Introduction to Cyber Crime

What is Cyber Crime

Cybercrime, or **computer-oriented crime**, is the crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".

According to the law enforcement agency , internet – related crimes can be divided into mainly two types as follows :

1. **Advanced cybercrime / high-tech crime :** Attack against computer hardware and software.
2. **Cyber – enabled crime :** Crime related to monetary , personal harassment and act of terrorism.

To make security against cyber crime , the individual has to adopt digital forensic tools to protect confidential data or any kinds of files on computer system.

On the basis of above types cyber crime can be categories into

1. Cybercrime against Persons
2. Cybercrime against Property
3. Cybercrime against Government

1. Cybercrime against Person

Cybercrime committed against persons includes crime such as harassment through email , false legal agreement , posting obscene materials and monetary fraud etc.

2. Cybercrime against Property

It include computer delivery , destruction of intetcual property rights and transfer of harmful virus to computer system.

3. Cybercrime against Government

This kind of cyber crime include cyber terrorism , spreading rumours for violence in society etc.

Based upon the cybercrime scope in society , we can divide it into two broad categories

1. **Violent or potentially violent cybercrime** : Violent or potentially violent cybercrime are those that pose a physical risk to some character or persons.

   For ex. Cyber terrorism , Cyber talking , Assaults by threats , child pornography.

2. **Non – violent cybercrime :** Non – violent cybercrime are those that do not directly pose a physical risk to some character or person , but indirectly they do pose a risk.

   For ex. Cyber theft , cyber trespass , cyber fraud , destructive cybercrime

1. **Hacking :** In simple words, hacking is an act committed by an intruder by accessing your computer system without your permission.

Hacker are usually technology buffs who have expert-level skills in one particular software program or language. Greed and sometimes voyeuristic tendencies may cause a hacker to break into systems to steal personal banking information, a corporation's financial data, etc. They also try and modify systems so hat they can execute tasks at their whims. Hackers displaying such destructive conduct are also called "Crackers" at times. they are also called "Black Hat". Whereas as "White Hat" hackers, these guys are against the abuse of computer systems. They attempt to break into network systems purely to alert the owners of flaws. It's not always altruistic, though, because many do this for fame as well, in order to land jobs with top companies, or just to be termed as security experts.

"Grey Hat" is another term used to refer to hacking activities that are a cross between black and white hacking.
There are generally three kinds of hacking

a. **SQL Injections:** An SQL injection is a technique that allows hackers to play upon the security vulnerabilities of the software that runs a web site. It can be used to attack any type of unprotected or improperly protected SQL database. This process involves entering portions of SQL code into a web form entry field – most commonly usernames and passwords – to give the hacker further access to the site backend, or to a particular user's account.
b. **Theft of FTP Passwords:** FTP password hacking takes advantage of the fact that many webmasters store their website login information on their poorly protected PCs. After hacking FTP information ,he then logs into the web site via the remote computer and modifies the web pages of original web deveoper.

c. Cross-site scripting: Cross-site scripting is a hard-to-find loophole in a web site, making it vulnerable to attack. In a typical XSS attack, the hacker infects a web page with a malicious client-side script or program. When you visit this web page, the script is automatically downloaded to your browser and executed. Typically, attackers inject HTML, JavaScript, VBScript, ActiveX or Flash into a vulnerable application to deceive you and gather confidential information.

2. Denial – Of – Service (DoS) Attacks: A DoS attack is a trial to make an online service unavailable by overloading the network traffic from multiple sources. It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload. This causes the resource (e.g. a web server) to crash or slow down significantly so that no one can access it. Using this technique, the attacker can render a web site inoperable by sending massive amounts of traffic to the targeted site. A site may temporarily malfunction or crash completely, in any case resulting in inability of the system to communicate adequately. DoS attacks violate the acceptable use policies of virtually all internet service providers.

"Distributed Denial of Service" (DDoS) attack wherein a number of geographically widespread perpetrators flood the network traffic.

3. **Trojan Attacks or Logic Bombs :** A logic bomb or trojan , also known as “slag code”, is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. The trojan need to be installed from an executable file(.exe) or a compiler . Once the trojan is installed , the hacker can use them to access all the sensitive or confidential and personal information or data.
The embedded piece of code destroys the software after a defined period of time or renders it unusable until the user pays for its further use

4. **Identity Theft and Credit Card Fraud :** Credit card frauds usually occur when individual disclose their confidential data such as credit card number , CVV number, secret code for transaction , expiry date etc. to an unknown person , who could be a potential hacker.

In this case card is stolen or lost or when mails are diverted from the actual recipient to the hacker. This kind of fraud is an identity fraud in which a hacker takes the necessary information about the credit card for their personal purpose.

A more serious concern is the use of your personal information with the help of stolen or fake documents to open accounts (or even worse, using your existing account) to take a loan in your name. These unscrupulous people can collect your personal details from your mailbox or trash can. (remember to shred all sensitive documents)

You won't know a thing until the credit card people track you down and tail you until you clear all your dues. Then for months and months you'll be fighting to get your credit restored and your name cleared.

5. **Cyber Pornography** : It distribute pornography over the internet by creating porn or obscene materials over internet.

6. **Salami slicing attack :** A “salami slicing attack” or “salami fraud” is a technique by which cyber-criminals steal money or resources a bit at a time so that there’s no noticeable difference in overall size. Stealing money electronically is the most common use of the salami slicing technique, but it’s not restricted to money laundering. The salami technique can also be applied to gather little bits of information over a period of time to deduce an overall picture of an organization. This act of distributed information gathering may be against an individual or an organization. Data can be collected from web sites, advertisements, documents collected from trash cans, and the like, gradually building up a whole database of factual intelligence about the target.

7. **Software Piracy** : Software piracy is the unauthorised use and distribution of computer software. Software developers work hard to develop these programs, and piracy curbs their ability to generate enough revenue to sustain application development. This affects the whole global economy as funds are relayed from other sectors which results in less investment in marketing and research.

The following constitute software piracy:

- Loading unlicensed software on your PC
- Using single-licensed software on multiple computers
- Using a key generator to circumvent copy protection
- Distributing a licensed or unlicensed (“cracked”) version of software over the internet and offline

“Cloning” is another threat. It happens when someone copies the idea behind your software and writes his own code to make duplicate software and spread malware over internet.

8. **Email Bombing or Spoofing** : Email spoofing refers to sending emails from an unknown or false sources. The hackers tries to send spam emails or emails that include attractive offers , which the individual accepts and fills certain details.

Email bombing is characterised by an abuser sending huge volumes of email to a target address resulting in victim's email account or mail servers crashing.

Email bombing is commonly carried out using botnets (private internet connected computers whose security has been compromised by malware and under the attacker's control) as a DDoS attack.

Email spamming worsens when the recipient replies to the email causing all the original addressees to receive the reply. Spammers collect email addresses from customer lists, newsgroups, chat-rooms, web sites and viruses which harvest users' address books, and sell them to other spammers as well. A large amount of spam is sent to invalid email addresses

9. **Forgery / Falsification** : Forgery refers to the action of forging a copy or imitation of a document, signature or banknote by altering original document. It is done to earn a huge profit by selling the forged resources.

10. **Phishing** : It is a fraud type wherein the hacker tries to get personal information , including login credentials or any bank account information, by showing genuine entity in email, message or other communication channels.

11. Cyber Terrorism or Data diddling :

Data Diddling is unauthorised altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track. In other words, the original information to be entered is changed, either by a person typing in the data, a virus that's programmed to change the data, the programmer of the database or application, or anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data.

For Ex. forging or counterfeiting documents and exchanging valid computer tapes or cards with prepared replacements. Electricity boards in India have been victims of data diddling by computer criminals when private parties were computerizing their system

12. Cyber Stalking : Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online. A cyber stalker doesn't physically follow his victim; he does it virtually by following his online activity to harvest information about the stalkee and harass him or her and make threats using verbal intimidation. It's an invasion of one's online privacy. Cyber stalkers harass their victims via email, chat rooms, web sites, discussion forums and open publishing web sites (e.g. blogs). **Internet Stalking: T**he stalker harasses the victim via the internet.

13. Cyber Defamation : It involve defamation of a persons or individual by a new virtual medium by creating wrong image in society.

14. Web jacking: The hacker takes control of a web site fraudulently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him. The owner of the web site has no more control and the attacker may use the web site for his own selfish interests.

Role of Computers in Cyber Crime

The computer plays the important role in crime also by extracting evidences , instrumentality , illegal imports or fruits of crime.

1. They can act as a communication tool
2. They can be the target of the attacker for criminal activity.
3. They can also be tangential to crime.

But apart from this Computer also plays the role in solving crime as

1. Witness can view the suspect's picture on computer.
2. DNA testing and finger print matching can be done by matching criminal previous records.
3. Database of criminal records maintain by computer system.
4. Simulations can be created by use of computers.
5. Plays the role of investigator in various case like fire, sketching of criminal

Introduction to Digital Forensic

Digital Forensic can be defined as follows :
Digital forensic is a series of steps to uncover and analyse electronic data through scientific method. The major goal of the process is to duplicate original data and preserve evidence and then performing the series of investigation by collecting , identifying and validating the digital information for the purpose of reconstructing past events.

OR

Digital forensic is a set of specific , predefined and accepted steps applied to digital media or digitally stored data by applying scientifically proven and derived technique , based on a solid legal / law

Foundation , to extract after –the- fact digital evidence with the goal of deriving the set of events or actions indicating a crime , where reconstruction of possible events can be used to validate the scientifically derived conclusions.

The field of digital forensic has made some rapid developments over the past few years due to the advancement in tools and systems that allow ordinary computer users to be proficient in performing difficult audit task of pirated copies of software products.

It also encompass, identify, analyse, recover and investigate digital evidences found in digital devices to detect cyber crimes.

Use of Digital Forensics

Digital Forensics Investigation (DFI) can be defined as follows :

Digital forensic investigation is a special types of investigation where the scientific procedure and technique used will be allowed to view the results as digital evidence to be admissible in a court of law.

The DFI can be divided into sub-categories as

i) Computer Forensic
ii) Network Forensic
iii) forensic data analysis and
iv) Mobile Forensics

A DFI is conducted by an appropriately certified investigator. The DFI is special types of investigation wherever scientific procedure and technique used to draw digital proof , to be allowable in court of law.

While performing a digital forensic investigation , the investigator should follow the following rules.

1) Minimal handling of the original
2) Account for any changes
3) Comply with the rules of evidence
4) Do not exceed your knowledge

By going through above rules, the investigator faces the following difficulties as follows:-

1. In computer system there are bulk amount of data. But only certain amount of data is valid as evidence. Hence to locate valid evidence , the investigator take huge amount time.
2. Most probably criminal delete evidence from computer system. So searching or recovering evidence is worthless or hard to detect.
3. If file is protected by secured password , then investigator read the data in unauthorized manner.
4. Cyber crime are different in various scenarios. Hence each and every time investigator has to follows different rules and tools and sometimes has to learn new technique for investigation.
5. Evidence may be located in multiple different types of digital devices.

Digital Evidence or Forensic Evidence

Digital Evidence is any information or data of value to an investigation that is stored on, received by , or transmitted by an electronic device.
Text Message , emails, pictures and videos and internet searches are some of the most common types of digital evidence.

Evidence can be stated as any information that can be confident or trusted and which proves something related to the case in a trial i.e it indicate that a certain substance or condition is present.

Types of Digital Forensics

1. Illustrative evidence : It also known as demonstrative evidence which represent an object which is a common form of proof. Ex. Photographs , X-rays, maps , models.
2. Electronic evidence : Those evidence or proof that can be obtained from an electronic source is called digital evidence. Ex. Emails , ATM transactions, cell phones logs etc.
3. Documented evidence : It is similar to illustrative evidence but proof is presented in writing or electronic media like contracts, invoices, printed email or photographs.

4. Explainable evidence (or Exculpatory) : This types of evidence is typically used in criminal cases in which it supports the dependant , either partially or totally removing their guilt in the case.

5. Substantial evidence : A proof introduced in the form of a physical object , whether whole or in part such as evidence might consists of dried blood , fingerprints and DNA samples etc.

6. Testimonial : It is a kind of evidence spoken by a spectator under oath or written evidence given under oath by an official declaration or affidavit.

Rules of Digital(Forensic)Evidence in Collection

1. Best Evidence Rule : It is defined as the most complete copy or a copy which includes all necessary parts of evidence which is closely related to the original evidence which must be confessed in court to prove its content without any expectation. The multiple copies of electronic media can be generated which will be taken into account in Best Evidence Rule.
2. Original Evidence : It is defined as the truth or real(original) copy of the evidence media which is given by client/victim.

3. Rules of Digital Evidence : The rule of forensic evidence are concerned with the amount, quality and type of proof which help to prove in litigation. This rule may varies according to crime types.

The following points must be considered

a) Admissible : The evidence must be able to be used in court.
b) Authentic : Evidence should act positively to an incident.
c) Complete : A proof that covers all perspective.
d) Reliable : There is no any chance of doubt about reality of the specialist's decision.
e) Believable : It should be understandable and believable to jury.

Challenges in Forensic Evidence Collection

In evidence collection , the technical complexity is a major issue in paper trial. The most difficult task for an evidence handler is to authentic the collected evidence and maintaining chain of custody and evidence validation at the judicial proceeding are necessary.

1. Authentication of Evidence : The evidence that are collected by any person/investigator should be collected using authenticate methods and technique because during court proceeding it must be admissible.
2. Chain of custody : Maintaining the chain of custody

Means that the evidences collected should not be accessed by any unauthorized individual and must be stored in a tamper proof manner. For each items as a proof , there must be a complete chain of custody record.

3. Evidence Validation : The evidence collection and produce in court having difference in time. To meet challenges of validation , original media matches the forensic duplication by using MD5 hashes. For every File MD5 hash values is generated within proper time period to make duplicated validated evidence.

Digital Forensic Investigation Process/Model/Framework

For doing any kind of investigation , we have to follow some sequential order of process.
In this section we are going to study main process model as follows.

1. Computer Forensic Incident Response Essentials(CFIRE) model

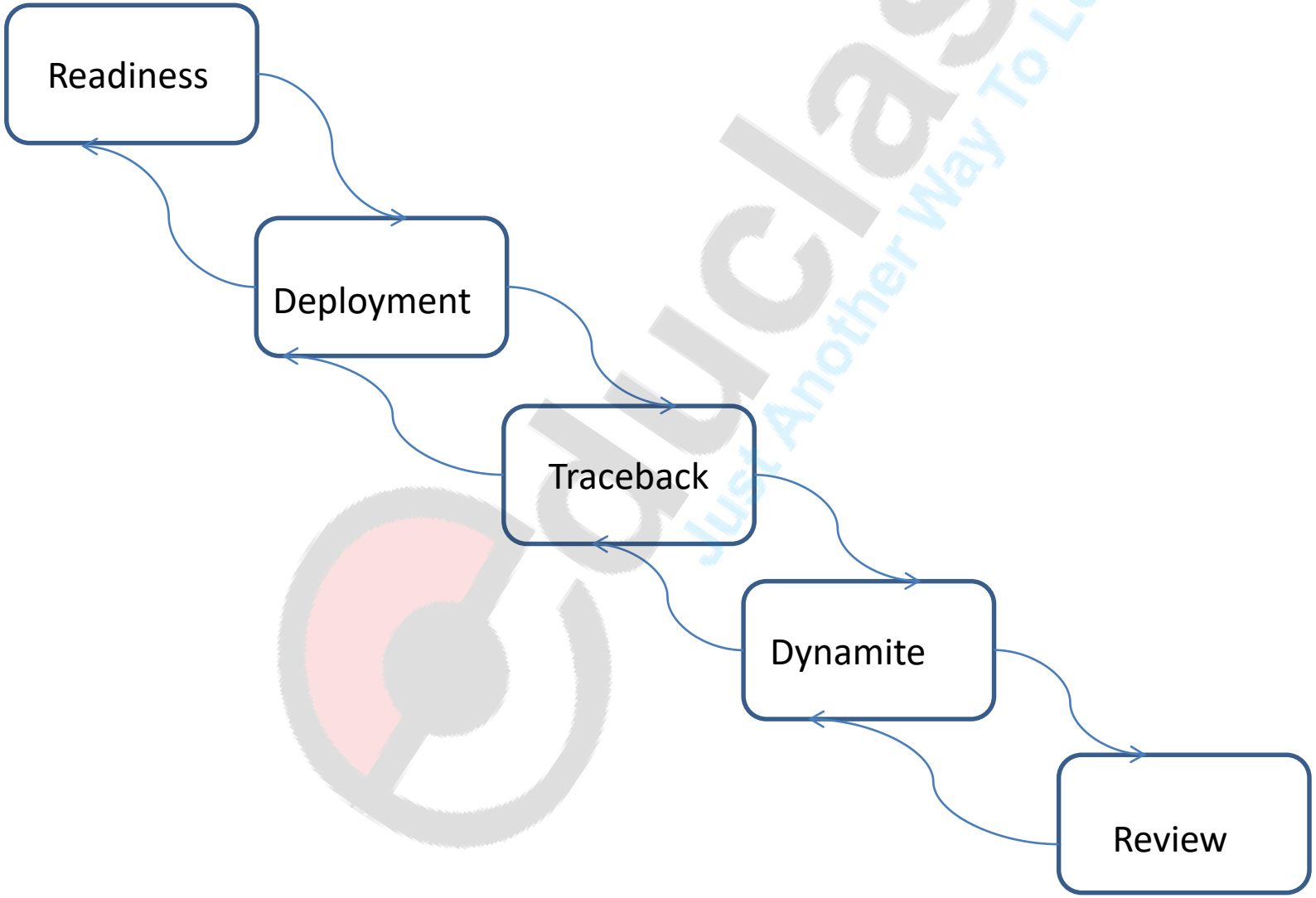
The above model designed by W.H. Kruse and J. Feiser with three main phase as follows.

1. Acquire the evidence without modifying or impairing the original.
2. Authenticate the evidence gathered against the original image.
3. Analyze the obtained evidence image without adulteration.

Model 2: A Road Map for Digital Forensic Research DFRWS

It is developed by Palmer with indexed process such as 1.identification 2. preservation 3. Collection 4.Examination 5.Analysis 6.Presentation

Model 3: Enhanced Integrated Digital Investigation Process (EIDIP) developed by Baryamureeba and Tushabe. The phases as follows



1. Readiness phase includes the training and coaching of personnel. It also involves establishing necessary infrastructure to deal with investigation.
2. Deployment phases involves providing instruments to detect incidents and affirm such incidents. In this phase it identify the incident and notify the concerned authority. Crime scene examined and critical evidence is gathered . And this evidence does to digital examination. After legal approval , search warrant issue and evidence submitted to valid authority.
3. In the trace back phase , the device use in criminal activites are obtained as evidence.