered down and removed for forensic analysis.
- COFEE helps the Law Enforcement Agencies even when there are no on-the scene computer forensic capabilities.
- It enables them to collect live volatile evidence more easily.
- On-the-scene, agents can run more than 150 commands on a live computer system. COFEE tool also provides reports in simple format that are easy for later interpretation. These reports can be used by experts and can also be used as supportive evidence for subsequent investigation and prosecution.
- The COFEE fool and its underlying framework can be tailored to effectively meet the needs of a particular investigation, that is, it can be fully customized. On the lighter side, one wonders if there will also be Total Evidence Analyzer (TEA) soon.

Q2: Is there a difference between computer security and computer forensics? Explain

BOX 5.2: Difference between Forensics Policy and Security Policy

Forensics Policy	**Security Policy**
forensics policy is a statement that clearly states which assets are forensically important. those It also specifies data needed for investigation into breach of those assets.	It is a statement that clearly specifies the allowed and disallowed elements with regard to security.
Forensics policy partitions space of all possible breaches or criminal activity into sets events that to are forensically noteworthy and those that are not.	It partitions the system states into "secure" and "unauthorized security" policy that helps implement mechanisms enforce system security policy.
It allows for mechanisms or design decision to enforce policy. Here is another way to understand the difference between security policy and forensics policy - violation of security policy	

leads to insecure information systems/application with vulnerabilities arising due to consequences of break-in or insider is misuse	
On the other hand, **violation of forensics policy means** lack of evidence which results in the loss of ability of an organization to prove guilty the people who are involved in cybercrime incidence.	
Example of forensics policy: 1.Goal is to capture data from network intrusions for possible prosecution. 2. Forensics policy states that all events identified as intrusions will have their associated data captured and preserved 3. Enforcement mechanisms: routine preservation of IDS, firewall, router and web server logs for some configurable length of time	

Q3: List various Computer Forensics services available, explain any two of them.

Box 5.3:
Digital forensics investigations and E-discovery

Digital evidence plays an important role in threat management life cycle, from incident response to high-stakes corporate litigation. Evidences involve computer hard drives, portable storage, floppy diskettes, portable music players and PDA's, etc.....
Key evidences often reside on more than a user hard drive or file server, requiring the capture and analysis of evidence from enterprise productivity servers, network logs or proprietary databases.
Many threats arise from illegal internet activities that extend beyond the firewall and require new investigative and forensics approaches. Forensics professionals need supporting solution for the acquisition, management and analysis of digital evidence.

Such computer forensics services include the following:

1. Data culling and targeting
2. Discovery/subpoena process
3. Production of evidence
4. Expert affidavit support
5. Criminal/Civil testimony
6. Cell phone forensics
7. PDA (Personal Digital Assistants) forensics

Specific client requests for forensics evidence extracting solution support include:

1. Index of files on hard drive
2. Index of recovered files
3. MS Office / user generate document extraction
4. Unique e-mail address extraction
5. Internet activity/ history
6. Keywords search
7. Chain of custody

8. Deleted file/ folder recovery
9. Instant messaging history recovery
10. Password recovery

- Such types of computer evidences are important because quite often the evidence becomes the deciding factor in a criminal, civil or employee dismissal action.
- Investigations involving **trade secrets, commercial disputes and misdemeanor and felony crimes** can be won or lost solely with the introduction of recovered E- mail and other documentation. If someone makes an attempt to delete, erase or otherwise hide critical evidence, you need the competent data recovery capabilities of forensics discoveries.

- Computer users typically "Delete" incriminating or sensitive computer files(For e.g., using tools such as "Deep Freeze", a software tool that is actually meant to protect your computer) but the information may still exist in slack space on the computer's hard drive that is hidden.
- This computer data may linger (remain) for months or even years. However , it can be recovered and documented using computer forensics methods and techniques.
- Unfortunately, there are many examples of computer usage in violation of computer policy**.** Sexual harassment, theft of trade secrets, abuse of the internet and unauthorized outside employment on company time are just few examples of violation that warrant a forensics examination of a computer.
- Even in investigations where hard drives are reformatted in an attempt to hide evidence, forensics discoveries can still potentially recover critical information.
- Forensics discoveries can also aid in recovering passwords for critical files that have been maliciously set or changed.
- There are further challenges; for example, many times, computer are reissued when employees leave.
- Computer that is used continuously may destroy the incriminating evidence that can be used against a former disgruntled employee
- Also, constant use of the computer may raise questions as to who created the incriminating evidence and when
- To prevent these problems and to preserve potentially valuable information, it is recommended that a strict chain of custody should be followed and the subject computer should be shut down, that is, the computer on which digital evidence is believed to be residing
- The following links (accessed on 28 March 2010) provide information about various tools including Deep Freeze
- http://software.informer.com/getfree-deep-format-recover/ (Deep Format Recover Tools):
- http://www.astahost.com/info.php/Deep-Freeze-Partition_12571.html (Deep Freeze-related Blog):
- http://www.hochstadt.com/protecting-your-computer-using-deep freeze (an article here explains how you can protect your computer using "Deep Freeze"):
- http://technodata.blogspot.com/2006/11/how-to-format-hard-disk-by- disk.html (this article explains how to format the hard disk);
- 5. http://www.softlist.net/search/deep-freeze-2000-xp/ (Deep Freeze 200 XP Free Downloads):
- http://www.pctechguide.com/forums/ubbthreads.php/topics/4391/Hard%20Disk%20re-format(technical blog):

Q4: Discuss the need for concept of Computer Forensics

5.4 Need for Computer Forensics,

- The convergence of information and communication technology (ICT) advances and the pervasive use of computer worldwide together have brought many advantages to mankind.
- At the same time, this tremendously high technical capacity of modern computer/computing devices provides avenues for misuse as well as opportunities for committing crime.
- This leads to new risks for computer users and also increased opportunities for social harm.
- The users, businesses and organizations worldwide have to live with a constant threat from hackers who use a variety of techniques and tools to break into the computer to steal information, change data and cause havoc.
- The widespread use of computer forensics is the result of two factors: 1. The increasing dependence of law enforcement on digital evidence. 2. Ubiquity of computers that followed from the microcomputer revolution.
- The media on which clues related to cybercrime reside may vary from case to case.
- There are many challenges for the forensics investigator because storage devices are getting miniaturized due to advances in electronic technology; for example, external storage devices such as mini hard disks (pen drives) are available in amazing shapes.
- Looking for digital forensics evidence (DFE) is like looking for a needle in the haystack.
- Here is a way to illustrate why there is always the need for forensics software on suspect media - the capacity of a typical regular hard disk is 500 GB (gigabytes).
- In an A4 size page, there are approximately 4,160 bytes (52 lines x 80 Characters = 4160 bytes assuming 1 byte per character). This is equivalent to 4 KB (kilobytes). An A4 size of paper sheet has thickness of 0.004 inches.
- Data of 4 MB (megabyte; 1,000 times of 4 KB) when printed on A4 size of paper would be 4 inches thick.
- Data of 4 GB if printed on A4 sheet would be 4,000 inches, that is, 1,000 times of be virtually impossible to "retrieve" relevant forensics data from this heap!! There comes the help from forensics MB.
- This would turn out to be 4 inches thick. The printout of 500 GB would be 500,000 inches!
- It would be virtually impossible to "retrieve" relevant forensics data from this heap!!

There comes the help from forensics software-it helps sieve relevant data from the irrelevant mass (vital few from trivial many as the proverb goes).

Fungibility:

- ***"Fungibility"*** means the extent to which the components of an operation or product can be inter- changed with similar components without decreasing the value of the operation or product.
- For a person to be considered as "identifiable person," he/she must always have the physical custody of a piece of evidence.
- Practically speaking, this means that a police officer or detective will take charge of a piece of evidence, document its collection and hand it over to an evidence clerk for storage in a secure place.

- All such transactions as well as every succeeding transaction between evidence collection and its appearance in court need to be completely documented chronologically to withstand legal challenges to the authenticity of the evidence.
- Documentation must include conditions under which the evidence is collected, the identity of all those who handled the evidence, duration of evidence custody, security conditions while handling or storing the evidence and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs (along with the signatures of persons involved at each step).
- Chain of custody is also used in most evidence situations to maintain the integrity of the evidence by providing documentation of the control, transfer and analysis of evidence.
- Chain of custody is particularly important in situations where sampling can identify the existence of contamination and can be used to identify the responsible party.

Box 5.4: Chain of Custody Example

CASE STUDY
Officer Amar collects the knife and places it into a container, then gives it to forensic technician Balan. Forensics technician Balan takes the knife to the laboratory and collects fingerprints and other evidence from the knife. He then gives the knife and all evidence gathered from the knife to evidence clerk Charu. Charu then stores the evidence until it needed, documenting everyone who has accessed the original evidence (the knife and original copies of the lifted fingerprints).

The chain of custody requires that from the moment the evidence is collected, every transfer of Evidence from one person to another person should be documented as it helps to prove that nobody else could have accessed that evidence. It is advisable to keep the number of evidence transfers as low as possible. In the courtroom, if the defendant challenges the chain of custody of the evidence, it can be proven that the knife in the evidence room is the same as found at the crime scene. However, if due to some discrepancies it cannot be proven who had the knife at a particular point in time. Then the chain of custody is broken and the defendant can ask to have the resulting evidence declares inadmissible.

Q5: Discuss the Cyber Forensics and Digital Evidence
Q6: Explain the rules of evidence

5.5 Cyber Forensics and Digital Evidence,

Cyberforensics can be divided into two main domains

1. Computer forensic
2. Network forensic

As compared the physical evidence digital visions is different in nature because of it has some unique characteristics.

- digital evidence is much easier to change or manipulate
- prefers digital copies can be made without harming original.

At the same time the integrity of digital evidence can be proven.
There are many forms of Cybercrimes sexual harassment cases-memos, letters, emails, obscene chats or embezzlement cases-spreadsheets, memos, letters, emails, online banking, information; corporate espionage by of memos, letters, emails and chats; and fraud through memos, letters, spreadsheet and email.

In case of computer crime or cybercrime computer forensic helps
computer forensic experts know the technique to retrieve the data from files listed in standard directory search hidden files deleted files deleted Email and password login IDS encrypted files hidden partitions etc., Typically the evidence is to decide on computer system used user created files use a protected files computer created files and on computer networks computer system have the following

1. Logical file system that consists of

- **File system:** It includes files, volumes, directories and folders, file allocation tables (FAT) as in the folder version of Windows Operating System, clusters, partitions, sectors.

- **Random access memory.**
- **Physical storage media:** It has magnetic force microscopy that can be used to recover data from overwritten area.
  - Slack space: It is a space allocated to the file but is not actually used due to internal fragmentation and
  - unallocated space.

2. User created files: It consists of address books, audio/video files, calendars, database files, spread- 2. sheets, E-Mails, Internet bookmarks, documents and text files.
3. Computer created files: It consists of backups, cookies, configuration files, history files, log files, Swap files, system files, temporary files, etc.
4. Computer networks: It consists of the Application Layer, the Transportation Layer, the Network Layer, the Data Link Layer. Readers who are not savvy with these terms

Box 5.5: The Father of Forensics Science the Sherlock Holmes of France:

Dr. Edmard Locard→ 1877-1966, Pioneer in Forensic Science and was popularly known as Sherlock Holmes of France.
He Formulated the basic principle of forensics science; " Every contact leaves a trace".
→ known as Locard's exchange principle.

Wherever he steps, wherever he touches, whatever he leaves, even without consciousness. Will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibres from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it. can diminish its value. In *other words, whenever two human beings come into contact. something from one is exchanged to the other, that is, dust, skin cells, hair etc.*

Link to know more: https://science.howstuffworks.com/locards-exchange-principle.htm/printable (11 September 20o9)

5.5.1. The Rules of Evidence

According to the "Indian Evidence Act 1872," "Evidence" means and includes:

1. All statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, are called oral evidence.
2. All documents that are produced for the inspection of the court are called documentary evidence.

Legal community believes that "electronic evidence" is a new breed of evidence. They also, at times, have an apprehension that the law of evidence as per Indian Evidence Act of 1872 may not hold good for electronic evidence. Some lawyers express doubts and apprehensions about the process of leading electronic evidence in the courts. However, this is not true; the traditional principles of leading evidence, along with certain newly added provisions in the Indian Evidence Act 1972 through the Information Technology Act (ITA) 2000, constitute the body of law applicable to electronic evidence. The challenges, however, need to be understood from the "rules of evidence" perspective.

Paper evidence, the process is clear and intuitively obvious. Digital evidence by its very nature Invisible to the eye. Therefore, the evidence must be developed using tools other than the is human eye.

There are number of contexts involved in actually identifying a piece of digital evidence:

1. Physical context: It must be definable in its physical form, that is, it should reside on a specific piece of media.

2. Logical context: It must be identifiable as to its logical position, that is, where does it reside relative to the file system.

3. Legal context: We must place the evidence in the correct context to read its meaning, this may require looking at the evidence as machine language, for example, American Standard Code for Information Interchange (ASCII).

The path taken by digital evidence can be conceptually depicted as shown in Fig. 5.3.

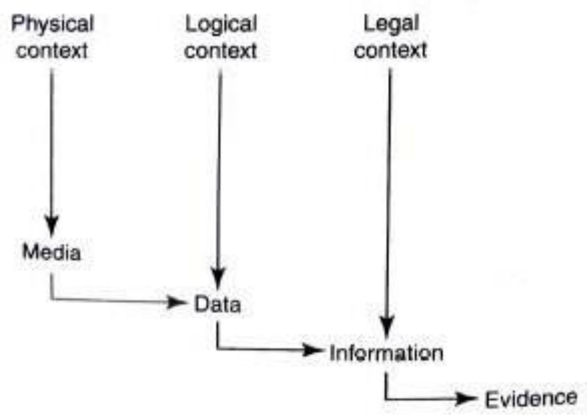


Fig. 5.3: Path of the digital evidence.

What are the guidelines for the (digital) evidence Collection Phase.

1. Adhere to your site's security policy and engage the appropriate incident handling and law enforcement personnel.
2. Capture a picture of the system as accurately as possible.
3. Keep detailed notes with date and times, if possible, generate an automatic transcript. Notes and printout should be signed and dated.
4. Not the difference between the system clock and coordinated universal time for each time stand provided indicate whether UTC or local time is used.
5. be prepared to testify perhaps your leader outlining all actions you to convert times detail notes will be vital.
6. minimise changes to the data as you are collecting it this is not limited to content changes avoid updating files or directly access time.
7. Remove external avenues for change.
8. when confronted with the choice between collection and analysis used to do collection first and analysis later.
9. Needless to say, your procedures should be implementable. As with any aspect of an incident response policy, procedures should be tested to ensure feasibility, particularly, in a crisis. If possible, procedures should be automated for reasons of speed and accuracy. Being methodical always helps.
10. For each device, a systematic approach should be adopted to follow the guidelines laid down in your collection procedure. Speed will often be critical; therefore, where there are a number of devices requiring examination, it may be appropriate to spread the work among your team to collect the evidence in parallel. However, on a single given system collection should be done step by step.
11. Proceed from the volatile to the less volatile; order of volatility is as follows:

    - Registers, cache (most volatile, i.e., contents lost as soon as the power is turned OFF); routing table, Address Resolution Protocol (ARP) cache, process table, kernel statistics, memory;
    - Temporary file systems;
    - disk;
    - remote logging and monitoring data that is relevant to the system in question;
    - physical configuration and network topology;
    - archival media (least volatile, i.e., holds data even after power is turned OFF).

12. we should make a bit-level copy of the system's media. If we wish to do forensics analysis we should make a bit-level copy of pour evidence copy for that purpose, as our analysis will almost certainly alter file access times. try to avoid doing forensics on the evidence copy.

Note: ***Address Resolution Protocol (ARP)*** is a very important part of IP networking.

ARP is used to connect O er (Network) to OSI Laver 2 (Datalink), For most of us this means that ARP is used to link to our IP addressing to our Ethernet addressing (MAC Addressing). For you to communicate with any device on you network, you must have the Ethernet MAC address for that device. If that device is not on your land you go to your default gateway.

In this case your rooter will be destination MAC address that your PC will communicate with they are two types of ARP entries Static and dynamic.

Most of the time you will use dynamic ARP and trees what does means that the ARP entry (the Ethernet Mac to the IP address link) is kept on a device for some period of time as long as it is being used.

The opposite of a dynamic ARP entry is static ARP entry. With the static ARP entry, you are manually entering the link between the Ethernet MAC address and IP address because of Management headache that lack of insignificant negative to using dynamic entries are used most of the time.

7. Expalin the Forensic Analysis of E-Mail
8. Briefly explain RFC2822

Forensics Analysis of E-Mail

Criminal use fake mail for various cybercrime offences. there are tools available but help create fake mail. forensic analysis of email is an important aspect of Cyber forensic analysis.
It help established the authenticity of an email when suspected.
As we know email are the common means of communication word White and the often the subject of forensic analysis.

Email system is the hardware and software that controls the flow of email.
The two most important components of an email system are the email server and email gateway.

Email server are computer set forward collect store and deliver an email to their clients and email gateways are the connections between the email server.

Mail server software is a network software that controls the flow of email and the mail clients of their helps each user read compose send and delete messages and email consists of two parts the header and the body.

Message he does are the important part of investigating email messages.

Theatre of an email is very important from forensic point of you a full header view of an email provides the inter part of emails journey from its Origins to its destination. the header view include sleep originating IP address and other useful information.

Header information very sweet email service provider Email application and system configuration.

Box 5.6: Electronic messages and an Indian Evidence Act

Section 88 of Indian Evidence Act is about presumption as an telegraphic messages it states the following
Presumption as to telegraphic messages the court may presume that a message forwarded from a telegraph office to the person to whom such message for ports to be address corresponds with the message delivered for transmission at the office from which the

message for post to be sent but the court shell not make up presumption as to the person but whom that message was delivered for transmission.

As per section 66a of c and Indian act any electronic mail electronic message for the purpose of causing convenience about the origin of such messages shall be punishable with imprisonment for a term which may extend to 2 to 3 years and with fine.

Typically, the sender's E-Mail address can be found after the "From" section of the header. However, that is not the only place it can be found. It can also be found under other sections depending on the E-Mail client uses. These sections include the following.

1. X-originating E-Mail;
2. X-sender;
3. return-path.

RFC2822

RFC2822 is the Internet Message Format. According to the Internet specification RFC2822, there are several formats of valid E-Mail addresses, like joshi@host.net, john@[10.0.3.19], "Joshi Ganesh'@host.net or "Joshi Ganesh"@[10.0.3.19]. Many E-Mail address validators on the Web fail to recognize some of those valid E-Mail addresses. Some examples of invalid E-Mail addresses are as follows:

1. joshi@box@host.net: Two at signs (@) are not allowed;
2. joshi@host.net: Leading dor () is not allowed;
3. joshi@-host.net: Leading dash (-) is not allowed in on domain name;
4. joshi@host.web: Web is not a valid top-level domain;
5. joshi@[10.0.3.1999]: Invalid IP address.

The RFC2822 standard applies only to the Internet Message Format and some of the semantics of messages contents. It contains no specification of the information in the envelope.
RFC2822 states that each E-Mail must have a globally unique identifier. It is included into the header of an E-Mail.

9.With neat diagram explain process model for understanding a seizure and handling of forensics evidence legal framework.

10. Discuss the following phases of Forensics life cycles
i) Preparation and Identification
ii) Collection and Recording

11. Discuss the following phases of Forensics life cycle
i) Storing and Transporting
ii) Examination/Investigation

12.Discuss the precautions to be taken when collecting electronic evidence.

5.6 Digital Forensic Life cycle,

As per FBI's (Federal Bureau of Investigation) view, digital evidence is present in nearly every crime scene. That is why law enforcement must know how to recognize, seize, transport and store original digital evidence to preserve it for forensics examination. Figure
5.5 shows the process model for understanding a seizure and handling of forensics evidence legal framework.

The cardinal rules to remember are that evidence

- 1. is admissible;
- 2. is authentic;
- 3. is complete;
- 4. is reliable;
- 5. is understandable and believable.

5.6.1. The Digital Forensic Process.

Digital forensic process needs to be understood in the legal context starting from preparation of the evidence to testifying.

Digital forensic evidences consist of exhibits each consisting of a sequence of BITS presented by witnesses in legal matter to help Jurors established the facts of the case and support or refute legal theories of the case.

the exhibit should be introduced and presented and our challenge by properly qualified people using a properly applied methodology that address is the legal theories and issue

Expert witness is very important and is associated with Digital forensic evidence. as per

the court procedure the exhibits are introduced as evidences by either side.

testimony is presented to established the process to identify collect preserve transport store analyse interpret at tribute and or reconstruct the information contained in the exhibit and to establish to the standard of proof required by the matter at hand that the evidence reflects the sequence of events that is asserted to have produced it.

The assumption is that adequate facts can be established for the introduction of an evidence exhibit.

people involved in the chain of custody need to justify a number of aspects relating to the evidence- the testimonial typically include the process of used for creating handling and introducing the evidence the method used for collecting the exhibit as well as the manner in which the exhibit is brought to court.

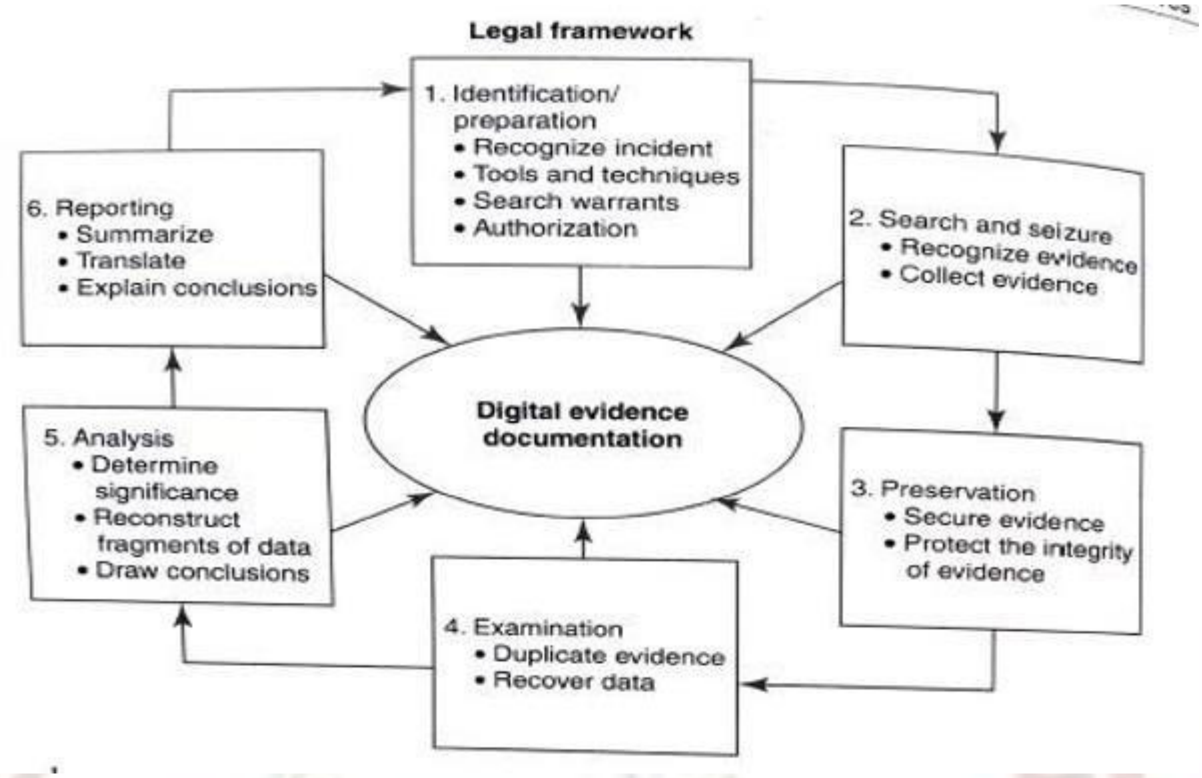


Fig. 5.5: Process model for understanding a seizure and handling of forensics evidence legal framework.

Box 5.8: **Forensics Experts What do they Do?**

The role of forensics experts has become a very special one in digital forensics and there are many reasons for it. Handling of digital evidence requires special expertise that come from training and experience.

A forensics expert team brings the following additional benefits:

1. Technology expertise:
This is perhaps the biggest advantage of partnership with a computer forensics expert. As an example of the technological complexity, consider the proliferation of operating systems in the last decade: mainframe operating systems, Windows 95/98, UNIX, Linux, Windows NT, Windows Server, Macintosh, Windows 2000, Windows XP and Novell Netware. Specific forensics tools must be used with each of these file systems, along with training and experience to interpret search results. Although some evidence may be found easily, other evidence may have been deleted, altered, hidden or encrypted. Forensics experts routinely deal with such complexities and nuances.

2. Forensics methodology: A comprehensive forensics methodology, repeatable and defensible, has become a key attribute in choosing a forensics expert firm. Proper use of a repeatable process prevents making the same mistake twice, ensures proper chain of custody, leverages successful techniques from prior cases, supports clear and concise testimony, and generally guarantees efficient forensics case management.

3. Experience and efficiency: The tools and methods of computer forensics examination are still in their infancy. Experts know how to quickly navigate through the variety of esoteric tools and procedures. Experts also have the experience to cull thousands of files based on patterns and keywords. Therefore, working with experts will efficiently produce relevant results for counsel.

5.6.2. The Phases in Computer Forensics/Digital Forensics

The Forensics life cycle involves the following phases namely.
1. Preparation and identification;
2. collection and recording;
3. storing and transporting;
4. examination/investigation;
5. analysis, interpretation and attribution;
6. reporting;
7. testifying.

To mention very briefly, the process involves the following activities:
1. Prepare: Case briefings (see Box 5.9), engagement terms, interrogatories, spoliation Prevention disclosure and discovery planning, discovery requests. ·
2. Record: Drive imaging, indexing, profiling, search plans, cost estimates, risk analysis.
3. Investigate: Triage images, data recovery, keyword searches, hidden data review, communicate
iterate. '
4. Report: Oral vs. written, relevant document production, search statistic reports, chain of custody reporting, case log reporting.
5. Testify: Testimony preparation, presentation preparation, testimony.

Let us take a brief look at each of the activities mentioned. Table 5.5 shows phase-wise outcome from the phases mentioned above.

Box 5.9: Case Briefings
In case briefings, consider the following:
seen all re~

1. Ensure that you know both your client 's and the adverse party's position. and have seen all relevant paperwork.
2. Try not to project a bias in the case description; the intent should be to consider the case objectively, and provide you with the good news and the bad news (bad news early can be good news)
3. Be upfront in discussing any limitations or restrictions on the forensics investigation including budgetary constraints, time deadlines, cooperation levels to be expected from the adverse party required travel, onsite or after-hours forensics imaging requirements, etc.

Preparing for the evidence and identifying the evidence
In order to be processed and applied evidence must be first identified as evidence. it can happen that there is an enormous amount of potential evidence of available for a legal matter and it is possible that the vast majority of the potential evidence may never get identified.
consider that every sequence of events within a single computer might cause interaction with files the file system in which day recite other processes and the program they are executive and the files they produce and manage and block files and file of various sorts.

Network environment these extents to all network devices potentially all over the world. evidence of an activity that cause Digital forensic evidences to come into being might be continuous contained in a time stamp associated with the different program in a different computer on the other side of the word that was offset from its usual pattern of behaviour by a few many microseconds.

If the evidence cannot be identified as relevant evidence it may be never be collected or process that all and may not even continue to exit in digital form by the time it is discovered to have relevance

Collecting and Recording Digital Evidence.

- Digital evidence can be collected from many sources.
- The sources are computers, cell phones, digital cameras hard drives, CD-ROM, USB memory devices and so on.
- Non-obvious sources include settings of digital thermometers, black boxes inside automobiles, RFID tags and webpages (which must be preserved as they are subject to change).
- Special care must be taken when handling computer evidence: most digital
- information is easily changed, and once changed it is usually impossible to detect that a change has taken place unless other measures have been taken.
- For this reason, it is common practice to calculate a cryptographic hash of an evidence file and to record that hash elsewhere, usually in an investigator's notebook, so that one can establish at a later point in time that the evidence has not been modified as the hash was calculated.
- Figures 5 .6 and 5.7 show the media that typically holds digital evidence.

Collecting volatile data requires special technical skills
If the machine is still active any intelligence that can be gained by examining the applications currently open is recorded.

if the machine is suspected of being used for illegal communication such as terrorist traffic not all of this information may be stored on the hard drive.
If information told solely in Random Access Memory and not recovered before powering down it may be lost.
This results in the need to collect volatile data from the computer at the onset of the response.

Memory falls under the family of solid-state non-time memory it is used in some drive USB sticks cell phone game console secure digital card and multimedia cards.

This technology differs from the normal hard disc by not containing any moving parts in every device that interact with our daily life.
The benefit of Embedded memory continues to increase life expectancy. figure 5.8 shows the various types of embedded memories inside a computer ROM, PROM, EPROM, EEPROM.

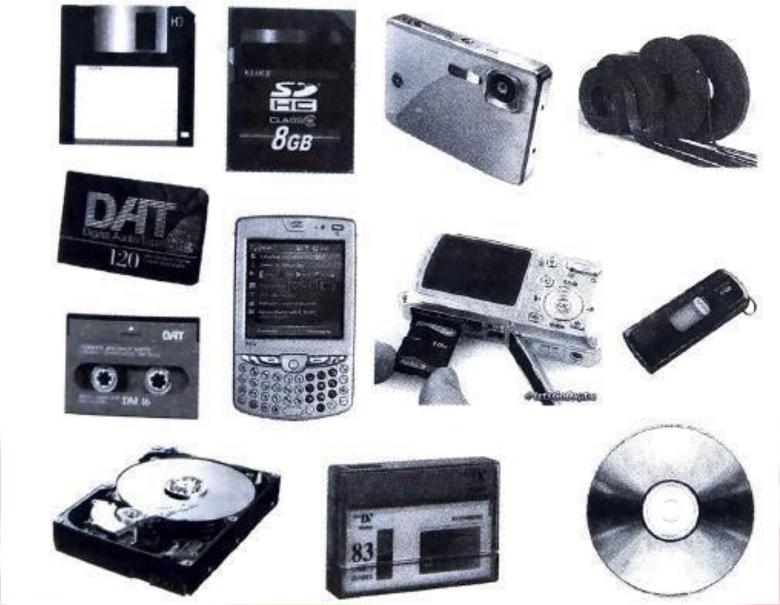


Fig. 5.6: Media that can hold digital evidences_.

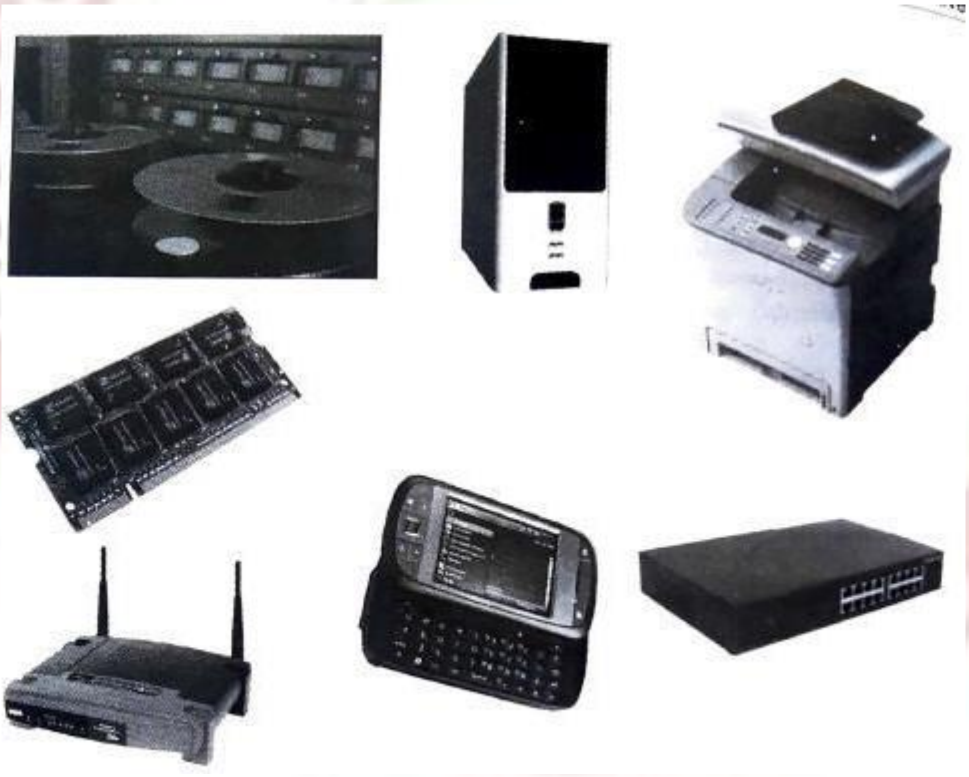


Fig. 5.7. Some more media that can hold digital evidences

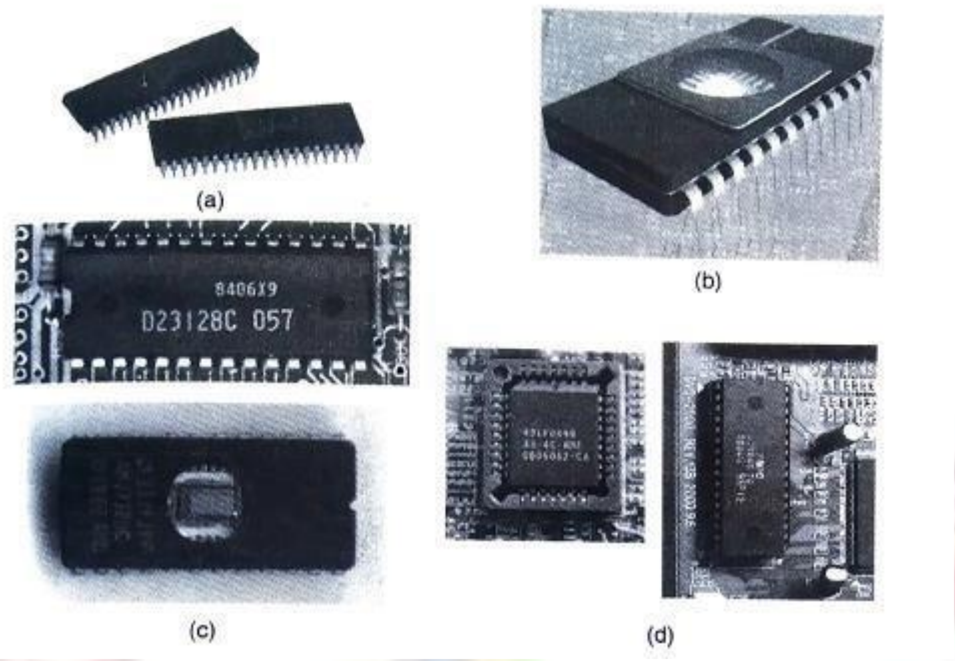


Fig. 5.8. Embedded memories inside computer.

Storing and Transporting digital Evidence

The following are specific practices char have been adopted in the handling of digital evidence.

1. Image computer media using a write-blocking tool to ensure that no data is added to suspect device;

2. Establish and maintain the chain of custody (refer co Section 5.7);

3. Document everything that has been done;

4. Only use cools and methods that have been tested and evaluated to validate their accuracy and reliability.

Storage must be adequately secure to assure proper "chain of custody

Many things can go wrong in storage, including decay over time; environment changes resulting in the presence of a necessary condition for preservation;

Examining/Investigating digital Evidence

Investigation in which the owner of the digital vision has not given consent to have his or her media examined as in some criminal cases some care must be taken to ensure that the forensic specialist has the legal authority to C copy and examine the data sometimes authority stems from search warrant.

It is understanding the difference between live and dead analysis after that we explain about the imaging of the media.

Traditionally computer for insect investigations for performed on a data at rest.

For a exam well the content of hard drives the scan we brought thought of as a analysis investigators were told to shut down computer system when they are impounded for fear that digital time bomb might cause data to be at rest.

Process of creating an exact duplicate of the original evidence media is often called imaging computer forensics software packages make this possible by converting an entire hard drive into a single searchable file is file is called an image.

Analysis, Interpretation and Attribution

Analysis, interpretation and attribution of evidence are the most difficult aspects encountered by most forensics' analysts.
In the digital forensics arena, there are usually only a finite number of possible events sequences that could have produced evidence; however, the actual number of possible sequences may be almost unfathomably large.
In essence, almost any execution of an instruction by the computing environment containing or generating the evidence may have an impact on the evidence. Basic ally, all digital evidence must be analysed to determine the type of information that is stored upon it.
For this purpose, specialty tools are used that can display information in a format useful to investigators. Such forensics tools include but are not limited to the following list.

1. Access Data's FTK
2. guidance Software's EnCase;
3. Dr. Golden Richard III's file carving tool Scalpel; "file carving" is the process of recovering files from an investigative target, potentially without knowledge of the file system structure;
4. Brian Carrier's Sleuth Kitl5l: The Sleuth Kit (TSK) is a library and collection of Unix- and Windows based tools and utilities to allow for the forensics analysis of computer systems.

Box 5.10: The file carving techniques are

File carving is a process of recovering the files from an investigative target, potential without knowledge of the file system structure. the process is based on information about the format of the file types of interest, as well as on assumption about how files are typically laid out on block devices.

if the file system metadata is used at all, it is typically used only for establishing cluster sizes and avoiding carving of undeleted file.

covering is an important technique for Digital forensic investigation and for simple data recovery.

Why using a database of headers and footers for specific file types file covers can retri files from a raw disc image regardless of the type of a file system on the disc image.

File carving ignore the file system and car of the images directly from the data blocks. in cases of fragmented files, the carbon returns in perfect photo but this image might be sufficient to identify the subject. (As in fig. 5.9)

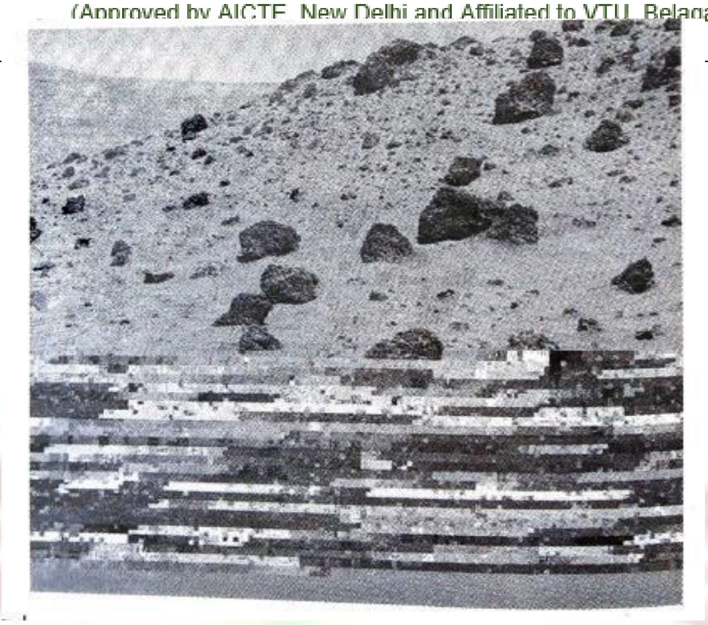


Fig 5.9: An image constructed fragmented file

Digital analysis is very important in Digital forensic because a digital investigation may encounter many forms of digital data and therefore there is a several types of digital analysis.
The different analysis types are based on interpretation obstruction layers which are generally part of the data design.

For example, consider the date on a hard disc which has been designed with several interpretation layers lowest layer me contain partitions or other containers that are used for volume management. Inside each partition is data that has been organised into a file system or database.
Data in the file system is interpreted to create file that contain data in an application specific format and requirement

What are the common digital analysis types:

1. **Media analysis:** It is analysis of the data from a storage device. This analysis does not consider any partitions or other operating system (OS)-specific data structures. If the storage device uses a fixed size unit, such as a sector, then it can be used in this analysis.
2. **Media management analysis:** It is analysis of the management system use d to organize media. This typically involves partitions and may include volume management or redundant array of independent (or inexpensive) disks (RAID, see Box 5.11) systems chat merge data from multiple storage devices into a single virtual storage device.
3. **File system analysis:** It is the analysis of the file system data inside a partition or disk. This typically involves processing the data to extract the contents of a fil e or to recover the contents of a deleted files.
4. **Application analysis:** It is the analysis of the data inside a file. Files are created by users and applications. The format of the contents is application-specific.

5. **Network analysis:** It is the analysis of data on a communications network. Network packers can be examined using the OSI Model to interpret the raw data into an application-level scream.
   Analysis types are
   OS analysis: An OS is an application; it is the first one that is run when a computer starts. This analysis examines another configuration file and output data of the OS to determine what events may be occurred.

   Executable analysis:
   executables are digital object that can cause events to occur and their frequently examine during intrusion investigation because the investigator needs to determine what events the executable could cause
6. **Image analysis:**
   image is a single searchable file.
   Digital images are the target of many digital investigations because some are Contraband.
   this type of analysis Looks for information about where the picture was taken and who are what is in the picture image analysis also includes examining images for evidence of steganography
7. **Video analysis**
   digital radio is used in security cameras and then personal videos cameras and webcams investigation of online predators can sometimes involve digital video from webcams this type of analysis examine the video for identification of objects in the video and the location where it was shot

Box: 5.11 The RAID Levels

RAID data acquisitions are performed as a part of Computer forensic. RAID stands for redundant array of independent discs.
It is category of disc drive that employees' multiple drives in combination for fault tolerance and performance.
The use of raid describe is frequent on servers, the uses not generally necessary for personal computer.
storage technology had become too expensive to place a large number of high-capacity hard drive in the servers.
the response to the situation came through the concept of raid subsequently rate become very popular.
Note that data stripping me spreading out block for each file access multiple disc drives. It was a system developed as a solution to link together a large number of low-cost hard drive with a view to form a single large capacity storage device that provided superior performance storage capacity and reliability as compared to the older storage solutions. since then, RAID become widely used and is deployed as an enterprise storage method in server market.
Attractiveness of RAID comes from the fat that the array of disc distributed the data across multiple discs. however, the computer user and operating system to the serve such. The different RAID levels are

level 0: this is nothing but a strip would Disc a rate without fault tolerance. it provides data stripping but no redundancy. this results in an improved performance however it does not deliver fault tolerance all data in the array is lost if one drive fails.

level 1: This is mirroring and duplex into provide disc mirroring. level 1 provides double the rate of read transaction for single discs, but provide the same bright transaction rate as single disc.

level 2: this is error correcting coding however it is not a typical implementation. this level is rarely used it stripes data at the bit level rather than at the block level.

This is bit interleaved parity level 3 provides byte level stripping with a dedicated parity disc. It is really used probably because it cannot service simultaneous multiple requests.

level 4: this is dedicated parity drive. its use is common for implementation of RAID. Level 4 offers block level stripping with the parity disc if a data disc fails. The parity data is used to create a replacement disc. there is a disadvantage to level 4 in that the parity dis can create write bottlenecks.
Level 5 this is the block interleaved distributed parity. the idea year is to provide data stripping at the bite level and also strike error correction information. level 5 results in excellent performance and good fault tolerance. it most popular among RAID implementation methods.

level 6 this is independent data disc with the double parity. this level provides block level striping with parity data distributed across all disks.

level 0+1: this is nothing but a mirror of stripes. it is not one of the original RAID levels. With this level used, to RAID 0 stripes are created and one RAID 1 mirror is created over them. The use of the level is typically seen for both replicating and sharing data among these.

Level 10 this is a stripe of mirrors however it is not considered to be an original red level. with this level multiple RAID 1 Mirrors are created, and RAID 0 stripe is created over these.
Level 7: this is a Trademark of STC (storage Computer Corporation) it at cashing to level 3 or 4.
RAID S: This is also known as parity rate it is an MNC corporation's priority stripped parity rate system used in its Symmetrix storage system.

Reporting:

Once the analysis is complete, a report is generated. The report may be in a written form or an oral testimony or it may be a combination of the two. Finally, evidence, analysis, interpretation and attribution

The following are the broad-level elements of the report:
1. Identity of the reporting agency;
2. case identifier or submission number;
3. case investigator;
4. identity of the submitter;
5. date of receipt;
6. date of report;
7. descriptive list of items submitted for examination, including serial number, make and model;
8. identity and signature of the examiner;

9. brief description of steps taken during examination, such as string searches, graphics image searches
and recovering erased files;
10. results/ conclusions.

Testifying
This face in wall of presentation and cross examination of expert witness.

Depending on the country and legal Framework in which a cyber cream cases register that is standards me apply with regard the issue of expert witnesses.

Digital forensic evidence is normally introduced by expert witness set in the case where non expert can bring the clarity to non-scientific issues by taking what they observed or did.

For example, and non-expert who works at a company may introduce the data here she extracted from a company data base and discuss how the database works and how it normally use from a non-technical standpoint.

To the extent that the witness is the custodian of a system or a content he or she can justify to matters related to that custodial Rose as well.

Only expert witness can address issues based on scientific, technical or other specialized knowledge.
A witness qualified as an expert by knowledge, skill, experience or education.
a). If a Testimony is based on sufficient facts or data.
b). Testimony is the product of reliable principles and methods
c). the witness as applied the principles and methods reliable

Table 5.5. Digital Forensic- Phase wise outputs.

Evidence preparation and identification	• Monitoring authorisation and management support, and obtained authorisation to do the investigation. • ensuring that operations and Infrastructures are able to support an investigation. • providing a mechanism for the incident to be detected and conformer. • providing a mechanism for the incident to be detected and conformer • creating an awareness so that the investigation is needed (I didn't if I the need for an investigation) • planning for getting the information needed from both inside and outside the investigation organization. • identifying the strategy policy and previous investigation • informing the subject of an investigation or other consent party that the investigation is taking place	plan authorisation warrant notification confirmation

collection and recording preserving and transportation	• Determine water particular piece of digital evidence is and identifying possible source of data • determine where the evidence is physically located the variable • Translating the media into data • ensuring integrity and authenticity of the digital evidence for example write protection hashes etc • packaging transporting and storing the digital evidence • preventing people from using the digital device or allowing other electromagnetic device to be used within an affected radius • recording the physical scene • duplicating the digital evidence using standardised and accepted procedure • ensuring the validity and integrity of evidence for later use	crime type potential evidence source media device event
examination investigation and analysis interpretation and attribution	• Determine Hing how the data is produced, when and why whom. • determine and validating the techniques to find and interpret significant data. • extracting hidden data, discovering the hidden data and matching the pattern. • recognising fbs pieces of digital evidence and assessing the skills level of suspect. • transform the data into more manageable size and form for analysis. • confirming or refuting allegations of suspicious activity. • identifying and locating potential evidence, possibly Within unconventional locations. • constructing detailed documentation for analysis and drawing conclusions based on evidence found. • determining significant based on evidence found. • testing and rejecting theories based on digital evidence. • organising the analysis results from the collected physical and digital evidence. • eliminating duplication of analysis • build a timeline • constructing a hypothesis of what occurred and comparing the extracted data with the target. • documenting the finding and all steps taken.	log files, file events log data information

presentation and reporting	• Preparing and presenting the information resulting from analysis phase. • determine the issues relevance of the information, its reliability and who can testify to it. • interpreting the statistical from analysis phase. • clarifying the evidence and documenting the finding. • summarizing and providing explanation of conclusions. • presenting the physical and digital evidence to a court or corporate management. • attempting to confirm each piece of evidence and each event in the chain either along with each other are independent of one evidence and or other events. • providing the validity of the hypothesis and defend it against criticism and challenge. • Communicating Relevant findings to a variety of audience management technical personally law enforcement.	evidence, report
disseminating the case	• Physical and digital property is return to proper owner. • determining how and what criminal evidence must be removed. • reviewing the investigation to identify areas of improvement. • discriminating the information from the investigation. • closing out the investigation and preserving knowledge gained	evidence explanation new policies and investigation procedures evidence the post investigation closed

5.7.3. Precautions to be taken when collecting Electronic Evidence.

Collection of evidence must happen with due care. special measures should be taken while conducting a forensic investigation if it is desired for the results to be used in a court of law one of the most important major is to ensure that the evidence has been accurately collected and that there is a clear chain of custody right from the scene of crime to the investigator and ultimately to the court. in order to comply with the need to maintain the integrity of digital dividend certain rules must be compiled with.

the general principles are

Principle 1:
No action taken by law enforcement Agencies or their agent should change data held on a computer or storage media, which may subsequently be relied upon in court.

Principle 2:

In exceptional circumstance, where a person finds it necessary to access original data held on a computer or storage media that person must be competent do so and be able to give evidence explaining the relevance and the implications of his/her actions.

Principle 3:

An Audit trail or other record of all the processes applied to computer waste electronic evidence should be created and preserved. An independent third party should be able to examine those process and achieve the same result.

Principle 4:

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

13.Explain the chain Custody Concepts in Cyber Forensics

5.7 Chain of Custody Concepts,

A chain of custody is the process of validating how many kinds of evidences have been gathered, tracked and protected on the way to a court of law

It is essential to get in the habit of protecting all evidences equally so that they will hold up in court. Forensic nvestigation professionals know that if you do not have a chain of custody, the evidence is worthless. They learn to deal with everything as if it would go to litigation.

Purpose of the chain of custody is that the proponent of a piece of evidence must demonstrate that it is what it purports to be.

In other words, there is a reliable information to suggest that the party offering the evidence can demonstrate the piece of evidence is actually, in fact, what the party claims it to be and can further demonstrate its origin and the handling of the evidence because it was acquired. The Chain of Custody is a chronological written record of those individuals who have had custody of the evidence from, its initial acquisition until its final disposition.

A chain of custody begins when an item of relevant evidence is collected, and the chain is maintained until the evidence is disposed off (Figs. 5.10 and 5.11). The chain of custody assumes continuous accountability. This accountability is important because, if not properly maintained, an item (of evidence) may be inadmissible

5.8 Network forensics.

- Open networks can be source of many network-based cyberattack
- Wireless Forensics
- Wireless Forensics is a discipline included within the computer forensics science, and specifically, within the network forensics field.
- The goal of wireless forensics is to provide the methodology and) tools required to collect network traffic that can be presented as valid digital evidence a court of law.

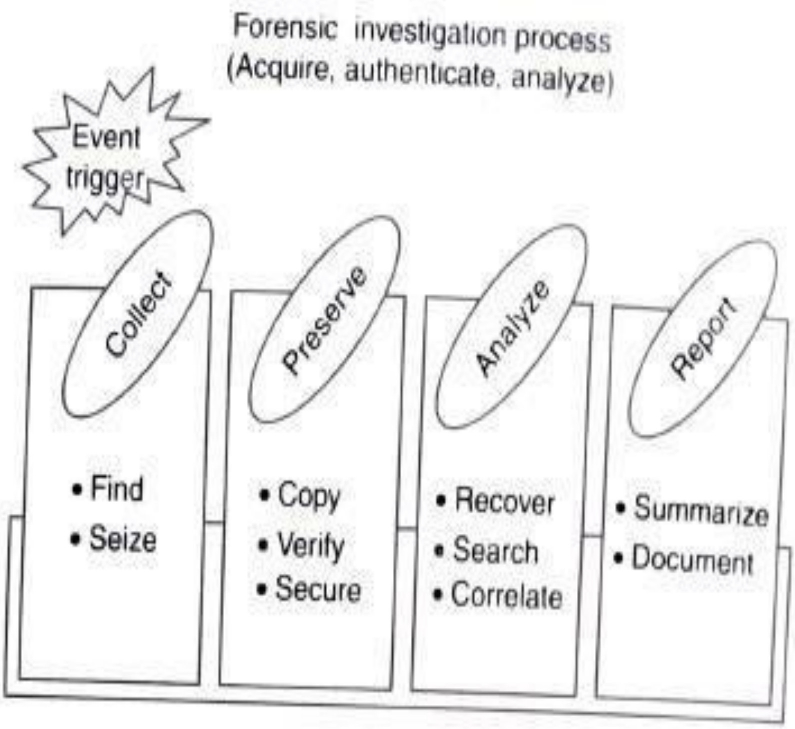


Fig. 5.10: Maintaining chain of custody

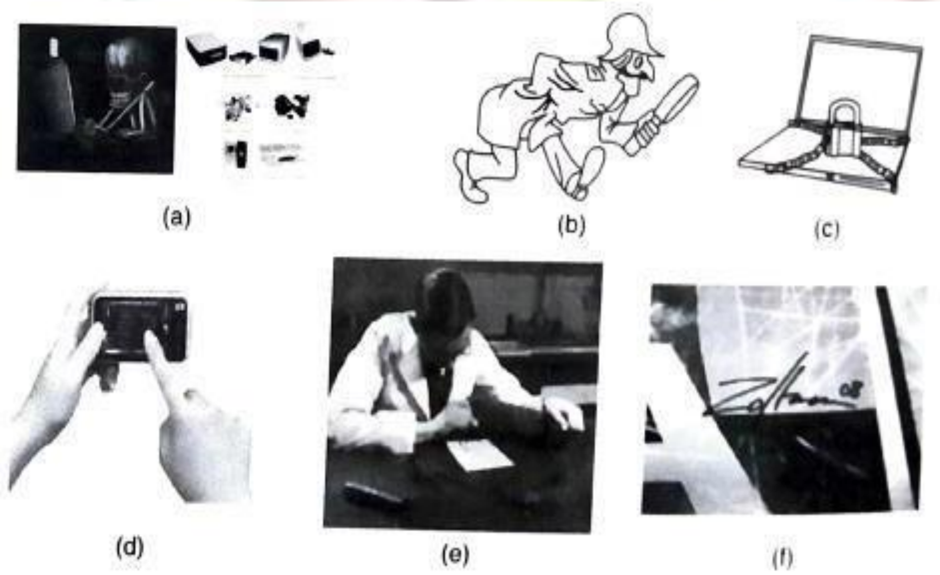


Fig. 5.11: Maintaining chain of custody 2. (a) Source of evidence - where did it come (b). Who found it? (c) Where was it stored/locked up? (d) Who touched it/tampered With it?
(e) What did they do to it? What did they do with it? (f) Human signature always required

******************************** END***********************************

||Jai Sri Gurudev ||

BGSKH Education Trust (R.) – A unit of Sri Adichunchanagiri Shikshana Trust(R.)

BGS College of Engineering and Technology (BGSCET)

Mahalakshmipuram, West of Chord Road, Bengaluru-560086

(Approved by AICTE, New Delhi and Affiliated to VTU, Belagavi)

Question Bank

Subject: Introduction to Cyber Security **Class:** AI and ML/AIDS/CSD

Subject code: BETCK105I/205I **Faculty:** Mrs. Jyothi R

Course Outcomes

CO1: Interpret the cybercrime terminologies
CO2: Analyze Cyber offenses and Botnets
CO3: Illustrate Tools and Methods used on Cybercrime
CO4: Analyze Phishing and Identity Theft
CO5: Justify the need of computer forensics

Module 5: Understanding Computer Forensics • Introduction, Historical Background of Cyberforensics, Digital Forensics Science, Need for Computer Forensics, Cyber Forensics and Digital Evidence, Digital Forensic Life cycle, Chain of Custody Concepts, network forensics

Sl. No.	**Questions**	**CO**	**BT**
1	Discuss the Historical Background of Cyberforensics	CO5	L2
2	Is there a difference between computer security and computer forensics? Explain	CO5	L2
3	List various Computer Forensics services available, explain any two of them.	CO5	L2
4	Discuss the need for concept of Computer Forensics	CO5	L2
5	Discuss the Cyber Forensics and Digital Evidence	CO5	L2
6	Explain the rules of evidence.	CO5	L2
7	Briefly explain RFC2822	CO5	L2
8	With neat diagram explain process model for understanding a seizure and handling of forensics evidence legal framework.	CO5	L2
9	Discuss the following phases of Forensics life cycles i) Preparation and Identification ii) Collection and Recording	CO5	L2
10	Discuss the following phases of Forensics life cycle i) Storing and Transporting **ii)** Examination/Investigation	CO5	L2
11	Discuss the precautions to be taken when collecting electronic evidence.	CO5	L2
12	Explain the importance of chain of custody concept. Provide illustrations to support the answer	CO5	L2
13	Briefly explain Network Forensics	CO5	L2