KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University)

(Established Under Section 3 of UGC Act, 1956)

Coimbatore-21

Department of Computer Science, Applications and Information Technology

M.Sc. Computer Science

Semester-II

19CSP202	**CYBER SECURITY**	**4H – 4C**

Instruction Hours / week: L: 4 T: 0 P: 0 **Marks:** Int : **40** Ext : **60** Total: **100**

COURSE OBJECTIVE

- To provides an overview of Information Security and Assurance.
- To provide an exposure to the spectrum of security activities methods methodologies and procedures with emphasis on practical aspects of Information Security.

COURSE OUTCOME

A student who successfully completes this course should at a minimum be able to:

- State the basic concepts in information security
- Explain concepts related to applied cryptography including the four techniques for crypto-analysis symmetric and asymmetric cryptography, digital signature, message authentication code, hash functions and modes of encryption operations.
- Explain common vulnerabilities in computer programs including buffer overflow Vulnerabilities time-of-check to time-of-use flaws incomplete mediation.

UNIT-I

Introduction to cybercrime: Introduction-Cybercrime: Definition and Information Security-who are cybercriminals? - Classification of cybercrimes. Cybercrime: The legal perspectives-cybercrimes: An Indian Perspective - cybercrime and the Indian ITA2000: Hacking and the Indian law(s) - A Global Perspective on cybercrimes: cybercrime and the Extended Enterprise - cybercrime Era: Survival Mantra for the Netizens - Concluding Remarks and Way Forward to Further Chapters.

UNIT-II

Cyber offenses: How Criminals Plan Them: Introduction: categories of Cybercrime -How criminals Plan the Attacks: Reconnaissance Passive Attacks Active Attacks Scanning and Scrutinizing Gathered Information Attack(Gaining and Maintaining the system Access) - social Engineering: Classification of Social Engineering – Cyber talking: Types of stalkers Cases Reported on Cyber stalking How stalking Works? real-life incident of Cyber stalking - Cybercafe and Cybercrimes - Botnets: The Fuel for cybercrime: Botnet - Attack Vector-Cloud Computing: Why cloud computing? Types of Services Cybercrime and Cloud Computing.

UNIT-III

Cybercrime: Mobile and wireless Devices-Introduction - Proliferation of Mobile and Wireless Devices - Trends in Mobility-Credit Card Frauds in Mobile and Wireless Computing Era: Types and Techniques of Credit Card Frauds - Security challenges Posed by Mobile Devices - Registry Settings for Mobile Devices - Authentication Service security: cryptographic security LDAP Security RAS Security Media Player Control Security Networking API Security - Attacks on Mobile/Cell Phones: Mobile Phone Theft Mobile Viruses Mishing Vishing Smishing Hacking Bluetooth.

UNIT-IV

Mobile Devices: Security Implication for Organizations – Managing Diversity and Proliferation of Hand-Held Devices Unconventional/ Stealth Storage Devices Threats through Lost and Stolen Devices Protecting Data on lost devices Educating the Laptop Users - Organizational Measures for Handling Mobile devices - Related Security Issues: Encrypting Organization Databases Including Mobile Devices in Security Strategy -Organizational Security Policies and Measures in mobile Computing Era: Importance of Security polices relating to mobile Computing Devices Operating Guidelines for Implementing Mobile Devices Security Polices Organizational Policies for the Use of Mobile Hand - Held Devices - Laptops: Physical Security Countermeasures.

UNIT-V

Tools and Methods Used in Cybercrime: Introduction - Proxy Servers and Anonymizers - Phishing: How Phishing Works? - Password Cracking: Online Attacks Offline Attacks Strong Weak and Random Passwords Random passwords - Keyloggers and Spywares: Software Keyloggers Hardware Keyloggers Anti Keylogger Spywares - Virus and Worms: Types of Virus - Trojan Horses and Backdoors: backdoor How to protect from Trojan Horses and Backdoors - Steganography: Steganalysis - DoS and DDoS Attacks: DoS AttacksClassification of DoS Attacks Types or Levels of DoS Attacks Tools Used to Launch DoS Attacks DDoS Attacks How to Protect from DoS/DDoS Attacks – SQL Injection: Steps for SQL Injection Attacks How to Prevent SQL Injection Attacks - Buffer Overflow: Types of Buffer Overflow How to Minimize Buffer Overflow - Attacks on Wireless Networks: Traditional Techniques of Attacks on Wireless Networks Theft of Internet Hours and Wi-fi-based Frauds and Misuses How to Secure the Wireless Networks.

SUGGESTED READINGS

1.Nina Godbole & SUNIT Belapure. (2013). CYBER SECURITY. New Delhi: Wiley India Pvt. Ltd.
2.Charles ,P. Pfleeger ,& Shari, L. Pfleeger. (2003).
3.Dieter Gollmann . (2006). Computer Security (2nd ed.). John Wiley & Sons.
Godbole, N. (2009).
4.Information Systems Security: Metrics Frameworks and Best Practices. New Delhi: Wiley India.
5.Marther, T., Kumaraswamy, S.,& Latif, S. (2009). Cloud Security and Privacy: An Enterprise Perceptive on Risk and Complaince. O'Reilly.

WEB SITES

1. http://www.csc.ncsu.edu/faculty/ning
2. csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

www2.warwick.ac.uk/fac/sci/dcs/teaching/modules/cs134/

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University)
(Established Under Section 3 of UGC Act, 1956)
DEPARTMENT OF CS, CA & IT
LESSON PLAN

STAFF NAME: Dr.Mohankumar M
SUBJECT NAME: Cyber Security **SUBJECT CODE: 19CSP202**
SEMESTER: II **CLASS: I M.Sc CS**

S.No	Lecture Duration (Period)	TOPICS TO BE COVERED	Support Materials/Page No's
		UNIT I	
1	1	Introduction -cybercrime: Definition and information security- who are cybercriminals?Classification of Cybercrimes	T1:1-16
2	1	E-mail spoofing,Spamming,Cyberdefamation,Internet Time Theft	T1:17-21
3	1	Salami Attack/Salami Technique,Data Diddling,Forgery, Web jacking-Newsgroup spam/crimes emanating from usenet newsgroup	T1:21-22
4	1	Industrial spying/Industrial Espionage,Hacking,online frauds,prnographic offenses	T1:22-27
5	1	software piracy,computer sabotage,e-mail bombing,usenetnewsgroup,computer network intrusions	T1:28-30
6	1	password sniffing, credit card frauds,identity theft,cybercrime: The legal perspectives an indian perspectives- Cybercrime and the indian ITA 2000(Hacking and the indian laws)	T1:30-34
7	1	A global perspective on Cybercrimes,Cyber crime and the extended enterprise,Cyber crime Era: survival mantra for the netizens	T1:36-39
8	1	Recapitulation and discussion of important question's	
Total no of periods planned for unit I	8		
		UNIT-2	
1	1	Introduction :cyberoffenses:How criminals plan Them-Categories of Cybercrime	T1:45
2	1	How criminals plan the Attacks:Reconnaissance,Passive Attacks	T1:49-50
3	1	Active Attacks,Scanning and scrutinizing Gathered information- Attack(gaining and maintaining the system Access) social Engineering :classification of social engineering	T1:54-62
4	1	cyberstalking:Types of Stalkers Case reported on cyberstalking,how stalking works	T1:65-66
5	1	Real life incident of cyberstalking-Cybercafe and Cybercrimes-Botnets:The fuel for Cybercrime- Botnets,Attack Vector	T1:67-73
6	1	Cloud computing:why cloud computing?-Types of	T1:75-76,77

		services,cybercrime and cloud computing	
Total no of periods planned for unit II	6	Recapitulation and discussion of important question's	
UNIT-3			
1	1	Introduction of Cybercrime :mobile and wireless Devices-Proliferation of mobile and wireless devices	T1:81-82
2	1	Trends in mobility-Credit card frauds in mobile and wireless computing era-Types and Techniques of credit card frauds	T1:84-87,88
3	1	Security Challenges posed by mobile devices, Registry settings for mobile devices	T1:91-92
4	1	Authentication Service Security,Cryptographic security- LDAP Security,RAS Security	T1:93-95
5	1	Media player control Security and Networking API Security,Attacks on Mobile/Cell Phones:mobile phone Theft	T1:98,99
6	1	Mobile Viruses,MishingVishing,smishing,Hacking bluetooth	T1:101-105
7	1	Recapitulation and discussion of important question's	
Total no of periods planned for unit III	7		
UNIT-4			
1	1	Mobile Devices:Security Implications for Organizations-Managing diversity and proliferation of Hand -Held Devices	T1:107
2	1	Unconventional/steath Storage Devices	T1:108
3	1	Threats through lost and stolen Devices-Protecting Data on Lost Devices,Educating the laptop users	T1:110,111
4	1	Organizational measures for handling mobiledevices related security issues	T1:112
5	1	Encrypting organizational databases-Including mobile devices in security strategy	T1:113
6	1	organizational security policies and measures in mobile computing era-Importance of security policies relating to mobile computing devices	T1:114
7	1	Operating guidelines for implementing mobile device security policies	T1:115
8	1	organizational policies for the use of mobile hand held devices-Laptops -physical security countermeasures	T1:116-117
9	1	Recapitulation and discussion of important question's	
Total no of periods planned for unit IV	9		
UNIT-5			
1	1	Introduction of Tools and Methods used in Cybercrime	T1:125
2	1	Proxy Servers and anonymizers-phishing: how phishing works,Password Cracking-online attacks,offline attacks	T1:129,131,134
3	1	Strong,weak and random passwords-Keyloggers and Spywares-Software keyloggers-Hardware keyloggers antikeyloggers,Spywares	T1:135,137,140

4	1	virus and worms:Types of virsus- Trojan horses and back doors, backdoor,how to protect from trojan horses and back doors	T1:143-153
5	1	Steganography -steganalysis -Dos and Ddos attacks -Dos Attacks-Classification of Dos attacks Types or levels of Dos Attacks	T1:155-158
6	1	Tools used to launch dos Attack Ddos Attacks How to protect fromDos/Ddos Attacks	T1:159-163
7	1	Sql injection-Steps for Sql Injection Attack- How to prevent Sql Injection Attacks	T1:164-167
8	1	Buffer overflow-Types of Buffer overflow,How to minimize Buffer overflow-Attacks on Wireless Networks	T1:168-171
9	1	Traditional Techniques of Attacks on Wireless Networks-Theft of internet hours and wifi based frauds and misuses-How to secure the wirless networks	T1;176,177,179
10	1	**Previous End Semester Question paper Discussion**	
Total no of periods planned for unit V	10		
Total Planned hrs	40		

TEXT BOOKS:

1. Nina Godbole and sunit Belapure,2013 Cyber Security .Wiley India pvt .Ltd.

REFERENCE BOOKS:

1. Charles p.Pfleeger and Shari l.Pfleeger.2003 security in computing,Pearson Education.
2. Dieter Gollmann.2006.Computer Security.2nd Edition.John Wiley & sons.
3. Godbole,N.(2009)Information Systems Security:Metrics,Frameworks and Best practices, Wiley India,New Delhi.
4. T.Marther,S.Kumaraswamy and S.Latif(2009),Cloud Security and privacy:An enterprise perceptive on Risk and compliance,O'Reilly

WEB SITES

1. https://www.csc.ncsu.edu/Faculty/ning-
2. csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
3. www2.warwick.ac.uk/fac/sci/dcs/teaching/modules/cs134/

UNIT-I
SYLLABUS

Introduction- cybercrime: Definition and information security, **Who are cyber criminals?, Classification of cybercrimes:** E-Mail Spoofing, spamming, cyber defamation, internet time theft, salami attack, data diddling, forgery, news group, industrial spying, hacking, online frauds, use net group, passwords sniffing, credit card fraud, identity theft, **The legal perspectives, An Indian perspective , Cybercrime and the Indian ITA 2000, A global perspective on cybercrimes:** Cybercrime and the extended enterprise, **Cybercrime Era:** Survival Mantra for the Netizens

Introduction to cybercrime:

- First recorded cybercrime place in year 1820.
- Indian corporate and government websites attacked or defaced more than 780 times between February 2000 and December 2002.
- Third December 2009,286 Indian websites rare hacked in 5 months between January and June 2009.
- Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cyber security addresses cybercrime as one major challenge underlines this.
- Cyber security plays an important role in the ongoing development of information technology, as well as Internet services.
- Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being.
- Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy.
- Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy.
- In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures.
- At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens.
- At the regional and international level, this entails cooperation and coordination with relevant partners.

- The formulation and implementation of a national framework and strategy for cyber security thus requires a comprehensive approach.
- Cyber security strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime.
- The development and support of cyber security strategies are a vital element in the fight against cybercrime.
- The legal, technical and institutional challenges posed by the issue of cyber security are global and far- reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation.
- In this regard, the World Summit on the Information Society (WSIS) recognized the real and significant risks posed by inadequate cyber security and the proliferation of cybercrime describing the multi stakeholder implementation process according to eleven action lines and allocating responsibilities for facilitating implementation of the different action lines.
- At WSIS, world leaders and governments designated ITU to facilitate the implementation of WSIS Action Line C5, dedicated to building confidence and security in the use of ICTs.
- In this regard, the ITU Secretary-General launched the Global Cyber security Agenda (GCA) on 17 May 2007, alongside partners from governments, industry, regional and international organizations, academic and research institutions.
- The GCA is a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cyber security and to enhance confidence and security in the information society.
- It builds on existing work, initiatives and partnerships with the objective of proposing global strategies to address today's challenges related to building confidence and security in the use of ICTs. Within ITU, the GCA complements existing ITU work programmes by facilitating the implementation of the three ITU Sectors' cyber security activities, within a framework of international cooperation.
- The Global Cyber security Agenda has seven main strategic goals, built on five work areas:
  1) Legal measures
  2) Technical and procedural measures
  3) Organizational structures
  4) Capacity building
  5) International cooperation.
- The fight against cybercrime needs a comprehensive approach. Given that technical measures alone cannot prevent any crime, it is critical that law-enforcement agencies are allowed to investigate and prosecute cybercrime effectively.

- Among the GCA work areas, "Legal measures" focuses on how to address the legislative challenges posed by criminal activities committed over ICT networks in an internationally compatible manner.
- "Technical and procedural measures" focuses on key measures to promote adoption of enhanced approaches to improve security and risk management in cyberspace, including accreditation schemes, protocols and standards.
- "Organizational structures" focuses on the prevention, detection, response to and crisis management of cyber attacks, including the protection of critical information infrastructure systems.
- "Capacity building" focuses on elaborating strategies for capacity-building mechanisms to raise awareness, transfer know-how and boost cyber security on the national policy agenda.
- Finally, "International cooperation" focuses on international cooperation, dialogue and coordination in dealing with cyber threats.
- The development of adequate legislation and within this approach the development of a cybercrime- related legal framework is an essential part of a cyber security strategy.
- This requires first of all the necessary substantive criminal law provisions to criminalize acts such as computer fraud, illegal access, data interference, copyright violations and child pornography.
- The fact that provisions exist in the criminal code that are applicable to similar acts committed outside the network does not mean that they can be applied to acts committed over the Internet as well.
- Therefore, a thorough analysis of current national laws is vital to identify any possible gaps.
- Apart from substantive criminal law provisions, the law-enforcement agencies need the necessary tools and instruments to investigate cybercrime.
- Such investigations themselves present a number of challenges.60 Perpetrators can act from nearly any location

Cybercrime definition:

- A crime conducted to which a computer was directly and significantly instrumented
- Cybercrime is any illegal behaviour directed by needs of electronics operations that targets security of computer system and the data processed by them.
- A crime commit using a computer and the internet to send a person (identity theft-particular person theft) or send contra band or stalk victims or distracts operations with programs.

Cyber security:

- There are 2 types of attack are prevalent
    1. Techno-crime
    2. Techno- vandalism

1. **Techno-crime:**
- In the techno crime consists of data theft, data delete, copy, preventions, corrupt, deface or damage

2. **Techno-vandalism:**
- These acts of brainless defacement.
- These acts of brainless defacement of website and are others activities such as copying files and publishing their contents.
- Publically are mutually in nature.

Who are Cybercrimes:

- Cybercrime involves such activities as credit card fraud; cyber stalking; defaming another online; gaining unauthorized access to computer systems; ignoring copyright. Software licensing and trade mark protecting; overriding encryption to make illegal copies; software piracy and stealing another's identity to perform criminal acts
- Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cyber security addresses cybercrime as one major challenge underlines this.
- Cyber security plays an important role in the ongoing development of information technology, as well as Internet services.
- Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being.
- Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy.
- Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy.
- In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures.
- At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of

3 types

Type1: Cyber criminals- Hungry for recognition

- Hobby hackers
- It professionals
- Politically motivated hackers
- Terrorist or organization

Type2:

- Not interested in recognition
- Psychological perverts
- Financially motivated hackers

State- sponsored

Type3:

- The insiders(employee)
- Disgruntled or former employees seeking revenge
- Competing companies using employees to gain economic advantage through data and or theft.
- Thus, the typical "motives" behind cybercrime seem to be greed, desire to gain power and/or publicity, desire for revenge, a sense of adventure, looking for thrill to access forbidden information, destructive mind set and desire to sell network security services

Classification of cybercrimes:

- Crime is defines 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 offender liable to punishment by the law"
- Cybercrimes are classified as follows:

1. Cybercrime against individuals:

- Electronic mail- spoofing and another frauds
- Phishing, Spear Phishing and its various others form such as Vishing and Smishing
- Computer-related fraud is one of the most popular crimes on the Internet, as it enables the offender to use automation and software tools to mask criminals' identities.
- Automation enables offenders to make large profits from a number of small acts. One strategy used by offenders is to ensure that each victim's financial loss is below a certain limit.
- With a "small" loss, victims are less likely to invest time and energy in reporting and investigating such crimes.504 One example of such a scam is the Nigeria Advanced Fee Fraud.
- Although these offences are carried out using computer technology, most criminal law systems categorize them not as computer-related offences, but as regular fraud.
- The main distinction between computer- related and traditional fraud is the target of the fraud.
- If offenders try to influence a person, the offence is generally recognized as fraud.
- Where offenders target computer or data-processing systems, offences are often categorized as computer-related fraud. Those criminal law systems that cover fraud, but do not yet include the manipulation of computer systems for fraudulent purposes, can often still prosecute the above-mentioned offences.
- The most common fraud offences include online auction fraud and advanced fee fraud.

2. Email spoofing:

- Hacking the mail.

- A spoofed email is one that appears to originate from one source but actually has been sent from another source
- Comparing different regional approaches (such as the CoE Convention on Cybercrime , the EU Framework Decision on Attacks against Information Systems, the Draft African Union Convention on Cyber Security and HIPSS, HIPCAR and ICB4PAC) to addressing concrete offences (e.g. illegal access) shows a large degree of consistency in the prescribed approach and methodology.
- All follow international best practices and it was therefore possible to use the model law developed by Caribbean experts as basis for the development of the HIPSSA and ICB4PAC model framework.
- In advance fee fraud, offenders send out e-mails asking for recipients' help in transferring large amounts of money to third parties and promise them a percentage, if they agree to process the transfer using their personal accounts.
- The offenders then ask them to transfer a small amount to validate their bank account data (based on a similar perception as lotteries – respondents may be willing to incur a small but certain loss, in exchange for a large but unlikely gain) or just send bank account data directly.
- Once they transfer the money, they will never hear from the offenders again. If they send their bank account information, offenders may use this information for fraudulent activities. Evidence suggests that thousands of targets reply to e-mails.
- Current researches show that, despite various information campaigns and initiatives, advance fee frauds are still growing – in terms of both the number of victims and total losses.

3. Spamming:

- Junk files anonomous
- People who create electronic spam are called spammers.
- Spam is the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately
- Although the most widely recognized from of spam is email spam, the team 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, video sharing sites.
- 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 unsolicited mail has become very high because the barrier to entry is low

- The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, who are forced to add extra capacity to cope with the deluge
- Spamming is widely detested, and has been the subject of legislation in many jurisdictions- for example , the CAN-SPAM Act of 2003
- Another definition of spamming is in the context of "search engine spamming". In this context, spamming is alteration or creation of a document with the intent to device an electronic catalog or a filling systems.
- Those who continually attempt to subvert or spam the search engines may be permanently excluded from the search index.
- Therefore, the following web publishing techniques should be avoided:
  1. Repeating key words
  2. Use of keywords that do not relate to the content on the site
  3. Use of fast meta refresh
  4. Redirection
  5. IP Cloaking
  6. Use of colored text on the same colour background
  7. Tiny text usage
  8. Duplication of pages with different URL's
  9. Hidden links
  10. Use of different pages that bridge to the same URL

4. Cyber defacement:

- Fake news(rumours),rollel type of activity
- Cyber defamation happens when the above takes place in an electronic form.
- Cyber defacement 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 email containing defamatory information to all friends of that person.
  1. It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives
  2. It many amount to defamation to make an imputation concerning a company or an association or collection of persons such as
  3. An imputation in the form of an alternative or expressed ironically, may amount to defamation
  4. No imputation is said to harm a person's reputation unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character person, or lowers the character of that person in respect, or lower the credit of that person, or causes it to believed that the body of that person is in a loathsome state or in state generally considered as disgraceful

- Libel is written defamation and slander is oral defamation. When determining whether or not defamation has taken place, the only issue to consider is whether a person of ordinary intelligence in society would believe that the words would indeed injure the person's reputation
- Even if there is no damage to a person's reputation, the person who made the allegations may still be held responsible for defamation

5. **Internet time theft:**
   - Banner's
   - 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 passwords, either by hacking or 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 identity time theft if the internet time has to be recharged often, even when one's own use of the internet is not frequent
   - The issue of internet time theft is related to the crimes conducted through "identity theft"
6. **Salami attack:**
   - Fully related to financial transaction.
   - Small changes to financial transaction do some problems may be occurred.
   - The attacks are used for committing financial crime. The idea here is to make 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 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. **Data diddling:**
   - Small changes.
   - A data diddling 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
8. **Forgery:**
   - To theft the data.
   - Counterfeit currency notes, postage and revenue stamps, mark sheets, etc. can be forged using sophisticated computers, printers and scanners
   - Outside many colleges there are miscreants soliciting the sale of fake mark sheets or even degree certificates

- These are made using computers and high quality scanners and printers
- In fact, this is becoming a booming business involving large monetary amount given to student gangs in exchange for these bogus but authentic certificates

9. Web jacking:

- To control other parties.
- Web jacking occurs when someone forcefully takes control of a website
- 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

10. News group spam:

- Fake news to spread other resources
- The word "spam" was usually taken to mean excessive multiple posting
- 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 email spam
- The newsgroups posting Bot Serdar Argic also appeared in early 1994, posting tens of thousands of messages to various newsgroups, consisting of identical copies of a political screed relating to the Armenian Genocide

11. Industrial Spying/ Industrial Espionage:

- Spying is not limited governments. Corporations, like governments, often spy on the enemy
- The internet and privately networked systems provide new and better opportunities for espionage
- 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 escrow organizations
- With the growing public availability of Trojans and spyware material , even low-skilled individuals are now inclined to generate high volume profit out of industrial spying
- This is referred to as "targeted attacks". This aspects of industrial spying is the one to be addressed in the fight against cybercrime
- Organizations subject to online extortion tend to keep quiet about it to avoid negative publicity about them
- There are also the email worms automating similar "data exfiltration features". Such files are uploaded on an FTP server owned by the cyber crooks, with the aim of stealing as much IP as possible wherever it can be and then selling it to people who are ready to pay it.

- There are two distinct business models for cybercrime applied to industrial spying: Selling Trojan-ware and Selling Stolen Intellectual Property

12. Hacking:

- Hack the user's details
- Although the purpose of hacking are many, the main ones are as follows:
  1. Greed
  2. Power
  3. Publicity
  4. Revenge
  5. Adventure
  6. Desire to access forbidden information
  7. Destructive mind set
     - Every act committed toward breaking into a computer and/or network is hacking and it is an offences.
     - Hackers, write or use ready-made computer programs to attack the target computer
     - They possess the desire to destruct and they get enjoyment out of such destruction
     - Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money
     - They extort money from some corporate giant threatening him to publish the stolen information that is critical in nature
     - Hackers, crackers and phrackers are some of the oft-heard teams. The original meaning of the word "hack" meaning an elegant, witty or inspired way of doing almost anything originated at MIT

13. Online frauds:

- Online theft.
- Spoofing websites and emails security alerts, hoax mails about virus threats lottery frauds and spoofing
- In spoofing websites and email security threats, fraudsters create authentic looking websites that are actually nothing but a spoof
- The purpose of these websites is to make the user enter personal information which is then used to access business and bank account
- Fraudsters are increasingly turning to email to generate traffic to these websites. This king of online fraud is common in banking and financial sector
- It is strongly recommended not to input any sensitive information that might help criminals to gain access to sensitive information, such as bank account details, even if the page appears legitimate

- Online auctions are now one of the most popular e-commerce services. Already back in 2006, goods worth more than USD 20 billion were sold on eBay, the world's largest online auction marketplace.
- Buyers can access varied or specialist niche goods from around the world. Sellers enjoy a worldwide audience, stimulating demand and boosting prices.
- Offenders committing crimes over auction platforms can exploit the absence of face-to-face contact between sellers and buyers.
- The difficulty of distinguishing between genuine users and offenders has resulted in auction fraud being among the most popular of cybercrimes.
- The two most common methods include offering non-existent goods for sale and requesting buyers to pay prior to delivery and buying goods and asking for delivery, with no intention of paying.
- In response, auction providers have developed protection systems such as the feedback/comments system.
- After each transaction, buyer and sellers leave feedback for use by other users513 as neutral information about the reliability of sellers/buyers. In this case, "reputation is everything" and without an adequate number of positive comments, it is harder for offenders to persuade targets to either pay for non-existent goods or, conversely, to send out goods without receiving payment first.
- However, criminals have responded and circumvented this protection through using accounts from third parties.
- In this scam called "account takeover",offenders try to get hold of user names and passwords of legitimate users to buy or sell goods fraudulently, making identification of offenders more difficult.

14. Use net groups:

- Sharing of particular message.
- Usenet is a popular means of sharing and distributing information on the web with respect to specific topic or subjects
- It is feasible to block specific news-groups, however, this cannot be considered as a definitive solution to illegal or harmful content.
- It is possible to put Usenet to following criminals use:
  1. distribution
  2. distribution/ sale of pirated software package
  3. distribution of hacking software
  4. sale of stolen credit card numbers
  5. sale of stolen data/ stolen property

15. Password sniffing:

- To product our password
- 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 setup adequately prosecute a person for impersonating another person online
- Laws designed to prevent unauthorized access to information may be effective in apprehending cracker using sniffer programs

15. Credit card frauds:

- Through fraud using credit card
- Information security requirements for anyone handling credit cards have been increased dramatically recently
- Millions of dollars may be lost annually by consumers who have credit card and calling cards numbers stolen from online database
- Security measures are improving, and traditional methods of law enforcement seem to be sufficient for prosecuting the thieves of such information
- Such attacks usually result in the implementation of stronger security systems

16. Identity theft:

- Information theft after that the hacker use the information in on use.
- The term identity theft – which is neither consistently defined nor consistently used – describes the criminal act of fraudulently obtaining and using another person's identity.
- These acts can be carried out without the help of technical means as well as online by using Internet technology.
- Wide media coverage, the results of various surveys analysing the extent of and loss caused by identity theft, as well as numerous legal and technical analyses published in recent years could easily lead to the conclusion, that identity-related offences are a 21st-century phenomenon.
- But this is not the case, as offences related to impersonation and the falsification and misuse of identity documents have existed for more than a century.
- Already back in the 1980s, the press intensively reported on the misuse of identity-related information.
- The emerging use of digital identities and information technology only changed the methods and targets of the offenders.
- Increasing use of digital information opened up new possibilities for offenders to gain access to identity-related information.
- Thus, the transformation process from industrialized nations to information societies has had a big influence on the development of identity-theft offences.
- Nonetheless, despite the large number of Internet-related identity-theft cases, digitization did not fundamentally change the offence itself, but merely created new targets and facilitated the development of new methods.

- The impact of the increasing use of Internet technology seems to be overestimated.
- Based on the results of a method analysis of identity-related offences, identity theft to a large degree remains an offline crime.
- In 2007, 20 per cent of the offences in the US542 were online scams and data breaches.
- Despite recent developments the offline identity theft remains highly relevant. The persisting importance of offline crimes is surprising, insofar as the digitization and moreover the globalization of network-based services has led to increasing use of digital identity- related information.
- Identity-related information is of growing importance, both in the economy and in social interaction. In the past, a "good name" and good personal relations dominated business as well as daily transactions.
- With the transfer to electronic commerce, face-to-face identification is hardly possible, and as a consequence identity-related information has become much more important for people participating in social and economic interaction.
- This process can be described as instrumentalization, whereby an identity is translated into quantifiable identity-related information.
- This process, along with the distinction between the more philosophical aspect of the term "identity" and the quantifiable identity-related information that enables the recognition of a person, is of great importance.
- The transformation process is not just relevant to Internet-related features of identity theft, as the impact of the development goes far beyond computer networks.
- Nowadays, the requirements of non-face-to-face transactions, such as trust and security, dominate the economy in general and not just e-commerce businesses.
- An example is the use of payment cards with a PIN (personal identification number) for purchasing goods in a supermarket.
- In general, the offence described as identity theft contains three different phases.
- In the first phase the offender obtains identity-related information. This part of the offence can for example be carried out by using malicious software or phishing attacks.
- The second phase is characterized by interaction with identity-related information prior to the use of the information within criminal offences.
- An example is the sale of identity-related information. Credit-card records are for example sold for up to USD
- The third phase is the use of the identity-related information in relation with a criminal offence. In most cases, the access to identity-related data enables the perpetrator to commit further crimes.
- The perpetrators are therefore not focusing on the set of data itself but the ability to use the data in criminal activities.

- Examples for such offence can be the falsification of identification documents or credit-card fraud.

Legal perspectives:

- First criminals justies resource manual 1978
- Computer related crimes any illegal for which knowledge of computer technology is essential for a successful proetution.
- International aspect for computer crime study in1983.
- Proper legislation is the foundation for the investigation and prosecution of cybercrime.
- However, law- makers must continuously respond to Internet developments and monitor the effectiveness of existing provisions, especially given the speed of developments in network technology.
- Historically, the introduction of computer-related services or Internet-related technologies has given rise to new forms of crime, soon after the technology was introduced.
- One example is the development of computer networks in the 1970s – the first unauthorized access to computer networks occurred shortly afterwards.
- Similarly, the first software offences appeared soon after the introduction of personal computers in the 1980s, when these systems were used to copy software products.
- It takes time to update national criminal law to prosecute new forms of online cybercrime.
- Indeed, some countries have not yet finished with this adjustment process. Offences that have been criminalized under national criminal law need to be reviewed and updated.
- For example, digital information must have equivalent status as traditional signatures and printouts.
- Without the integration of cybercrime-related offences, violations cannot be prosecuted.
- The main challenge for national criminal legal systems is the delay between the recognition of potential abuses of new technologies and necessary amendments to the national criminal law.
- This challenge remains as relevant and topical as ever as the speed of network innovation accelerates.
- Many countries are working hard to catch up with legislative adjustments. In general, the adjustment process has three steps: adjustment to national law, identification of gaps in the penal code, and drafting of new legislation.
- Specific departments are needed within national law-enforcement agencies, which are qualified to investigate potential cybercrimes.
- The development of computer emergency response teams (CERTs), computer incident response teams (CIRTs), computer security incident response teams (CSIRTs) and other research facilities have improved the situation.

- To ensure effective legislative foundations, it is necessary to compare the status of criminal legal provisions in the national law with requirements arising from the new kinds of criminal offences.
- In many cases, existing laws may be able to cover new varieties of existing crimes (e.g. laws addressing forgery may just as easily be applied to electronic documents).
- The need for legislative amendments is limited to those offences that are omitted or insufficiently covered by the national law.
- Based on experience, it may be difficult for national authorities to execute the drafting process for cybercrime without international cooperation, due to the rapid development of network technologies and their complex structures.
- Drafting cybercrime legislation separately may result in significant duplication and waste of resources, and it is also necessary to monitor the development of international standards and strategies.
- Without the international harmonization of national criminal legal provisions, the fight against transnational cybercrime will run into serious difficulties, due to inconsistent or incompatible national legislations.
- Consequently, international attempts to harmonize different national penal laws are increasingly important.
- National law can greatly benefit from the experience of other countries and international expert legal advice.
- he second situation in which law-enforcement agencies are allowed to access stored computer data outside their territory is when the investigators have obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data. This authorization is heavily criticized.2508
- One main concern is the fact that the provision in its current wording probably contradicts fundamental principles of international law.
- Based on international law, investigators have to respect national sovereignty during an investigation.
- They are especially not allowed to carry out investigations in another state without the consent of the competent authorities in that state.
- The decision whether such permission should be granted is not in the hands of an individual, but of the state authorities, since interference with national sovereignty does not only affect the rights of the individual, but also state concerns.
- By ratifying the Convention on Cybercrime, countries partly dismiss the principle and allow other countries to carry out investigations affecting their territory.
- Another concern is the fact that does not define procedures for the investigation.
- Based on the text of the provision, it is not necessary for the same limitations to be applied that exist in domestic law with regard to comparable domestic investigations. Interestingly enough, such a restriction was included in the draft text of the Convention on Cybercrime presented in the beginning of 2000

Globalization:

- Globalized information is done an interesting number of Transe national offences

Cybercrime Indian perspectives:

- Fourth highest number of internet users in the world.
- There are 45 billion internet resources in India.
- 37% cyber café-browsing center-remaining 1990's internet not is usually. 57%(18 to 35 years old)
- Mobile internet used only
- Information technology act recorded the cybercrime 50% in the year 2007 recorded.
- Related in 46% to cyber pornography followed by hacking.
- In over 60% of the layers affentere between 18 to 30 of the years according to the crime in 2007 report of the national crime record.

Cybercrime and Indian ITA 2000:

- ITA 2000 in acted after the united nation journal assembly resolution in January 30,1997 by adopting the model law electronic commerce adopted by united nations commission on international trade law.
- It was enacted into consideration UNICITRAL modes of law on electronic commerce in year 1996.

Hacking and Indian law:

- Cybercrime are punishable under the 2 categories
- ITA 2000 and the IPC
- A total of 207 the cases of cybercrimes were registered under the ITA 2007 compared to cases registered in 2006 under the IPC to 339 where recorded in 2007 compare with 3x11 cases in 2006.
- The identification of illegal content is a challenge for the hosting provider. Especially for popular providers with many websites, manual searches for illegal content on such a great number of websites would be impossible. As a result, the drafters of the Directive decided to limit the liability of hosting providers.
- However, unlike in the case of the access provider, the liability of the host provider is not excluded.
- As long as the host provider has no actual knowledge of illegal activities or illegal content stored on its servers, it is not liable.
- Here, an assumption that illegal content could be stored on the servers is not considered equivalent to actually having knowledge of the matter.
- If the provider obtains concrete knowledge about illegal activities or illegal content, it can only avoid liability if it immediately removes the illegal information. Failure to react immediately will lead to liability of the hosting provider.

- Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communications technologies, and use regional and international conventions, arrangements and precedents in these reviews.
- Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime.
- Determine the current status of national cybercrime authorities and procedures, including legal authorities and national cybercrime units, and the level of understanding among prosecutors, judges and legislators of cybercrime issues
- Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally.
- Examine national participation in international efforts to combat cybercrime, such as the round-the- clock Cybercrime Point of Contact Network.
- Determine the requirements for national law enforcement agencies to cooperate with international counterparts to investigate transnational cybercrime in those instances in which infrastructure is situated or perpetrators reside in national territory, but victims reside elsewhere.

1. Sec -43 (penalty for damage to computer system etc.)	Punishment fine Rs.1 core
2. Sec-66 (hacking with computer system)	fine 62 lakh imprisonment for 3 years
3. Sec-67(publishing of information which is electronic form)	fine 1 lakh imprisonment of 5 years and double conviction on second offences
4. Sec-68(power of controller to give directory)	Fine up to 20 lakh and imprisonment of 3 years.
5. Sec-70(product systems) attempting or security access to computer of another person without their knowledge.	Imprisonment of up to 10 years.

6. Sec-72(penalty reach of confidentiality and privacy attempting or securing access for computer for breaking confidentiality of the information of computer)	Five up to 1 lakh and imprisonment of up to 2 years.
7. Sec-73(penalty for publishing digital signature certificate false in certain particulars(publishing false digital signature false in certain particular))	Fine 1 lakh imprisonment of 2 years
8. Sec-74(publication for fraud purpose)	Imprisonment of term 2 years and fine 1 lakh.

The intensity of the protection of religions and their symbols differs between countries.

- A number of concerns are expressed with regard to criminalization. It is pointed out in the 2006 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression that in "many countries, overbroad rules in this area are abused by the powerful to limit non-traditional, dissenting, critical, or minority voices, or discussion about challenging social issues".
- The 2008 Joint Declaration highlights that international organizations, including the United Nations General Assembly and Human Rights Council, should resist from the further adoption of statements supporting the idea of criminalizing defamation of religions.
- The question whether this requires criminalization of defamation is controversial.
- Concerns regarding the criminalization of defamation are especially related to potential conflict with the principle of "freedom of speech".
- Thus, a number of organizations have called for a replacement of criminal defamation laws.
- The UN Special Rapporteur on Freedom of Opinion and Expression and the OSCE Representative on Freedom of the Media have stated: "Criminal defamation is not a justifiable restriction on freedom of expression; all criminal defamation laws should be abolished and replaced, where necessary, with appropriate civil defamation laws".
- Despite these concerns, some countries1826 have implemented criminal law provisions that criminalize libel, as well as the publication of false information.
- It is important to highlight that even in the countries that criminalize defamation the number of cases varies considerably.

While in the United Kingdom nobody in 2004 and just one suspect in 2005 was charged with libel, the German crime statistics record defamation offences for 2006.The Council of Europe Convention on Cybercrime, the Commonwealth Model Law and the Stanford Draft do not contain any provisions directly addressing these acts.

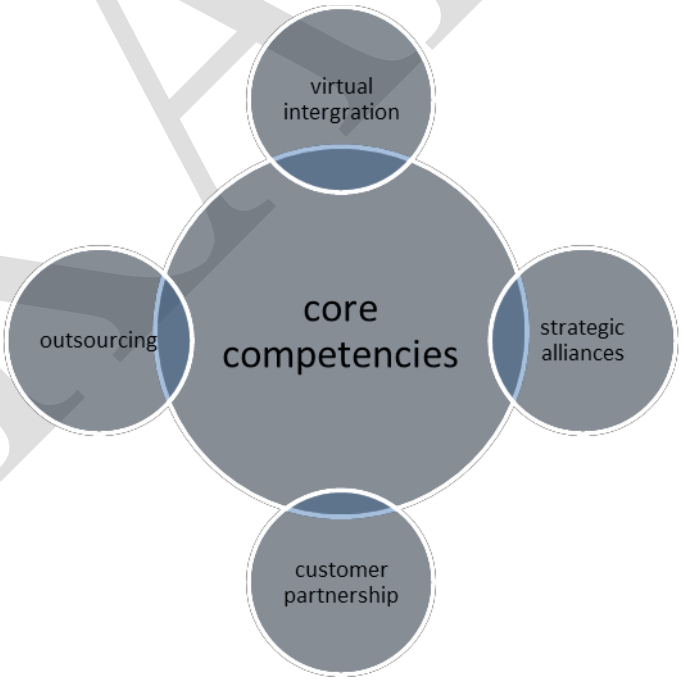
A global perspective of cybercrimes:

- In Australia cybercrime as narrow statutory meaning as used in the cybercrime ad 2001 which detail against computer data and system.
- COE's (council of eruopes)cybercrime treaty is used as a umbrella term to refer to a array of criminal activity including data and system related content and copyright offences
- Countries taking actions against spam although this status is form the ITU (International Telecommunication version) conducted in 2005.
- After intensive discussions1098 about topics and methodology of a comprehensive UNODC study related to cybercrime, the UN Member States received a questionnaire in early 2012.
- At the same time an online portal was developed. The complex questionnaire contains various questions related to different fields of cybercrime legislation such as definitions, criminalization and procedural instruments.
- Member states were requested to provide information about the status of their legislation as well as the implementation of different regional standards (such as the Convention on Cybercrime).
- In 2013 these results were submitted to the Commission on Crime Prevention and Criminal Justice
- In 2013 UNODC published the first results of the study.
- The study is the most complex so far and contains results from 69 Member States that responded.
- In addition to responses from the member states the study includes the results of the review of 500 publicly available documents and information submitted by more than 40 companies and 16 academic institutions.
- The study highlights that the reach of regional harmonization instruments – such as the Council of Europe Convention on Cybercrime – is limited. In addition the study shows that other regional instruments are equally important.
- The expert working group met in February 2013 and submitted the matter to the Commission on Crime Prevention and Criminal Justice.
- In April 2013 the Commission on Crime Prevention and Criminal Justice for the first time discussed the results of the study.
- Resolution 22/7 discusses the work done without going into detail.
- Instead the Commission calls upon the member states to review the results, asks the expert group to continue the work and requests the secretariat to translate the study into all UN languages.
- During the 23rd meeting the topic Cybercrime was addressed by various speakers.

- Despite various calls for a global harmonization the Commission did not take a decision in this regard. Instead it focusses more on capacity building by underlining the global Capacity Building Program run by UNODC

Cybercrime the extended enterprise:

- It is a continuing of that the airline user is not adquiatly educated to understanding thread and how to product one self.
- It is the responsibility of each user to become of the thread as well as the operations that connectivity and presents with the concept of extended enterprise.
- The extended enterprise can only successful if all of the component and individual have the information they need in order to business effectively and extended enterprise is a loosely coupled self organization network that combine a economic output to provide and service to the market.
- The interconnected feature of information and communication technologies security overall can only way fully promoted when the users can fully awareness of the existing thread and dangerous.
- Government and business and the international community must therefore proactively help users access information on how to product themselves.
- International co operations of the levels of government industry and consumers, business and technical throws to allow a global and co-ordinate approach to archiving global cyber security is the key.



Survival mantra for the Netizens:

- Netizens are the internet users netizes is some one whose spends considerable time online and also has a considerable presents online.
- 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
- The 5P Netizen matra for online security is:
  1. Precaution
  2. Prevention
  3. Protection
  4. Preservation
  5. Perseverance
- 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 cyber crimes
- There are also a few incidents where police have pursued false cases on innocent IT professionals
- More importantly, users must try and save any electronic information trail on their computers
  1. Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures.
  2. Elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime.
  3. Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems. 4. Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.

     5. Development of strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries.

     6. Development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas.

     7 Advice on potential framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

     - Cybercrime can be committed using only fairly basic equipment.

- Committing offences such as libel or online fraud needs nothing more than a computer and Internet access and can be carried out from a public Internet café. More sophisticated offences can be committed using specialist software tools.
- The tools needed to commit complex offences are widely available over the Internet often without charge. More sophisticated tools cost several thousand dollars.
- Using these software tools, offenders can attack other computer systems at the press of a button.
- Standard attacks are now less efficient, as protection software companies analyse the tools currently available and prepare for standard hacking attacks.
- High-profile attacks are often individually designed for specific targets.585 Software tools are available that enable the offender to carry out DoS attacks, design computer viruses, decrypt encrypted communication or illegally access computer systems.
- A second generation of software tools has now automated many cyber scams and enables offenders to carry out multiple attacks within a short time. Software tools also simplify attacks, allowing less
- In the early days of computer technology, the ability of law enforcement to carry out investigations involving digital data was limited by a lack of computer forensic equipment and expertise.
- The growing importance of digital evidence has spawned an increasing number of computer forensic laboratories.
- Yet, while the logistical aspects of the issue can be solved fairly easily, a number of challenges remain.
- The underlying reason for these challenges is the fact that, despite a number of similarities between digital evidence and other categories of evidence, there are major differences.
- Some of the general principles, such as the requirement that the evidence be authentic, complete, reliable and accurate and that the process of obtaining the evidence take place in line with the legal requirements, still hold good.
- Alongside the similarities, however, there are a number of aspects that make digital evidence unique and therefore require special attention when dealing with digital evidence in criminal investigations.
- Analysing and evaluating digital evidence requires special skills and technical understanding which is not necessarily covered in the education received by judges, prosecutors and lawyers.
- They therefore rely increasingly on the support of experts in the recovery of digital evidence.
- While this situation is not significantly different from other sophisticated investigation techniques, such as DNA sequencing, it prompts the need for necessary debate on the consequences for such dependence.

- evidence and require qualification of the associated uncertainty

Possible questions:

Part-B (2 Marks)

1. Define cybercrime?
2. What are the Classification of cybercrime?
3. Who are the cyber criminals and its types
4. What is meant by salami attack?
5. Write short notes on password sniffing?
6. What is identity theft?

Part-C (6 Marks)

1. Explain about the classification of cybercrimes?
2. Elaborate about the credit card frauds?
3. Explain about the legal perspective in an Indian perspective?
4. Explain the global perspective on cybercrimes?
5. Explain in your own words what you understand about the cybercrime and the extended enterprise?

UNIT- II
SYLLABUS

Cyber offences: How criminals plan them, categories of cybercrime, **How criminals plan the attack:** reconnaissance, passive attack, active attack, scanning and scrutinizing gathered information, attack, **Social engineering:** Classification of social engineering, **Cyber stalking:** Types of stalkers, cases reported on cyber stalking, how stalking works?, real-life Incident of cyber stalking, **Cyber café and cybercrimes, Botnets:** The fuel cybercrime, bot net, **Attack vector, Cloud computing:** why cloud computing, types of services, cybercrime and clod computing.

Introduction: cyber offences: How criminals plan them

- 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 purpose.
- People who commit cybercrimes are known as "Crackers"
- **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.
- **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
- **Cracker:** it is the act of breaking into computers. Creaking is a popular, growing subject on the internet. Many sites are devoted to supplying crackers with program that allow them to crack computers. Some of these programs contain dictionaries for guessing passwords. Others or used to break into phone lines .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, wardialers and worms.

- **Phreaking:** this is a notorious art of breaking into phone or other communication system. Phreaking sites on the internet or popular among crackers and other criminals
- **Wardialer:** It is the program that automatically dials phone numbers looking for computers on the other end.
- The categories of vulnerabilities that hackers typically search for are the following:
- 1. In adequate border protection
- 2. Remote access servers(RASs) with weak, access controls
- 3. Application servers with well-known exploits
- 4. Misconfigured systems and system with default configuration
- **Black hat:** A black hat is also called a "cracker" or" dark side hackers". Such a person is a malicious or criminal cracker
- **White hat:** a white hat hacker is considered an ethical hacker. White hat hacker is a person who is ethically opposed to the abuse of computer systems. A "white hat" generally focuses on securing IT systems.
- One of the first questions that frequently come up when countries start to address cybercrime is: Shall this take place within the context of law enforcement or cyber security? The distinction between the two topics is challenging.
- The topics are clearly interrelated as indicated by the fact that the 2010 UN General Assembly's Resolution on Cyber security addresses cybercrime as one major challenge.
- Cybercrime can therefore be seen as integral element of any approach to enhance cyber security – however it is certainly only one component of a cyber security strategy.
- Taking this into consideration underlines the inter-disciplinary nature of both topics and consequently the need to engage different stakeholders within the government in the process.
- The development of a national response to cybercrime very often involves different ministries
- Since many computer crimes involve the exchange of data, the ability to also intercept these processes or otherwise use data related to the exchange process can become an essential requirement for successful investigations.
- The application of existing telephone surveillance provisions and provisions related to the use of telecommunication traffic data in cybercrime investigations has turned out to be difficult in some countries.
- The difficulties encountered are related to technical issues as well as legal issues. From a legal point of view, authorization to record a telephone conversation does not necessarily include authorization to intercept data-transfer processes.

Categories of cybercrime:

Cybercrimes can be categorized based in the following:

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

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, copyright violation, harassment. However, this also makes difficult or trace and apprehend the criminals.
2. **Crimes targeted at property:** This includes stealing mobile devices such as cell phone, laptops, personal digital assistant (PDA), and removable media.
3. **Crimes targeted at organizations:** Cyber terrorism is one of the distinct crimes against organizations/governments. Attackers 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 systems.
4. **Single event of cybercrime:** it is the single event from the perspective of the victim, For example, unknowing open an attachment that may contain virus that will infect the system(PC/laptop), This is known as hacking of fraud.
5. **Series of events:** This involves attacker interacting with the victims, 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.

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 attackers are usually used to alter the system 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 breaches of confidentiality.
- In addition to the active and passive categories, attacks can be categorized as either inside or outside. An attack originating and/or attempted within the security perimeter of an organization is an inside attack; it is usually attempted by an "insider'' who gains access to more resources than expected. An outside attack s attempted by a source outside the security perimeter, maybe attempted by an insider and/or an outsider, who is indirectly with the organization, it is attempted through the internet or a remote access connection.
- 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

Reconnaissance:

- The literal meaning of "Reconnaissance" is an act of reconnaissance –explore , often with the goal of finding something or somebody.
- In the world of "hacking", reconnaissance phase begins with "Foot printing"- this s the preparation towards pre-attack phase, and involves accumulating data about the target's environment and computer architecture to find ways to intrude into that environment.
- Foot printing 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: active and passive attacks.
- The first step in most investigations is to prove that the offender had the ability to commit the crime.
- One of the main tasks of forensic experts is the examination of seized hardware and software.
- Checks can either be performed on the spot during the search of the suspect's premises or after seizure.
- To enable such investigation, first responders usually seize all relevant storage devices – each of them potentially carrying millions of files that quite often pose a logistical challenge.
- As pointed out above, the principles of relevance and effectiveness are of great importance for the admissibility of digital evidence.
- Identifying and selecting the relevant hardware is therefore one of the major tasks within an investigation.
- An analysis of available hardware components can, for example, prove that the suspect's computer was capable of carrying out a denial-of-service attack or is equipped with a chip that prevents manipulations of the operating system.
- Hardware analysis can also be necessary in the process of identifying a suspect.
- Some operating systems analyse the hardware configuration of a computer system during an installation process and submit it to the software producer.
- If the suspect's hardware profile can be detected based on information from the software company, hardware analysis can be helpful to verify that the seized computer system matches.

Hardware analysis does not necessarily mean focusing on physical components attached to a computer system. Most operating systems keep logs of hardware that was attached to a computer system during an operation.

- Based on the entries in log files such as the Windows Registry, forensic examiners can even identify hardware that was used in the past but was not present during the search and seizure procedure.

Passive attack:

- A passive attack involves gathering information about a target without his/her knowledge. It can be as simple is watching a building to identify what time employees enter the building premises.

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 websites 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
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 server or infrastructure devices a company may be using on its network.

- Network sniffing is another means of passive attack to yield useful information such as internet protocol (IP) address ranges, hidden servers or network, and other available services on the system or network.
- The principle of passive nationality refers to jurisdiction based on the nationality of the victim.
- Taking into account the overlapping with the principle of territory, it is only relevant if a national became victim of a crime while being outside the country.
- The application of the principle is controversially discussed– especially because it indicates that foreign law is insufficient to protect foreigners – but it has gained more acceptance in the last decades.
- One – non Internet-specific – codification of the principle of passive nationality is section of the German Penal Code.
- Name of the tools:
  1. Google Earth
  2. Internet Archive
  3. Professional community
  4. People search
  5. Domain name configuration

- The reason why different investigation techniques are necessary is not only due to the independence of place of action and the crime scene.
- It is in most cases a combination of a number of the above- mentioned challenges for law-enforcement agencies that make cybercrime investigations unique.
- If the offender is based in a different country, uses services that enable anonymous communication and, in addition, commits the crimes by using different public Internet terminals, the crime can hardly be investigated based on traditional instruments like search and seizure alone.
- To avoid misunderstanding, it is important to point out that cybercrime investigations require classic detective work as well as the application of traditional investigation instruments – but cybercrime investigations face challenges that cannot be solved solely using traditional investigation instruments.
- Some countries have already developed new instruments to enable law-enforcement agencies to investigate cybercrime, as well as traditional crimes that require the analysis of computer data.
- As is the case with regard to the substantive criminal law, the Council of Europe Convention on Cybercrime contains a set of provisions that reflect wide accepted minimum standards regarding procedural instruments required for cybercrime investigations.

Active attacks:

- An active attack involves probing to discover individual hosts to conform the information gathered in the passive attack phase.
- It involves the risk of detecting and is also called "Rattling doorknobs" or "Active reconnaissance".
- The principle of nationality refers to jurisdiction exercised with regard to activities of nationals abroad.
- It is related to the power of the state to regulate the behaviour of its nationals not only within its territory but also abroad.
- This principle is more common in civil law countries than common law countries.
- As a consequence common law countries tend to compensate the lack of jurisdiction based on the principle of nationality by a more extensive interpretation of the principle of territoriality.
- With regard to the fact that Internet-related crimes can be committed without leaving the country the principle is of less relevance when it comes to cybercrime cases.
- However, it can be highly relevant in the context of production of child pornography for the purpose of distributing it though computer networks
- Active reconnaissance can provide conformation to an attacker about security measures in place.
- Name of the tools:
  1. Arping

2. Bing
3. Dig
4. Fping
5. Hmap
6. Hping

Scanning and scrutinizing gathering 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
  2. **Network scanning:** Understand IP address and related information about the computer network systems.
  3. **Vulnerability scanning:** Understand the existing weaknesses in the system.
- A port is an interface on a computer to which one can connect a device .TCP/IP protocol suite made out of the two protocols.
- TCP/IP and UDP is used universally to communicate on the internet.
- The scrutinizing phase s always called "enumeration" in the hacking world. The objective behind this step is to identify:
  1. The valid user accounts or groups;
  2. Network resources and/or shared resources
  3. OS and different applications that are running on the OS

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/application
  4. Hide the files
  5. Cover the tracks- delete the access logs, so that there is no trail illicit activity.

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 engineering usually uses telecommunication or internet to get them to do something that s against the security, practices of the organization.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationship with insiders.
- T s an art of exploiting the trust of people, which is not doubted while speaking in a normal manner.,
- The goal of social engineer is to fool someone into providing valuable information or access to that information.
- Social engineer studies the human behaviour 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 successful social engineers is that they receive information without any suspicion.

Classification of social engineering:

Human based social engineering:

- Human-based engineering refers to person-to person interaction to get the required/desired information.

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.
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 help-desk worker will help him/her in gaining access to the system.
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.
5. **Shoulder surfing:** this 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 called dump stering ,binning, trashing, grabing or garbage gleaning. "Scavenging" is another term to describe these habit.

Computer-based social engineering:

- Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet

1. **Fake E-mails:** The attacker sends fake emails to numerous users in such that the user finds it as a legitimate mail. This activity is also called "Phishing". It is an attempts to entice the internet users to reveal their sensitive personal information, such as username and passwords, credit card details by impersonating as a trustworthy and legitimate organization and/or an individual. Banks, financial institutes and payment gateways are the common targets. Phishing is typically carried out through email 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. The term "Phishing" has been evolved from the analogy that Internet scammers are using email lures to fish for passwords and financial data.
2. **E-mail attachments:** E-mail attachments are used to send malicious code to a victim's system, which will automatically get executed. Viruses, Trojans and worms can be included cleverly into the attachments to entice a victim to open the attachment.
3. **Pop-up window:** Pop-up windows are also used, in a similar manner to email attachments. Pop-up windows with special offers or free stuff can encourage a user to unintentionally install malicious software.

- **Social engineering indeed is a serious concern as revealed by the following past statistics on numbers:**
    1. As per Microsoft corporation recent research, there is an increase in the number of security attacks designed to steal personal information or the instances of tricking people to provide it through social engineering. According to an FBI survey, on average 41% of security related losses are the direct result of employees stealing information from their companies. The average cost per internal incident was 1.8 million
    2. The federal trade commission report of 2005 shows that "more than one million consumer fraud and ID theft complaints have been filed with federal, state, and local law enforcement agencies and private organizations".
    3. According to a 2003 survey, " An estimated 3.6 million or 3.1% of American household become victims of ID theft in 2004",
    4. This means that now, more than ever, individuals are at high risk of having their PI stolen and used by criminals for their own personal gain.
- Involvement in the collection of digital evidence requires complex skills, since the techniques used to collect evidence that is stored on the hard drive of a home computer and those employed to intercept a data- transmission process are significantly different.
- Especially when it comes to high level-offenders, investigators are often confronted with situations that call for quick decisions.

- One example is whether a running computer system should be turned off or not, and how this procedure should be carried out. To avoid interfering with the integrity of relevant digital evidence, a common instruction is to pull the plug, as this stops any alteration of files.
- However, such a disruption of energy can activate encryption and thereby hinder access to stored data.
- First responders, who undertake the first steps to collect digital evidence, bear a significant responsibility for the entire investigation process, as any wrong decision can have a major impact on the ability to preserve relevant evidence.
- If they make wrong decisions on preservation, important traces can be lost.
- Forensic experts need to ensure that all relevant evidence is identified.
- This can be difficult if offenders hide files in a storage device in order to prevent law-enforcement agencies from analysing the content of the file.
- Forensic investigations can identify hidden files and make them accessible.
- Similar recovery processes are necessary if digital information has been deleted.
- Files that are deleted by simply placing them in a virtual trash bin does not necessarily render them unavailable to law-enforcement agencies, as they may be recovered using special forensic software tools.
- However, if offenders are using tools to ensure that files are securely deleted by overwriting the information, recovery is in general not possible.
- The collection of evidence can also face challenges if criminals are trying to prevent access to relevant information by using encryption technology.
- Such technology is more and more frequently used. Given that this prevents law-enforcement agencies from accessing and examining the encrypted information, the use of encryption technology entails significant challenges for law-enforcement agencies.
- Forensic experts can try to decrypt encrypted files. If this is not possible, they can support law-enforcement agencies in developing strategies to gain access to encrypted files, for example by using a key logger.
- Involvement in the collection of evidence includes the evaluation and implementation of new instruments.
- One example of a new approach is the debate on remote forensic tools.
- Remote forensic tools enable investigators to collect evidence remotely in real time or remotely monitor a suspect's activity without the suspect being aware of investigations on his system.
- Where such a tool is available, it can play a role in the development of a strategy to collect digital evidence.

Cyber stalking:

- The dictionary meaning of "stalking" is an "act or process of following prey stealthily-trying to approach somebody or something".

Cyber stalking 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 behaviour includes false accusations, monitoring, transmission of thefts, ID theft, damage or data or equipment.
- Cyber stalking refers to the use of Internet and/or other electronic communications devices to stalk another person.
- It involves harassing or threatening behaviour that an individual will conduct repeatedly.

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 makes sure that 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. The victim is not aware that the internet has been used to perpetuate an attack against them.

Cases Reported on Cyber stalking:

- The majority of cyber stalkers are men and the majority of their victim are women. However, there also have been many instances of cyber stalking by strangers.
- The rule against hearsay is another principle that is particularly relevant for common law countries.
- Hearsay evidence is evidence given by a witness in court of a statement made by some other person out of court, when such evidence is tendered to prove the truth of the statement.
- Under common law, hearsay evidence was generally inadmissible; but in civil proceedings this rule was abolished in the UK by the Civil Evidence Act 1995, which provides for the admissibility of hearsay evidence subject to statutory safeguards, and preserves a number of common law exceptions to the rule against hearsay.
- According to the common law rule against hearsay, an assertion other than one made by a person while giving oral evidence in the proceedings and tendered as evidence of the facts asserted is inadmissible

An out-of-court statement, for the purposes of the rule, means any statement other than one made by a witness in the course of giving his evidence, and could include, for example, a statement made in previous legal proceedings.

- Thus, the statement may have been made unsworn or on oath, orally, in writing or even by way of signs or gestures, by any person, whether or not called as a witness in the proceedings in question.
- In addition, the rule intends to enable cross-examination of the real witness and expose weaknesses in a statement.
- Instead, it is necessary that a witness with personal knowledge directly proves this. Not only can a witness testimony contain inadmissible hearsay but also exhibits may contain inadmissible hearsay.
- A number of reasons have been advanced to justify the common law rule against hearsay, such as the danger of manufactured evidence, relating to the potential unreliability of hearsay evidence.
- The rules governing the admissibility of hearsay evidence now apply if the purpose, or one of the purposes, of the person making the statement appears to the court to have been to cause another person to believe the matter, or to cause another person to act or a machine to operate on the basis that the matter is as stated.
- Having regard to the fact that data collected during an investigation intend to prove the truth of the matter asserted in the digital evidence itself, strict application of the rule is problematical in an age where very often digital evidence is the most relevant category of evidence in court proceedings, and some common law countries have started to implement statutory exceptions to the hearsay rule.
- Evidence produced by computers, cameras or other machines without incorporating any human statement cannot be hearsay.
- Under common law, it used to be held that visual images, even when produced by human hands, were not "statements" of any facts they purported to represent and therefore could not be hearsay. But there is now express provision to the contrary.
- Where no statutory exceptions exist, the application of the rule to digital evidence is questioned by pointing out that it only applies to statements that contain within them assertions made by human persons.
- Information generated mechanically without human intervention would on this basis not be considered as potentially hearsay evidence unless the process of creating the software is used as an argument to apply the rule even in those cases.

How Stalking Works?

- It is seen that stalking works following steps:

1. Personal information gathering about the victim: Name; family background; contact details such as cell phone and telephone numbers; address of residences as well as of the office, E-Mail address; date of birth.

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 victim through E-mail. The letters may have tone of loving, threatening or can 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 favours or threaten the victim.
5. The stalker may post the victim's personal information on any website. The stalker will use attractive language to invite the interested persons.
6. Whosoever comes across the information, start calling the victim on the given contact details
7. Some stalkers subscribe/ register the email account of the victim to innumerable, such kind of unsolicited emails

Real-Life Incident of Cyber stalking:

- Cyber stalking does not have a standard definition but it can be defined to mean threatening, unwarranted behaviour or advances directed by one person towards another person using Internet and other forms of online communication channels as medium.
- Internet service providers (ISPs) play an important role in many cybercrime investigations, since most users are utilizing their services to access the Internet or store websites.
- The fact that in some cases the ISPs have the technical capability to detect and prevent crimes and to support law-enforcement agencies in their investigations has prompted an intensive debate on the role of ISPs in cybercrime investigations
- Obligations discussed range from the mandatory implementation of prevention technology to voluntary support of investigations.
- Forensic experts can also support an investigation by preparing requests that are submitted to service providers and assisting the investigators in producing adequate case histories which are necessary to prove the reliability of the collected evidence. Cooperation between law-enforcement agencies and ISPs in such investigations requires the application of certain procedures.
- The Council of Europe Guidelines for the Cooperation of Law Enforcement and ISPs contain a set of fundamental procedures, including issues such as providing explanations and assistance regarding investigation techniques and prioritization, and the assistance of forensic experts can be useful in this respect to improve the efficiency of procedures.
- Close cooperation with ISPs is especially relevant in connection with the identification of a suspect. Suspects who commit cybercrime do leave traces.
- Traffic data analysis, like the examination of log-files kept by ISPs, can lead the investigators to the connection used by the offender to log on to the Internet.

- Offenders can try to hinder investigations by making use of anonymous communication technology.
- But even in this case, investigations are not impossible if investigators and ISPs cooperate closely.
- One example is the forensic tool CIPAV (Computer and Internet Protocol Address Verifier) that was used in the US to identify a suspect who had been using anonymous communication services.
- Another example of cooperation between ISPs and investigators is e-mail investigation. E-mails have become a very popular means of communication.
- To avoid identification, offenders sometimes use free e-mail addresses which they were able to register using fake personal information.
- However, even in this case, examination of header information and log-files of the e-mail provider will in some instances enable identification of the suspect.
- The need to cooperate and communicate with providers is not limited to ISPs. Since some crimes such as phishing and the commercial distribution of include financial transactions, one strategy to identify the offender is to obtain data from financial institutions involved in the transactions.
- Based on a request from the investigators, the credit-card companies analysed their customer records to identify customers who used their credit card to purchase on the specific website.
- Such investigations are more challenging when anonymous payment methods are used.

Cyber cafe and Cybercrimes:

- In February 2009, Nielsen survey on the profile of cyber cafes users in India, it was found that 90% of the audience.
- Hence, it is extremely important to understand the IT security and governance practiced in the cyber cafe.
- In the past several years, many instances have been reported in India, where cyber cafes are known to be used for either real or fake terrorist communication
- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of many have also happened through cyber cafes.
- Cyber criminals can either install malicious program such as key loggers and/or spyware or launch an attack on the target- techniques used.
- 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) 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 cyber cafes had installed the software called "Deep Freeze" for protecting the computers from prospective malware attacks. Although such intent is noble, this software happens to help cyber criminals hood wink the investigating agencies
4. Annual maintenance contract 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.
5. Cybercafé owners have very less awareness about IT Security and IT Governance.
    - Here, are few tips for safety and security while using the computer in a cyber cafe:

1. **Always logout:** while checking E-Mails or logging into chatting services such as instant messaging or using any other service that requires a username and a password, always click "logout" or "sign out" before leaving the system. However, do not save login information through options that allow automatic login. Disable such options before login.
2. **Stay with the computer:** while surfing/browsing, one should not leave the system unattended for any period of time. If one has to go out, logout and close all browser windows.
3. **Clear history and temporary:** Internet Explorer save pages that have visited in the history folder and in temporary Internet files. Passwords may also be stored in the browser if that option has been enabled on the computer that have used. Wait for the process to finish before leaving the computer.
4. **Be alert:** One should have to stay alert and aware of the surroundings while using a public computer. Snooping over the shoulder is an easy way of getting username and password.
5. **Avoid online financial transaction:** Ideally one should avoid online banking, shopping or other transactions that require one to provide personal, confidential and sensitive information such as credit card bank account details. One should change the passwords using a more trusted computer, such as at home and/or in office.
6. **Change password:** Changing the passwords in the best practise
7. **Virtual keyboard:** The advantage of virtual keyboard is designed to protect passwords from malicious "spyware" and "Trojan programs". Use of virtual keyboard will reduce the risk of passwords theft.
8. **Security warnings:** display the security warnings very clearly.

Botnets: The Fuel for Cybercrime

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 term, a Bot is automated computer program.
- 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 with a malicious program that allows cyber criminals to control the infected machines remotely without the user's knowledge.
- "Zombie networks" have become a source of income for entire group of cyber criminals.
- If someone wants to start a "business" and has no programming skills, there are plenty of "Bot for sale" offers on forums. Obfuscation and encryption of these programs code can also be ordered in the same way to protect them from detecting by antivirus tools. Another option is to steal an existing Botnet.
- **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 was 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 message
- **Spam dexing:** It is also known as 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 systems, usually one or more web servers. These systems are compromised at attackers using a variety of methods.
- One can ensure following to secure the system:
  1. **Use antivirus and anti-Spyware and keep it up-to-date**: It is important to remove and/or quarantine the viruses. The settings of these software should be done during the installation so that these software get updated automatically on a daily basis.
  2. **Set the OS to download and install security patches automatically**: OS companies issue the security patches for flaws that are found in these systems.
  3. **Use a firewall to protect the system from hacking attacks while it is connected on the Internet**: A firewall is a software and/or hardware that is designed to block unauthorized access while permitting authorized communications. A firewall is different from antivirus protection.
  4. **Disconnect from the Internet when you are away from your computer**: Attackers cannot get into the system when the system in disconnected from the Internet.

Firewall, antivirus, anti-Spyware software are not foolproof mechanisms to get access to the system.

5. **Downloading the freeware only from websites that are known trustworthy:** It is always appealing to download free software(s) such as games, file-sharing programs, customized toolbars. However, one should remember that many free software(s) contain other software, which may include Spyware.
6. **Take an immediate action if your system is infected:** If your system is found to be infected by a virus, disconnect it from the Internet immediately. Then scan the entire system with fully updated antivirus and anti-Spyware software. Report the unauthorized access to ISP and to the legal authorities. Change all the passwords immediately.

Attack vector:

- An "attack vector" is a path or means by which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome. Attack vector enable attackers to exploit system vulnerabilities, including the human element.
- Attack vector include viruses, E-Mail attachments, webpages, pop-up windows, instances messages, chat rooms, and deception. All of these methods involve programming except, deception.
- To some extent, firewalls and antivirus software can block attack vectors. However, no protection methods is totally attack-proof.
- A defence method that is effective today may not remain so for long because attackers are constantly updating attack vectors.
- The attack vectors described here are how most of them are launched.

1. **Attack by E-Mail:** The hostile content is either embedded in the message or linked to by the message. Sometimes attacks combine the two vectors, so that if the message does not get you, the attachment will. Spam is almost always carrier for scams, fraud, dirty tricks, or malicious action of some kind
2. **Attachments (and other files):** Malicious attachments install malicious computer code. The code could be a virus, Trojan Horses, 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 a just malicious computer code that one needs to monitor. Social engineering and other forms of deception that are often an attack vector too.
4. **Hackers:** Hackers/crackers are a formidable attack vector because, unlike ordinary malicious code, people are flexible and they can improvise. Hackers/crackers use a variety of hacking tools, heuristics, and social engineering to gain access to computers and online accounts. They often install a Trojan Horse to commandeer the computer for their own use.

5. **Heedless guests(attack by webpage):** Counterfeit websites are used to extract personal information. Such websites look very much like the genuine websites they imitate. 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 worms. In most cases, a firewall will block system worms. Many of these system worms install Trojan Horses. If the worms is successful, it propagate rapidly. The worm owner soon has thousands of "zombie" computers to use for more mischief.
7. **Malicious macros:** Microsoft Word and Microsoft Excel are some of the examples that allow macros. A macro does something a spreadsheet, for example. Macros can also be used for malicious purpose. If one using P2P software then his/her system is more vulnerable to hostile exploits.
8. **Foist ware (sneak ware):** Foist ware is the software that adds hidden components to the system on the sly. Spyware is the most common form of foist ware. Foist ware is quasi-legal software bundled with some attractive software.
9. **Virus:** These are malicious computer codes that hitch a ride and make the payload. Virus vectors include E-Mail attachments, downloaded files, worms
    - One of the most fundamental requirements for the admissibility of both traditional categories of evidence and digital evidence alike is the legitimacy of evidence.
    - This principle requires that digital evidence has been collected, analysed, preserved and finally presented in court in accordance with the appropriate procedures and without violating the fundamental rights of the suspect.
    - Both the requirements relating to the collection, analysis, preservation and finally presentation of the evidence in court and the consequences of a violation of the suspect's rights differ from country to country.
    - Principles and rules that can possibly be violated range from fundamental rights of a suspect such as privacy to failure to respect procedural requirements.
    - Due to the often inadequate legislation, general principles of evidence are frequently applied to digital evidence.
    - The requirements for the collection of digital evidence are mainly set by criminal procedural law.
    - In most countries, the interception of content data for example requires a court order and an extension of a search to remote storage devices requires that they be located in the same country.
    - If interception takes place without a court order, the appropriate procedures are violated, and the investigation might therefore interfere with the rights of the suspect.
    - The requirements for preservation of evidence are less often defined by law.

- However, the fundamental principle of the necessity to protect the integrity of digital evidence is certainly a guideline.
- Investigators need to make sure that evidence is not altered in any unauthorized manner from the time it was created, transmitted or stored by an authorized source.
- Protecting integrity is necessary in order to ensure reliability and accuracy and to comply with the principle of legitimacy.
- The procedures for the presentation of evidence in court are rarely defined by law.
- As stated above, not only the requirements but also the consequences of a violation of procedures and the rights of the suspect vary significantly.
- While some countries consider evidence to be inadmissible only if collected in a manner which seriously violates the suspect's rights (and not, for example, if only formal requirements were violated) and do not exclude such evidence, other countries – especially those applying the fruit of the poisonous tree doctrine – apply other standards for admissibility.
- In addition to hardware analysis, software analysis is a regular task in cybercrime investigations.
- Computer software is necessary to operate a computer system. In addition to the operating systems, additional software tools can be installed to gear the functioning of computer systems to the demand of the user.
- Forensic experts can analyse the functioning of software tools in order to prove that a suspect was capable of committing a specific crime.
- They can, for example, investigate whether the suspect's computer system contains a software that enables the encryption of data in pictures.
- An inventory of software tools installed on the suspect's computer can also help to design further investigation strategies.
- If, for example, the investigators find encryption software or tools used to delete files securely, they can specifically search for encrypted or deleted evidence.
- Investigators can also determine the functions of computer viruses or other forms of malicious software and reconstruct software-operation processes.
- In some cases, where illegal content has been found on suspects' computers, the suspects have claimed that they did not download the files but that it must have been done by computer virus.
- In such cases, forensic investigations can try to identify malicious software installed on the computer system and determine its functions.
- Similar investigations can be carried out if a computer system could have been infected and turned into part of a botnet.

Furthermore, software analysis can be important to determine if a software is produced solely for committing crimes or can be used for legitimate as well as illegal purposes (dual use).

- This differentiation can be relevant, insofar as some countries limit criminalization of the production of illegal devices to those that are either solely or primarily designed to commit crimes.
- Data-related investigations are not confined to the software function, but also include analysis of non- executable files such as pdf-documents or video files.
- These investigations range from content analysis of specific files to automatic keyword search for text files and image search for known images on the suspect's computer.
- File analysis also includes the examination of digital documents that might have been forged as well as metadata investigation.
- Such analysis can determine the time2231 the document was last opened or modified.
- Furthermore, metadata analysis can be used to identify the author of a file containing a threatening message, or the serial number of the camera that was used to produce a image.
- Authors can also be identified based on linguistic analysis, which can assist in determining if the suspect has written articles before and left information that can help identification in this context.

Cloud computing:

- The growing popularity of cloud computing and virtualization have made it possible, the next target of cybercriminals. Cloud computing services, while offering considerable benefit and cost savings, move servers outside the organizations security perimeter, which makes it easier for cybercriminals to attack these systems.
- Cloud computing is Internet based development and use of computer technology. The term cloud is used as a metaphor for the Internet, based on the cloud drawing used to depict the Internet in computer networks.
- The differentiation between "computer data" in Subparagraph and "subscriber information" in Subparagraph seems at first sight not to be necessary, insofar as subscriber information that is stored in digital form is also covered by Subparagraph
- The first reason for the differentiation stems from the different definitions of "computer data" and "subscriber information".
- Unlike "computer data", the term "subscriber information" does not require that the information be stored as computer data.
- The Council of Europe Convention on Cybercrime enables the competent law authorities to submit information that is kept in non-digital form.
- Cloud computing is a term used for hosted services delivered over the Internet.

- A cloud service has three distinct characteristics which differentiate if from traditional hosting:
  1. It is sold on demand
  2. It is elastic terms of usage
  3. The service is fully managed by the provider

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 database. 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 and continuous Internet connectivity instead of servers and other hardware.

- **Service provider:** Go Grid, Google App Engine, App Nexus, Microsoft Live Mesh, Force.com

Types of Services:

- Services provided by cloud computing 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 services.
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 API. Developers should take notice that there are not any interoperability standards; therefore, some providers may not allow to take 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

Cybercrime and Cloud Computing:

- Nowadays, prime area of the risk in cloud computing is protection of user data.
- **Area:**

1. Elevated user access
2. Regulatory compliance

3. Location of the data
4. Segregation of data
5. Recovery of the data
6. Information security violation reports
7. Long-term viability

- The Internet is one of the fastest-growing areas of technical infrastructure development.
- Today, information and communication technologies (ICTs) are omnipresent and the trend towards digitization is growing.
- The demand for Internet and computer connectivity has led to the integration of computer technology into products that have usually functioned without it, such as cars and buildings.
- Electricity supply, transportation infrastructure, military services and logistics – virtually all modern services depend on the use of ICTs.
- Although the development of new technologies is focused mainly on meeting consumer demands in western countries, developing countries can also benefit from new technologies.
- With the availability of long-distance wireless communication technologies such as WiMAX5 and computer systems that are now available for less than USD 2006, many more people in developing countries should have easier access to the Internet and related products and services.
- The influence of ICTs on society goes far beyond establishing basic information infrastructure.
- The availability of ICTs is a foundation for development in the creation, availability and use of network-based services. E-mails have displaced traditional letters
- online web representation is nowadays more important for businesses than printed publicity materials; and Internet-based communication and phone services are growing faster than landline communications.
- The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for developing countries.
- ICT applications, such as e-government, e-commerce, e-education, e-health and e-environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas.
- ICT applications can facilitate the achievement of millennium development targets, reducing poverty and improving health and environmental conditions in developing countries.

- The second reason for the distinction between "computer data" and "subscriber information" is that it enables law-makers to implement different requirements with regard to the application of the instruments.
- It is for example possible to impose stricter requirements for a production order under Subparagraph, as this instrument allows law-enforcement agencies to get access to any kind of computer data, including content data.
- The differentiation between the real-time collection of traffic data and the real-time collection of content data shows that the drafters of the Convention on Cybercrime realized that, depending on the kind of data law-enforcement agencies get access to, different safeguards need to be implemented.
- With the differentiation between "computer data" and "subscriber information", Article of the Council of Europe Convention on Cybercrime enables the signatory states to develop a similar system of graded safeguards with regard to the production order
- Given the right approach, context and implementation processes, investments in ICT applications and tools can result in productivity and quality improvements.
- In turn, ICT applications may release technical and human capacity and enable greater access to basic services. In this regard, online identity theft and the act of capturing another person's credentials and/or personal information via the Internet with the intent to fraudulently reuse it for criminal purposes is now one of the main threats to further deployment of e-government and e-business services.
- The costs of Internet services are often also much lower than comparable services outside the network.
- E-mail services are often available free of charge or cost very little compared to traditional postal services.
- The online encyclopaedia Wikipedia can be used free of charge, as can hundreds of online hosting services.
- Lower costs are important, as they enable services to be used by many more users, including people with only limited income. Given the limited financial resources of many people in developing countries, the Internet enables them to use services they may not otherwise have access to outside the network.
- One approach is to authorize law-enforcement agencies to break encryption if necessary.
- Without such authorization, or the possibility of issuing a production order, investigation authorities could be unable to collect the necessary evidence.
- In addition, or as an option, investigators can be authorized to use key logger software to intercept a passphrase to an encrypted file in order to break an encryption.

Another approach is to limit the performance of encryption software by restricting key length.

- Depending on the degree of the limitation, this would enable investigators to break keys within a reasonable period of time.
- Opponents of such a solution fear that the limitations would not only enable investigators to break encryption, but also economic spies trying to obtain access to encrypted business information.
- In addition, the restriction would only stop offenders using a stronger encryption if such software tools are available.
- This would first of all require international standards to prevent producers of strong encryption products from offering their software in countries without proper restrictions on key length.
- In any event, offenders could relatively easily develop their own encryption software with no limit on key length.

Possible questions:

Part-B (2 Marks)

1. What is meant by active attack?
2. What is meant by passive attack?
3. Write short notes on cloud computing?
4. Describe social engineering
5. List out the Classification of social engineering?
6. Write short notes on threats through lost and stolen devices

Part-C (6 Marks)

1. What are the categories of cybercrime?
2. Explain about the passive and active attack
3. Describe about the social engineering and its classification of social engineering?
4. What is meant by cyber stalking and cyber cafe & how stalking works?
5. Write short notes on botnets?
6. Elaborate about the cloud computing and its various functionality?

UNIT- III
SYLLABUS

Introduction: Mobile and wireless devices, Treads in mobility, credit card frauds in mobile and computing era: types and techniques of credit card frauds, **Security Challenges posed by Mobile Devices, Registry settings for Mobile Devices, Authentication service security:** Cryptographic security for mobile devices, LDAP security for hand held mobile computing devices, RAS security for mobile devices, Media player Control Security, Networking API Security for Mobile Computing Application, **Attacks on Mobile/Cell phones:** Mobile phone theft, Mobile Viruses, Mishing, Vishing, Smishing, Hacking Bluetooth

Introduction of Cybercrime: Mobile and Wireless Devices:

Introduction:

- In the recent years, the use of laptops, personal digital assistants (PDAs) and mobile phone has grown from limited users communities to widespread desktop replacement and broad deployment.
- According to Quocirca Insight Report (2009), by the end of 2008 around 1.5 billion individual around the world had the Internet access.
- Remote connection has extended from fixed location dial-in to wireless-on-move, and smart hand-held devices such as PDAs have become networked, converging with mobile phones.
- Furthermore, the maturation of the PDA and advancement in cellular phone technology have converged into a new category of mobile phone devices: the smartphone.
- Smartphones combine the best aspects of mobile and wireless technologies and blend them into a useful business tool.
- These technological developments presents a new set of security challenges to the global organizations
- The Internet can be used to spread misinformation, just as easily as information.
- Websites can present false or defamatory information, especially in forums and chat rooms, where users can post messages without verification by moderators.
- Minors are increasingly using web forums and social networking sites where such information can be posted as well.

- Criminal behaviour can include the publication of intimate photographs or false information about sexual behaviours.
- In most cases, offenders take advantage of the fact that providers offering cheap or free publication do not usually require identification of authors or may not verify ID.
- This makes the identification of offenders complicated. Furthermore, there may be no or little regulation of content by forum moderators.
- These advantages have not prevented the development of valuable projects such as the online user-generated encyclopaedia
- Where strict procedures exist for the regulation of content.
- However, the same technology can also be used by offenders to publish false information or disclose secret information
- It is vital to highlight the increased danger presented by false or misleading information. Defamation can seriously injure the reputation and dignity of victims to a considerable degree, as online statements are accessible to a worldwide audience.
- The moment information is published over the Internet, the author often loses control of this information.
- Even if the information is corrected or deleted shortly after publication, it may already have been duplicated and made available by people that are unwilling to rescind or remove it. In this case, information may still be available on the Internet, even if it has been removed or corrected by the original source.
- Examples include cases of "runaway e-mails", where millions of people can receive salacious, misleading or false e-mails about people or organizations, where the damage to reputations may never be restored, regardless of the truth or otherwise of the original e-mail.
- Therefore the freedom of speech and protection of the potential victims of libel needs to be well balanced.
- The Internet is not only used for direct attacks, but also as a forum for soliciting, offers and incitement to commit crimes unlawful sale of products and providing information and instructions for illegal acts
- Many countries have put in place regulations on the trade of certain products.
- Different countries apply different national regulations and trade restrictions to various products such as military equipment.
- A similar situation exists for medicines – medicines which are available without restriction in some countries may need prescription in others.
- Cross-border trade may make it difficult to ensure that access to certain products is restricted within a territory.
- Given the popularity of the Internet, this problem has grown.
- Web shops operating in countries with no restrictions can sell products to customers in other countries with restrictions, undermining these limitations.

- Prior to the Internet, it was difficult for most people to access instructions on how to build weapons.
- The necessary information was available (e.g. in books dealing with chemical aspects of explosives), but time- consuming to find.
- Today, information on how to build explosives is available over the Internet and ease of access to information increases the likelihood of attacks.

Proliferation of mobile and wireless devices:

- Incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A long list of options is available to the mobile users. A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls.
- As the term "mobile devices" includes many products. Provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices.
- Many types of mobile computers have been introduced since 1990's. They are as follows:

1. **Portable computers:** It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some "setting-up" and an AC power source.
2. **Tablet PC:** It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touch-screen with a stylus and handwriting recognition software.
3. **Internet tablet:** It is the internet appliance in tablet form. Unlike a Tablet PC, the internet tablet does not have much computing power and its applications suite is limited. The internet tablets typically features an MP3 and video player, a Web browser , a chat application and a picture viewer
4. **Personal digital assistant (PDA):** It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.
5. **Ultra mobile PC:** It is a full-featured, PDA-sized computer running a general-purpose operating systems (OS).
6. **Smart phone:** It is a PDA with an integrated cell phone functionality. Current smartphones have a wide range of features and installable applications.
7. **Carputer:** It is a computing device installed in an automobile. It operates as a wireless computer, sound systems, global positioning system (GPS) and DVD player. It also contain word processing software and is Bluetooth compatible.
8. **Fly Fusion Pentop Computer:** It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

- Wireless refers to the method of transferring information between a computing device and a data source without a physical connection. Not all wireless communication technologies are mobile.

- Mobile computing does not necessarily require wireless communication. In fact, it may not require communication among devices at all.

Trends in mobility:

- Mobile computing is a moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking. "iPhone" from Apple and Google-led "Android" phones are the best example of this trend and there are plenty of other developments that point in this direction.
- This smart mobile technology is rapidly gaining popularity and the attackers are among its biggest fans.
- It is worth noting the trends in mobile computing
- Types of mobility
- **User mobility:** User interaction model
- **Device mobility:** Smaller, battery –driven devices, multiple heterogeneous networks or often no network position becomes parameter
- **Session mobility:** Issues in data distribution
- **Service mobility (code mobility):** Distributed life cycle management security is strong issue.
- The new technologies 3G networks are not entirely build with IP data security. Moreover, IP data world when compared to voice-centric security threats is new to mobile operators.
- They are numerous attacks that can be committed against mobile networks and they can originate from two primary vectors.
- Popular types of attacks against 3G mobile networks are as follows:
  1. **Malwares, viruses and worms:** Although many users are still in the transient process of switching from 2G, 2.5G to 3G, it is a growing need to educate the community people and provide awareness of such threats that exists while using mobile devices.
  2. **Denial-of-service (DoS):** The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable. Botnets/zombies are used to create enough traffic to impose that kind of damage.
  3. **Overbilling attack:** Overbilling involves an attacker hijacking subscriber's IP address and then using it to initiate downloads that are not "Free downloads" or simply use it for his/her own purpose.
  4. **Spoofed policy development process (PDP):** These types of attacks exploit the vulnerabilities in the GTP(General Radio Service(GPRS) Tunneling Protocol)
  5. **Signalling-level attacks:** The Session Initiation Protocol (SIP) is a signalling protocol used in IP multimedia subsystem (IMS) networks to provide Voice Over Internet Protocol (VoIP) services

Credit Card Frauds in Mobile and Wireless Computing Era:

- These are new trends in cybercrime that are coming up with mobile computing-mobile commerce and mobile banking. Credit card frauds are now becoming commonplace given the ever-increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone.
- Mobile credit card transactions are now very common; new technologies combine low-cost mobile phone technologies with the capabilities of a point-of-sale (POS) terminal.
- Wireless credit card processing is a relatively new service that will allow a person to process credit cards electronically, virtually anywhere.
- Credit card companies, normally, do a good job of helping consumers resolve identity (ID) theft problems once they occur.
- But they could reduce ID fraud even if they more if they given consumers better tools to monitor their accounts and limit high-risk transactions.
- There is a system available from an Australian company "Alacrity" called closed-loop environment for wireless (CLEW).
- CLEW which is a registered trademark of Alacrity used here only to demonstrate the flow in this environment.
- Over the last few years, law-enforcement agencies around the world have highlighted the urgent need for adequate investigation instruments.
- Taking this into consideration, it is perhaps surprising that the Council of Europe Convention on Cybercrime has been criticized with regard to procedural instruments.
- The criticism focuses mainly on the aspect that the Convention on Cybercrime contains a number of provisions that establish investigation instruments but only one provision that deals with safeguards.
- In addition, it can be noted that unlike for the substantive criminal law provisions in the Convention on Cybercrime, there are only very few possibilities for national adjustments in respect of the implementation of the Convention on Cybercrime.
- The criticism as such focuses mainly on the quantitative aspects.
- It is correct that the Convention on Cybercrime follows the concept of centralized regulation of safeguards instead of attaching them individually to each instrument.
- But this does not necessarily mean a weaker protection of suspects' rights.
- The Council of Europe Convention on Cybercrime was designed from the outset as an international framework and instrument for the fight against cybercrime that is not limited solely to the Council of Europe member countries.
- While negotiating the necessary procedural instruments, the drafters of the Convention on Cybercrime, which included representatives from non-European countries like the United States and Japan, realized that the existing national approaches related to safeguards and especially the way these protected the suspect in the various criminal law systems were so different that it would not be possible to provide one detailed solution for all Member States.

- The drafters of the Convention on Cybercrime therefore decided not to include specific regulations in the text of the Convention, but instead to request Member States to ensure that fundamental national and international standards of safeguards are applied.

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

- If the law provides central standards that apply to all investigation instruments, these principles shall apply to Internet-related instruments as well.
- In case the domestic law is not based on a centralized regulation of safeguards and conditions, it is necessary to analyse the safeguards and conditions implemented with regard to traditional instruments that are comparable to Internet-related instruments.
- But the Convention on Cybercrime does not refer solely to existing safeguards in national legislation.
- This would have the drawback that the requirements for application would differ in such a way that the positive aspects of harmonization would no longer apply.
- To ensure that signatory states which might have differing legal traditions and safeguards in place implement certain standards, the Council of Europe Convention on Cybercrime defines the minimum standards by referring to fundamental frameworks, such as the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights instruments.
- As the Convention on Cybercrime can be signed and ratified also by countries that are not members of the Council of Europe, it is important to highlight that

not only the United Nations International Covenant on Civil and Political Rights but also the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms will be taken into consideration when evaluating the systems of safeguards in signatory states that are not members of the Council of Europe Convention on Cybercrime.

- European Court of Human Rights has undertaken efforts to define more precisely standards that govern electronic investigations and especially surveillance.
- Today, case law has become one of the most important sources for international standards in respect of investigations related to communication.
- The case law takes particularly into consideration the gravity of the interference of the investigation, its purpose and its proportionality.
- Fundamental principles that can be extracted from case law are: the need for a sufficient legal basis for investigation instruments, the requirement that the legal basis must be clear with regard to the subject, competences of the law-enforcement agencies need to be foreseeable and surveillance of communication can only be justified in context of serious crimes.
- In addition to this, Council of Europe Convention on Cybercrime takes into account the principle of proportionality.
- This provision is especially relevant for signatory states that are not members of the Council of Europe.
- In cases where the existing national system of safeguards does not adequately protect suspects, it is mandatory for Member States to develop the necessary safeguards within the ratification and implementation process.

Types and Techniques of Credit Cards frauds:

Traditional Techniques:

- The traditional and the first type of credit card fraud is paper-based fraud- application fraud, wherein a criminals uses stolen or fake documents such as utility and bank statements that can be build up useful personally Identifiable Information (PII) to open an account in someone else's name.
- Application fraud can be divided into

1. **ID theft:** Where an individual pretends to be someone else
2. **Financial fraud:** Where an individual gives false information about his or her financial status to acquire credit.

- Illegal use of lost and stolen cards is another form of traditional techniques. Stealing credit card is either by pick pocket or from postal service before it reaches its final destination

Modern Technique:

- Sophisticated techniques enable criminals to produce fake and doctored cards. Then there are also those who use skimming to commit fraud.

1. **Triangulation:** It is another method of credit card fraud and works in fashion as explained further.
   - The criminal offers the good with heavy discounted rates through a website designed and hosted by him, which appears to be legitimate merchandise website.
   - The customer register on this website with his/her name, address, shipping address and valid credit card details.
   - The criminal orders the goods from a legitimate website with the help of stolen credit card details and supply shipping address have been provided by the customer while registering on the criminal's website.
   - The goods are shipped to the customer and the transaction gets completed.
2. **Credit card generators:** It is another modern techniques- computer emulation software- that create valid credit cards. These are available for free download on the Internet.

Security Challenges Posed by Mobile Devices:

- Mobility brings two main challenges to cyber security: first, on the hand-held devices, information is being taken outside the physically controlled environment
- and second remote access back to the protected environment is being granted.
- Perception of the organizations to those cyber security challenges are important in devising appropriate security operating procedure.
- As the number of mobile device users increases, two challenges are presented: one at the device level called "micro challenges" and another at the organizational level called "macro challenges".
- Some well-known technical challenges in mobile security are: managing the registry setting and configurations, authentication service security, cryptography security, Lightweight Directory Access Protocol (LDAP) security, remote access server (RAS) security, media player control security, networking application program interface (API) security.
- Unlike the fundamental principles described above, the safeguards mentioned here do not necessarily need to be implemented with regard to any instrument but only if appropriate in view of the nature of the procedure concerned. The decision as to when this is the case is left to the national legislatures.
- An important aspect related to the system of safeguards provided by the Council of Europe Convention on Cybercrime is the fact that the ability of law-enforcement agencies to use the instruments in a flexible way on the one hand and the guarantee of effective safeguards on the other depends on the implementation of a graded system of safeguards.

- The Convention on Cybercrime does not explicitly hinder the parties from implementing the same safeguards (e.g. the requirement of a court order) for all instruments, but such an approach would influence the flexibility of the law-enforcement agencies.
- The ability to ensure an adequate protection of the suspect's rights within a graded system of safeguards depends largely on balancing the potential impact of an investigation instrument with the related safeguards.
- To achieve this it is necessary to differentiate between less and more intensive instruments.
- If the intensity of an investigation instrument and the potential impact on a suspect are correctly evaluated and the safeguards are designed in line with the results of the analysis, the system of graded safeguards does not lead to an unbalanced system of procedural instruments.

Registry Settings for Mobile Devices:

- Registry settings on mobile devices through an example: Microsoft ActiveSync is mean for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook.
- In this context, registry setting becomes an important issue given the ease with which various applications allow a free flow of information.
- Thus, establishing trusted groups through appropriate registry setting becomes crucial. One of the most prevalent areas where this attention to security is applicable is within "group policy".
- Group policy is one of the core operations that are performed by Windows Active Directory.
- Even if users go through every control panel setting and group policy option, they may not get the computer to the desired baseline security.
- For example, only way to get a Windows computer to a security level that will be near bullet proff is to make additional registry changes that are not exposed through any interface.

Authentication Service Security:

- There are two components of security in mobile computing: security of devices and security in networks. A secure network access involves mutual authentication between the device and the base stations or web servers.
- This is to ensure that only authenticated devices can be connected to the network for obtain the requested services.
- Offenders can take certain measures to complicate investigations. In addition to using software that enables anonymous communication, identification can be complicated if the suspect is using public Internet terminals or open wireless networks.

- Restrictions on the production of software enabling the user to hide his/her identity and on making public Internet access terminals available that do not require identification could help law-enforcement agencies to conduct investigations more efficiently.
- An example of an approach to restrict the use of public terminals to commit criminal offences is which was converted into a law in 2005
- This provision forces anybody who intends to offer public Internet access to apply for authorization.
- In addition, the person in question is obliged to request identification from his/her customers prior to giving them access to use the service.
- Since a private person who sets up a wireless access point is in general not covered by this obligation, monitoring can quite easily be circumvented if offenders make use of unprotected private networks to hide their identity.
- It is questionable whether the extent of improvement in investigations justifies the restriction of access to the Internet and to anonymous communication services.
- Free access to the Internet is today recognized as an important aspect of the right of free access to information that is protected by the constitution in a number of countries.
- Registration obligation can interfere with the right to operate Internet services without authorization, as emphasized by the 2005 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression.
- It is likely that the requirement for identification will affect the use of the Internet, insofar as users will then always have to fear that their Internet usage is monitored.
- Even when users know that their activities are legal, it can still influence their interaction and usage.
- At the same time, offenders who want to prevent identification can easily circumvent the identification procedure.
- They can, for example, use prepaid phonecards bought abroad which do not require identification to access the Internet.
- Similar concerns arise with regard to legislation targeting anonymous communication services.
- There is an ongoing debate on whether similar instruments discussed with regard to encryption technology should be applied to anonymous communication technology and services.
- Apart from the conflict between protecting privacy and ensuring the ability to investigate offences, the arguments against the practicability of the various legal approaches to address the challenge of encryption (especially lack of enforceability) apply equally to anonymous communication.
- Authentication service security is important given the typical attacks on mobile devices through wireless networks.

- DoS attacks, traffic analysis, eavesdropping, man-in-the-middle attacks and session hijacking.

Cryptographic Security for Mobile Devices:

- Cryptographic generated address (CGA). CGA is Internet Protocol version 6 (IPv6) that addresses up to 64 address bits that are generated by hashing owner's public-key address.
- The address the owner uses is the corresponding private key to assert address ownership and to sign message sent from the address without a public-key infrastructure (PKI) or other security infrastructure.
- Deployment of PKI provides many benefits for users to secure their financial transactions initiated from mobile devices.
- CGA- based authentication can be used to protect IP-layer signalling protocols including neighbour discovery and mobility protocols.
- It can also be used for key exchange in opportunistic Internet Protocol Security.

LDAP Security for Hand-Held Mobile Computing Devices:

- LDAP is a software protocol for enabling anyone to locate individuals, organizations and other resources such as files and devices on the network.
- In a network, a directory tells you where an entity is located in the network. LDAP is a light weight version of Directory Access Protocol (DAP) because it does not include security features in its initial version.

RAS Security for Mobile Devices:

- RAS is an important consideration for protecting the business-sensitive data that may reside on the employee's mobile devices.
- In addition to being vulnerable to unauthorized access on their own, mobile devices also provide a route into the system with which they connect.
- By using a mobile devices to appear as a registered user to those systems, a would-be cracker is then able to steal data or compromise corporate systems in other ways.
- Another threat comes from the practice of port scanning. First, attackers use a domain name system (DNS) server to locate the IP address of a connected computer.
- Protecting against port scanning requires software that can trap unauthorized incoming data packets and prevent a mobile device from revealing its existence and ID.
- The security of a RAS system can be divided into following three areas:

1. The security of the RAS server
2. The security of the RAS client
3. The security of data transmission

Media Player Control Security:

- Music and video are the two important aspects in day-to-day aspects for the young generation. Various leading software development organizations have been warning the

users about the potential security attacks on their mobile devices through the "music gateways".

- Microsoft had warned people that a series of flows in its windows media player could allow a malicious hacker to hijack people's computer systems and perform a verity of actions.
- According to this warning from Microsoft, in the most serve exploit of a flaw, a hacker could take over a computer systems and perform any task the computer's owner is allowed to do, such as opening files or accessing certain parts of a network.
- Files could be created which allow the attacker to download and use the code on the user's machine or media files could be created that will create buffer overrun errors.
- It also contains information that the OS continually references during an operations. In the registry, some keys control the behaviour of the Windows Media Player control.
- Microsoft, through its developer network MSDN, describes details of registry value settings on the mobile devices.
- Efforts to protect content are not limited to songs and films. Some TV stations (especially pay-tv channels) encrypt programmes to ensure that only paying customers can receive the programme.
- Although protection technologies are advanced, offenders have succeeded in falsifying the hardware used as access control or have broken the encryption using software tools.
- Without software tools, regular users are less able to commit such offences. Discussions on the criminalization of copyright violations not only focus on file-sharing systems and the circumvention of technical protection, but also on the production, sale and possession of "illegal devices" or tools that are designed to enable the users to carry out copyright violations.
- File-sharing technology is not only used by ordinary people and criminals, but also by regular businesses.
- Not all files exchanged in file-sharing systems violate copyrights. Examples of its legitimate use include the exchange of authorized copies or artwork within the public domain.
- Nevertheless, the use of file-sharing systems poses challenges for the entertainment industry.
- It is unclear to what extent falls in sales of CD/DVDs and cinema tickets are due to the exchange of titles in file-sharing systems.
- Research has identified millions of file-sharing users481 and billions of downloaded files.
- Copies of movies have appeared in file-sharing systems before they were officially released in cinemas483 at the cost of copyright-holders.
- The recent development of anonymous file-sharing systems will make the work of copyright-holders more difficult, as well as that of law-enforcement agencies.

- The entertainment industry has responded by implementing technology designed to prevent users from making copies of CDs and DVDs such as content scrambling systems (CSS), an encryption technology preventing content on DVDs from being copied.
- This technology is a vital element of new business models seeking to assign access rights to users more precisely. Digital rights management (DRM) describes the implementation of technologies allowing copyright-holders to restrict the use of digital media, where customers buy limited rights only (e.g. the right to play a song during one party).
- DRM offers the possibility of implementing new business models that reflect copyright-holders' and users' interests more accurately and could reverse declines in profits.

Networking API Security for Mobile Computing Application:

- With the advent of electronic commerce (E-Commerce) and its further off-shoot into M-Commerce, online payments are becoming a common phenomenon with the payment gateway accessed remotely and possibly wirelessly.
- There are organizations announcing the development of various APIs to enable software and hardware developers to write single applications that can be used to target multiple security platforms present in a range of devices such as mobile phones, portable media players, set-top boxes and home gateways.
- Most of these developments are targeted specifically at securing a range of embedded and consumer protects, including those running OSs such as Linux, Symbian, Microsoft Windows CE and Microsoft Windows Mobile.
- Only basic equipment is needed to commit computer crimes.
- Committing an offence requires hardware, software and Internet access. With regard to hardware, the power of computers is growing continuously.
- There are a number of initiatives to enable people in developing countries to use ICTs more widely.
- Criminals can commit serious computer crimes with only cheap or second-hand computer technology – knowledge counts for far more than equipment.
- The date of the computer technology available has little influence on the use of that equipment to commit cybercrimes.
- Committing cybercrime can be made easier through specialist software tools. Offenders can download software tools designed to locate open ports or break password protection.
- Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices.
- The last vital element is Internet access. Although the cost of Internet access is higher in most developing countries than in industrialized countries, the number of Internet users in developing countries is growing rapidly. Offenders will generally not subscribe to an Internet service to limit their chances of being identified, but prefer services they can use without (verified) registration.
- A typical way of getting access to networks is the so-called "wardriving". The term describes the act of driving around searching for accessible wireless networks.

- The most common methods criminals can use to access the network fairly anonymously are public Internet terminals, open (wireless) networks, hacked networks and prepaid services without registration requirements.
- Law-enforcement agencies are taking action to restrict uncontrolled access to Internet services to avoid criminal abuse of these services.
- In Italy and China, for example, the use of public Internet terminals requires the identification of users.
- However, there are arguments against such identification requirements. Although the restriction of access could prevent crimes and facilitate the investigations of law-enforcement agencies, such legislation could hinder the growth of the information society and the development of e-commerce.
- It has been suggested that this limitation on access to the Internet could violate human rights.
- For example, the European Court has ruled in a number of cases on broadcasting that the right to freedom of expression applies not only to the content of information, but also to the means of transmission or reception.
- In the case Autronic v. Switzerland, the court held that extensive interpretation is necessary since any restriction imposed on the means necessarily interferes with the right to receive and impart information.
- If these principles are applied to potential limitations on Internet access, it is possible that such legislative approaches could entail violation of human rights.

Attacks on Mobile/Cell phones:

Mobile phone theft:

- Mobile phones have become an integral part of everybody's life and the mobile phone has transformed from being a luxury to a bare necessity.
- Increase in the purchasing power and availability of numerous low cost handsets have also lead on an increase in mobile phone users.
- Many Insurance Companies have stopped offering Mobile Theft Insurance due to a large number of false claims.
- Another reason is increasing demand for Wi-Fi zones in the metropolitans and extensive usage of cell phones in the youths with lack of awareness/knowledge about the vulnerabilities of the technology
- The following factors contribute for outbreaks on mobile devices:

1. **Enough target terminals:** The first palm OS virus was seen after the number of palm OS devices reached 15 million. The first instances of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito.
2. **Enough functionality:** Mobile devices are increasingly being equipped with office functionality and already carry critical data and application, which are often protected insufficiently.

3. **Enough connectivity:** Smartphones offers multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connection. Therefore, unfortunately, the increased amount of freedom also offers more choices for virus writers.

Mobile viruses:

- A mobile virus is similar to a computer virus that targets mobile phones data or applications/software installed in it. Virus attacks on mobile devices are no longer an exception or proff-of-concept nowadays.
- In total, 40 mobile virus families and more than 300(+) mobile viruses have been identified. Readers may visit viruses.
- It is interesting to note that, like computer virus hoax, variants of mobile phone virus hoax have been circulating since 1999. These hoax message either will be sent through E-Mail or through SMS to the mobile users.
- Following are some tips to mobile from mobile malware attacks
  1. Download or accept programs and content only from a trusted source.
  2. If a mobile is equipped with Bluetooth, turn it OFF or set it to non-discoverable mode when it is not use and/or not required to use.
  3. If a mobile is equipped with beam, allow it to receive incoming beams, only from the trusted source.
  4. Download and install antivirus software for mobile devices.
- Offenders have developed techniques to obtain personal information from users, ranging from spyware to "phishing" attacks.
- "Phishing" describes acts that are carried out to make victims disclose personal/secret information.
- There are different types of phishing attacks, but e-mail-based phishing attacks contain three major phases.
- In the first phase, offenders identify legitimate companies offering online services and communicating electronically with customers whom they can target, e.g. financial institutions.
- Offenders design websites resembling the legitimate websites requiring victims to perform normal log in procedures, enabling offenders to obtain personal information (e.g. account numbers and online banking passwords).
- In order to direct users to spoofing sites, offenders send out e-mails resembling e-mails from the legitimate company, often resulting in trademark violations.
- The false e-mails ask recipients to log in for updates or security checks, sometimes with threats (e.g. to close the account) if users do not cooperate.
- The false e-mail generally contains a link that victim should follow to the spoof site, to avoid users manually entering the correct web address of the legitimate bank.
- Offenders have developed advanced techniques to prevent users from realizing that they are not on the genuine website.

- As soon as personal information is disclosed, offenders log in to victims' accounts and commit offences such as the transfer of money, application for passports or new accounts, etc.
- The rising number of successful attacks proves phishing's potential.
- More than 55 000 unique phishing sites were reported to APWG717 in April 2007. In January 2014, the number of unique phishing sites detected rose to almost Phishing techniques are not limited to accessing passwords for online banking only.
- Offenders may also seek access codes to computers, auction platforms and social security numbers, which are particularly important in the United States and can give rise to "identity theft" offences

Mishing:

- Mishing is a combination of mobile phone and Phishing. Mishing attacks are attempted using mobile phone technology. M-Commerce is a fast becoming a part of everyday life.
- Mobile phone for purchasing goods/services and for banking, could more vulnerable to a Mishing scam.
- A typical Mishing attacker uses a call termed as Vishing or message (SMS) known as Smishing.

Vishing:

- Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward.
- The term is a combination of V- voice and phishing
- Vishing is usually used steal credit card numbers or other related data used in ID theft schemes from individual.
- Vishing attacks include:

1. ID theft
2. Purchasing luxury goods and services
3. Transferring money/ funds
4. Monitoring the victim's bank account
5. Making applications for loans and credit cards.

How vishing works:

- The criminals can initiate a vishing attack using a variety of methods, each of which depend upon information gathered by the criminal and criminal's will to reach a particular audience.

1. Internet E-Mail: It is also called Phishing mail
2. Mobile text messaging: It is also a form of social engineering, wherein a pretexter hides his/her purpose and/or identity to get the personal information/ sensitive data about another individual.

3. Voice mail: Here, victim is forced to call on the provided phone numbers, once he/she listens to voicemail.
4. Direct phone call: Following are the steps detailing on how direct phone call works:
   - The criminal gathers cell/mobile phone numbers located in a particular region and/or steals cell/ mobile phone numbers after accessing legitimate voice messaging company.
   - The criminal often uses a war dialer to call phone numbers of people from a specific region, and that to from the gathered list of phone numbers
   - When the victim answers the call, an automated recorded message is played to alert the victim that his/her credit card has had fraudulent activity and/or his/her bank account has had unusual activity.
   - Once the victim enters these details, the criminal has the necessary information to make fraudulent use of the card or to access the account
   - Such calls are often used to harvest additional details such as date of birth, credit card expiration date,

- There are various definitions of "computer forensics". It can be defined as "the examination of IT equipment and systems in order to obtain information for criminal or civil investigation".
- When committing crimes, offenders leave traces. This statement is valid in traditional investigations as well as computer investigations.
- The main difference between a traditional investigation and a cybercrime investigation is that a cybercrime investigation generally requires specific data-related investigation techniques and can be facilitated by specialized software tools.
- In addition to adequate procedural instruments, carrying out such analysis requires that the authorities possess the ability to manage and analyse the relevant data. Depending on the offences and the computer technology involved, the requirements in terms of procedural investigation tools and forensic analysis techniques differ and present unique challenges.

How to protect from Vishing attacks:

- Following are some tips protect oneself from Vishing attack:
  1. Be suspicious about all unknown callers.
  2. Do not trust caller ID. It does not guarantee whether the call is really coming from that number, that is, from the individual and/or company-caller ID spoofing is easy
  3. Be aware and ask question, in case someone is asking for your personal or financial information
  4. Call them back.

5. Report incidents: Report Vishing calls to the nearest cyber police cell with the number and name that appeared on the caller ID as well as the time of the information talked about or heard in a recorded message

Smishing:

- Smishing is a criminal offences conducted by using social engineering techniques similar to Phishing. The name is derived from "SMS PhISHING".
- SMS-Short Message Service-is the text message communication component dominantly used into mobile phones.

How to protect from Smishing Attack:

- Following are some tips protect oneself from Smishing Attacks

1. Do not answer a text message
2. Avoid calling any phone numbers
3. Never click on a unwanted link

Hacking Bluetooth:

- Bluetooth is an open wireless technology standard used for communication over short distances between fixed and/or mobile devices
- Bluetooth is a short-range wireless communication service/technology that uses the 2.4-GHz frequency range for its transmission/communication
- The older standard –Bluetooth 1.0 has a maximum transfer speed of 1 Mbps compared with 3 Mbps by Bluetooth 2.0
- This makes Bluetooth use simple and straightforward, and it also makes easier to identify the target for attackers.
- The attacker installed special software for list of software(s) which are termed as Bluetooth hacking tools on the laptop and then install a Bluetooth antenna.
- Once a software tool is used by the attackers finds and connects to a vulnerable Bluetooth-enabled cell phone, it can do things like download address book information, photos, calendars, SIM card details, make long-distance phone calls using the hacked device, bug phone calls and much more.
- Blue jacking, Blue snarfing, Blue bugging and Car Whisperer are common attacks that have emerged as Bluetooth-specific security issues.

1. **Blue jacking:** It means Bluetooth+ Jacking where Jacking is short name for hijack- act of taking over something. Blue jacking is sending unsolicited messages over Bluetooth-enabled devices such as mobile phones, PDAs or computers. Blue jacking is harmless, as blue jacked users generally do not understand what has happened and hence they may think that their phone is malfunctioning
2. **Blue snarfing:** It is unauthorized access from a wireless device through a Bluetooth connection between cell phones, PDAs and computers.

3. **Blue bugging:** It allows attackers to remotely access a user's phone and use its features without use's attention. Eavesdrop on phone conversations and connect to the Internet.
4. **Car Whisperer:** It is a piece of software that allows attackers to send audio to and receive audio from a Bluetooth-enabled car stereo. The researchers are also investigating about possibility of an attacker accessing a telephone address book once the connection gets established with the Bluetooth system through this kind of attack

Fraud and computer-related fraud:

- Computer-related fraud is one of the most popular crimes on the Internet, as it enables the offender to use automation and software tools to mask criminals' identities.
- Automation enables offenders to make large profits from a number of small acts.
- One strategy used by offenders is to ensure that each victim's financial loss is below a certain limit.
- With a "small" loss, victims are less likely to invest time and energy in reporting and investigating such crimes.
- One example of such a scam is the Nigeria Advanced Fee Fraud.
- Although these offences are carried out using computer technology, most criminal law systems categorize them not as computer-related offences, but as regular fraud.
- The main distinction between computer- related and traditional fraud is the target of the fraud. If offenders try to influence a person, the offence is generally recognized as fraud.
- Where offenders target computer or data-processing systems, offences are often categorized as computer-related fraud.
- Those criminal law systems that cover fraud, but do not yet include the manipulation of computer systems for fraudulent purposes, can often still prosecute the above-mentioned offences.
- The most common fraud offences include online auction fraud and advanced fee fraud.

Online fraud:

- Online auctions are now one of the most popular e-commerce services.
- Already back in 2006, goods worth more than USD 20 billion were sold on eBay, the world's largest online auction marketplace.
- Buyers can access varied or specialist niche goods from around the world. Sellers enjoy a worldwide audience, stimulating demand and boosting prices.
- Offenders committing crimes over auction platforms can exploit the absence of face-to-face contact between sellers and buyers.

- The difficulty of distinguishing between genuine users and offenders has resulted in auction fraud being among the most popular of cybercrimes.
- The two most common methods include offering non-existent goods for sale and requesting buyers to pay prior to delivery and buying goods and asking for delivery, with no intention of paying.
- In response, auction providers have developed protection systems such as the feedback/comments system.
- After each transaction, buyer and sellers leave feedback for use by other users as neutral information about the reliability of sellers/buyers.
- In this case, "reputation is everything" and without an adequate number of positive comments, it is harder for offenders to persuade targets to either pay for non-existent goods or, conversely, to send out goods without receiving payment first.
- However, criminals have responded and circumvented this protection through using accounts from third parties.514 In this scam called "account takeover", offenders try to get hold of user names and passwords of legitimate users to buy or sell goods fraudulently, making identification of offenders more difficult.
- In advance fee fraud, offenders send out e-mails asking for recipients' help in transferring large amounts of money to third parties and promise them a percentage, if they agree to process the transfer using their personal accounts.
- The offenders then ask them to transfer a small amount to validate their bank account data (based on a similar perception as lotteries – respondents may be willing to incur a small but certain loss, in exchange for a large but unlikely gain) or just send bank account data directly.
- Once they transfer the money, they will never hear from the offenders again. If they send their bank account information, offenders may use this information for fraudulent activities.
- Evidence suggests that thousands of targets reply to e-mails.
- Current researches show that, despite various information campaigns and initiatives, advance fee frauds are still growing – in terms of both the number of victims and total losses.
- Computer-related forgery describes the manipulation of digital documents.
- The offence can for example be committed by creating a document that appears to originate from a reliable institution, manipulating electronic images (for example, pictures used as evidence in court) or altering text documents.
- The falsification of e-mails is an essential element of phishing, which is a serious challenge for law- enforcement agencies worldwide.
- "Phishing" seeks to make targets disclose personal/secret information.
- Often, offenders send out e-mails that look like communications from legitimate financial institutions used by the target.

- The e-mails are designed in a way that it is difficult for targets to identify them as fake e-mails.
- The e-mail asks recipient to disclose and/or verify certain sensitive information.
- Many victims follow the advice and disclose information enabling offenders to make online transfers etc.
- In the past, prosecutions involving computer-related forgery were rare, because most legal documents were tangible documents.
- Digital documents play an ever more important role and are used more often.
- The substitution of classic documents by digital documents is supported by legal means for their use, e.g. by legislation recognizing digital signatures.
- Criminals have always tried to manipulate documents.
- With digital forgeries, digital documents can now be copied without loss of quality and are easily manipulated. For forensic experts, it is difficult to prove digital manipulations, unless technical protection is used to protect a document from being falsified.
- Unlike a real casino, large financial investments are not needed to establish online casinos.
- In addition, the regulations on online and offline casinos often differ between countries.
- Tracing money transfers and proving that funds are not prize winnings, but have instead been laundered, is only possible if casinos keep records and provide them to law-enforcement agencies.
- Current legal regulation of Internet-based financial services is not as stringent as traditional financial regulation.
- Apart from gaps in legislation, difficulties in regulation arise from challenges in customer verification, since accurate verification may be compromised, if the financial service provider and customer never meet.
- In addition, the lack of personal contact makes it difficult to apply traditional know-your-customer procedures. Furthermore, the Internet transfers often involve the cross-border participation of providers in various countries.
- Finally monitoring transactions is particularly difficult if providers allow customers to transfer value in a peer-to-peer model.
- The term identity theft – which is neither consistently defined nor consistently used – describes the criminal act of fraudulently obtaining and using another person's identity.
- These acts can be carried out without the help of technical means as well as online by using Internet technology.
- Wide media coverage, the results of various surveys analysing the extent of and loss caused by identity theft, as well as numerous legal and technical analyses

published in recent years could easily lead to the conclusion, that identity-related offences are a 21st-century phenomenon.

- But this is not the case, as offences related to impersonation and the falsification and misuse of identity documents have existed for more than a century.
- Already back in the 1980s, the press intensively reported on the misuse of identity-related information.
- The emerging use of digital identities and information technology only changed the methods and targets of the offenders.
- Increasing use of digital information opened up new possibilities for offenders to gain access to identity-related information.
- Thus, the transformation process from industrialized nations to information societies has had a big influence on the development of identity-theft offences.
- Nonetheless, despite the large number of Internet-related identity-theft cases, digitization did not fundamentally change the offence itself, but merely created new targets and facilitated the development of new methods.
- The impact of the increasing use of Internet technology seems to be overestimated. Based on the results of a method analysis of identity-related offences, identity theft to a large degree remains an offline crime.
- In 2007, 20 per cent of the offences in the US542 were online scams and data breaches.
- Despite recent developments the offline identity theft remains highly relevant.
- The persisting importance of offline crimes is surprising, insofar as the digitization and moreover the globalization of network-based services has led to increasing use of digital identity- related information.
- Identity-related information is of growing importance, both in the economy and in social interaction.
- In the past, a "good name" and good personal relations dominated business as well as daily transactions.
- With the transfer to electronic commerce, face-to-face identification is hardly possible, and as a consequence identity-related information has become much more important for people participating in social and economic interaction.
- This process can be described as instrumentalization, whereby an identity is translated into quantifiable identity-related information.
- This process, along with the distinction between the more philosophical aspect of the term "identity" and the quantifiable identity-related information that enables the recognition of a person, is of great importance.
- The transformation process is not just relevant to Internet-related features of identity theft, as the impact of the development goes far beyond computer networks.

- Nowadays, the requirements of non-face-to-face transactions, such as trust and security, dominate the economy in general and not just e-commerce businesses.
- An example is the use of payment cards with a PIN (personal identification number) for purchasing goods in a supermarket.
- In general, the offence described as identity theft contains three different phases.
- In the first phase the offender obtains identity-related information.
- This part of the offence can for example be carried out by using malicious software or phishing attacks.
- The second phase is characterized by interaction with identity-related information prior to the use of the information within criminal offences.
- An example is the sale of identity-related information.
- Credit-card records are for example sold for up to USD 60.
- The third phase is the use of the identity-related information in relation with a criminal offence.
- In most cases, the access to identity-related data enables the perpetrator to commit further crimes.
- The perpetrators are therefore not focusing on the set of data itself but the ability to use the data in criminal activities.
- Examples for such offence can be the falsification of identification documents or credit-card fraud.
- The methods used to obtain data in phase one cover a wide range of acts. The offender can use physical methods, for example stealing computer storage devices with identity-related data, searching trash or mail theft.
- In addition, they can use search engines to find identity-related data. "Googlehacking" or "Googledorks" are terms that describe the use of complex search-engine queries to filter through large amounts of search results for information related to computer security issues as well as personal information that can be used in identity-theft scams.
- One aim of the perpetrator can for example be to search for insecure password protection systems in order to obtain data from the system.
- Reports highlight the risks involved with the legal use of search engines for illegal purposes.
- Similar problems are reported with regard to file-sharing systems.
- The United States Congress discussed recently the possibilities of exploiting file-sharing systems to obtain personal information that can be abused for identity theft.
- Apart from that, the offenders can make use of insiders, who have access to stored identity-related information, to obtain that information.

- The 2007 CSI Computer Crime and Security Survey561 shows that more than 35 per cent of the respondents attribute a percentage of their organization's losses greater than 20 per cent to insiders.
- In 2013, a survey showed that 23 per cent of the electronic crimes are linked to insiders and that 53 per cent of the respondents believe that insider attacks are more damaging than outsider attacks.

- Finally the perpetrators can use social engineering techniques to persuade the victim to disclose personal information. In recent years perpetrators have developed effective scams to obtain secret information (e.g. bank-account information and credit-card data) by manipulating users through social engineering techniques.
- The type of data the perpetrators target varies. The most relevant data are social security and passport numbers, date of birth, address and phone numbers, and passwords.

Possible questions

Part-B (2 Marks)

1. Explain: Mishing, Vishing, Smishing
2. Difference between LDAP security and RAS security?
3. What is cryptographic security?
4. Write short notes on credit card frauds?
5. Explain about the media player control security

Part-C (6 Marks)

1. Explain the mobile and wireless devices?
2. Explain the credit card frauds in mobile and wireless computing
3. What is the authentication service security and cryptographic security
4. Explain in your own words what you understand about the LDAP security and RAS security\
5. Explain about the hacking Bluetooth
6. Discuss in detail about media player control

UNIT- IV
SYLLABUS

Mobile devices: security implications for organizations, managing diversity and proliferation of hand held devices, unconventional/ stealth storage devices, threads through lost and stolen devices, protecting data on lost devices, educating the laptop users. **Organizational Measures for Handling Mobile:** Devices-related security issues, encrypting organizational database, including mobile devices in security strategy. **Organizational security polices and Measures in Mobile Computing Era:** Importance of security polices relating to mobile computing devices, operating guidelines for implementing mobile device security policies, organizational polices for the use of Mobile Hand-Held devices. **Laptops:** Physical Security Countermeasures

Mobile Devices: Security Implications for Organizations:
Managing Diversity and Proliferation of Hand-Held Devices:

- Focus on the micro issues at the organization level. Organizations will implement security procedures and tools extensively, whereas others will place more value on cost and convenience.
- In addition, employee should be encouraged to register with the IT department any devices they use for themselves, so that access can be provisioned in a controlled manner and de-provisioned appropriately when the employee leaves
- Younger works are pushing many enterprises to embrace mobility solutions. These younger workers prefer instant/text messaging instead of E-Mail, and frequently use social networking services such as Facebook, My Space and Twitter
- They often preferred to use personal, consumer-oriented devices in the work environment, and adapt quickly to new technology.
- These different points of view between younger and older workers have created a mobility generational gap.

Unconventional/ Stealth Storage Devices:

- Emphasize upon widening the spectrum of mobile devices and focus on secondary storage devices, such as compact disk and universal serial bus drives and employees.
- As the technology is advancing, the devices continue to decrease in size and emerge in new shapes and sizes- unconventional/stealth storage devices available nowadays are difficult to detect and have become a prime challenges for organizational security.
- Firewall and antivirus software are no defences against the threat of open USB ports.
- The features of the software allows system administrator to:

1. Monitor which users or group can access USB Ports, Wi-Fi and Bluetooth adapters, CD read-only memories and other removable devices.
2. Control the access to devices depending on the time of the day and day of the week
3. Set devices in read-only mode
4. Protect disks from accidental or intentional formatting

Threads through Lost and Stolen Devices:

- The cyber security threat under this scenario is scary; owing to a general lake of security in mobile devices, often not the value of the hand-held device that is important but rather the content that, if lost or stolen, can put a company at a serious risk of sabotage, exploitation or damage to its professional integrity, as most of the times the mobile hand-held devices are provided by the organization.
- This shows that the popularity of mobile devices is increasing at a rapid rat; however, people have not been educated about the importance of securing them.
- Mobile users are in an even worse position now because they are far more reliant on their mobile devices to storage large amounts of sensitive information with very few concerned about backing it up or protecting it.

Protecting Data on Lost Devices:

- At an individual level, employees need to worry about this. There are two reasons why cyber security needs to addresses this issue: data that are persistently stored on the device and always running applications.
- There are two precautions that individuals can take to prevent disclosure of the data stored on a mobile device
  (a) Encrypting sensitive data
  (b) Encrypting entire file system
- Data that are stored on the hard disks in persistent memory or on removable memory sticks should be protected
- There are solutions using which individuals can enforce a self-destruct policy to destroy privileged data on a lost device or create a database action to delete data on a user's device using a suitable tool.
- Writing the emergency contact information on the device itself is unlikely to be very helpful.

Educating the Laptop Users:

- According to year 2004 finding, through one survey, it was found, that some 86% of employees with laptops admitted to installing software onto their machines when outside of the office, with many using their laptops to access peer-to-peer websites and downloading illegal music files and movies.

- As per one survey of 500 European business laptop users, Malicious code, such as spyware and viruses, is infecting laptops and consequently business networks when they are reconnected to the corporate systems.
- This shows how much role "perception" plays in terms of most people perceiving laptops as greater culprits compared with other innocuous-looking mobile hand-held devices.
- Software asserts on laptops become more complex as more applications are used on an increasingly sophisticated OS with divers connectivity options.

Organizational Measures for Handling Mobile Devices-Related Security Issues:
Encrypting organizational Databases:

- Critical and sensitive data reside on database and with the advances in technology, access to these data is not impossible through hand-held devices.
- It is clear that to protect the organization's data loss, such as databases need encryption. Advanced Encryption Standard (AES) for block ciphers by the Institute of National Institute of Technology (NIST)
- The other algorithm is used to implement strong encryption of database files in the Multi-Dimensional Space Rotation (MDSR) algorithm developed by Casio
- Strong encryption means that it is much harder to break, but it is also has a significant impact on performance. Database file encryption technology, using either the AES or the MDSR algorithms, make the database file inoperable without the key.
- When using a strong encryption, lose the key, data are completely inaccessible. The key is a case-sensitive and must be entered correctly to access database.
- When a device that is identified as lost or stolen connects to the organization servers, IT department can have the server send a package to destroy privileged data on the devices.

Including Mobile Devices in Security Strategy:

- Encryption of corporate databases in not the end of everything. However, enterprises that do not want to include mobile devices in their environments often use security as an excuse, saying they fear the loss of sensitive data could result from a PDA being stolen or an unsecured wireless connection being used.
- Their concerns are no longer viable. There are technologies available to properly secure devices. These should be good enough for most organizations.
- A few things that enterprises can use are:
- Implement strong asset management, virus checking, loss prevention and other controls for mobile systems that will prohibit unauthorized access and the entry of corrupted data.
- Investigate alternatives that allow a secure access to the company information through a firewall, such as mobile VPN's
- Develop a system of more frequent and through security audits for mobile devices.
- Understands how important an issue security is within a company's overall strategy.
- User accounts are closely monitored for any unusual activity for a period of time.

- In summary, statistical information is useful to draw attention to the continuing and growing importance of the issue, and it is necessary to point out that one of the major challenges related to cybercrime is the lack of reliable information on the extent of the problem, as well as on arrests, prosecutions and convictions.
- As already stated, crime statistics often do not list offences separately, and available statistics on the impact of cybercrime are in general unable to provide reliable information about the scale or extent of offences at a level sufficient for policy-makers.
- Without such data, it is difficult to quantify the impact of cybercrime on society and to develop strategies to address the issue.
- Nevertheless, the statistics can serve as a basis for determining trends, which can be found by comparing results over several years, and serve as guidance with regard to the process of reporting cybercrime.
- The following numbers have been extracted from different surveys.
- As further discussed below, they are not necessarily representative, and are thus presented only to give an insight into the results of such surveys.

- Credit card and bank account information are among the most popular information advertised on underground economy services.
- The prices range between USD 0.85-USD 30 (single credit card information) and USD 15-USD 850
- In 2007, auction fraud was among the top Internet scams in the US, with an average loss of more than USD 1 000 per case.
- In 2005, losses as a result of identity-related offences in the US totalled USD 56.6 billion.180
- The financial and personal cost of cybercrime varies significantly among single incidents in Ireland, generating aggregate costs of over EUR 250 000.181
- A single computer security company created more than 450 000 new malicious code signatures in a single quarter.
- A quarter of all companies responding to a questionnaire in 2010 reported operational losses as a result of cybercrime.
- Decreasing number of denial-of-service and computer-virus attacks reported by security professionals between 2004 and 2008.
- In 2009, the United States, China, Brazil, Germany and India were among the countries reporting most malicious activities.
- In 2014, the global annual loss due to cybercrime was estimated between 375 and 575 billion USD.
- With an estimated loss equivalent to 1.6 per cent of the whole GDP, Germany is the country most affected by cybercrime.
- In the US, the losses are an estimated 0.64 per cent of the GDP, in Brazil 0.32 per cent of the GDP and in Kenya 0.01 per cent.

- The average cost of data breaches are 136 USD per capita. As a consequence of a single hacking attack related to a customer database the company Sony experienced direct costs of around 170 000 000 USD.
- There are several concerns related to the use of such surveys in determining the extent and impact of cybercrime.
- It is very difficult to provide reliable estimations of financial losses.
- Some sources estimate losses to businesses and institutions in the United States due to cybercrime to be as high as USD 67 billion in a single year; however, it is uncertain whether the extrapolation of sample survey results is justifiable.
- This methodological criticism applies not only to losses, but also to the number of recognized offences.
- Another difficulty related to statistical information is the fact that very often either unreliable or non- verifiable information is repeatedly quoted.
- One example of this relates to statistical information on the commercial aspects of Internet child pornography. Several analyses quote, for example, that Top Ten Reviews estimated that Internet child pornography generates USD 2.5 billion annually worldwide.
- Yet Top Ten Reviews does not provide any background information on how the research was undertaken.
- Bearing in mind that Top Ten Review claims on its website that the company "gives you the information you need to make a smart purchase.
- Through our side-by-side comparison charts, news, articles, and videos we simplify the buying process for consumers", there may be serious concerns as to the use of such data. Another example of figures quoted without verifiable reference was discovered by the Wall Street Journal in 2006.
- While investigating a quotation that child pornography is a multi-billion dollar business the journalist reported that two main documents containing information about revenues from USD 3 billion to 20 billion – a publication from NCMEC and one from the Council of Europe – referred to institutions that did not confirm the numbers.

Organizational Security Policies and Measures in Mobile Computing Era:
Importance of Security Policies relating to Mobile Computing Devices:

- Not only would this be a public relation (PR) disaster, but it could also violate laws and regulations. One should give a deep through about the potential legal troubles for a public company whose sales reports, employee records or expansion plans may fall into wrong hands.
- When controls cannot be implemented to protect data in the event they are stolen, the simplest solution is to prevent users from storing proprietary information on platforms deemed to be insufficiently secure.
- The scenarios described the following:

1. A CEO's administrative assistant uses a cell phone to arrange ground transportation that reveals the CEO's identity and location.
2. The finance and accounting staff discusses earning of press released and one participant on the call is using a cell phones.

Operating Guidelines for Implementing Mobile Devices Security Policies:

- Organizations can, however, reduce the risk that confidential information will be accessed from lost or stolen mobile devices through the following steps:
  1. Determine whether the employees in the organization need to use mobile computing devices at all, based on their risks and benefits within the organization, industry and regulatory environment
  2. Implement additional security technologies, as appropriate to fit both the organization and the types of devices used
  3. Standardize the mobile computing devices and the associated security tools being used with them.
  4. Centralized management of mobile computing devices. Maintain an inventory so that know who is using what kind of devices.
  5. Establish patching procedures for software on mobile devices.
  6. Label the devices and register them with a suitable service that helps return recovered devices to the owners.

Organizational Policies for the Use of Mobile Hand-Held Devices:

- The first step in securing mobile devices is creating company policies that address the unique issues these device raise.
- There are many ways to handle the matter of creating policy for mobile devices. One way is creating a distinct mobile computing policy. Another way is including such devices under existing policy.
- As a part of this approaches, between, where mobile devices fall under both existing general policies and a new one
- There may not be a need for separate policies for wireless, LAN, wide area network (WAN). Because a properly written network policy can cover all connections to the company data, including mobile and wireless.
- It is never too early to start planning for mobile devices, even when a company, at a given point of time, cannot afford creating any special security policies mitigate the threats posed by mobile computing devices to cyber security.
- A growing number3of websites present material that is in some countries covered by provisions related to religious offences, e.g. anti-religious written statements.
- Although some material documents objective facts and trends this information may be considered illegal in some jurisdictions.
- Examples include the defamation of religions or the publication of cartoons.

- The Internet offers advantages for those who wish to debate or deal critically with a subject – people can leave comments, post material or write articles without having to disclose their identity.
- Many discussion groups are based on the principle of freedom of speech.
- Freedom of speech is a key driver behind the Internet's success, with portals that are used specifically for user-generated content.
- Whilst it is vital to protect this principle, even in the most liberal countries the application of principles of freedom of speech is governed by conditions and laws.
- The differing legal standards on illegal content reflect the challenges of regulating content.
- Even where the publication of content is covered by provisions relating to freedom of speech in the country where the content is available, this material can be accessed from countries with stricter regulations.
- The "cartoon dispute" in 2005 demonstrated the potential for conflict.
- The publication of twelve editorial cartoons in the Danish newspaper Jyllands-Posten led to widespread protests across the Muslim world.
- As with illegal content, the availability of certain information or material is a criminal offence in some countries.
- The protection of different religions and religious symbols differs from country to country.
- Some countries criminalize the use of derogatory remarks in respect of the Holy Prophet or the defiling of copies of the Holy Quran, while other countries may adopt a more liberal approach and may not criminalize such acts.

Laptops:

- Wireless capability in these devices has also raised cyber security concerns owing to the information being transmitted over other, which makes it hard to detect. The organizations can take in the face of cyber security threat brought by the wide-spreading use of laptops.
- The theft of laptops have always been a major issue, according to the cyber security industry and insurance company statistics.
- Cyber criminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market.
- Very few laptop thieves are actually interested in the information that is contained in the laptop. Most laptops contain personal and corporate information that could be sensitive
- Such information can be misused if found by a malicious user. However, this is not true.

Physical Security Countermeasures:

- Organizations are heavily dependent upon a mobile workforce with access to information, no matter where they travel.

- Management also has to take care of creating awareness among the employees about physical security countermeasures by continuous training monitoring of organizational policies and procedures about these physical security countermeasures

1. **Cables and hardware locks**: The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops. These cables come with a variety of options such as number locks, key locks and alarms. The other disadvantages of security cables is when the laptop is locked to an object that is not fixed or is weak enough for anyone to break it. In certain cases of laptops thefts, the dismantled or smashed the fixed item to which the laptop was attached to.
2. **Laptop safes:** Safes made of polycarbonate-the same material that is used in bulletproof windows, police riot shields and bank security screens- can be used to carry and safeguard the laptops.
3. **Motion sensors and alarms:** Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these device are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places. They also source the password and encryption keys and prevent access to the OS.
4. **Warning labels and stamps:** Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft. Such labels are highly recommended for the laptops issued to top executive and/or key employees of the organization.
5. **Other measures for protecting laptops are as follows:**
   - Engraving the laptop with personal details.
   - Keeping the laptop close to oneself wherever possible
   - Carrying the laptop in a different and unobvious bag making it unobvious to potential thieves
   - Creating the awareness among the employees to understand the responsibility of carrying a laptop and also about the sensitivity of the information contained in the laptop.
   - Making a copy of the purchase receipt, laptop serial number and description of the laptop.
   - Never leaving the laptop unattended in public places
   - Disabling IR ports and wireless cards and removing PCMCIA cards when not in use.

- Most reports, guides or publications on cybercrime begin by defining the terms “computer crime” and “cybercrime”. In this context, various approaches have been adopted in recent decades to develop a precise definition for both terms.

- Before providing an overview of the debate and evaluating the approaches, it is useful to determine the relationship between "cybercrime" and "computer-related crimes".
- Without going into detail at this stage, the term "cybercrime" is narrower than computer-related crimes as it has to involve a computer network.
- Computer-related crimes cover even those offences that bear no relation to a network, but only affect stand-alone computer systems.
- During the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, two definitions were developed within a related workshop: Cybercrime in a narrow sense (computer crime) covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them.
- Cybercrime in a broader sense covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.
- One common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity.
- There are several difficulties with this broad definition. It would, for example, cover traditional crimes such as murder, if perchance the offender used a keyboard to hit and kill the victim.
- Another broader definition is provided in Article 1.1 of the Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism, which points out that cybercrime refers to acts in respect to cyber systems.
- Some definitions try to take objectives or intentions into account and define cybercrime more precisely, such as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks"
- These more refined descriptions exclude cases where physical hardware is used to commit regular crimes, but they risk excluding crimes that are considered as cybercrime in international agreements such as the Commonwealth Model Law on Computer and Computer-related Crime or the Council of Europe Convention on Cybercrime
- For example, a person who produces USB99 devices containing malicious software that destroys data on computers when the device is connected commits a crime as defined by Article 4 of the Convention on Cybercrime.
- However, since the act of deleting data using a physical device to copy malicious code has not been committed through global electronic networks, it would not qualify as cybercrime under the narrow definition above.
- Such acts would only qualify as cybercrime under a definition based on a broader description, including acts such as illegal data interference.
- The variety of approaches, as well as the related problems, demonstrates that there are considerable difficulties in defining the terms "computer crime" and "cybercrime"

- The term "cybercrime" is used to describe a range of offences including traditional computer crimes, as well as network crimes.
- As these crimes differ in many ways, there is no single criterion that could include all acts mentioned in the different regional and international legal approaches to address the issue, whilst excluding traditional crimes that are just facilitated by using hardware.
- The fact that there is no single definition of "cybercrime" need not be important, as long as the term is not used as a legal term.
- Instead of referring to a definition, the following chapters will be based on a typology-related approach**.**
- The term "cybercrime" is used to cover a wide variety of criminal conduct As recognized crimes include a broad range of different offences, it is difficult to develop a typology or classification system for cybercrime.
- One approach can be found in the Convention on Cybercrime, which distinguishes between four different types of offences:
  1. offences against the confidentiality, integrity and availability of computer data and systems
  2. computer-related offences
  3. content-related offences and
  4. copyright-related offences
- This typology is not wholly consistent, as it is not based on a sole criterion to differentiate between categories.
- Three categories focus on the object of legal protection: "offences against the confidentiality, integrity and availability of computer data and systems"; content-related offences; and copyright- related offences.
- The fourth category of "computer-related offences" does not focus on the object of legal protection, but on the method used to commit the crime. This inconsistency leads to some overlap between categories.
- In addition, some terms that are used to describe criminal acts cover acts that fall within several categories.
- Nonetheless, the four categories can serve as a useful basis for discussing the phenomena of cybercrime.
- The criminal abuse of information technology and the necessary legal response are issues that have been discussed ever since the technology was introduced.
- Over the last 50 years, various solutions have been implemented at the national and regional levels.
- One of the reasons why the topic remains challenging is the constant technical development, as well as the changing methods and ways in which the offences are committed.
- Crime statistics can be used by academia and policy-makers as a basis for discussion and for the ensuing decision-making process.

- Furthermore, access to precise information on the true extent of cybercrime would enable law-enforcement agencies to improve anti-cybercrime strategies, deter potential attacks and enact more appropriate and effective legislation.
- However, it is difficult to quantify the impact of cybercrime on society on the basis of the number of offences carried out in a given time-frame.
- Such data can in general be taken from crime statistics and surveys, but both these sources come with challenges when it comes to using them for formulating policy recommendations.
- The following numbers have been extracted from national crime statistics. As further discussed below, they are not intended to be representative of either the global development of cybercrime or of the true extent of cybercrime at the national level, and are thus presented only to provide an insight into country information.
- For 2013 the US Internet Complaint Centre reports a 48.8 per cent increase in reported losses compared with 2012.
- German Crime Statistics indicate that the overall number of Internet-related crimes increased by 12.2 per cent in 2013 compared with 2012.
- It is unclear how representative the statistics are and whether they provide reliable information on the extent of crime.
- There are several difficulties associated with determining the global threat of cybercrime on the basis of crime statistics.
- First of all, crime statistics are generally created at the national level and do not reflect the international scope of the issue.
- Even though it would theoretically be possible to combine the available data, such an approach would not yield reliable information because of variations in legislation and recording practices.
- Combining and comparing national crime statistics requires a certain degree of compatibility that is missing when it comes to cybercrime.
- Even if cybercrime data are recorded, they are not necessarily listed as a separate figure.
- Furthermore, statistics only list crimes that are detected and reported. Especially with regard to cybercrime, there are concerns that the number of unreported cases is significant.
- Businesses may fear that negative publicity could damage their reputation. If a company announces that hackers have accessed their server, customers may lose faith.
- The full costs and consequences could be greater than the losses caused by the hacking attack.
- On the other hand, if offenders are not reported and prosecuted, they may go on to re-offend. Victims may not believe that law-enforcement agencies will be able to identify offenders.
- Comparing the large number of cybercrimes with the few successful investigations, they may see little point in reporting offences.

- As automation of attacks enables cybercriminals to pursue a strategy of reaping large profits from many attacks targeting small amounts the possible impact of unreported crimes could be significant.
- For only small amounts, victims may prefer not to go through time-consuming reporting procedures.
- Reported cases are often the ones that involve very large amounts.

.

- As surveys often only count incidents without providing further information or details, it is difficult to draw conclusions with regard to trends.
- One example is the United States CSI195 Computer Crime and Security Survey 2007 that analyses the number of computer-related offences committed, among other trends.
- It is based on the responses of 494 computer security practitioners from US corporations, government agencies and financial institutions in the US.
- The survey documents the number of offences reported by respondents between 2000 and 2007.
- It shows that, since 2001, the proportion of respondents who experienced and acknowledged virus attacks or unauthorized access to information decreased.
- The survey does not explain why this decrease has occurred.
- The surveys on cybercrime are unable to provide reliable information about the scale or extent of offences.
- The uncertainty about the extent to which offences are reported by targets, as well as the fact that no explanation for the reducing numbers of cybercrimes can be found, render these statistics open to interpretation.
- At present, there is insufficient evidence for predictions on future trends and developments.
- The offence described as “hacking” refers to unlawful access to a computer system, one of oldest computer-related crimes.
- Following the development of computer networks, this crime has become a mass phenomenon.
- Famous targets of hacking attacks include the US National Aeronautics and Space Administration (NASA), the US Air Force, the Pentagon, Yahoo, Google, eBay and the German Government.
- Examples of hacking offences include breaking the password of password-protected websites and circumventing password protection on a computer system.
- But acts related to the term “hacking” also include preparatory acts such as the use of faulty hardware or software implementation to illegally obtain a password to enter a computer system, setting up “spoofing” websites to make users disclose their passwords and installing hardware and software-based key logging methods that record every keystroke – and consequently any passwords used on the computer and/or device.

- The motivation of offenders varies. Some offenders limit their activities to circumventing security measures only in order to prove their abilities.
- Others act through political motivation – one example is a recent incident involving the main United Nations website.
- In most cases, though, the motivation of the offender is not limited to illicit access to a computer system.
- Offenders use this access to commit further crimes, such as data espionage, data manipulation or denial- of-service (DoS) attacks.
- In most cases, illegal access to the computer system is only a vital first step.
- Many analysts recognize a rising number of attempts to illegally access computer systems, with over 250 million incidents recorded worldwide during the month of August 2007 alone.
- Three main factors have supported the increasing number of hacking attacks: inadequate and incomplete protection of computer systems, development of software tools that automate the attacks, and the growing role of private computers as a target of hacking attacks.
- Hundreds of millions of computers are connected to the Internet, and many computer systems are without adequate protection in place to prevent illegal access.
- Analysis carried out by the University of Maryland suggests that an unprotected computer system that is connected to the Internet is likely to experience attack within less than a minute.
- The installation of protective measures can lower the risk, but successful attacks against well-protected computer systems prove that technical protection measures can never completely stop attacks.
- Recently, software tools are being used to automate attacks.
- With the help of software and pre- installed attacks, a single offender can attack thousands of computer systems in a single day using one computer.
- If the offender has access to more computers – e.g. through a botnet – he/she can increase the scale still further.
- Since most of these software tools use preset methods of attacks, not all attacks prove successful.
- Users that update their operating systems and software applications on a regular basis reduce their risk of falling victim to these broad-based attacks, as the companies developing protection software analyse attack tools and prepare for the standardized hacking attacks.
- High-profile attacks are often based on individually-designed attacks. The success of those attacks is often not the result of highly sophisticated methods, but the number of attacked computer systems.
- Tools enabling these standardized attacks are widely available over the Internet – some for free, but efficient tools can easily cost several thousand US dollars.

- One example is a hacking tool that allows the offender to define a range of IP-addresses (e.g. from 111.2.0.0 to 111.9.253.253).
- The software allows for the scanning for unprotected ports of all computers using one of the defined IP-addresses.
- Access to a computer system is often not the primary motivation of an attack.
- Since business computers are generally better protected than private computers, attacks on business computers are more difficult to carry out using pre-configured software tools.
- Over the past few years, offenders have focused their attacks increasingly on private computers, since many private computers are inadequately protected.
- Further, private computers often contain sensitive information (e.g. credit card and bank account details).
- Offenders are also targeting private computers because, after a successful attack, offenders can include the computer in their botnet and use the computer for further criminal activities.
- Illegal access to a computer system may be viewed as analogous to illegal access to a building and is recognized as a criminal offence in many countries.
- Analysis of different approaches to the criminalization of computer access shows that enacted provisions in some cases confuse illegal access with subsequent offences or attempt to limit criminalization of illegal access to grave violations only.
- Some provisions criminalize the initial access, while other approaches limit the criminal offence only to those cases where the accessed system is protected by security measures or the perpetrator has harmful intentions or data was obtained, modified or damaged.
- Other legal systems do not criminalize mere access, but focus on subsequent offences.
- A more recent analysis shows a trend towards more sophisticated and targeted attacks in addition to the broad and wide-scale attacks that have dominated previous decades.
- While large scale attacks are following an opportunistic approach and can easier be carried out, targeted attacks will require more energy from the offender but are significantly more effective and damaging for the victim.
- Sensitive information is often stored in computer systems.
- If the computer system is connected to the Internet, offenders can try to access this information via the Internet from almost any place in the world.
- The Internet is increasingly used to obtain trade secrets.
- The value of sensitive information and the ability to access it remotely makes data espionage highly interesting.
- In the 1980s, a number of German hackers succeeded in entering US government and military computer systems, obtaining secret information and selling this information to agents from a different country.
- Offenders use various techniques to access victims' computers, including software to scan for unprotected ports or circumvent protection measures, as well as "social engineering".

- The last approach especially, which refers to a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people into breaking normal security procedures, is interesting as it not based on technical means.
- In the context of illegal access it describes the manipulation of human beings with the intention of gaining access to computer systems.
- Social engineering is usually very successful, because the weakest link in computer security is often the users operating the computer system.
- One example is "phishing", which has recently become a key crime committed in cyberspace and describes attempts to fraudulently acquire sensitive information (such as passwords) by masquerading as a trustworthy person or business in a seemingly official electronic communication.
- Although the human vulnerability of users opens the door to the risk of scams, it also offers solutions.
- Well-educated computer users are not easy victims for offenders using social engineering.
- As a consequence, user education should be an essential part of any anti-cybercrime strategy.
- In addition, technical measures can be taken to prevent illegal access.
- OECD highlights the importance of cryptography for users, as cryptography can help improve data protection.
- If the person or organization storing information uses proper protection measures, cryptographic protection can be more efficient than any physical protection.
- The success of offenders in obtaining sensitive information is often due to the absence of protection measures.
- Since important information is increasingly being stored in computer systems, it is essential to evaluate whether the technical protection measures taken by the users are adequate, or if law-makers need to establish additional protection by criminalizing data espionage.
- Although offenders usually target business secrets, data stored on private computers are also increasingly targeted.
- Private users often store bank-account and credit-card information on their computer.
- Offenders can use this information for their own purposes or sell it to a third party.
- Credit-card records are for example sold for up to USD 60.
- Hackers' focus on private computers is interesting, as the profits from business secrets are generally higher than the profits to be made from obtaining or selling single credit-card information.
- However, since private computers are generally less well protected, data espionage based on private computers is likely to become even more profitable.
- There are two approaches to obtaining information.

- Offenders can access a computer system or data storage device and extract information; or try to manipulate the user to make them disclose the information or access codes that enable offenders to access information.
- Offenders often use computer tools installed on victims' computers or malicious software called spyware to transmit data to them.
- Various types of spyware have been discovered over recent years, such as key loggers.
- Key loggers are software tools that record every keystroke typed on an infected computer's keyboard.
- Some key loggers send all recorded information to the offender, as soon as the computer is connected to the Internet.
- Others perform an initial sort and analysis of the data recorded to transmit only major data discovered.
- Similar devices are also available as hardware devices that are plugged in between the keyboard and the computer system to record keystrokes on the keyboard.
- Hardware-based key loggers are more difficult to install and detect, as they require physical access to the computer system.
- However, classical anti-spyware and anti-virus software is largely unable to identify them.
- Apart from accessing computer systems, offenders can also obtain data by manipulating the user.
- Recently, offenders have developed effective scams to obtain secret information by manipulating users using social engineering techniques.
- "Phishing" has recently become one of the most important crimes related to cyberspace.
- The term "phishing" is used to describe a type of crime that is characterized by attempts to fraudulently acquire sensitive information, such as passwords, by masquerading as a trustworthy person or business in an apparently official electronic communication.
- Developments such as "big data", where companies collect large amounts of data in order to carry out sophisticated analysis changed the relevance of data breaches in the threat landscape.
- If offenders get access to large databases with personal data of customers the mere data breach can lead to significant costs for the affected company – even if the offenders don't use the data to commit further offences.2
- The average cost of data breaches is 136 USD per capita
- As a consequence of a single hacking attack related to a customer database, the Sony company experienced direct costs of around 170 000 000 USD.
- Research published in 2014 indicates that the amount of data available on cyber black markets, which were obtained through data breaches, include credentials from up to 360 million accounts.

- Offenders can intercept communications between users (such as e-mails) or other forms of data transfers in order to record the information exchanged.
- In this context, offenders can in general target any communication infrastructure and any Internet service
- Most data-transfer processes among Internet infrastructure providers or Internet service providers are well protected and difficult to intercept.
- However, offenders search for weak points in the system. Wireless technologies are enjoying greater popularity and have in the past proved vulnerable.
- Nowadays, hotels, restaurants and bars offer customers Internet access through wireless access points.
- However, the signals in the data exchanges between the computer and the access point can be received within a radius of up to 100 metres.
- Offenders who wish to intercept a data-exchange process can do so from any location within this radius.
- Even where wireless communications are encrypted, offenders may be able to decrypt the recorded data.
- To gain access to sensitive information, some offenders set up access points close to locations where there is a high demand for wireless access (e.g. near bars and hotels).
- The station location is often named in such a way that users searching for an Internet access point are more likely to choose the fraudulent access point.
- If users rely on the access provider to ensure the security of their communication without implementing their own security measures, offenders can easily intercept communications.
- The use of fixed lines does not prevent offenders from intercepting communications.
- Data transmissions passing along a wire emit electromagnetic energy.
- If offenders use the right equipment, they can detect and record these emissions and may be able to record data transfers between users' computers and the connected system, and also within the computer system.
- Most countries have moved to protect the use of telecommunication services by criminalizing the illegal interception of phone conversations.
- However, given the growing popularity of IP-based services, law- makers may need to evaluate to what extent similar protection is offered to IP-based services.
- Computer data are vital for private users, businesses and administrations, all of which depend on the integrity and availability of data.
- Lack of access to data can result in considerable damage.
- Offenders can violate the integrity of data and interfere with them by deleting, suppressing or altering computer data.
- One common example of the deletion of data is the computer virus.
- Ever since computer technology was first developed, computer viruses have threatened users who failed to install proper protection.
- Since then, the number of computer viruses has risen significantly.

- Not only has the number of virus attacks increased, but also the techniques and functions of viruses have changed.
- Previously, computer viruses were distributed through storage devices such as floppy disks, whilst today most viruses are distributed via the Internet as attachments either to e-mails or to files that users download.
- These efficient new methods of distribution have massively accelerated virus infection and vastly increased the number of infected computer systems.
- The computer worm SQL Slammer was estimated to have infected 90 per cent of vulnerable computer systems within the first 10 minutes of its distribution.
- The financial damage caused by virus attacks in 2000 alone was estimated to amount to some USD 17 billion.289 In 2003, it was still more than USD 12 billion.
- Most first-generation computer viruses either deleted information or displayed messages.
- Recently, payloads have diversified.
- Modern viruses are able to install back-doors enabling offenders to take remote control of the victim's computer or encrypt files so that victims are denied access to their own files, until they pay money to receive the key.
- Based on reports published by security companies the number of computer viruses and other forms of malicious software increases continuously with up to 30 million new malware strings per year.
- Kaspersky reports that in 2013 they detected more than 300 000 new malicious files every day.
- The fact that most of those numbers are published by security companies that sell anti-virus software is certainly a challenge when determining the reliability of such data.
- But the development indicates that decades after the first computer virus was discovered malicious software is still a major challenge for Internet safety.
- The same concerns over attacks against computer data apply to attacks against computer systems.
- More businesses are incorporating Internet services into their production processes, with benefits of 24-hour availability and worldwide accessibility.
- If offenders succeed in preventing computer systems from operating smoothly, this can result in great financial losses for victims.
- Attacks can be carried out by physical attacks on the computer system.
- If offenders are able to access the computer system, they can destroy hardware. For most criminal legal systems, remote physical cases do not pose major problems, as they are similar to classic cases of damage or destruction of property.
- However, for highly profitable e-commerce businesses, the financial damages caused by attacks on the computer system are often far greater than the mere cost of computer hardware.
- More challenging for legal systems are web-based scams. Examples of these remote attacks against computer systems include computer worms and denial-of-service (DoS) attacks.

- Computer worms are a subgroup of malware (like computer viruses).
- They are self-replicating computer programs that harm the network by initiating multiple data-transfer processes.
- They can influence computer systems by hindering the smooth running of the computer system, using system resources to replicate themselves over the Internet or generating network traffic that can close down availability of certain services
- While computer worms generally influence the whole network without targeting specific computer systems, DoS attacks target specific computer systems.
- A DoS attack makes computer resources unavailable to their intended users.
- By targeting a computer system with more requests than the computer system can handle, offenders can prevent users from accessing the computer system, checking e-mails, reading the news, booking a flight or downloading files.
- In 2000, within a short time, several DoS attacks were launched against well-known companies such as CNN, eBay and Amazon.303 Similar attacks were reported in 2009 on government and commercial websites in the US and South Korea.
- As a result, some of the services were not available for several hours and even days.
- The prosecution of DoS and computer-worm attacks poses serious challenges to most criminal law systems, as these attacks may not involve any physical impact on computer systems.
- Apart from the basic need to criminalize web-based attacks, the question of whether the prevention and prosecution of attacks against critical infrastructure needs a separate legislative approach is under discussion.
- Despite the development of technical prevention tools and mitigation strategies denial of service attacks remain a challenge for companies and government institutions.
- Some researches indicate that the threat of such attacks and the related costs are increasing.
- Legal approaches to criminalize the illegal content should not interfere with the right to freedom of expression.
- The right to freedom of expression is for example defined by principle of the Johannesburg Principles on National Security and Freedom of Expression.
- However, principle clarifies that the right to freedom of expression may be subject to restrictions.
- While a criminalization of illegal content is therefore not per se precluded, it has to be strictly limited.
- Such limitations are especially discussed with regard to the criminalization of defamation.
- The 2008 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression and others points out that vague notions such as providing communications and the glorification or promotion of terrorism or extremism should not be criminalized.
- These legal challenges are complex, as information made available by one computer user in one country can be accessed from nearly anywhere in the world.

- If "offenders" create content that is illegal in some countries, but not in the country they are operating from, prosecution of the "offenders" is difficult, or impossible.
- There is much lack of agreement regarding the content of material and to what degree specific acts should be criminalized.
- .
- This makes the identification of offenders complicated.
- Furthermore, there may be no or little regulation of content by forum moderators.
- These advantages have not prevented the development of valuable projects such as the online user-generated encyclopaedia, Wikipedia, where strict procedures exist for the regulation of content.
- However, the same technology can also be used by offenders to publish false information or disclose secret information
- It is vital to highlight the increased danger presented by false or misleading information.
- Defamation can seriously injure the reputation and dignity of victims to a considerable degree, as online statements are accessible to a worldwide audience.
- The moment information is published over the Internet, the author often loses control of this information.
- Even if the information is corrected or deleted shortly after publication, it may already have been duplicated and made available by people that are unwilling to rescind or remove it.
- In this case, information may still be available on the Internet, even if it has been removed or corrected by the original source.
- Examples include cases of "runaway e-mails", where millions of people can receive salacious, misleading or false e-mails about people or organizations, where the damage to reputations may never be restored, regardless of the truth or otherwise of the original e-mail.
- Therefore the freedom of speech and protection of the potential victims of libel needs to be well balanced.

Possible questions

Part-B (2 Marks)

1. Write short notes on lost and stolen devices?
2. List out the importance and security policies?
3. How to protecting data on lost devices?

Part-C (6 Marks)

1. Explain unconventional/ stealth storage devices
2. Explain the concept of educating the laptop users
3. Discuss in detail about organizational measures for handling mobile devices related security issues
4. Elaborate about the organizational security policies and measures
5. Explain about the operating guidelines for implementing mobile devices and security polices

UNIT- V
SYLLABUS

Introduction: Tools and methods used in cybercrime, proxy servers and anonymizers, Phishing: How phishing works, **Password cracking:** Online attacks, offline attacks, Strong, weak and Random passwords, **Key loggers and spywares:** Software key loggers, hard ware key loggers, anti-key loggers, Spywares, **Virus and worms:** Types of viruses, **Trojan Horses and Backdoors:** Backdoor, Hoe to protect from Trojan Horses and Backdoors, **Steganography:** Steg-analysis, **DoS and DDoS Attacks:** DoS attacks, classification of DoS attacks, types or level of DoS attacks, Tools used to Launch DoS attack, DDoS attacks, How to protect from DoS/ DDoS attacks, **SQL injection:** Steps for SQL Injection Attack, How to prevent SQL injection attacks, **Buffer overflow:** Types of Buffer Overflow, How to minimize Buffer Overflow, **Attacks on wireless Networks:** Traditional Techniques of Attacks on wireless networks, theft of internet hours and Wi-Fi based frauds and misuses, How to secure the wireless networks

Introduction of Tools and Methods used in Cybercrime:

- Network attack incidents revel that attackers are often very systematic in launching their attacks. The basic stages of an attack are described here to understand how an attacker can compromise a network here:
  1. **Initial uncovering:** The first step is called as reconnaissance, the attacker gathers information, as much as possible, about the target by legitimate means- searching the information about the target on the Internet by Googling social networking websites and people finder websites
  2. **Network probe:** At the network probe stage, the attacker uses more invasive techniques to scan the information. Usually, a "ping sweep" of the network IP addresses is performed to seek out potential targets, and then a "port scanning" tool is used to discover exactly which services are running on the target system
  3. **Crossing the line toward electronic crime (E-crime):** Now the attackers is towards committing what is technically a "computer crime". Exploits usually include vulnerabilities in common gateway interface (CGI).certain programming errors can be used by attackers to compromise system and are quite common practice. Once the attackers are able to access a user account without many privileges, 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.

4. **Capturing the network**: The attacker will usually install that set of rules that replace existing files and services with Trojan files and services that have a backdoor password. This allows to attacker to return to the system at will, which means the attacker has "captured" the network**.** There are a number of "hacking tools" which can clean up log files and remove any trace of an intrusion; most of the time , they are individual programs written by hackers. Once the attacker has gained to access one system, he/she will then repeat the processing by using the system as a stepping stone to access other systems deeper within the network, as most networks have fewer defences against attacks from internal sources.
5. **Grab the data:** Now the attacker has "captured network", he/she takes advantage of this/her position to steal confidential data, customer credit card information, deface web pages, alter processes and even lunch attacks at other sites from network, causing a potentially expensive and embarrassing situation for an individual and or for an organization.
6. **Covering tacks:** 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.

Proxy Servers and Anonymizers:

- The proxy server is a computer on a network which act as an intermediary for connections with other computer on that network
- The attacker first connects 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. 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. A proxy server has following purposes:

1. Keep the systems behind the curtain
2. Speed up access to resource. It is usually used to cache the webpages from a web server
3. Specialized proxy server are used to filter unwanted content such as advertisement
4. Proxy server can be used as IP addresses multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address
    - One of the advent age of a proxy server is that its cache memory can serve all users. If one or more websites are requested frequently, may be different users, it is likely to be in the proxy's cache memory, which will improve user response time. In fact are special servers available known as cache servers.

- An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untrat6ceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information
- The anonymizer hides/removes all the identifying information from a user's computer while the user suffers on the Internet, Which ensure the privacy of the user.
- With the switch from analogue to digital, digitization461 has enabled the entertainment industry to add additional features and services to movies on DVD, including languages, subtitles, trailers and bonus material. CDs and DVDs have proved more sustainable than records and videotapes.
- Digitization has opened the door to new copyright violations. The basis for current copyright violations is fast and accurate reproduction.
- Before digitization, copying a record or a videotape always resulted in a degree of loss of quality. Today, it is possible to duplicate digital sources without loss of quality, and also, as a result, to make copies from any copy.
- The most common copyright violations include the exchange of copyright-protected songs, files and software in file-sharing systems or through share-hosting services and the circumvention of digital rights management (DRM) systems.
- File-sharing systems are peer-to-peer-based network services that enable users to share files, often with millions of other users.
- After installing file-sharing software, users can select files to share and use software to search for other files made available by others for download from hundreds of sources.
- Before file-sharing systems were developed, people copied records and tapes and exchanged them, but file-sharing systems permit the exchange of copies by many more users.
- Peer-to-peer (P2P) technology plays a vital role in the Internet. In 2007, over 50 per cent of consumer Internet traffic was generated by P2P networks.
- The number of users is growing all the time – a report published by the OECD estimates that some 30 per cent of French Internet users have downloaded music or files in file-sharing systems, with other OECD countries showing similar trends.
- File-sharing systems can be used to exchange any kind of computer data, including music, movies and software.
- Historically, file-sharing systems have been used mainly to exchange music, but the exchange of videos is becoming more and more important.
- The technology used for file-sharing services is highly sophisticated and enables the exchange of large files in short periods of time.
- First-generation file-sharing systems depended on a central server, enabling law-enforcement agencies to act against illegal file-sharing in the Napster network.

- Unlike first- generation systems (especially the famous Napster service), second-generation file-sharing systems are no longer based on a central server providing a list of files available between users.
- The decentralized concept of second-generation file-sharing networks makes it more difficult to prevent them from operating. However, due to direct communications, it is possible to trace users of a network by their IP- address.
- Law-enforcement agencies have had some success investigating copyright violations in file- sharing systems. More recent versions of file-sharing systems enable forms of anonymous communication and will make investigations more difficult.
- File-sharing technology is not only used by ordinary people and criminals, but also by regular businesses.
- Not all files exchanged in file-sharing systems violate copyrights. Examples of its legitimate use include the exchange of authorized copies or artwork within the public domain.
- Nevertheless, the use of file-sharing systems poses challenges for the entertainment industry. It is unclear to what extent falls in sales of CD/DVDs and cinema tickets are due to the exchange of titles in file-sharing systems. Research has identified millions of file-sharing users and billions of downloaded files.
- Copies of movies have appeared in file-sharing systems before they were officially released in cinemas at the cost of copyright-holders.
- The recent development of anonymous file-sharing systems will make the work of copyright-holders more difficult, as well as that of law-enforcement agencies.
- The entertainment industry has responded by implementing technology designed to prevent users from making copies of CDs and DVDs such as content scrambling systems (CSS), an encryption technology preventing content on DVDs from being copied.
- This technology is a vital element of new business models seeking to assign access rights to users more precisely.
- Digital rights management ((DRM) describes the implementation of technologies allowing copyright-holders to restrict the use of digital media, where customers buy limited rights only
- DRM offers the possibility of implementing new business models that reflect copyright-holders' and users' interests more accurately and could reverse declines in profits.
- One of the biggest difficulties with these technologies is that copyright-protection technology can be circumvented.

- Offenders have developed software tools that enable the users to make copy-protected files available over the Internet free of charge or at low prices. Once DRM protection is removed from a file, copies can be made and played without limitation.
- Efforts to protect content are not limited to songs and films. Some TV stations (especially pay-tv channels) encrypt programmes to ensure that only paying customers can receive the programme.
- Although protection technologies are advanced, offenders have succeeded in falsifying the hardware used as access control or have broken the encryption using software tools.

Phishing:

- While checking electronic mail one day a user find a message from the bank threating him/her to close the bank account if he/she does not reply immediately. Although the message seems to be suspicious from the message, it is difficult to conclude that it is a fake/false E-Mail.
- Phishing with email message that spoof or mimic banks, credit card companies or other business such as Amazon and eBay. These message look authenticate and attempt to get users personal information.

How Phishing Works?

1. **Planning:** Criminals, usually called as phishers, decide the target and determine how to get E-Mail address of that target or customers of that business. Phishers often use mass mailing and address collection techniques spammers.
2. **Setup:** Once phisher know which business/business house to spoof and who their victims are, they will create methods for delivering the message and to collect the data about the target. Most often this involves email addresses and a web page.
3. **Attack:** This is the step people are most familiar with- the phisher sends a phony message that appears to be from a reputable source
4. **Collection:** Phishers record the information of victim 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

- Phishers started off as being part of popular hacking culture.

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.
- 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. Example of guessable passwords include:
  1. Blank
  2. The words like "password", "passcode", and "admin"
  3. User's name or login name
  4. Name of the user's friend/relative/pet
  5. User's vehicle number, office number, resident number or mobile number
  6. Series of letters from the "QQWERTY" keyboard
  7. Simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters
- An attacker can also create a script file 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 resources.
- To ensure confidentially of passwords, the password verification data is usually not stored in a clear text format
- When a user attempt to login to the system by entering the password, the same function is applied to entered value and result is compared with the stored value. If they match, user gains the access; this process is called authentication.
- The most commonly used hash function can be computed rapidly and the attacker can test these hashes with the help of the passwords hacking tools.
- Usually, an attacker follows common approach- repeatedly making guesses for the password.
- Password cracking attacks can be classified under three categories as follows:
  1. Online attacks
  2. Offline attacks
  3. Non-electronic attacks

- Having access to passwords for accounts allows perpetrators to change the settings of the account and use it for their own purposes.
- They can for example take over an e-mail account and use it to send out mails with illegal content or take over the account of a user of an auction platform and use the account to sell stolen goods.
- Like the SSN, information regarding financial accounts is a popular target for identity theft.
- This includes cheque and saving accounts, credit cards, debit cards, and financial planning information. Such information is an important source for an identity thief to commit financial cybercrimes.
- Identity theft is a serious and growing problem. In the first half of 2004, 3 per cent of United States households fell victim to identity theft.
- In 2012 the Bureau of Justice Statistics announced that 7 per cent of all persons aged 16 or older in the US experienced at least one identity theft incident in 2012.
- In the United Kingdom, the cost of identity theft to the British economy has been calculated at GBP 1.3 billion every year.
- Estimates of losses caused by identity theft in Australia vary from less than USD 1 billion to more than USD 3 billion per year.
- The 2006 Identity Fraud Survey estimates the losses in the United States at USD 56.6 billion in 2005.
- The 2013 Identity Fraud report estimates the losses for 2012 at 20.9 billion. Losses may be not only financial, but may also include damage to reputations.
- In reality, many victims do not report such crimes, while financial institutions often do not wish to publicize customers' bad experiences.
- The actual incidence of identity theft is likely to far exceed the number of reported losses.
- Identity theft is based on the fact that there are few instruments to verify the identity of users over the Internet.
- It is easier to identify individuals in the real world, but most forms of online identification are more complicated. Sophisticated identification tools (e.g. using biometric information) are costly and not widely used.
- There are few limits on online activities, making identity theft easy and profitable.
- One phenomenon that is close related to the development towards "big data" is the increasing number of identity-related information that is available on "dark markets"
- If offenders break into data bases with millions of customer records a significant number might be sold afterwards.
- Research published in 2014 for example indicates that the amount of identity-related information available on cyber black markets that were obtained through data breaches, for example include credentials from up to 360 million accounts.

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-middle attack, also termed as "bucket-brigade attack" or sometimes "Janus attack"
- This type of attack is used to obtain the password for E-Mail accounts on public websites such as Yahoo, Hotmail and Gmail and can also used to get the password for financial websites that would like to gain access to banking websites
- 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.

Offline Attacks:

- Mostly offline attacks are performed from a location other than the target 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
- **Types:** Dictionary attack, Hybrid attack, Brute force attack

Strong, Weak and Random Password:

- A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found by executing a brute force attack and by using a subset of all possible passwords
- A strong passwords is long enough, random or otherwise difficult to guess- producible only by the user who chooses it
- The length of time deemed to be too long will vary with the attacker, the attacker's resources, the ease with which a password can be tried and the value of the password to the attacker.
- Some of the examples of "weak passwords"
  1. Susan: Common personal names
  2. aaaa: Repeated letters, can be guessed
  3. Abc123: can be easily guessed
  4. Password: used very often- trivially guessed
  5. December12: using the date of a forced password change is very common
  6. 1234: can be easily guessed
  7. Rover: common name for a pet, also dictionary word

Random Passwords:

- The difficulty in remembering such a password increases the chance that the user will write down the password, which makes it more vulnerable to a different attack

- Whether this represents a net reduction in security depends on whether the primary threat to security is internal or external
- A password can, at first sight, be random, but if you really examine it, it is just a pattern. One of these types of passwords is 268465. Although short, it is not easily guessed
- Many users dislike these measures, particularly when they have not been taken through security awareness training.
- The imposition of strong random passwords may encourage the user to write down passwords, store them in personal digital assistants (PDA) or cell phones and share them with others against memory failure, increasing the risk of disclosure
- The general guidelines applicable to the password policies, which can be implemented organization-wide, are as follows:

1. Passwords and user logon identities should be unique to each authorized user
2. Passwords should consist of a minimum of eight alphanumeric characters
3. Passwords should be kept private, that is, not shared with friends, colleagues. They shall not be coded into programs or noted down anywhere
4. User accounts should be froze after five failed logon attempts. All erroneous password entries should be recorded in an audit log for later inspection and action, as necessary
5. Session should be suspended after 15 minutes of inactivity and require the passwords to be re-entered
6. Successful logons should display the date and time of the last logon and logoff
7. Logon IDs and passwords should be suspended after a specified period of non-use

- Similarly, netizens should practice password guidelines to avoid being victim of getting their personal email accounts hacked/attacked by the attackers

1. Passwords used for business email accounts, personal email accounts and banking/financial user accounts should be kept separate
2. Passwords should be minimum eight alphanumeric characters
3. Passwords should be changed every 30/45 days
4. Passwords should not be shared with relative and/or friends
5. Passwords used previously should not be used while renewing the password
6. In case email accounts/user accounts have been hacked, respective agencies/institutes should be contacted immediately

Key loggers and Spywares:

- Key stroke logging, often called key logging, is the practice of noting 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 key logger is quicker and easier way of capturing the password and monitoring the victim's IT savvy behaviour. It can be classified as software key logger and hardware key logger

Software key loggers:

- Software key loggers 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 key loggers are installed on a computer system by Trojans viruses without the knowledge of the user
- Cyber criminals always install such tools on the insecure computer systems available in public places
- **Software key loggers are:**
  1. Elite key logger
  2. Cyber spy
  3. Powered key logger
  4. Spy Buddy
  5. Perfect key logger

Hardware key loggers:

- To install these key loggers, physical access to the computer system is required
- Hardware key loggers 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
- Each key press on the keyboard of the ATM gets registered by these key loggers.

Anti -key loggers:

- Anti-key logger is a tool that can detect the key loggers installed on the computer system and also can remove a tool.
- Advantages of anti-key loggers as follows:
  1. Firewalls cannot detect the installations of key loggers on the systems; hence, anti-key loggers can detect installations of key loggers
  2. This software does not require regular updates of signature bases to work effectively such as other anti-virus and anti-spy programs; if not updated, it does not serve the purpose, which makes user at risk
  3. It prevents ID theft
  4. It secure E-Mail and instant messaging/chatting

Spywares:

- Spywares is a type of malware 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 users personal computer.
- Sometimes, however, spywares such as key loggers are installed by the owner of shared, corporate or public computer on purpose to secretly monitor other users

- It is clearly understood from the term spyware that is secretly monitors the user. The features and function of such spywares are beyond simple monitoring
- Spyware programs collect personal information about the victim, such as Internet surfing habits/patterns and website visited
- The spyware also redirect internet surfing activity by installing another stealth utility on the user's computer system
- Various spywares are:
  1. Spy
  2. Spector pro
  3. Remote spy
  4. Stealth Recorder
  5. Wiretap professional

Virus and worms:

- Computer virus is a program that can "infect" legitimate programs by modifying them to include a possibly "evolved" copy of itself. Virus 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 can often spread without any readily visible symptoms. A virus can start on event-driven effects, time-driven effects 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 behaviour
  5. Halt the system
  6. Just replicate themselves to propagate further harm
- 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
- 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, Crime ware and other malicious unwanted software as well as viruses
- 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 hide malicious functions

1. **Different types:**
   Virus: stealth virus, self- modified virus, encryption with variable key virus, polymorphic code virus

   Worms: email worms, internet worms, IRC worms, file-sharing networks worms

2. **spread mode:**
   Virus: Needs a host program to spread

   Worm: self, without user intervention

3. **What is it? :**
   Virus: A computer virus is a software program that can copy itself and infect the data or information, without the user's knowledge. However, to spread to another computer, it needs a host program that carries the virus

   Worms: A computer program is a software program, self- replication in nature, which spreads through a network with or without user intervention

4. **Inception:**
   Virus: The creeper virus was considered as the first known virus. It was spread through ARPANET in the early 1970's

   Worms: The name worm originated from the shockwave rider, a science fiction novel published in 1975 by John F shock and john A Hupp at Xerox PARC published a paper in 1982, the worm programs and after that name was adopted

5. **Prevalence:**
   Virus: over 100,000 known computer viruses have been there through not all have attacked computers

   Worm: prevalence for virus is very high as against moderate prevalence for a worm.

Types of viruses:

- Computer viruses can be categorized based on attacks on various elements of the system and can put the system and personal data on the system in danger
  1. **Boot sector viruses:** It infects the storage media on which OS is stored and which is used to start the computer system. The entire data/programs are stored on the floppy disks and hard drives in smaller sections called sectors. The first sector is called the BOOT and it carries the master boot record. Boot sector viruses often spread to other systems when shared infected disks infected disks and pirated software(s) are used

2. **Program viruses:** These viruses become active when the program file is executed. Once these program files get infected, the virus makes copies of itself and infects the other programs on the computer system.
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. It will infect the local drive and other programs on the victim's computer systems
4. **Stealth viruses:** It camouflages and/or makes itself and so detecting this type of virus is very difficult. It can disguise itself such a way that antivirus software also cannot detect it thereby preventing spreading into the computer system. It alters its file size and conceals itself in the computer memory to remain in the system undetected
5. **Polymorphic viruses:** It acts like a "chameleon" that changes its virus signature every time it spread through the system. Hence, it is always difficult to detect polymorphic virus with the help of an antivirus program. Polymorphic generators that can be linked with the existing viruses. These generation are not viruses but the purpose of these generators to hide actual viruses under the cloak of polymorphism
6. **Macro viruses:** Many applications such as Microsoft Word and Micro soft Excel, support MACROs. These macros are programmed as a micro embedded in a document. This type of virus relatively new and may get slipped by the anti-virus software if the user does not have most recent version installed on his/her system
7. **Active X and Java Control:** All the web browsers have settings about Active X and Java Controls. Little awareness is needed about managing and controlling these settings of a web browser to prohibit and allow certain functions to work.

- The computer worm is self-replicating malware computer program. It uses a computer network to send copies of itself to other nodes and it may do without any user intervention.

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 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 from Greek mythology about the Trojan War.
- Some typical example of Trojan are as follows:
  1. They erase, overwrite or corrupt data on a computer
  2. They help to spread other malware such as viruses
  3. They deactivate or interfere with anti-virus and firewall programs
  4. They allow remote access to your computer
  5. They upload and download files without knowledge
  6. They reinstall themselves after being disabled
  7. They disable the task manager

8. They disable the control panel

Back door:

- A back door is a means of access to a computer program that bypass security mechanism. A programmer may sometimes install a backdoor so that program can be accessed for troubleshooting or other purposes
- A back door work 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 black door is a one of the most dangerous parasite, as it allow a malicious person to perform any possible action on a compromised system
- Programmers sometimes leave such backdoors in their software for diagnostics and troubleshooting purposes.
- Attackers often discover these undocumented features and use them to intrude into the system
- Few examples of backdoors Trojans:
  1. **Back Orifice:** It is well-known example of backdoor Trojan designed for remote system administration. It enables a user to control a computer running the Microsoft Windows OS from a remote location
  2. **Bit frost:** It is another backdoor Trojan that can infect Windows95 through vista. It uses typical server, server builder and client backdoor program configuration to allow a remote attacker, who uses client, to execute arbitrary code on the compromised machine
  3. **SAP backdoors:** SAP is an Enterprise Resource Planning (ERP) system and now days ERP is the heart of business technological platform. Back doors can present into SAP user master that support an authentication mechanism when a user connects to access SAP and ABAP program modules which support SAP business objects
  4. **Onapsis Bizploit:** It is the open-source ERP penetration testing framework developed by the Onapsis Research Labs.

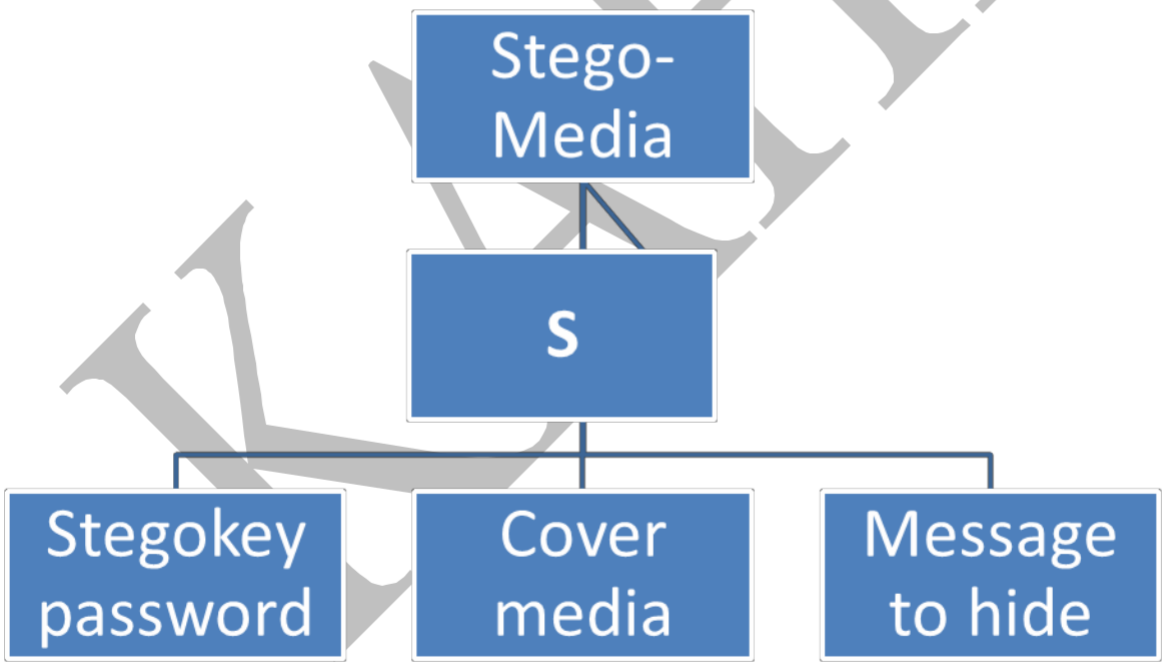
How to protect from Trojan Horses and Backdoors:

1. **Stay away from suspect websites/web links:** Avoid downloading free/pirated software that often get infected by Trojan, worms, viruses and other things.
2. **Surf on the web cautiously:** Avoid connecting with and/or downloading any information from peer-to-peer networks, which are most dangerous networks to spread Trojan Horses and other threats.p2p networks create files packed with malicious software, and then rename them to files with the criteria search that are used while surfing the information on the web.

3. **Install antivirus/Trojan remover software:** nowadays antivirus software have built-in feature for protecting the system not only from viruses and worms but also from malware such as Trojan Horses

Steganography:

- Steganography is a Greek word that means "sheltered writing". It is a method that attempts to hide the existence of a message or communication
- The word Steganography comes from the two Greek words: steganos meaning "covered" and graphein meaning "to write" that means "concealed writing".
- This idea of data hiding is not a novelty. It has been used for centuries all across the world under different regimes
- The term "cover" or "cover medium" is used to describe the original, innocent message, data, audio, still, video and so on. It is the medium that hides that secret message
- It must have parts that can be altered or used without damaging or noticeably changing the cover media.
- If the cover media are digital, these alterable parts are called "redundant bits". These bits are a subset can be replaced with a message that is intended to be hidden



Cover medium+ Embedded message+ stego key= Stego-medium

Steg-analysis:

- Steg analysis 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 determines whether or not they have a payload encoded into them, and if possible recover it

Dos and DDoS Attacks:

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

DoS Attack:

- In this type of criminal act, the attacker floods the bandwidth of the victim's network or fills his email 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 techniques 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 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
- Dos attacks to include:
  1. Unusually slow network performance
  2. Unavailability of a particular website
  3. Inability to access any website
     - 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:

- **Bandwidth attacks:** loading any website takes certain time. Loading means complete webpage appearing on the screen and system is awaiting user's input
- **Logic attacks:** These kind of attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack
- **Protocol attacks:** protocols here are rules that are to be followed to send data over network.

- **Unintentional DoS attack:** This is a scenario where a website ends up denied not due to a deliberate 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:

- **Flood attack:** This is a earliest from of DoS attack and it also known as ping flood. 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. It is very simple to launch, but to prevent it completely is the most difficult
- **Ping of death attack:** The ping of death attack sends oversized internet control message protocol packets, and it is one of the core protocol of the IP suite.
- **SYN attack:** It is also termed as TCP SYN Flooding. In the transmission control protocol handshaking of network connections is done with SYN and ACK message. The fills the buffer space for SYN message on the target system, preventing other systems on the network from communicating with the target system
- **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
- **Nuke:** Nuke is an old DoS attack against computer networks consisting of fragmented or otherwise invalid ICMP packets sent to the target. A string of out-of-band data was sent to TCP port 139 of the victim's machine, causing it to lock up and display a Blue Screen of Death

Tools Used to Launch DoS Attack:

- A DoS attack is usually an attack of last resort because it is considered to be an unsophisticated attack as the attacker does not gain access to any information but rather annoys the target and interrupts the service
- **Tools:**
  1. Jolt2
  2. Nemesy
  3. Targa
  4. Crazy pinger
  5. Some Trouble

DDoS 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 victim" and the main target is called "primary victim".
- Attackers can also break into systems using automated tools that exploit flaws in program that listen for connections from remote hosts

How to protect from DoS/DDoS Attacks:

- Implement router filters. This will lessen exposure to certain DoS attack
- Enable quota system's on Os if they are available
- If such filters are available for systems, install patches to guard against TCP SYN flooding
- Invest in redundant and fault-tolerant network configurations
- Disable any unused or network service. This can limit the ability of an attacker to take advantage of these service to execute a DoS attack
- Observe systems performance and establish base lines for ordinary activity use the base line to gauge usual levels of disk activity, central processing unit usage or network traffic
- Establish and maintain appropriate password policies, especially access to highly privileged accounts such as Unix root or Microsoft Windows NT Administrator

SQL Injection:

- Structured Query Language (SQL) is a database computer language designed for managing data in relational database management system.
- SQL injection is a code injection techniques that exploits a security vulnerability occurring in the database layer of an application
- SQL injection attacks are also known as SQL insertion attacks
- Attackers target the SQL servers- common database servers used by many organizations to store confidential data
- During an SQL injection attack, malicious code is inserted into a web form field or the website's code to make a system execute a command shell or other arbitrary commands
- The attacker determines whether a database and the tables residing into it are vulnerable, before launching an attack

How to prevent SQL Injection Attacks:

- **Input validation:**
  1. Replace all single quotes to two single quotes
  2. Sanitize the input: user input needs to be checked and cleaned of any characters or strings that could possibly be used maliciously.
  3. Numeric values should be checked while accepting a query string value
  4. Keep all text boxes and form fields as short as possible to limit the length of user input.
- **Modify error reports:** SQL errors should not be displayed to outside users and to avoid this, the developer should handle or configure the error reports very carefully
- **Other preventions:**
  1. The default system accounts for SQL server 2000 should never be used
  2. Isolate database server and web server
  3. Most often attacker may make use of several extended stored procedures

Buffer overflow:

- Buffer overflow or buffer over run, is an anomaly where a process stores in a buffer outside the memory the programmer has set aside for it.
- The extra data overwrites adjacent memory, which may contain other data, including program variables and program flow control data.
- This may result in erratic program behaviour, including memory access errors, incorrect errors, program termination or a breach of the system security

Types of buffer overflow:

1. Stack based buffer overflow:
    - Stack buffer over floes occurs when a program writes to a memory addresses on the program's call stack side the intended data structure-usually a fixed length buffer.
    - "stack" is a memory space in which automatic variables are allocated
    - Function parameters are allocated on the stack and also not automatically initialized by the systems, so they usually have garbage in them until they are initialized
    - Once a function has completed its cycle, the reference to the variable in the stack is removed.
    - The attackers may exploit stack-based buffer overflows to manipulate the program in various way by over writing:
        1. A local variable that is near the buffer in memory on the stack to change the behaviour of the program that may benefit the attacker
        2. The return address in a stack frame. Once the function returns, execution will resume at the return address as specified by the attacker, usually a user input—filled buffer
        3. A function pointer, or exception handler, which is subsequently executed
- The factors that contribute to overcome the exploits are:
- Null bytes in addresses
- Variability in the location of shell code
- Differences between environments

2. Heap buffer over flow:
    - Heap buffer overflow occurs in the heap data area and may be introduced accidently by an application programmer, or it may result from the deliberate exploit
    - In either case, the overflow occurs when an application copies more data into a buffer than the buffer was designed to contain

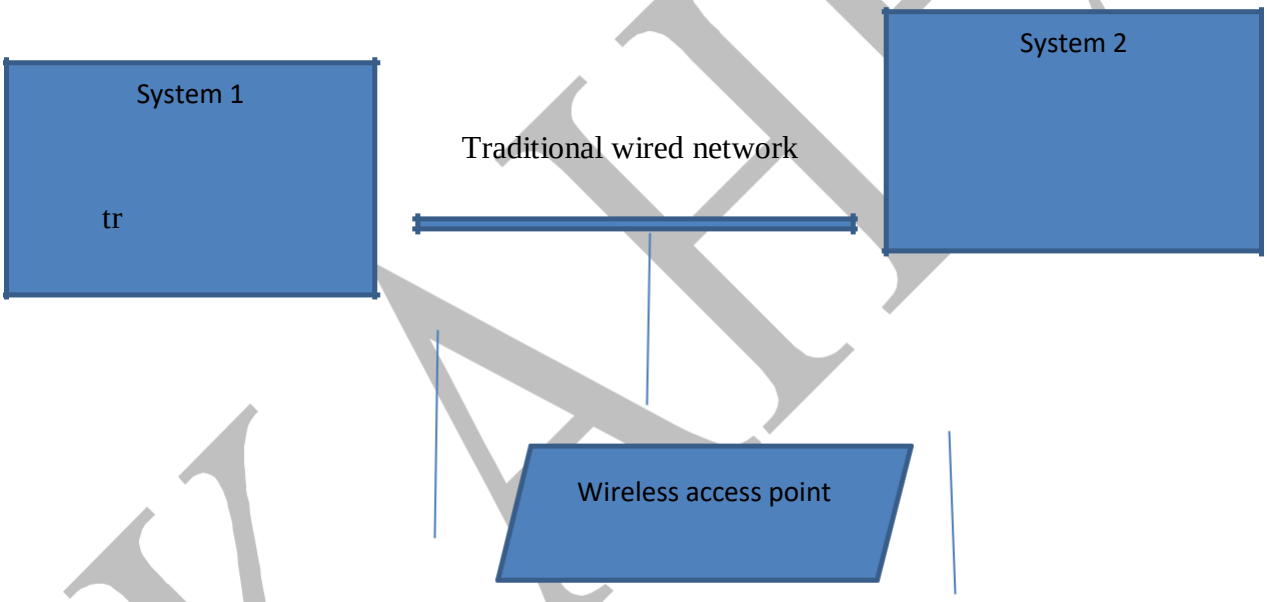
- Memory on the heap is dynamically allocated by the application at run-time and normally contains program data
- Exploitation is performed by corrupting this data in specific ways to cause the application into over write internal structures such as linked list pointers
- The canonical heap overflow techniques overwrites dynamic memory allocation linkage and uses the resulting pointers exchange to overwrite to overwrite a program function pointer

How minimize buffer overflow:

1. **Assessment of secure code manually:**
   - Buffer overflow occurs when a program or process tries to store more data in a buffer than it was intended to hold.
   - The input validation after scanf() function that reads user input into a buffer is very essential
2. **Disable stack execution:**
   - Malicious code causes input argument to the program, and it resides in the stack and not in the code segment.
   - Any code that attempts to execute any other code residing in the stack will cause a violation
   - Therefore, a simplest solution is to invalidate the stack to execute any instructions.
   - In normally resides in the stack in the stack frame of the containing function and thus requires the stack to be executable
   - However. A version of the Linux kernel that enforces the non-executable stack is freely available
3. **Compiler tools:**
   - Over the years, compilers have become more and more aggressive in optimizations and the checks they perform.
   - Various compiler tools already offer warnings on the use of unsafe constructs such as gets(), strcpy()
   - Developers should be educated to restructure the programming code if such warnings are displayed
4. **Dynamic run-time checks:**
   - An application has restricted access to prevent attacks. This methods primarily relies on the safety code being preloaded before an application is executed
   - This preloaded component can either provide safer versions of standard unsafe functions or it can ensure that return addresses are not overwritten
   - It then checks the distance to the nearest return address and when the function executes, it make sure that address is not overwritten

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 allows individuals to access calendars, email address, phone number lists and the internet
- Wireless networks extended the range of traditional wireless networks by using radio waves to transmit data to wireless- enabled devices such as laptops and PDAs.
- The following are different types of "mobile workers"



Tethered/remote workers:

- This is considered to be an employee who generally remains at a single point of work, but is remote to the central company systems. This includes home workers, tele- cottagers and in some cases, branch workers

Roaming user:

- This is either an employee who works in an environment

Nomad:

- This category covers employees requiring solutions in hotel rooms and other semi-tethered environments where modern use is still prevalent, along with the increasing use of multiple wireless technologies and devices

Road warrior:

- This is the ultimate mobile user and spends little time in the office; however, he/she requires regular access to data and collaborative functionality while on the move, in transit or in hotels, this type includes sales and field forces

Traditional Techniques of Attacks on Wireless Networks:

1. **Sniffing**: It is eavesdropping on the network and is the simplest of all attacks. Sniffing is the simple process of intercepting wireless data that is being broadcasted on an unsecured network. The attacker usually install the sniffers remotely on the victim's system and conducts activities such as
    1. Passive scanning of wireless network
    2. Detection of SSID
    3. Collecting the MAC address
    4. Collecting the frames to crack WEP
2. **Spoofing:** The primary objective of this attack is to successfully masquerade the identity by falsifying data and thereby gaining an illegitimate advantage. It causes unsuspecting computers to automatically connect to the spoofed network instead of the real one.
    1. MAC address spoofing: It is a technique of changing an assigned media access control address of a networked device to a different one
    2. IP spoofing: It is a process of creating IP packets with the forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computer system

3. Frame spoofing: frames themselves are not authenticated in 802.11 networks and hence when a frame has a spoofed source address, it cannot be detect unless the address is entirely faked/bogus.

Theft of Internet Hours and Wi-Fi-based Frauds and Misuses:

- Information communication technology (ICT) is within reach of people nowadays and most of the new systems are equipped for mobile wireless Internet access as more and more people are opting for Wi-Fi in their home
- This enables the internet on the finger tip of home users and in case, unfortunately, he/she visits a malicious web page, the router is exposed for an attack
- It appears that more and more people are logging on for free. An interesting question is whether "stealing" wireless internet is illegal
- The act of wardriving is searching for wireless networks by moving vehicle using a portable computer PDA.
- WAP to gain access to computer on an network, be aware of the local laws/legislations where you are doing it because dangerous from security and privacy as well legal perspective
- Computer-related fraud is one of the most popular crimes on the Internet, as it enables the offender to use automation and software tools to mask criminals' identities.
- Automation enables offenders to make large profits from a number of small acts. One strategy used by offenders is to ensure that each victim's financial loss is below a certain limit. With a "small" loss, victims are less likely to invest time and energy in reporting and investigating such crimes.
- One example of such a scam is the Nigeria Advanced Fee Fraud.
- Although these offences are carried out using computer technology, most criminal law systems categorize them not as computer-related offences, but as regular fraud.
- The main distinction between computer- related and traditional fraud is the target of the fraud. If offenders try to influence a person, the offence is generally recognized as fraud.
- Where offenders target computer or data-processing systems, offences are often categorized as computer-related fraud.
- Those criminal law systems that cover fraud, but do not yet include the manipulation of computer systems for fraudulent purposes, can often still prosecute the above-mentioned offences. The most common fraud offences include online auction fraud and advanced fee fraud.

How to secure the wireless networks:

1. Change the default setting of all the equipments/components of wireless network
2. Enable WAP/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
8. Avoid proving the network a name which can be easily identified
9. Upgrade router's firmware periodically
10. Assign static IP addresses to devices
11. Enable firewalls on each computer and the router
12. Position the router or AP safely
13. Periodic and regular monitor wireless network security

Possible questions

Part-B (2 marks)

1. Write short notes on proxy servers?

2. What is steganography?

3. Write short notes on SQL injection?
4. List out the steps for SQL injection attack?
5. Describe buffer overflow?
6. What is phishing?

Part-C (6 marks)

1. Describe about the tools and methods used in cybercrime
2. Explain the proxy servers& Anonymizers
3. What is key loggers& types of key loggers explain in detail?
4. Explain how phishing works with example?
5. Explain the types of viruses with example?
6. Elaborate the role of steganography?
7. Discuss the Dos& DDoS attack?
8. Describe about the SQL injection and how to prevent the attack?
9. What is buffer overflow and explain its types & how to minimize the buffer overflow?