KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University)
(Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.

DEPARTMENT OF COMPUTER SCIENCE, CA & IT

SUBJECT : CYBER SECURITY **SEMESTER : VI**

SUBJECT CODE : 15CSU603B **CLASS : III B.Sc.CS**

COURSE OUTCOME :
This course provides an overview of Information Security and Assurance. Students will be exposed to the spectrum of security activities, methods, methodologies, and procedures with emphasis on practical aspects of Information Security.

COUIRSE OBJECTIVE:

- State the basic concepts in information security, including security policies, security models, and security mechanisms.
- Explain concepts related to applied cryptography, including plain-text, cipher-text, the four techniques for crypto-analysis, symmetric cryptography, 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
Cyberoffenses: 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 - Cyberstalking: Types of stalkers, Cases Reported on Cyberstalking, How stalking Works?, real-life incident of Cyberstalking - Cybercafe and Cybercrimes

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.

UNIT-IV

Mobile Devices: Security Implication for Organizations – Managing Diversity and Proliferation of Hand-Held Devices, Unconventional/ Steath 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:

UNIT-V

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.

TEXT BOOK

1. Nina Godbole and Sunit Belapure. 2013. CYBER SECURITY. Wiley India Pvt. Ltd.

REFERENCES

1. Charles P. Pfleeger and Shari L. Pfleeger. 2003.
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 Complaince, O’Reilly.

WEB SITES

1. http://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/

ESE MARK ALLOCATION

1	Section –A 20 * 1 = 20	20
2	Section – B 5 * 8 = 40	40
	Total	60

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University)
(Established Under Section 3 of UGC Act 1956)
Coimbatore – 641 021.

LECTURE PLAN
DEPARTMENT OF COMPUTER SCIENCE

Subject : CYBER SECURITY **Subcode : 15CSU603B**
CLASS : III-B.Sc (CS) **Semester: VI**
STAFF NAME: S.Joyce

UNIT-I

S.No	Lecture Duration (Hours)	Topics to be Covered	Support Materials
1	1	Introduction to cybercrime :Introduction	T1.Pg: 1
2	1	Cybercrime: Definition	T1.Pg: 1-12
3	1	Information Security	T1.Pg: 13-15
4	1	Who are cybercriminals?	T1.Pg: 16
5	1	Classification of cybercrimes: E-Mail Spoofing, Spamming, Cyber defamation, Internet Time Theft, Salami Attack, Data Diddling.	T1.Pg: 17-21
6	1	Classification of cybercrimes: Forgery, Web Jacking, Newsgroup Spam, Industrial Spying, Hacking, Online Frauds.	T1.Pg: 22,23
7	1	Classification of cybercrimes: Pornographic Offenses , Sofware Piracy, Computer Sabotage, E-mail Bombing.	T1.Pg: 27-30
8	1	Classification of cybercrimes: Usenet Newsgroup, Computer Instrusions, Password Sniffing, Credit Card Frauds, Identity Theft	T1.Pg: 30,31
9	1	Cybercrime: The legal perspectives	T1.Pg: 32
10	1	cybercrimes: An Indian Perspective	T1.Pg: 32
11	1	cybercrime and the Indian ITA2000: Hacking and the Indian law(s)	T1.Pg: 34

12	1	A Global Perspective on cybercrimes: cybercrime and the Extended Enterprise	T1.Pg: 36-39
13	1	cybercrime Era: Survival Mantra for the Netizens	T1.Pg: 39
14	1	Concluding Remarks and Way Forward to Further Chapters.	T1.Pg: 40
15	1	Recapitulation and Discussion of Important Questions	
Total No. of Hours Planned for Unit I			15
Text Book:		1. Nina Godbole and Sunit Belapure. 2013. CYBER SECURITY. Wiley India Pvt. Ltd.	

UNIT-II			
S.No	**Lecture Duration (Hours)**	**Topics to be Covered**	**Support Materials**
1	1	Cyber offenses: How Criminals Plan Them	T1.Pg: 45
2	1	Introduction	T1.Pg: 46,47
3	1	categories of Cybercrime	T1.Pg:48
4	1	How criminals Plan the Attacks: Reconnaissance,	T1.Pg: 49,50
5	1	Passive Attacks, Active Attacks	T1.Pg: 51-58
6	1	Scanning and Scrutinizing Gathered Information,	T1.Pg: 58-60
7	1	Attack (Gaining and Maintaining the system Access)	T1.Pg: 61
8	1	social Engineering	T1.Pg: 61
9	1	Classification of Social Engineering	T1.Pg: 62-64
10	1	Cyberstalking: Types of stalkers,	T1.Pg: 65
11	1	Cases Reported on Cyberstalking,	T1.Pg: 66
12	1	How stalking Works?,	T1.Pg: 66
13	1	real-life incident of Cyberstalking	T1.Pg: 67
14	1	Cybercafe and Cybercrimes	T1.Pg: 67-71
15	1	Recapitulation and Discussion of Important Questions	
Total No. of Hours Planned for -Unit II			15

Text Book:	1. Nina Godbole and Sunit Belapure. 2013. CYBER SECURITY. Wiley India Pvt. Ltd.

UNIT-III

S.No	Lecture Duration (Hours)	Topics to be Covered	Support Materials
1	1	Cybercrime: Mobile and wireless Devices	T1.Pg: 81
2	1	Introduction	T1.Pg: 81
3	1	Proliferation of Mobile and Wireless Devices	T1.Pg: 82
4	1	Trends in Mobility	T1.Pg: 84
5	1	Credit Card Frauds in Mobile and Wireless Computing Era	T1.Pg: 87
6	1	Types and Techniques of Credit Card Frauds	T1.Pg: 88-90
7	1	Security challenges Posed by Mobile Devices	T1.Pg: 91
8	1	Registry Settings for Mobile Devices	T1.Pg: 92
9	1	Authentication Service security	T1.Pg: 93
10	1	cryptographic security	T1.Pg: 93
11	1	LDAP Security	T1.Pg: 94
12	1	RAS Security	T1.Pg: 95-97
13	1	Media Player Control Security	T1.Pg: 98
14	1	Networking API Security	T1.Pg: 98
15	1	Recapitulation and Discussion of Important Questions	
Total No. of Hours Planned for -Unit III			15

Text Book:	1.Nina Godbole and Sunit Belapure. 2013. CYBER SECURITY. Wiley India Pvt. Ltd.

UNIT-IV

S.No	Lecture Duration (Hours)	Topics to be Covered	Support Materials
1	1	Mobile Devices	T1.Pg: 107
2	1	Security Implication for Organizations	T1.Pg: 107
3	1	Managing Diversity	T1.Pg: 107
4	1	Proliferation of Hand-Held Devices	T1.Pg: 107
5	1	Example: TrustZone Technology for Mobile Devices	T1.Pg: 108
6	1	Unconventional	T1.Pg: 109

7	1	Steath Storage Devices	T1.Pg: 110
8	1	Threats through Lost and Stolen Devices	T1.Pg: 110
9	1	Example: Getting Lost!	T1.Pg: 111
10	1	Protecting Data on lost devices	T1.Pg: 111
11	1	Educating the Laptop Users	T1.Pg: 112
12	1	Most Important management or support issues for laptops	T1.Pg: 112
13	1	Organizational Measures for Handling Mobile	T1.Pg: 112
14	1	Recapitulation and Discussion of Important Questions	
Text Book:		1.Nina Godbole and Sunit Belapure. 2013. CYBER SECURITY. Wiley India Pvt. Ltd.	
Total No. of Hours Planned for -Unit IV			14
UNIT-V			
S.No	**Lecture Duration (Hours)**	**Topics to be Covered**	**Support Materials**
1	1	Encrypting Organizational Databases	T1.Pg: 113
2	1	Including Mobile Devices in Security Strategy	T1.Pg: 113
3	1	Organizational Security Policies and Measures in mobile Computing Era	T1.Pg: 114
4	1	Importance of Security polices relating to mobile Computing Devices	T1.Pg: 114
5	1	Operating Guidelines for Implementing Mobile Devices Security Polices	T1.Pg: 115
6	1	Organizational Policies for the Use of Mobile Hand - Held Devices	T1.Pg: 116
7	1	Laptops	T1.Pg: 116
8	1	Physical Security Countermeasures	T1.Pg: 117

9	1	Cables and Hardwired locks, Laptop safes	T1.Pg: 117
10	1	Motion sensors and Alarms	T1.Pg: 118
11	1	Warning labels and stamps	T1.Pg: 119
12	1	Other measures for protecting laptops	T1.Pg: 119
13	1	Recapitulation and Discussion of Important Questions	
14	1	Discussion of Previous ESE Question Papers	
15	1	Discussion of Previous ESE Question Papers	
16	1	Discussion of Previous ESE Question Papers	
Total No. of Hours Planned for Unit V			16
Text Book:		1.Nina Godbole and Sunit Belapure. 2013. CYBER SECURITY. Wiley India Pvt. Ltd.	
Total No. of Hours : 75			

UNIT-I

SYLLABUS

Introduction to cybercrime: Introduction-Cybercrime: Definition and Information Security-who are cyber criminals? - 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.

Introduction:

- ❖ The internet in India is growing rapidly. It has given rise to new opportunities in every field we can think of be it entertainment, business, sports or education.
- ❖ There're two sides to a coin. Internet also has it's own disadvantages is Cyber crime illegal activity committed on the internet.

DEFINING CYBER CRIME:

- Crime committed using a computer and the internet to steal data or information.
- Illegal imports.
- Malicious programs.

What is Cyber Crime?

- Cybercrime is not a new phenomena
- The first recorded cybercrime took place in the year 1820.
- In 1820, JosephMarie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics.

This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new echnology. **This is the first recorded cyber crime!**

Alternative definitions for cybercrime:

- Any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation or prosecution
- Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers
- Any financial dishonesty that takes place in a computer environment.
- Any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom
- **"*Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that target the security of computer systems and the data processed by them*".**
- Hence cybercrime can sometimes be called as ***computer-related crime, computer crime, E-crime, Internet crime, High-tech crime….***

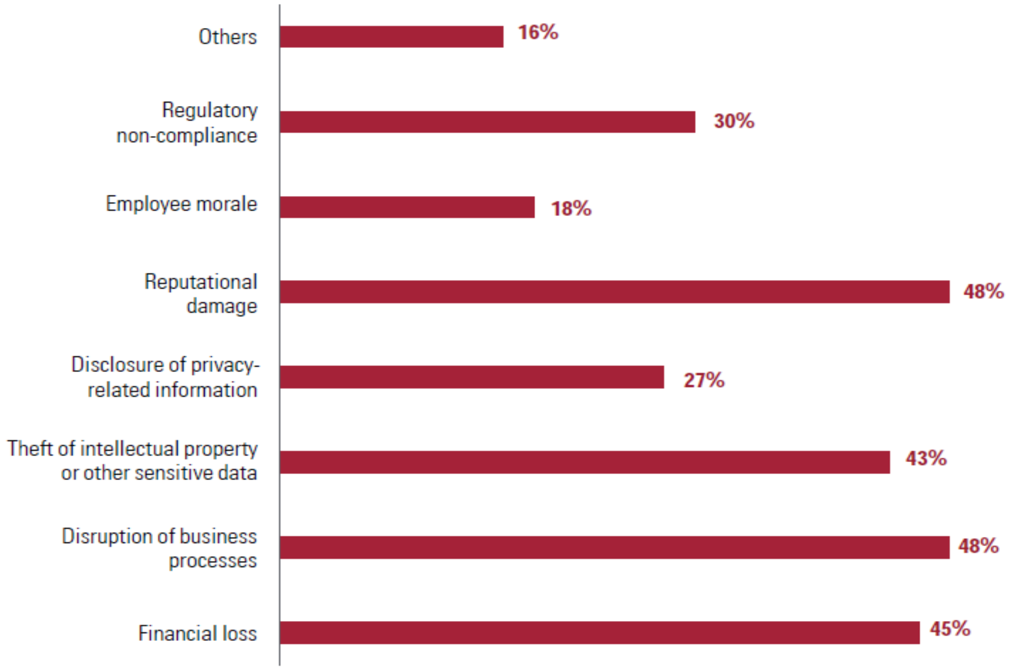
Cybercrime specifically can be defined in number of ways…

- A crime committed using a computer and the internet to steal a person's identity (identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs.

- Crimes completed either on or with a computer
- Any illegal activity through the Internet or on the computer.
- All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW.
- Cybercrime refers to the act of performing a criminal act using cyberspace as communication vehicle.
- **Two types of attacks are common:**
  - **Techno- crime : *Active attack***
    - Techno Crime is the term used by law enforcement agencies to denote criminal activity which uses (computer) technology, not as a tool to commit the crime, but as the subject of the crime itself. Techno Crime is usually pre-meditated and results in the *deletion, corruption, alteration, theft or copying of data on an organization's systems*.
    - Techno Criminals will usually probe their prey system for weaknesses and will almost always leave an electronic 'calling card' to ensure that their pseudonym identity is known.
  - **Techno – vandalism: *Passive attack***
    - Techno Vandalism is a term used to describe *a hacker or cracker* who breaks into a computer system with the *sole intent of defacing and or destroying its contents*.

- Techno Vandals can deploy *'sniffers'* on the Internet to locate soft (insecure) targets and then execute a range of commands using a variety of protocols towards a range of ports. If this sounds complex - it is! The best weapon against such attacks is a firewall which will hide and disguise your organization's presence on the Internet.

Survey result - Impact of cybercrime in India



Source: Cybercrime survey report 2014, KPMG in India

Cybercrime and information security:

- Lack of information security give rise to cybercrime
- Cybersecurity: means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

Challenges for securing data in business perspective:

- Cybercrime occupy an important space in information security due to their impact.
- Most organizations do not incorporate the cost of the vast majority of computer security incidents into their accounting
- The difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost
- Financial losses may not be detected by the victimized organization in case of Insider attacks : such as leaking customer data

Cybercrime trends over years

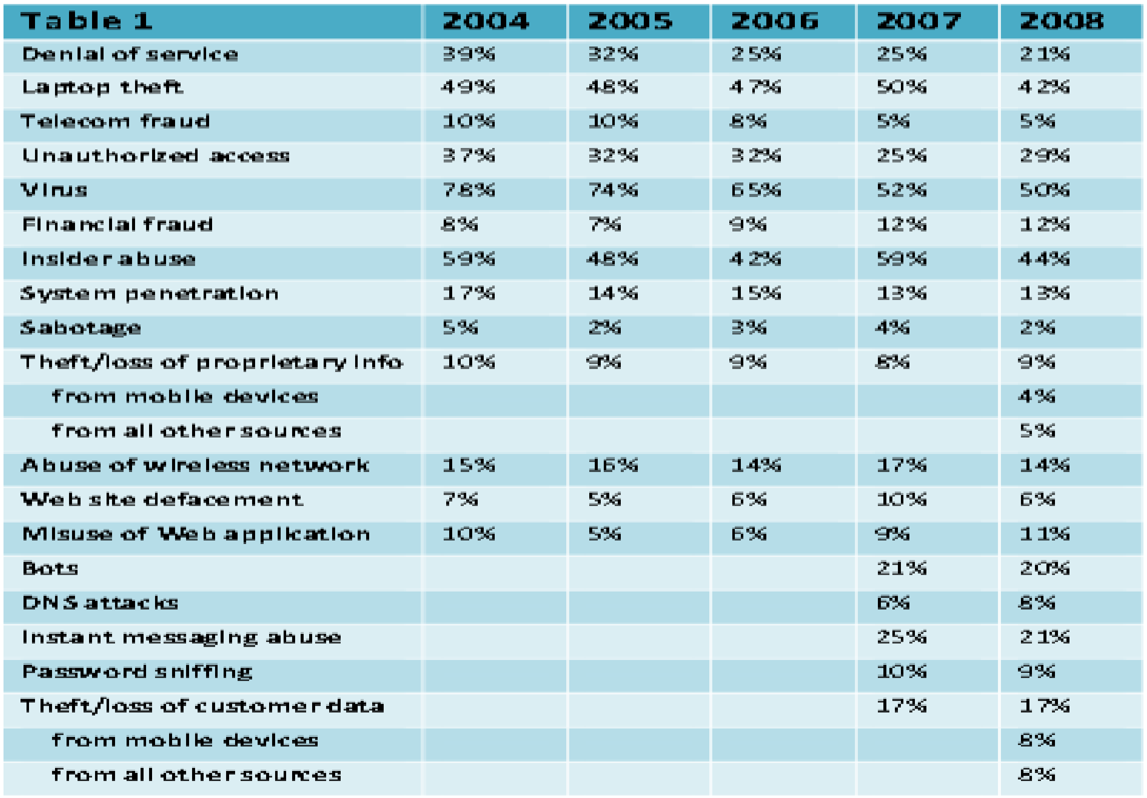


Table 1	2004	2005	2006	2007	2008
Denial of service	39%	32%	25%	25%	21%
Laptop theft	49%	48%	47%	50%	42%
Telecom fraud	10%	10%	8%	5%	5%
Unauthorized access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial fraud	8%	7%	9%	12%	12%
Insider abuse	59%	48%	42%	59%	44%
System penetration	17%	14%	15%	13%	13%
Sabotage	5%	2%	3%	4%	2%
Theft/loss of proprietary info	10%	9%	9%	8%	9%
from mobile devices					4%
from all other sources					5%
Abuse of wireless network	15%	16%	14%	17%	14%
Web site defacement	7%	5%	6%	10%	6%
Misuse of Web application	10%	5%	6%	9%	11%
Bots				21%	20%
DNS attacks				6%	8%
Instant messaging abuse				25%	21%
Password sniffing				10%	9%
Theft/loss of customer data				17%	17%
from mobile devices					8%
from all other sources					8%

Who are Cybercriminals:

- Are those who conduct acts such as:
  - Child pornography
  - Credit card fraud
  - Cyberstalking
  - Defaming another online
  - Gaining unauthorized access to computer systems
  - Ignoring copyrights
  - Software licensing and trademark protection
  - Overriding encryption to make illegal copies
  - Software piracy

Stealing another's identity to perform criminal acts.

Categorization of Cybercriminals:

- **Type 1: Cybercriminals- hungry for recognition**
  - **Hobby hackers**
    - A person who enjoys exploring the limits of what is possible, in a spirit of playful cleverness. May modify hardware/ software
  - **IT professional(social engineering):**

  - **Ethical hacker**
- **Politically motivated hackers :**
  - promotes the objectives of individuals, groups or nations supporting a variety of causes such as : Anti globalization, transnational conflicts and protest
- **Terrorist organizations**
  - Cyberterrorism
  - Use the internet attacks in terrorist activity
  - Large scale disruption of computer networks , personal computers attached to internet via viruses

Type 2: Cybercriminals- not interested in recognition:

- **Psychological perverts**
  - Express sexual desires, deviates from normal behavior
  - Poonam panday
- **Financially motivated hackers**
  - Make money from cyber attacks
  - Bots-for-hire : fraud through phishing, information theft, spam and extortion
- **State-sponsored hacking**
  - Hacktivists
  - Extremely professional groups working for governments
  - Have ability to worm into the networks of the media, major corporations, defense departments

Type 3: Cybercriminals- the insiders:

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

Motives behind cybercrime:

- Greed
- Desire to gain power
- Publicity
- Desire for revenge
- A sense of adventure
- Looking for thrill to access forbidden information
- Destructive mindset
- Desire to sell network security services
-

Classification of cybercrimes:

1. Cybercrime against an individual
2. Cybercrime against property
3. Cybercrime against organization

4. Cybercrime against Society
5. Crimes emanating from Usenet newsgroup

1. Cybercrime against an individual:

- Electronic mail spoofing and other online frauds
- Phishing, spear phishing
- spamming
- Cyberdefamation
- Cyberstalking and harassment
- Computer sabotage
- Pornographic offenses
- passwordsniffing

2.Cybercrime against property:

- Credit card frauds
- Intellectual property(IP) crimes
- Internet time theft

3.Cybercrime against organization:

- Unauthorized accessing of computer
- Password sniffing
- Denial-of-service attacks
- Virus attack/dissemination of viruses
- E-Mail bombing/mail bombs
- Salami attack/ Salami technique
- Logic bomb
- Trojan Horse
- Data diddling
- Industrial spying/ industrial espionage
- Computer network intrusions
- Software piracy

4.Cybercrime against Society:

- Forgery
- Cyberterrorism
- Web jacking

5.Crimes emanating from Usenet newsgroup:

- Usenet groups may carry very offensive, harmful, inaccurate material
- Postings that have been mislabeled or are deceptive in another way
- Hence service at your own risk

History of Usenet groups:

- In 1979 it was developed by two graduate student
- s from Duke University in North Carolina (UNC) as a network that allowed users to exchange quantities of information too large for mailboxes
- Usenet was designed to facilitate textual exchanges between scholars.
- Slowly, the network structure adapted to allow the exchange of larger files such as videos or images.

Usenet groups as a "safe" place?

- Usenet newsgroups constitute one o the largest source of child pornography available in cyberspace
- This source useful for observing other types of criminal or particular activities: online interaction between pedophiles, adult pornographers and writers of pornographic stories.
- Usenet for sharing illegal content

Criminal activity on Oracle USENET Newsgroups:

- This interesting SearchOracle article on Oracle security bloopers, we see the risks with engaging the unsavory inhabitants of the Oracle USENET newsgroup, a forum laced with profanity, pornography and, according to this note, criminal Oracle hackers:
- "I subscribe to several Usenet groups so I can keep my skills current. Well, a few years ago a DBA needed some assistance and posted a question in which he shared his tnsnames.ora file and wondered why he could not connect to SQL*Plus with the following syntax:
- sqlplus system/SecurePswd@prod
- Almost immediately several people connected to this person's production system and was able to fish around the system. Numerous people emailed the DBA back and pointed out that he just broadcasted to the world his production connection string and password. How crazy is that?"

E-Mail Spoofing:

- E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.
- To send spoofed e-mail, senders insert commands in headers that will alter message information.
- It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say.
- Thus, someone could send spoofed e-mail that appears to be from you with a message that you didn't write.

- Classic examples of senders who might prefer to disguise the source of the e-mail include a sender reporting mistreatment by a spouse to a welfare agency
- Although most spoofed e-mail falls into the "nuisance" category and requires little action other than deletion, the more malicious varieties can cause serious problems and security risks.
- For example, spoofed e-mail may purport to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information -- any of which can be used for a variety of criminal purposes.
- The Bank of America, eBay, and Wells Fargo are among the companies recently spoofed in mass spam mailings.
- One type of e-mail spoofing, self-sending spam, involves messages that appear to be both to and from the recipient.

Spamming:

- People who create electronic spam : spammers
- Spam is abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately
- Spamming may be
  - E-Mail Spam
  - Instant messaging spam
  - Usenet group spam
  - Web search engine spam
  - Spam in blogs, wiki spam
  - Online classified ads spam
  - Mobile phone messaging spam
  - Internet forum spam
  - Junk fax spam
  - Social networking spam.
- Spamming is difficult to control
- Advertisers have no operating costs beyond the management of their mailing lists
- It is difficult to hold senders accountable for their mass mailings
- Spammers are numerous

Search engine spamming:

- Alteration or creation of a document with the intent to deceive an electronic catalog or a filing system
- some web authors use “subversive techniques” to ensure that their site appears more frequently or higher number in returned search results.
- remedy: permanently exclude from the search index

Avoid the following web publishing techniques:

- Repeating keywords
- Use of keywords that do not relate to the content on the site
- Use of fast meta refresh
  - change to the new page in few seconds.

- Redirection
- IP cloaking:
    - including related links, information, and terms.
- Use of colored text on the same color background
- Tiny text usage
- Duplication of pages with different URLs
- Hidden links

Cyber defamation:

- The tort of cyber defamation is considered to be the act of defaming, insulting, offending or otherwise causing harm through false statements pertaining to an individual in cyberspace.
- Example: someone publishes defamatory matter about someone on a website or sends an E-mail containing defamatory information to all friends of that person.

It may amount to defamation when

- If imputation to a deceased person would harm the reputation of that person, and is intended to be hurtful to the feelings of his family or other near relatives
- An imputation is made concerning a company or an association or collection of people as such.
- An imputation in the form of an alternative or expressed ironically
- An imputation that directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person.

Types of defamation:

- **Libel** : written defamation
- **Slander**: oral defamation
- The plaintiff must have to show that the defamatory statements were unlawful and would indeed injure the person’s or organization’s reputation.
- When failed to prove, the person who made the allegations may still be held responsible for defamation.

Cyber defamation cases:

- In first case of cyber defamation in India (14 dec 2009),
    - the employee of a corporate defamed its reputation was sending derogatory and defamatory emails against the company.
    - In this case the Court(delhi court) had restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails.
    - The court passed as important ex-parte injunction.
- In another case, accused posted obscene, defamatory and annoying message about a divorcee woman and also sent emails to the victim.
    - The offender was traced and was held guilty of offences under section 469, 509 IPC and 67 of IT Act, 2000.
- Other defamation cases:

- A malicious customer review by a competitor could destroy a small business.
- A false accusation of adultery on a social networking site could destroy a marriage.
- An allegation that someone is a “crook” could be read by a potential employer or business partner

Internet Time Theft:

- Occurs when an unauthorized person uses the Internet hours paid for by another person
- Comes under hacking
- The person get access to someone else’s ISP user ID and password, either by hacking or by gaining access to it by illegal means
- And uses the internet without the other person’s knowledge
- This theft can be identified when Internet time is recharged often, despite infrequent usage.
- This comes under “identity theft”.

Salami attack/ salami technique:

- Are used for committing financial crimes.
- The alterations made are so insignificant that in a single case it would go completely unnoticed.
- Example: a bank employee inserts a program, into the bank’s serve, that deduces a small amount from the account of every customer every month,
- The unauthorised debit goes unnoticed by the customers, but the employee will make a sizable amount every month.

Salami attack: real life examples:

- Small “shavings” for Big gains!
- The petrol pump fraud

Data diddling:

- Data diddling involves changing data input in a computer.
- In other words, information is changed from the way it should be entered by a person typing in the data.
- Usually, a virus that changes data or a programmer of the database or application has pre-programmed it to be changed.
- For example, a person entering accounting may change data to show their account, or that or a friend or family member, is paid in full. By changing or failing to enter the information, they are able to steal from the company.
- To deal with this type of crime, a company must implement policies and internal controls.
- This may include performing regular audits, using software with built-in features to combat such problems, and supervising employees.

Real life example:

Doodle me Diddle:

- Electricity board in India have been victims to data diddling programs inserted when private parties computerized their systems.

Forgery :

- The act of forging something, especially the unlawful act of counterfeiting a document or object for the purposes of fraud or deception.
- Something that has been forged, especially a document that has been copied or remade to look like the original.
- Counterfeit currency notes, postage, revenue stamps, marksheets, etc., can be forged using sophisticated computers, printers and scanners.

Real life case:

- **Stamp Paper Scam – a racket that flourished on loopholes in the system**
- Abdul Karim Telgi, the mastermind of the multi-crore counterfeiting, printed fake stamp papers worth thousands of crores of rupees using printing machines purchased illegally with the help of some conniving officials of the Central Govt.'s Security Printing Press (India Security Press) located in Nasik. These fake stamp papers penetrated in more than 12 states through a widespread network of vendors who sold the counterfeits without any fear and earned hefty commissions.
- **Amount swindled** Rs. 172 crores
- Telgi is in jail serving his 13 plus 10 years term

Web jacking:

- This term is derived from the term hi jacking.
- In these kinds of offences the hacker gains access and control over the web site of another.
- He may even change the information on the site.
- 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
- This may be done for fulfilling political objectives or for money

Real life examples:

- recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein.
- Further the site of Bombay crime branch was also web jacked.
- Another case of web jacking is that of the 'gold fish' case. In this case the site was hacked and the information pertaining to gold fish was changed.

Industrial spying/ Industrial Espionage:

- Industrial espionage is the covert and sometimes illegal practice of investigating competitors to gain a business advantage.

- The target of investigation might be a trade secret such as a proprietary product specification or formula, or information about business plans.
- In many cases, industrial spies are simply seeking any data that their organization can exploit to its advantage.

Real life case:

- A Chinese Trojan horse email campaign targeted some 140 senior Israeli defense corporation employees (2013) involved in highly classified, sensitive security projects.
- The email was made to appear as if it came from a known German company that regularly works with the Israeli defense industry.
- However, it turned out to contain a Trojan horse, which, according to the report, attempted to funnel information from the recipients' computers.
- The Trojan horse was noticed by computer defense systems and shut down.
- The defense establishment then realized how many Israelis received the email, and reportedly tracked the malicious program down to Chinese defense industries.
- The incident led security companies to reiterate to employees computer security guidelines**.**

Hacking

Every act committed toward breaking into a computer and/ or network is hacking.

Purpose

- Greed
- Power
- Publicity
- Revenge
- Adventure
- Desire to access forbidden information
- Destructive mindset

History of hacking:

- *hacking* is any technical effort to manipulate the normal behavior of network connections and connected systems.
- A *hacker* is any person engaged in hacking.
- The term "hacking" historically referred to constructive, clever technical work that was not necessarily related to computer systems.
- M.I.T. engineers in the 1950s and 1960s first popularized the term and concept of hacking.
- the so-called "hacks" perpetrated by these hackers were intended to be harmless technical experiments and fun learning activities.
- Later, outside of M.I.T., others began applying the term to less honorable pursuits. for example, several hackers in the U.S. experimented with methods to modify telephones for making free long-distance calls over the phone network illegally.

- As computer networking and the Internet exploded in popularity, data networks became by far the most common target of hackers and hacking.

Hacking vs. Cracking

- Malicious attacks on computer networks are officially known as *cracking* ,
- while *hacking* truly applies only to activities having good intentions.
- Most non-technical people fail to make this distinction, however.
- Outside of academia, its extremely common to see the term "hack" misused and be applied to cracks as well.

There are 3 types of modern hackers

- **Black Hats:** Criminal Hackers.
  - Possess desire to destruction
  - Hack for personal monetary gains : Stealing credit card information, transferring money from various bank accounts to their own account, extort money from corporate giant by threatening.
- **White Hats:** Ethical Hackers.
  - Network Security Specialist.
- **Grey Hats:** Deals in both of the above (jack of all trades, master of none).

Real life case:dec 2009 NASA site hacked via SQL Injection

- Two NASA sites recently were hacked by an individual wanting to demonstrate that the sites are susceptible to SQL injection.
- The websites for NASA's Instrument Systems and Technology Division and Software Engineering Division were accessed by a researcher, who posted to his blog screen shots taken during the hack.
- The researcher, using the alias "c0de.breaker," used SQL injection to hijack the sites.
- SQL injection is an attack process where a hacker adds additional SQL code commands to a page request and the web server then tries to execute those commands within the backend database
- The NASA hack yielded the credentials of some 25 administrator accounts.
- The researcher also gained access to a web portal used for managing and editing those websites.
- In this particular case, the researcher found the vulnerabilities, made NASA aware of them, then published findings after the websites had been fixed.
- An attacker, however, could have tried to use that web server as an entry point into other systems NASA might control or edit the content of the sites and use them for drive-by downloads.

The story..

- LOS ANGELES, CA – Octuplet mom Nadya Suleman launched a website to solicit donations for her family, but it was immediately hacked by a group of vigilante mothers!
- The website originally featured photos of all eight octuplets, a thank you note from Suleman, images of children’s toys and a large donation button for viewers to send

money through. Suleman also provided an address where people can send items such as diapers and formula.

- Suleman was perhaps not prepared for the backlash she was to receive, as the site was hacked and brought down within hours. The original homepage was left up but defaced, as seen in the screenshot.
- The site was tagged by the famous hacker group MOD, also known as the Mothers of Disappointment. The mysterious group has a history of attacking personal sites they disapprove of, including Britney Spears when she infamously hung dry her sons on a clothes line after a bath, and Angelina Jolie for being Angelina Jolie.
- Weekly World News could not reach any members for comment, however reporters did receive a short note from an anonymous e-mail address:
- The site has since been restored, and Suleman's PR representative has stated they are now taking extra security measures to arm against future attacks.

Online frauds :

- Fraud that is committed using the internet is "online fraud." Online fraud can involve financial fraud and identity theft.
- Online fraud comes in many forms.
    - viruses that attack computers with the goal of retrieving personal information, to email schemes that lure victims into wiring money to fraudulent sources,
    - "phishing" emails that purport to be from official entities (such as banks or the Internal Revenue Service) that solicit personal information from victims to be used to commit identity theft,
    - to fraud on online auction sites (such as Ebay) where perpetrators sell fictional goods.
    - E-Mail spoofing to make the user to enter the personal information : financial fraud
    - Illegal intrusion: log-in to a computer illegally by having previously obtained actual password. Creates a new identity fooling the computer that the hacker is the genuine operator. Hacker commits innumerable number of frauds.

Pornographic offenses: Child pornography

Means any visual depiction, including but not limited to the following:

1. Any photograph that can be considered obscene and/ or unsuitable for the age of child viewer.
2. Film ,video, picture;
3. Obscene Computer generated image or picture

Software piracy:

- Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.
- End-user copying
- Hard disk loading with illicit means
- Counterfeiting

- Illegal downloads from internet

Buying Pirated software have a lot to lose:

- Getting untested software that may have been copied thousands of times.
- Potentially contain hard-ware infecting viruses
- No technical support in case of software failure
- No warranty protection
- No legal right to use the product

Computer sabotage:

- Computer sabotage involves deliberate attacks intended to disable computers or networks for the purpose of disrupting commerce, education and recreation for personal gain, committing espionage, or facilitating criminal conspiracie.
- Through viruses, worms, logic bombs
- Chernobyl virus
    - The Chernobyl virus is a computer virus with a potentially devastating payload that destroys all computer data when an infected file is executed.,
- Y2K virus
    - Y2K bug, also called Year 2000 bug or Millennium Bug, a problem in the coding of computerized systems that was projected to create havoc in computers and computer networks around the world at the beginning of the year 2000

E-mail bombing/mail bombs:

- In Internet usage, an *email bomb* is a form of net abuse consisting of sending huge volumes of *email* to an address in an attempt to overflow the mailbox or overwhelm the server where the *email* address is hosted in a denial-of-service attack.
- Construct a computer to repeatedly send E-mail to a specified person’s E-mail address.
- Can overwhelm the recipient’s personal account and potentially shut down the entire system.

Computer network intrusions:

- An intrusion to computer network from anywhere in the world and steal data, plant viruses, create backdoors, insert trojan horse or change passwords and user names.
- An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
- The practice of strong password

Password sniffing:

- Password sniffers are programs that monitor and record the name and password of network users as they login, jeopardizing security at a site.
- Through sniffers installed, anyone can impersonate an authorized user and login to access restricted documents.

Credit card frauds:

- Credit card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction.
- The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.
- Credit card fraud is also an adjunct to identity theft.

Identity theft:

- Identity theft is a fraud involving another person's identity for an illicit purpose.
- The criminal uses someone else's identity for his/ her own illegal purposes.
- Phishing and identity theft are related offenses
- Examples:
  - Fraudulently obtaining credit
  - Stealing money from victim's bank account
  - Using victim's credit card number
  - Establishing accounts with utility companies
  - Renting an apartment

Filing bankruptcy using the victim's name

Real life cases:

- Dr.Gerald Barnbaum lost his pharmacist license after committing Medicaid fraud. He stole the identity of Dr. Gerald Barnes and practiced medicine under his name. A type 1 diabetic died under his care. "Dr. Barnes" even worked as a staff physician for a center that gave exams to FBI agents. He's currently serving hard time.
- Andrea Harris-Frazier Margot Somerville lost her wallet on a trolley. Two years later she was arrested. Andrea Harris-Frazier had defrauded several banks—using Somerville's identity—out of tens of thousands of dollars. The real crook was caught.
- Abraham Abdallah
  A busboy named Abraham Abdallah got into the bank accounts of Steven Spielberg and other famous people after tricking his victims via computer, getting sufficient data to fake being their financial advisors—then calling their banks…and you know the rest.

Cybercrime: The legal perspective:

- Cybercrime possess a mammoth challenge
  Computer crime: Criminal Justice Resource Manual(1979)
- Any illegal act for which knowledge of computer technology is essential for a successful prosecution. International legal aspects of computer crimes were studied in 1983
- Encompasses any illegal act for which the knowledge of computer technology is essential for its perpetration

- The network context of cyber crime make it one of the most globalized offenses of the present and most modernized threats of the future.

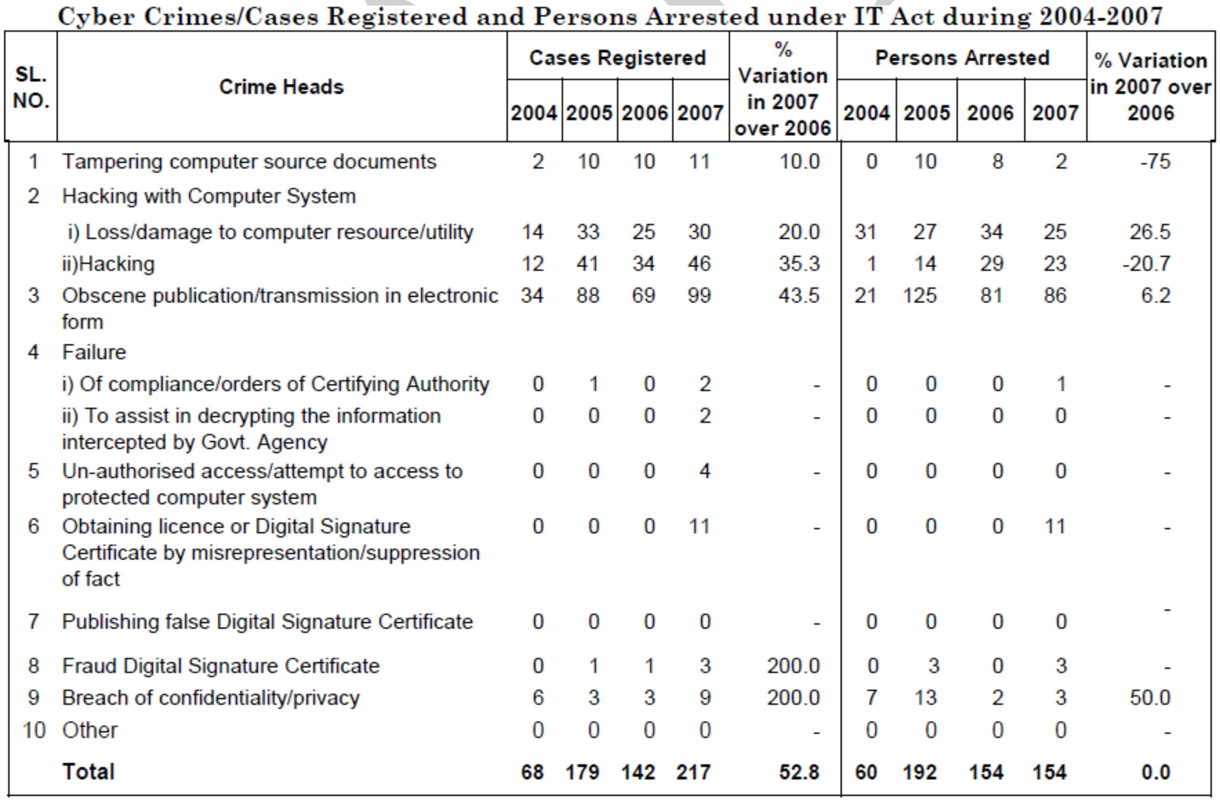
Solution:

- Divide information system into segments bordered by state boundaries.
- Not possible and unrealistic because of globalization
- Or incorporate the legal system into an integrated entity obliterating these state boundaries.

Cybercrimes: An Indian Perspective:

- India has the fourth highest number of internet users in the world.
- 45 million internet users in India
- 37% - in cybercafes
- 57% are between 18 and 35 years
- The Information Technology (IT) Act, 2000, specifies the acts which are punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T.
- 217 cases were registered under IT Act during the year 2007 as compared to 142 cases during the previous year (2006)
- Thereby reporting an increase of 52.8% in 2007 over 2006.
- 22.3% cases (49out of 217 cases) were reported from Maharashtra followed by Karnataka (40), Kerala (38) and Andhra Pradesh and Rajasthan (16 each).

Cybercrimes: An Indian Perspective:



Cyber Crimes/Cases Registered and Persons Arrested under IT Act during 2004-2007

SL. NO.	Crime Heads	Cases Registered				% Variation in 2007 over 2006	Persons Arrested				% Variation in 2007 over 2006
		2004	2005	2006	2007		2004	2005	2006	2007	
1	Tampering computer source documents	2	10	10	11	10.0	0	10	8	2	-75
2	Hacking with Computer System										
	i) Loss/damage to computer resource/utility	14	33	25	30	20.0	31	27	34	25	26.5
	ii)Hacking	12	41	34	46	35.3	1	14	29	23	-20.7
3	Obscene publication/transmission in electronic form	34	88	69	99	43.5	21	125	81	86	6.2
4	Failure										
	i) Of compliance/orders of Certifying Authority	0	1	0	2	-	0	0	0	1	-
	ii) To assist in decrypting the information intercepted by Govt. Agency	0	0	0	2	-	0	0	0	0	-
5	Un-authorised access/attempt to access to protected computer system	0	0	0	4	-	0	0	0	0	-
6	Obtaining licence or Digital Signature Certificate by misrepresentation/suppression of fact	0	0	0	11	-	0	0	0	11	-
7	Publishing false Digital Signature Certificate	0	0	0	0	-	0	0	0	0	-
8	Fraud Digital Signature Certificate	0	1	1	3	200.0	0	3	0	3	-
9	Breach of confidentiality/privacy	6	3	3	9	200.0	7	13	2	3	50.0
10	Other	0	0	0	0	-	0	0	0	0	-
	Total	**68**	**179**	**142**	**217**	**52.8**	**60**	**192**	**154**	**154**	**0.0**

Incidence of Cyber Crimes in Cities:

- 17 out of 35 mega cities did not report any case of Cyber Crime i.e, neither under the IT Act nor under IPC Sections) during the year 2007.
- 17 mega cities have reported 118 cases under IT Act and 7 megacities reported 180 cases undervarious section of IPC.
- There was an increase of 32.6% (from 89 cases in 2006 to 118 cases in 2007) in cases under IT Act as compared to previous year (2006),
- and an increase of 26.8% (from 142 cases in 2006 to 180 cases in 2007) of cases registered under various section of IPC
- Bengaluru (40), Pune (14) and Delhi (10) cities have reported high incidence of cases (64 out of 118 cases) registered under IT Act, accounting for more than half of the cases (54.2%) reported under the Act.

Cybercrime and the Indian ITA2000:

Objectives of IT legislation in India

The Government of India enacted its Information Technology Act 2000 with the objectives stating officially as:

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

What does IT Act 2000 legislation deals with?

The Act essentially deals with the following issues:

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cyber crimes.

Why did the need for IT Amendment Act 2008 (ITAA) arise?

The IT Act 2000, being the first legislation on technology, computers, e-commerce and e-communication, the was the subject of extensive debates, elaborate reviews with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some obvious omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology based cases with the IT Act also being referred in the process with the reliance more on IPC rather on the ITA.

Thus the need for an amendment – a detailed one – was felt for the I.T. Act. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the I.T. Act and comparing it with similar legislations in other nations and to suggest recommendations. Such recommendations were analyzed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures, the consolidated amendment called the**Information Technology Amendment Act 2008** was placed in the Parliament and passed at the end of 2008 (just after Mumbai terrorist attack of 26 November 2008 had taken place). The IT Amendment Act 2008 got the President assent on 5 Feb 2009 and was made effective from 27 October 2009.

Notable features of the ITAA 2008 are:

- Focusing on data privacy
- Focusing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognizing the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- Authorizing an Inspector to investigate cyber offenses (as against the DSP earlier)

2. **Structure of IT Act**

- **How is IT Act structured?**

The Act totally has 13 chapters and 90 sections. Sections 91 to 94 deal with the amendments to the four Acts namely Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934. The Act has chapters that deal with authentication of electronic records, electronic signatures etc.

Elaborate procedures for certifying authorities and electronic signatures have been spelt out. The civil offence of data theft and the process of adjudication and appellate procedures have been described. Then the Act goes on to define and describe some of the well-known cyber crimes and lays down the punishments therefore. Then the concept of due diligence, role of intermediaries and some miscellaneous provisions have been described.

- **What is the applicability of IT Act?**

The Act extends to the whole of India and except as otherwise provided, it also applies to any offence or contravention there under committed outside India by any person.

Rules and procedures mentioned in the Act have also been laid down in a phased manner, defined as recently as April 2011.

For the sake of simplicity, here we will be only discussing the various penalty and offences defined as per provisions of ITA 2000 and ITAA 2008. Please note that wherever the terms IT Act 2000 or 2008 are used, they refer to same act because the IT Act now includes amendments as per IT 2008 Amendment Act.

Specific exclusion(s) to the Act where it is not applicable are:

- Negotiable instrument (other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
- A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
- A trust as defined in section 3 of the Indian Trusts Act, 1882
- A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition

HACKING AND THE INDIAN LAW(S):

The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology **Act**, 2000. The Computer as a Target :-using a computer to attack other computers. e.g. **Hacking**, Virus/Worm attacks, DOS attack etc. ... Cyber Crime regulated by Cyber **Laws** or Internet **Laws**.

Actually, 'Hackers' are very intelligent people who use their skill in a constructive and positive manner. They help the government to protect national documents of strategic importance, help organizations to protect documents and company secrets, and even sometimes help justice to meet its end by extracting out electronic evidence. Rather, these are people who help to keep computer criminals on the run.

Now dealing with the second part, i.e., what are such cyber criminals called? The actual word for such criminals is not 'hacker' but 'cracker'.
First I would like to explain the term 'Hacker', because there is a great misconception regarding it. I made a field study by a questionnaire method taking few samples amongst the youths across the country. In that study, for the question regarding explaining the term 'hacking', most of the samples were just beating around the bush. The responses were as follows: -

Knowledge About The Term Hacking
# 30% Do Not Know At All
# 5% Know Exactly What It Is
# 65% have Wrong Idea

Analyzing the above chart, we can see that it is only 5% of people who know exactly, what hacking means. Rest all other either don't know at all or they have a wrong notion about it. 65% of them believe hacking to be of a criminal nature.

So as to eliminate the fallacies in its connotation, I would like to begin with its meaning. Hackers are generally computer programmers who maintain network systems, secure documents, etc. So anyone who has a good hand on computer programming can be termed as 'hacker' in general.

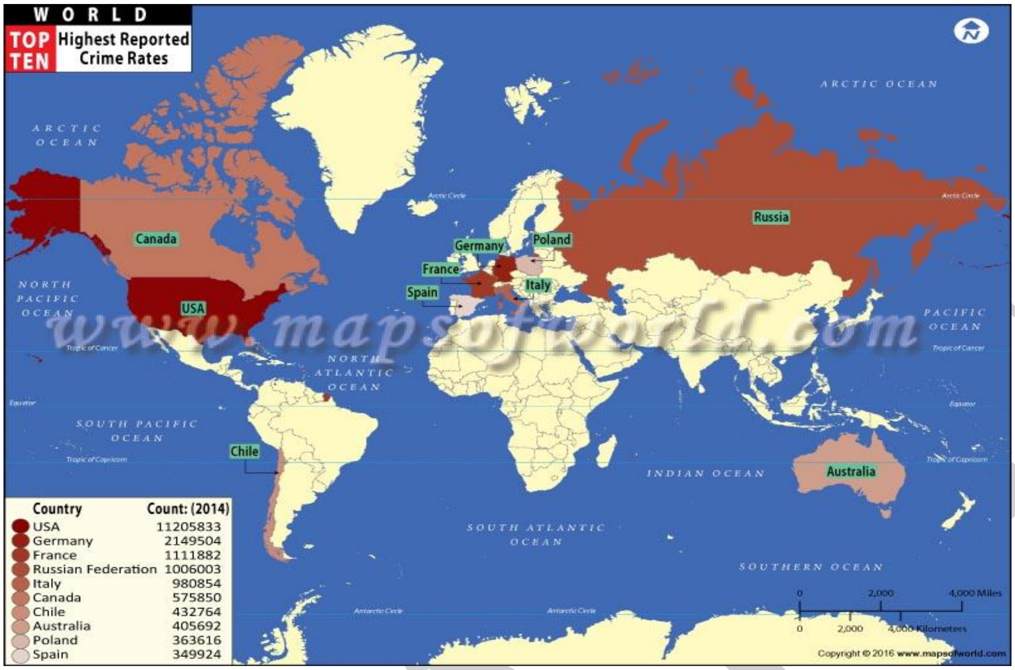
Ankit Fadia, who is a great master mind of India in the field of 'Hacking', has said:
"Traditionally, hackers were computer geeks who knew almost everything about computers and were widely respected for their wide array of knowledge. But over the years, the reputation of hackers has been steadily going down. Today, they are feared by most people and are looked upon as icons representing the underground community of our population."

There have been numerous hacking attacks on Indian government websites where state government websites or defense websites have been hacked. Some time back, the Principal Comptroller of defense accounts website was hacked due to which defense officials could not access their salary information.

The government, to reduce hacking of precise work, has agreed to the proposal of DEITY, which is the department of information and technology to stop using popular email ids for official purpose and has sanctioned a budget of Rs. 100 cores to safeguard the data. The websites of state governments have also been hacked in the past.

The official website of Maharashtra government was hacked, and the hackers were not traceable. There have been some professional hackers in India who have taken huge amounts to hack data from websites. In the infamous case of Amit Tiwari, who was a global hacker, he has hacked more than 950 accounts since 2003 and was caught by the police only in 2014. This shows the lack of evidence and the difficulty in arresting a hacker.

A Global Perspective on cybercrimes:



Country	Count: (2014)
● USA	11205833
● Germany	2149504
● France	1111882
● Russian Federation	1006003
● Italy	980854
● Canada	575850
● Chile	432764
● Australia	405692
● Poland	363616
● Spain	349924

It refers to illegal internet-mediated activities that often take place in global electronic networks. Cybercrime is "international" or "transnational" – there are 'no cyber-borders between countries'.

International cybercrimes often challenge the effectiveness of domestic and international law and law enforcement. Because existing laws in many countries are not tailored to deal with cybercrime, criminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments or difficulties of being traced.

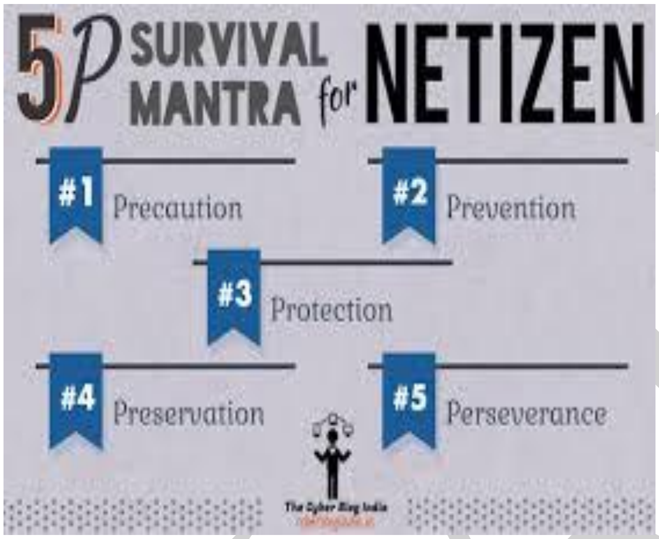
No matter in developing or developed countries, governments and industries have gradually realized the colossal threats of cybercrime on economic and political security and public interests. However, complexity in types and forms of cybercrime increases the difficulty to fight back. In this sense, fighting cybercrime calls for international cooperation.

Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale.

U.S.-China's cooperation is one of the most striking progress recently because they are the top two source countries of cybercrime.

Cybercrime and the Extended Enterprise: The term "extended enterprise" acknowledges that organizations are no longer just made up of employees and management working under one roof, but also encompass partners, suppliers, service providers, and customers. Fast forward to the digital present where it has taken on a whole new meaning and a whole new set of risks. Enterprises today exchange information almost completely online with more providers and partners, in more ways and more places than ever, enabled by technologies such as cloud computing, virtualization, and social networking.

Cybercrime Era: Survival Mantra for the Netizens:



Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. It is very difficult to classify crimes in general into distinct groups as many crimes evolve on a daily basis. Even in the real world, crimes like rape, murder or theft need not necessarily be separate. However, all cybercrimes involve both the computer and the person behind it as victims, it just depends on which of the two is the main target. Hence, the computer will be looked at as either a target or tool for simplicity's sake. For example, hacking involves attacking the computer's information and other resources. It is important to take note that overlapping occurs in many cases and it is impossible to have a perfect classification system.

Slang term derived from the combination of the words "Internet" and "citizen." The term netizen is used to describe people who use the Internet to participate in or contribute to an Internet group or society. The word may also be used to describe an individual who spends a lot of time on the net.

POSSIBLE QUESTIONS

PART-B

1. Define cybercrime. What are the two types of attack in cybercrime?

2. Write about cybercrime and the Indian ITA 2000.

3. Define Cybercrime and explain about information security.

4. Discuss about Global perspective on Cybercrime.

5. Define cyber criminals. What are the different type of cyber criminals?

6. Explain about cyber crime era – survival mantra for the netizens.

7. How are cybercrimes classified? Explain any ten briefly.

8. Define cybercrime. What are the two types of attack in cybercrime?

9. Write about "Indian legal perspective on cybercrime".

KARPAGAM ACADEMY OF HIGHER EDUCATION
COIMBATORE - 21
DEPARTMENT OF COMPUTER SCIENCE,CA & IT
CLASS : III B.Sc COMPUTER SCIENCE
BATCH : 2015-2018

Part -A Online Examinations **(1 mark questions)**

SUBJECT: Cyber Security **SUBJECT CODE: 15CSU603B**

S.NO	Questions	opt1	opt2	opt3	opt4	Answer
1	People who create electronic spam are called ___________________	Cybercrime	Cyberfraud	Spammers	Criminals	Spammers
2	_______________ web publishing techniques should be avoided.	Redirection	Hidden links	Spamming	Both A and B	Both A and B
3	_______________ is written defamation.	Libel	Slander	Cyberdefamation	B only	Libel
4	________________ is oral defamation.	Libel	Slander	Cyberdefamation	B only	Slander
5	Salami attack are used for committing____________________crimes.	Rawdata	Financial	Social media	Cyber fraud	Financial
6	_______________ occurs when someone forcefully takes control of a website.	E-mail spoofing	Identity theft	Web jacking	Online fraud	Web jacking
7	____________ as theft of software through the illegal copying of genuine programs or the countesfeiting and distibution of products to pass for the original.	Softwarepiracy	Computer sabotage	Forgery	Web jacking	Software piracy
8	________________ system accommodate an increasing no.of transnational offenses.	Legal perspective	Globalised information	Indian perspective	Only B	Globalised information
9	NCRB is a____ .	National Crime Record Bureau	Netizen Crime Record Bureau	Nationalism Crime Record Bureau	Network Crime Record Bureau	National Crime Record Bureau
10	Cybercrimes are punishable under two categories____________________	ITA 2000 and IPC	ITA 2000	IPC	Only A	Only A
11	Cyber terrorism was coined in______________	1998	1997	2002	1887	1997
12	SPI stands for______________________	Sensitive Personal Information	System Personal Information	Security Personal Information	Structure Personal Information	Sensitive Personal Information
13	In 2006 how many percentage of financial fraud crimes occur______________	12%	38%	55%	9%	9%

14	Usenet spam "Jesus is Coming soon" was posted on ____________ year.	12 March 1884	18-Jan-94	15-Apr-97	18-Jan-96	18-Jan-94
15	__________________ are some of the ofthread terms.	Crackers	Hackers	Criminals	Both A and B	Both A and B
16	Who break into computer system?	Hackers	Crackers	Cyberfraud	Cybercriminals	Crackers
17	______________________use a false identity to trap the children.	Hackers	Pedophiles	Crackers	Cybercriminals	Pedophiles
18	The abbreviation of COPPA is _____________________	Childrens Online Privacy Protection Act	Child Online Privacy Protection Act	Cybercrime Online Privacy Protection Act	Cyberfraud Online Privacy Protection Act	Childrens Online Privacy Protection Act
19	"Power of controller to give directon" is under the category of _________________ section.	Section 43	Section 67	Section 68	Section 72	Section 68
20	The abbreviation of ICT is _____________________	Information Communication Technology	Internet Communication Technology	Information Crime Technology	International Crime Technology	Information Communication Technology
21	_________________ is where users mentally travel through metrics of data.	Cybersquatting	Cyberpunk	Cyberspace	Cyberwarfare	Cyberspace
22	______________ is the act of registering a popular internet address,usually a company name,with the internet selling it to its rightful owner.	Cyber warfare	Cybersquatting	Cyberspace	Cyberpunk	Cybersquatting
23	______________ is a premediated act against a system,with the corruptor damage part of or the complete system.	Techno crime	Techno vandalism	Both A and B	A only	Technocrime
24	The abbreviation of IPR is ____________________________	International Property Right	Intellectual Property Right	Intellectual Process Right	International Product Right	Intellectual Property Rights
25	_______________________ is a harmful acts committed from as against a compuer or network.	Cybercriminals	Cyberfraud	Id theft	Cybercrimes	Cybercrime
26	The cybercrime harsome stigma attached and is notorious due to the word "terrorism" and "terrorist" attached _________________	Cyberterrorist	Cyber war	Cyber crime	Cyber terrorism	Cyber terrorism
27	______________refers to an attack using mail programs to deceive or coar internet users.	Spoofing	Spamming	Phishing	Bombs	phishing
28	_________________ covers protection from unauthorized occurs,users,disclosure,disruption,modificaton and destruction.	Cybercrime	crime	Cybersecurity	Cyber criminals	Cybersecurity

29	Phnographic is due to__________________	Lack of awareness	Lack of objectivity	Lack of product	Lack of theft	Lack of awareness
30	The abbreviation of OEM is ____________________	Original Effective Product	Original Elective Product	Original Edition Product	Oriented Edition Product	Original Edition Product
31	__________________ is the activity of run a virus program activities.	Triggers	Sabotage	Tracker	Hacking	Trigger
32	______________________is a event depend program create to do something only when a certain event occurs.	Logic bomb	Computer sabotage	Identity theft	Software piracy	Logic bomb
33	____________ refers to send a large no.of email to victim.	Crashing	Mail server crashing	Hacking	Cracking	Mail server crashing
34	The abbreviation of EMP is _________________________	Excessive Money Posting	Extensible More Posting	Excessive Multiple Posting	Extensing Multiple Posting	Excessive Multiple Posting
35	The abbreviation of PCI is ________________________	Postal Card Industry	Payment Card Individual	Payment Card Industry	Postal Card Individual	Payment Card Industry
36	PCI-DSS related to what type of frauds?	Software piracy	Creditcard	Pancard	Spoofing	Credit Card
37	Netizen are divided into _________ categories.	1	5	4	3	5
38	Organized criminals belong to what type of criminals?	Type 1	Type 2	Type 3	Type 4	Type 2
39	Former employees seeking revenge belongs to what type of criminals?	Type 2	Type 3	Type 1	A only	Type 3
40	____________ is a fraud involving another person identity for an illicit purpose.	Software piracy	Identity theft	Spamming	Spoofing	Identity theft
41	___________ will create a cell for cyber security	Cyberfraud	Cybercrime	Cyberwar	Cyberattack	Cybercrime
42	________ is performed without weapons in the network devices	Cyberfraud	Cybercrime	Cyberwar	Cyberattack	Cyberwar
43	Cybercrime is divided into -------- and -------------	Technology and technocrime	cyber terrorist and cyber terrorism	crime and criminals	Technocrime and Techno vandalism	Technocrime and Techno vandalism
44	The unwanted information are created in -------------	Technocrime	Technovandalism	Cyberspace	Cybercrime	Technovandalism
45	Hungry for recognition hackers belongs to what type of cybercriminals	Type I	Type II	Type III	All the above	Type I
46	Type II cybercriminals are only concern with the --------------	Revenge	Hobby	Money	None of the above	Money

47	Type III cybercriminals are worked for ---------------	Revenge	Hobby	Money	None of the above	Revenge
48	You will using a other person facebook id is called ----------------	Spamming	Spoofing	Hacking	Internet Time Theft	Internet Time Theft
49	Salami attacker are usually attack in the --------------	Bank	Schools	College	All the above	Bank
50	The management fix this person is worked in another company is called --------------	Industrial Spying	Spoofing	Spamming	Software Piracy	Individual Spying
51	Hackers are dominate the rule of ---------------	Computer Network Intrusion	Computer Networking Intrusion	Computer Network Industry	Computer Network Import	Computer network intrusion
52	________ at the site whoever install this sniffer can the impersonate an authorised user	Jeo Parasising security	Cyber Security	Cyber Criminals	Cyberspace	Jeo Parasising security
53	OTP means ________	One Time Password	One Time Pin	One Target Password	One Time Pincode	One Time Password
54	OTP is used for -------------	Credit card fraud	Spoofing	Spamming	Cyber terrorism	Credit card frauds
55	The first comprehensive presentation of computer crime is held on _______	1970	1979	1977	1966	1979
56	_______ makes it one of th most globalised offenses of the presents	Cyber crimes	Cyber fraud	Cyberspace	Cyberwar	Cybercrime
57	IAMAI -----------	Internet and Mobile Association of India	Internet and Modem Association of India	Internet and Mobile Association of Italy	Internet and Mobile Automation of India	Internet and Mobile Association of India
58	ITA and IPC -------------	Information Television ACT and Indian Penal Code	Intraction Technology ACT and Indian Penal Code	Information Technology ACT and International Penal Code	Information Technology ACT and Indian Penal Code	Information Technolody ACT and Indian Penal Code
59	A total of 207 cases of cybercrime were registered under the ---------------	IT act 2009	IT act 2005	IT act 2007	IT act 2000	IT act 2007
60	Section 74 ---------	Publication for fradulent purposes	Publication for cybercafe purposes	Publication for software purposes	Publication for software piracy	Publication for fradulent purposes

UNIT-II

SYLLABUS

Cyberoffenses: 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 - Cyberstalking: Types of stalkers, Cases Reported on Cyberstalking, How stalking Works?, real-life incident of Cyberstalking - Cybercafe and Cybercrimes .

Cyberoffenses:

- Cyber crime, or computer oriented crime, is crime that involves a computer and a network.
- The computer may have been used in the commission of a crime, or it may be the target.
- **Cybercrimes can be defined as:** "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".
- Cybercrime may threaten a person or a nation's security and financial health.

How Criminals Plan Them:

Introduction:

Cyber crime or Cyber attacks are categorized into five types, it can be categorized based on some factors.

1. Target of the crime
2. Whether crime require series of events or perform in single events.

Cyber Attack Meaning : Attack in which Cyber criminals can be targeted against person, property or organization include government, business and social.

CYBER SECURITY: TYPES OF CYBER CRIME

1. CRIME TARGETED TO PERSON (INDIVIDUAL)

The cyber criminals exploit human weakness such as avidity and innocence. This kind of cyber-attack include financial frauds, copyright violation, harassment, sale of stolen or non–existing items etc. Latest technology development and growth of internet cyber criminals have a new attacking tools that make them to expand group of potential victim.

2. CRIME TARGETED AT ASSETS

In this kind of crime include stealing property such as mobile devices, laptop, pen drive, CD, DVD, iPad etc. sometime attacker may insert harmful program such as Trojan virus and disturbed function of hard disk and pen drive. Shortcut virus is one type of Trojan used to steal information from computer. It’s like cyber Attack on Sony mobile.

3. CYBER CRIME AGAINST ORGANIZATION

Cyber attacks perform against organization is also called as Cyber terrorism. Cyber attackers use computer and internet to perform Cyber terrorism, by stealing private information or destroying valuable files, damaging programs file or taking control of network system.It’s like cyber attacks on banks.

4. CYBER ATTACKS USING SINGLE EVENT

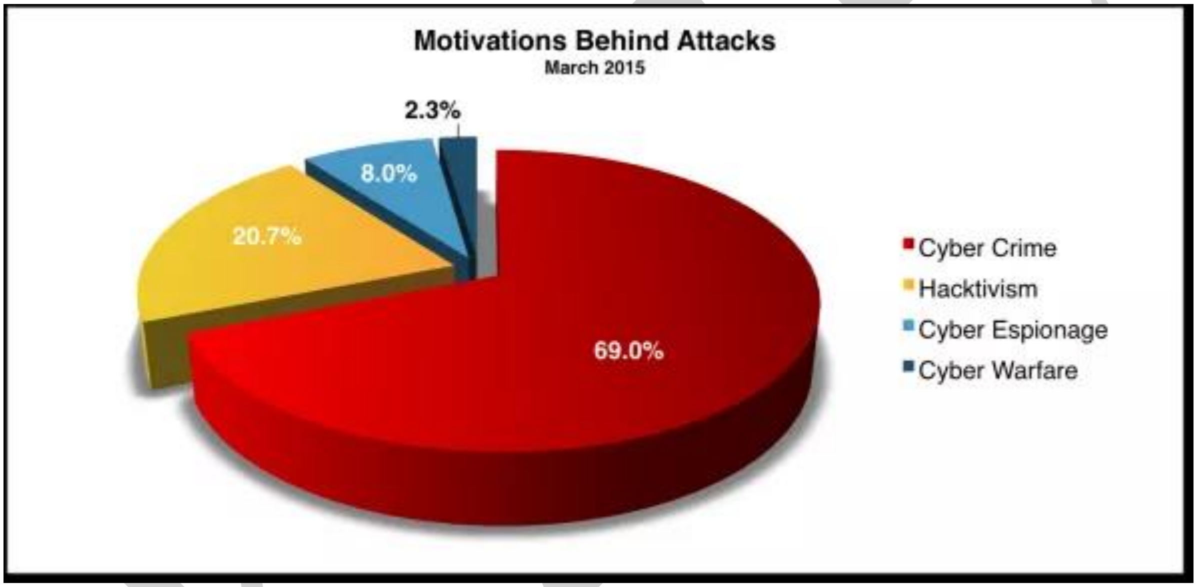
This type of Cyber attacks perform in single event from victim point of view. For example, mistakenly open email may contain virus. Representation of incorrect website called as phishing and steal valuable financial information. This kind of attack is also called as hacking or online fraud.

5. CYBER ATTACKS CONSIDERING SERIES OF EVENT

Sometime attacker perform series of event to track victim, interacting with victim. For example attacker perform communication with victim using phone or chat room establish connection with victim and then explore or steel valuable information. Know days this kind of attack getting viral so be aware before accepting friend request in Facebook or Whatsapp.

Once you know types of cyber attacks and how cyber criminal plan to attack then it is very easy to avoid cyber crime.

HOW CYBER CRIMINALS PLAN CYBER ATTACKS:



Cyber Attacks statistics India image source : hackmageddon

How Cyber Criminals Plan cyber Attacks

Cyber Criminals use many tool and methods to locate vulnerability of their victim. Criminal mostly categorized as.

1. Passive attacks
2. Active Attacks

Attackers can be categorized as inside attacker or outside attacker. Attacks perform within the organization is called inside attack whereas attacker get information from outside is called outside attack. Inside attack are always more dangerous than outside, because inside attackers has get more resources than outsider.Following are three major phases are involved in planning of cyber crime.

1. RECONNAISSANCE

This is first step towards cyber attacks, it is one kind of passive attack. “Reconnaissance” means an act of reconnoitering. In this phase attacker try explore and gain every possible information about target.

In hacking world, Hacking start with “foot printing”. Foot printing provide overall system structure, loop holes and exploration of those vulnerability. Attacker utilize this phase is to understand system, personal information, networking ports and services.

CYBER ATTACKER USE TWO STEPS TO GATHER THIS INFORMATION.

Passive Attacks: Passive attacks used to gain information about individual or organization. It exploit confidential information. Passive attacks involve gaining data about a target without target knowledge. Now day’s passive attack are much easier

- Use Google or other search engine: Gather information by searching on Google.
- Social Media: Search on social media like Facebook, Twitter, and LinkedIn.
- Use properly privacy setting in social media to avoid
- Organization Website: Attacker may get employee information using organizational website.
- Blog or press release: This are new source where attacker easily get company or individual information. Company.

- Job Posting: Search job profile provide valuable information about person an Job profile for technical person can give data about type of technology that is, software, server, database or network devices a company using on its network.
- Network Sniffing: This attack use to gather information such as IP address, network range, hidden server and other valuable services on network.

Active attacks: Active attack mostly used to manipulate or alter the system. It may effect on integrity, authenticity and availability of data. Information from passive phase is act as input to active phase. In this phase attacker verify gather information (IP address, network range, hidden server, personal information). This is very important as cyber attacker point of view, it provide security measure.

2. SCANNING AND SCRUTINIZING :

In this phase attacker collect validity of information as well as find out existing vulnerability. It is key phase before actual attack happen.

- Port scanning: Identify all ports and services (open / closed)
- Network scanning: Verify IP address and network information before cyber attacks.
- Vulnerability scanning: Checking loop hole in system.

Scrutinizing phase is also called enumeration.

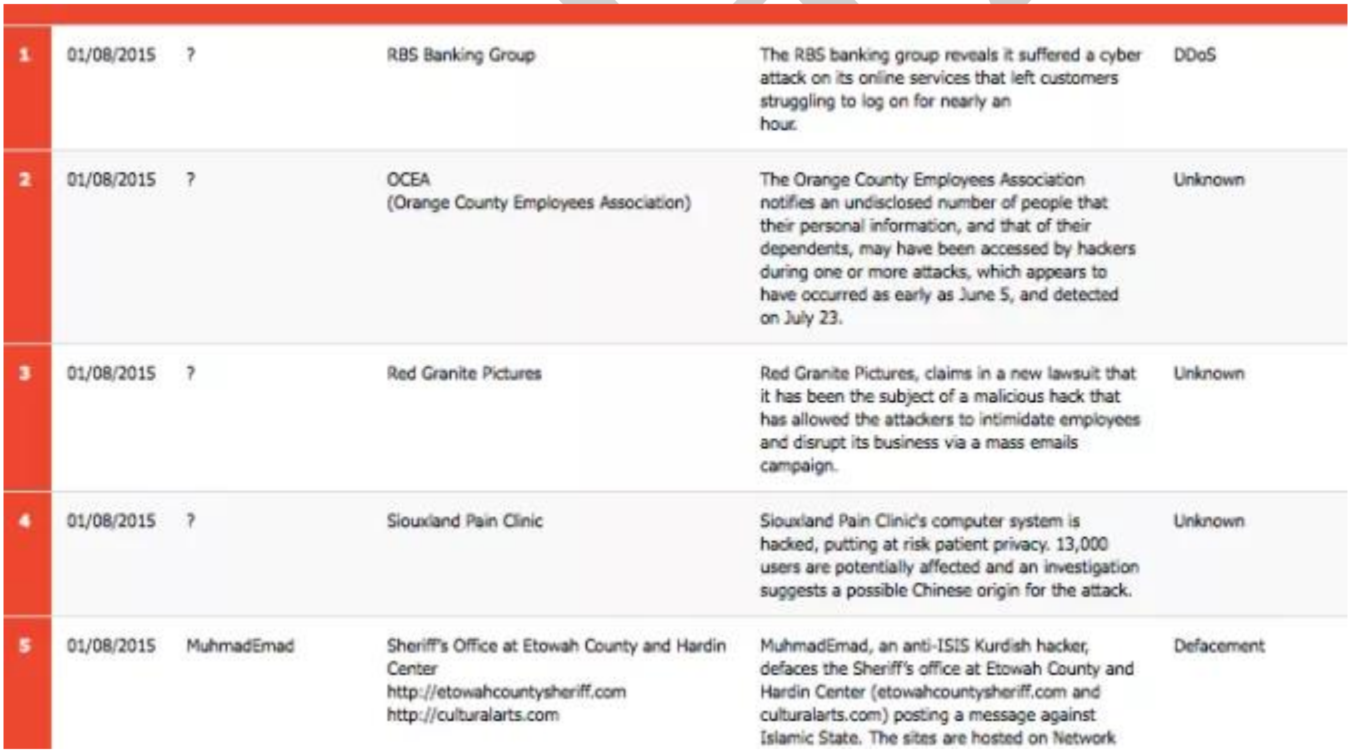
- Validate user accounts and groups
- Find out list of network resource and how many network devices are shared?
- Different types of OS and application.

3. LAUNCHING AN ATTACK

Using step two information actual launching attack to gain system information. Once step two complete cyber attacker ready to launch attack.

1. Crack the password.
2. Exploit the privilege
3. Execute malicious command
4. Hide the files
5. Final but most important is cover the track.

Recent cyber attacks



1	01/08/2015	?	RBS Banking Group	The RBS banking group reveals it suffered a cyber attack on its online services that left customers struggling to log on for nearly an hour.	DDoS
2	01/08/2015	?	OCEA (Orange County Employees Association)	The Orange County Employees Association notifies an undisclosed number of people that their personal information, and that of their dependents, may have been accessed by hackers during one or more attacks, which appears to have occurred as early as June 5, and detected on July 23.	Unknown
3	01/08/2015	?	Red Granite Pictures	Red Granite Pictures, claims in a new lawsuit that it has been the subject of a malicious hack that has allowed the attackers to intimidate employees and disrupt its business via a mass emails campaign.	Unknown
4	01/08/2015	?	Siouxland Pain Clinic	Siouxland Pain Clinic's computer system is hacked, putting at risk patient privacy. 13,000 users are potentially affected and an investigation suggests a possible Chinese origin for the attack.	Unknown
5	01/08/2015	MuhmadEmad	Sheriff's Office at Etowah County and Hardin Center http://etowahcountysheriff.com http://culturalarts.com	MuhmadEmad, an anti-ISIS Kurdish hacker, defaces the Sheriff's office at Etowah County and Hardin Center (etowahcountysheriff.com and culturalarts.com) posting a message against Islamic State. The sites are hosted on Network	Defacement

Cyber Attack News

Social Engineering:

Definition(s) of Social Engineering

- The term "Social Engineering" can be defined in various ways, relating to both physical and cyber aspects of that activity. Wikipedia defines social engineering as:
- "...the art of manipulating people into performing actions or divulging confidential information".

Other authors have provided the following definitions:

- "An outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system".
- "The practice of deceiving someone, either in person, over the phone, or using a computer, with the express intent of breaching some level of security either personal or professional".
- "Social Engineering is a non-technical kind of intrusion relying heavily on human interaction which often involves tricking other people into breaking normal security procedures" the attacker uses social skills and human interaction to obtain information about an organization or their computer systems.
- In reality Social Engineering can be any of these definitions depending on the circumstances that surround the attack.
- Social Engineering is actually a hackers manipulation of the natural human tendency to trust so as to get sensitive information needed to gain access to a system. Social
- Engineering does not require high level of technical expertise but requires the individual to have decent social skills.

Many people, for several decades have used social engineering as a method to research and collect data. These early social engineers would use the gathered information as a form of blackmail against the other organizations. Social engineering has been used to gain unauthorized access into several huge organizations. A hacker who spends several hours trying to break passwords could save a great deal of time by calling up an employee of the organization, posing as a helpdesk or IT employee, and can just asking for it.

Out of the blue you receive an email informing you about a large sum of money that is trapped in a foreign bank account a wealthy politician has died leaving a large sum of money. The sender is asking your help to transfer the money out of the country. You will receive a huge reward as well. The sender asks you to give them your bank account details to transfer the money then asks you to pay transfer fee/tax to transfer money out of the country. This fee may start with a small amount but will increase. The criminal will make up new fees that is necessary to be paid to receive your reward. It does not matter how much you pay, you will never receive your reward. This is a "scam" a type of social engineering and this particular scam is commonly known as "419 scam" an advanced fee fraud.

Criminals can use sophisticated attacks to gain access to your computer or trick you and obtain money. But they have another easier and non sophisticated tool in their arsenal called "social engineering". Social engineering uses human interaction(social skills) and obtains confidential information. The obtained information is then used in accessing the user accounts or according to the above example the user is tricked in obtaining money.

Classification of Social Engineering:

Social engineering attacks may be divided into two categories.

1. Computer based social engineering.
2. Human based social engineering.

Computer based social engineering attacks may include the below.

- Email attachments
- Fake websites
- Pop-up windows

On-line Scams
Emails sent by scammers may have attachments that include malicious code inside the attachment. Those attachments may include Keyloggers to capture users passwords,Viruses, Trojans, or worms.

Worm attacks
Attackers will trick users to click on a link or download a file then click on it, the executable file is a worm and will propagate from computer to computer copying itself.

A well known example is the “LoveLetter” worm that comes as an attachment in an email. The email requests the user to open an attachment in an email. When the users opens the attachment the worm copies itself to all the contacts in the users address book. This worm overloaded a huge number of email servers in the year 2000.

Sometimes pop-up windows can also be used in social engineering attacks. pop-up windows that advertise special offers may tempt users to unintentionally install malicious software.

Phishing attacks
This type of social engineering attack commonly uses emails to trick users in getting credentials to their bank accounts or maybe email accounts. The email mostly claims to be from a well known source, a highly reputed organization, and asks the user to click on a link that takes the users to a site similar to the organizations web site but this site is a fraudulent website that harvests users credentials. The fraudsters use these credentials to gain access to bank or email accounts and steal important information and money.

How to avoid being a victim

- Do not input confidential information into websites without checking the website security.
- Make sure the site is legitimate by checking the URL of the web site.
- Do not click on links inside suspicious emails.

- Fraudsters may even use events such as natural disasters(Asian Tsunami, Hurricane Katrina) or popular events(Olympics) for their benefit, be aware.
- If you are unsure of the legitimacy of an email try calling the company directly with the use of contact information used previously.
- Do not click or download suspicious attachments from email senders that you have not heard before.
- Use email filters, firewalls, virus guards to reduce the threat.
- When you are on the web, be aware that pop-ups that advertise bargains may request you to install malicious software to claim prices.

What can you do if you are a victim

- If you think you have entered your user id and password to a fraudulent website change your password as soon as possible.
- Inform the necessary authorities of the fraudulent object.
- If financial information have been compromised, close down or lock account to prevent harm.

In human-based social engineering attacks, the social engineer interacts directly with the target to get information.
An example of this type of attack would be where the attacker calls the database administrator asking to reset the password for the targets account from a remote location by gathering the user information from any remote social networking site of the XYZ company.
Human-based social engineering can be categorized as follows:

• **Piggybacking**: In this type of attack the attacker takes advantage by tricking authorized personnel to get inside a restricted area of the targeted company, such as the server room. For example, attacker X enters the ABC company as a candidate for an interview but later enters a restricted area by tricking an authorized person, claiming that he is a new employee of the company and so doesn't have an employee ID, and using the targets ID card.

• **Impersonating**: In this type of attack, a social engineer pretends to be a valid employee of the organization and gains physical access. This can be perfectly carried out in the real world by wearing a suit or duplicate ID for the company. Once inside the premises, the social engineer can gain valuable information from a desktop computer.

• **Eavesdropping**: This is the unauthorized listening to of communication between two people or the reading of private messages. It can be performed using communication channels such as telephone lines and e-mails.

- **Reverse social engineering**: This is when the attacker creates a persona that appears to be in a position of authority. In such a situation, the target will ask for the information that they want. Reverse engineering attacks usually occur in areas of marketing and technical support.

- **Dumpster diving**: Dumpster diving involves looking in the trash can for information written on pieces of paper or computer printouts. The hacker can often find passwords, filenames, or other pieces of confidential information in trash cans.

- **Posing as a legitimate end user**: In this type of attack, the social engineer assumes the identity of a legitimate user and tries to get the information, for example, calling the helpdesk and saying, "Hi, I am Mary from the X department. I do not remember my account password; can you help me out?"

Cyberstalking:

Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass.

Cyberstalking is often accompanied by realtime or offline stalking. In many jurisdictions, such as California, both are criminal offenses. Both are motivated by a desire to control, intimidate or influence a victim. A stalker may be an online stranger or a person whom the target knows. He may be anonymous and solicit involvement of other people online who do not even know the target.

Cyberstalking is a criminal offense under various state antistalking, slander and harassment laws. A conviction can result in a restraining order, probation, or criminal penalties against the assailant, including jail.

Types of Cyberstalking:

Cyberstalking cases differ from regular stalking in that it is technologically based, though some cyberstalkers escalate their harassment to include physical stalking as well. A cyberstalker acts of out of anger, or a need to control, or gain revenge over another person through threats, fear, and intimidation. There are several types of cyberstalking, including:

- Harassing the victim
- Embarrassing and humiliating the victim
- Exerting financial control by emptying the victim's bank accounts, or by ruining his credit
- Isolating the victim by harassing his family, friends, and employer
- Frightening the victim by using scare tactics and threats

Cases reported on cyberstalking:

Cyberstalking and Production of Child Pornography:

On January 23, 2013, James S. Allen of Baltimore, Michigan was indicted by a federal grand jury on 18 counts of cyberstalking, and 5 counts of production of child pornography. Between April and August of 2012, the defendant used the Internet and his cell phone to stalk 18 female victims in New York, some of whom were minors at the time of the abuse. Allen threatened the victims by telling them he had found nude pictures of them on the Internet, and told them where to find the photos. The website he sent the victims to was actually a phishing site, where he sought to obtain the victims' email addresses and passwords, allowing him to take control of their email accounts.

In addition, Allen threatened his victims with publication of their photos if they did not have a Skype chat session with him. Once the victims entered into the chat Skype, Allen demanded they take their clothing off and engage in sexual acts. If they refused, he would distribute the nude photos. One by one the girls contacted police. Because some of the girls were minors, Allen faces child pornography charges in addition to cyberstalking charges.

How stalking works:

Identifying Cyberstalking

It is sometimes difficult for a person who is being harassed or stalked to realize the situation is a criminal act that should be reported to the authorities. In deciding whether a situation is truly stalking, the victim should consider whether the perpetrator is acting with malice and premeditation. Stalking activities are often a repetitive, obsession-based vendetta, directed personally at the victim. This behavior continues even when the victim has personally warned the perpetrator to stop.

Key factors to identifying cyberstalking cases include:

- **False accusations**. A cyberstalker often tries to damage the reputation of his victim by posting false information on social media websites or blogs. A perpetrator may even create fictitious websites or other accounts for the purpose of spreading false rumors and allegations about the victim.
- **Gathering information about the victim**. A cyberstalker may try to gather as much information as possible about the victim by interacting with the victim's friends, family, and colleagues. In serious cases, a cyberstalker may hire a private investigator.
- **Monitoring victim's activities**. A cyberstalker may attempt to trace his victim's IP address, or hack into the victim's social media accounts and emails to learn about his online activities.
- **Encouraging others to harass the victim.** The offender may encourage the involvement of third parties to harass the victim.
- **False victimization**. It is not uncommon for a cyberstalker to claim the victim is harassing him, taking the position of victim in his own mind.

Protecting Yourself Against Cyberstalking:

The U.S. Department of Justice has issued recommendations for people who believe they are victims of cyberstalking. The first step should be to demand the stalker to stop all contact, and stop the harassing actions. Additionally, in order to facilitate prosecution of the perpetrator, the victim should:

1. **Save all emails, messages, and other communications for evidence.** It is vital that these are not altered in any way, and that the electronic copies are kept, rather than only printouts.
2. **Save all records of threats against the victim's safety or life.** This includes any written or recorded threats, and logs of the date, time, and circumstances of verbal threats.
3. **Contact the perpetrator's internet service provider.** Internet service providers (ISP) prohibit their users from using their service to harass others. Contacting the ISP may result in discontinuation of the harasser's internet service, and will put the ISP on notice to maintain record of the harasser's internet use.
4. **Keep detailed records of contact with ISP and law enforcement officials.** It is important to keep a log of all reports made to any agency or provider, and to obtain copies of the official reports when available.

Real life incident of Cyberstalking:

- A woman contacted police in 2003, claiming someone had given her private information, including her location and her description, to men through a dating service. The woman discovered the act when she was contacted by two different men, each of whom stated they had previously talked with her, and arranged a personal encounter.
- Claire began being harassed by strangers after someone made a post on the Internet offering sexual services in her name. The post included private information, including her phone number and home address.
- After John and his girlfriend broke up, he began stalking her by planting a prepaid GPS-enabled cell phone under her car. John tracked his ex-girlfriend's movements, and followed her by logging into the cell phone account online. John also called his upwards of 200 times a day.

There have been a number of high-profile legal cases in the United States related to cyberstalking, many of which have involved the suicides of young students. In thousands of other cases, charges either weren't brought for the cyber harassment or were unsuccessful in obtaining convictions. As in all legal instances, much depends on public sympathy towards the victim, the quality of legal representation and other factors that can greatly influence the outcome of the crime – even if it will be considered a crime.

CYBERCAFE: A cybercafe is a business which allows people to pay for access to the Internet. Most cybercafe provide computers, snacks, and beverages to their customers.

Another name for a cybercafe is an Internet cafe. Such places often look just like cafes or coffee shops, with the addition of computer terminals. Cybercafes are especially useful for travelers who need a place to check their email or book flights and hotel rooms online. The original cafe of this kind opened in 1988 in South Korea, but the term cybercafe was first used in 1994, when innovator Ivan Pope opened one in London.

Cybercrime:

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitive or malicious purposes.

Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime.

POSSIBLE QUESTIONS

PART-B

1. How are cybercrimes classified? Explain with examples.
2. Discuss about cybercafe and cybercrime
3. How criminals plan the attack?
4. Define social engineering. What are the classification of social engineering.
5. What is cyberstalking? How stalking works?
6. Elaborate a real – life incident of cyberstalking?

KARPAGAM ACADEMY OF HIGHER EDUCATION
COIMBATORE - 21
DEPARTMENT OF COMPUTER SCIENCE,CA & IT
CLASS : III B.Sc COMPUTER SCIENCE
BATCH : 2015-2018

Part -A Online Examinations **(1 mark questions)**

SUBJECT: Cyber Security **SUBJECT CODE: 15CSU603B**

S.NO	QUESTIONS	OPT 1	OPT 2	OPT 3	OPT 4	ANSWERS
1	Technology is a _________________________as it can be used for both good and bad purposes.	single-edged sword	double-edged sword	No-edged sword	None of the above	Double-edged sword
2	_____________________ is a program that automatically dials phone numbers looking for computer on the other end	Phreaking	Wardialer	only B	Brute force	Wardialer
3	______________________sites on the internet are popular among crackers and other criminals	Wardialer	Phreaking	Hacking	Cracking	Phreaking
4	The abbreviation of CIA is _________________________	Control Intelligence Agency	Controllable Intelligence Agency	Centre Intelligence Agency	Central Intelligence Agency	Central Intelligence Agency
5	______________ is a person who is ethically opposed to the abuse of computer systems	Black hat hacker	Grey hat hacker	white hat hacker	None of the above	White hat hacker
6	________ is another means of passive attack to yield information.	Network sniffing	E-mail spoofing	only A	Both A and B	only A
7	An active attack involves the risk of detection and is also called as_________________________	Rattling the door nobs	Active reconnaissance	Door nobs	Both A and B	Both A and B
8	_________________ is to gathered information for the validity of the information as well as to identify as existing vulnerabilities.	Scanning	Reconnaissance	Scanning and Scrutinizing	Only C	Only C
9	The objectives of scanning is of ___________________	Two types	Three types	Four types	Five types	Three types
10	______________ understand the existing weakness in the system.	Port scanning	Network scanning	Vulnerability scanning	URL scanning	Vulnerability Scanning
11	The scrutinizing phase is always called___________________ in the hacking world.	Privileges	Enumeration	Malicious	Cracking	Enumeration

12	____________________involves gaining sensitive information or unauthorized access privileges with insiders.	Social executing	Social architecturing	Social engineering	social builder	Social engineering
13	____________________attacker pretends to have permission from an authorized source to use a system.	Calling technical support	Posing as an important user	Impersonating an employee or valid user	None of the above	None of the above
14	Cybercrimes such as stealing of bank passwords are happened through______________	Internet	Shoulder sniffing	Dumpster diving	Cybercafes	Cybercafes
15	_____________refers to the use of Internet and other electronic communications devices to stalk another person.	Online stalking	Offline stalking	Cyber bullying	Cyberstalking	Cyberstalking
16	____________________is a term used for collection of software robots.	Botnet	Network	Internet	Computing software	Botnet
17	Set the ___________________ to download and install security patches automatically.	Vectors	OS	Computing system	Software	OS
18	_____________ stalkers aim to start the interaction with the victim directly with the help of the internet.	Offline	Cyber	Online	None of the above	Online
19	________________hostile content is either embedded in the message or linked by the message.	Attack by deception	Attack by Worms	Attack by E-mail	Sneakware	Attack by E-mail
20	_____________ is a broadest market.	IaaS	SaaS	Both A and B	PaaS	SaaS
21	People with the tendency to cause damages or carrying out illegal activities will use it for ____________	Good purpose	Bad purpose	Both A and B	Only B	Ony B
22	People who commit cybercrimes are known as ______________	Hackers	Criminals	Crackers	Crimers	Crackers
23	The term ____________ is usally connected to computer criminals.	Phreaker	Hacker	Brute force	Cracker	Cracker
24	The abbreviation of RAS is _____________________	Remote Access Server	Remote Axes Server	Remote Access Service	Remove Access Service	Remote Access Server
25	A black hat is also called a ___________________	Cracker	Hacker	Dark side hacker	Both A and C	Both A and C

26	A white hat hacker is considered an____________	Dark side hacker	Dark side cracker	Ethical hacker	None of these	Ethical hacker
27	________________ is one of the distinct crimes against organizations/governments.	Cyberterrorism	Cybercrime	Crimes	Attackers	Cyberterrorism
28	The abbreviation of NSA is _____________________	National Service Agency	Netizen Service Agency	National Security Agency	National Servicing Agency	National Security Agency
29	Single event of cybercrime is the __________________ from the perspective of the victim.	Double event	Single event	Only B	None of these	Ony B
30	_______________ are usually used to alter the system whereas passive attacks attempt to gain information about the target.	Passive attack	Attack	Active attacks	Both A and D	Active attacks
31	_________________ is the first phase and is treated as passive attacks.	Scanning	Scrutinizing	Scanning and Scrutinizing	Reconnaissance	Reconnaissance
32	An attacker attempts to gather information in ______________ phases.	Three	One	Two	Four	Two
33	____________ understand IP addresses and related information about the computer network systems.	Network scanning	Port scanning	Vulnerability scanning	Transfer scanning	Network scanning
34	____________________ is an art of exploiting the trust of people,which is not doubted while speaking in a normal manner.	Social builder	Social architecture	Social engineering	Only B	Social engineering
35	_________________ involves looking in the trash for information written on pieces of paper or computer printouts.	Sholder surfing	Dumpster diving	Using a third person	Calling technical support	Dumpster diving
36	The ________________ sends fake E-mails to numerous users in such that the user finds it as a legitimate mail.	Cracker	Hacker	Attacker	Criminal	Attacker
37	There are ______________ types of stalkers.	One	Two	Three	Four	Two

38	The abbreviation of ITA is _________________	India Information Technology Act	Indian Informative Technology Act	Indian Information Technology Act	Indian Informations of Technology Act	Indian Information Technology Act
39	_______________ websites and other similar websites with indecent contents are not blocked.	Pornographic	Cybercrime	Cybercafe	None of these	Pornographic
40	The abbreviation of FIR is __________________	First Information Feport	Final Information Report	First Informative Report	Final Innovative Report	First Information Report
41	_____ use the world wide web and internet to an optimam level for all illegal activities to store data. Context, account information etc.	cybercrime	cybercriminal	cyberwar	cyber security	cybercriminal
42	_______ it is a technique used to fing password or encryption keys	Brufe force hacking	blue force hacking	brute force hacking	brule hacking	brute force hacking
43	_____ is a popular, growing subject on the internet	hacking	attacking	cracking	attacker	cracking
44	An _____ would look to exlpoit being vulnarabilities in the network most often so because the networks are not adequetly protected	hackers	attackers	crackers	attacking	attackers
45	____ is a person who uses his knowledage of vulnerability and exploits for private gain rather than reveoling them either to the general public or to the manufacture for correction	white hat	grey hat	brown hat	Black hat	Black hat
46	A ______ hacker is one who thinks before acting or commanding a malice or non malice deed	white hat	brown hat	grey hat	black hat	brown hat
47	______ use many method and tools to locate the vulnerability of the target	criminals	cybercriminal	hackers	crackers	criminals
48	_________ may affect the avaoilability integrity authenticity of data were us passive attracts lead to the branches of confidentiality	scanning	passive attack	active attacks	none of these	active attacks
49	______ gaining and maintaining the system assets	passive attack	active attack	reconnaissance	launching an attack	launching and attack

50	Literal meaning of _____ is an reconnoitering explore often which the goal of finding something or somebody	reconnaissance	active attack	passive attack	launching an attack	reconnaissance
51	______ identifing open and close ports and service	network scanning	port scanning	vulnerability scanning	all the above	port scanning
52	______ is a key step to examine intelligently while gathering information about the target	scrutinizing	scanning	both a and b	only b	scanning
53	__________ is an act of systematically scanning a computer ports	port scanning	network scanning	vulnerability scanning	all the above	port scanning
54	________ social engineering refer to person to person interaction to get the required/desired information	computer based	human based	both a and b	only b	human based
55	Is is a technique of gathering information such as username and password over a person shoulder	dumpster diving	calling technical support	shoulder surfing	using a third person	shoulder surfing
56	______ socail engineering refer to an attempt made to get the required/desired information by using computer software/internet	human based	computer based	both a and b	only b	computer based
57	__________ are also used in a similar manner to email attachment	pop-up windows	email attachment	fake email	none of theses	pop-up windows
58	An ____ 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	zero day attack	payload	attack vector	none of these	attack vector
59	The term ________ is used as metaphor for the internet based on the cloud driving used to depict the internet in computer networks	cloud	network	both a and b	none of these	cloud
60	_______ is a set of software and development tools hosted on the providers servers	cloud-as-a-service	infrastructure-as-a-service	software-as-a-service	platform-as-a-service	platform-as-a-service

UNIT-III

SYLLABUS

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.

CYBERCRIME:

MOBILE AND WIRELESS DEVICES:

Introduction :

A wide range of mobile devices are in use today, including (smart) phones, media players, tablets, and notebook PCs. These devices are typically network-connected for most of the time they are switched on. This poses a well-known, albeit not well-understood, threat from cyber criminals. Apart from the ‘obvious’ mobile devices, a growing number of everyday objects are also ‘always/often connected’, including road vehicles of all kinds (cars, lorries, etc.), RFID tags embedded in all sorts of devices, chip-based payment cards, including proximity-based cards, electronic key fobs, and public transport vehicles.

These are just the mobile devices – many everyday fixed objects are also rapidly becoming Internet connected, including ‘smart’ buildings, e.g. shops, restaurants, homes, and workplaces, and installations within buildings, such as domestic appliances and factory machinery. Of course, traditional mobile devices (such as phones, PCs, etc.) have been the main focus of security and privacy concerns. Whilst there are very major issues for such systems, perhaps other devices pose an even greater threat.

It may well be that the possibilities for crime (and countermeasures) involving such everyday devices have not been properly thought through, and this issue forms the main focus of this paper. The remainder of this paper is structured as follows. The main cyber (and hence cyber crime) threats to mobile devices are reviewed. We then look at how these threats apply to some of the less well-studied classes of mobile device, and the news is not always good.

One reason for problems in all categories of mobile devices and systems is that systems have evolved piecemeal, and there is no overall security architecture. As with all IT products, the pressure to release the latest innovation always takes precedence over the need for security. Moreover threats arise from ‘accidental’ functionality; systems are interconnected because we ‘might as well’, without thought about the possible consequences.

PROLIFERATION OF MOBILE AND WIRELESS DEVICES:

Mobile computing along with Wireless Technology, is the next stage in the evolution of computing bringing about substantial benefits to both organizations and individuals. Wireless Local Area Networks (WLAN) are growing popular at a rapid rate, enabling users to access to vital information anywhere and anytime and proving to be both time and cost effective to organizations across many sectors.

The implementation of Wireless Technology introduces new threats and risks to the information of the organization and corporate assets that may have been previously overlooked. Organizations need to understand the importance of constantly securing their information, whether the information is stored locally, or accessed remotely. Since its conception in 1980, many organizations are experimenting in implementing WLAN's using a variety of technologies; such as infrared and radio wave technology (Uskela, 1997). Corporate IT teams, with the introduction of wireless devices such as; Personal Digital Assistants (PDA'S), Laptops and Smart phones need to learn and adopt new security technologies and methodologies to target the unique requirements of the organization.

The IEEE 802.11 standard, which describes wideband wireless applications (Uskela, 1997), was sanctioned in 1997. Organizations are now implementing this standard to expand their physical reach. Wireless Technology enables businesses to create new partners compared to traditional wired technology which otherwise inhibits this expansion (Quay, 2002). The implementation of this technology allows users to work beyond the confines of the office by communicating over air waves. Additionally, wireless technology may cause a cost saving to the organization by enabling network connections formerly that are too expensive to connect with physical connections (Quay, 2002).

Today almost every business aspect involves the use of IT. Organizations are investing large amounts of capital in implementing new technologies to create a broader spectrum of business associates. A greater capital gain and return on investment (ROI) is achieved with a broader reach. There are very few users and companies not utilizing mobile devices whether it is a laptop or handheld device. This high usage of mobile devices requires great emphasis be placed on securing both the stored and communicated information. Security should be a priority as this information can contain valuable corporate data.

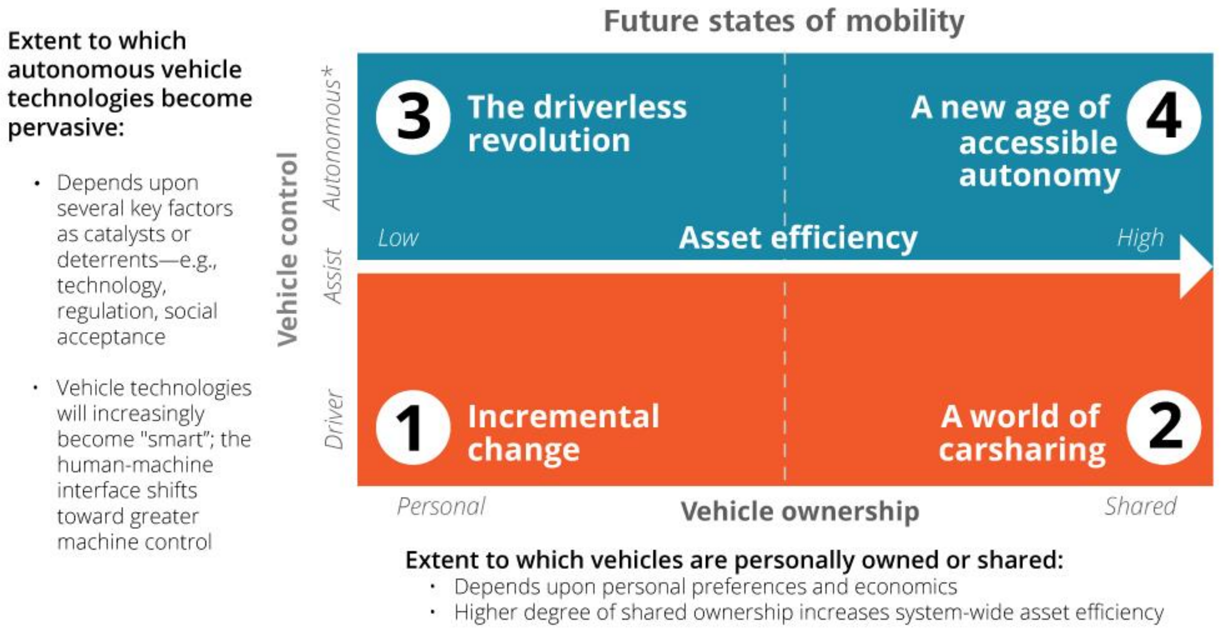
It is imperative that users of mobile devices follow a mobile security policy, personal or corporate, to protect this data (Burling, 2005). The objective of this paper is to identify the major risks of wireless devices and networks and its effects on corporate governance. The paper will secondly determine appropriate measures through which organizations can secure their information by understanding the importance of risk assessment before implementing new technologies.

This will be accomplished by first identifying the threats to wireless technology and address ways in which organisations can safeguard their assets on a wireless network. The paper will then look at the Corporate Governance and its effects and how it plays a role in securing stored and communicated information in a wireless environment.

Trends in mobility:

The extended global automotive industry is undergoing an unprecedented transformation to a new mobility ecosystem, what we call **a new age of accessible autonomy** driven by social trends and the driverless revolution. The pace of change is breathtaking, as established leaders and nimble disruptors make bold plays to win and governments look to catalyze the future of mobility.

Figure 1. The future states of mobility


Future states of mobility
Extent to which autonomous vehicle technologies become pervasive:
Depends upon several key factors as catalysts or deterrents—e.g., technology, regulation, social acceptance
Vehicle technologies will increasingly become "smart"; the human-machine interface shifts toward greater machine control
Vehicle control
Autonomous*
Assist
Driver
3 The driverless revolution
A new age of accessible autonomy 4
Low
Asset efficiency
High
1 Incremental change
A world of carsharing 2
Personal
Vehicle ownership
Shared
Extent to which vehicles are personally owned or shared:
Depends upon personal preferences and economics
Higher degree of shared ownership increases system-wide asset efficiency

*Fully autonomous drive means that the vehicle's central processing unit has full responsibility for controlling its operation and is inherently different from the most advanced form of driver assist. It is demarcated in the figure above with a clear dividing line (an "equator").

Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

CREDIT CARD FRAUDS IN MOBILE AND WIRELESS COMPUTING ERA:

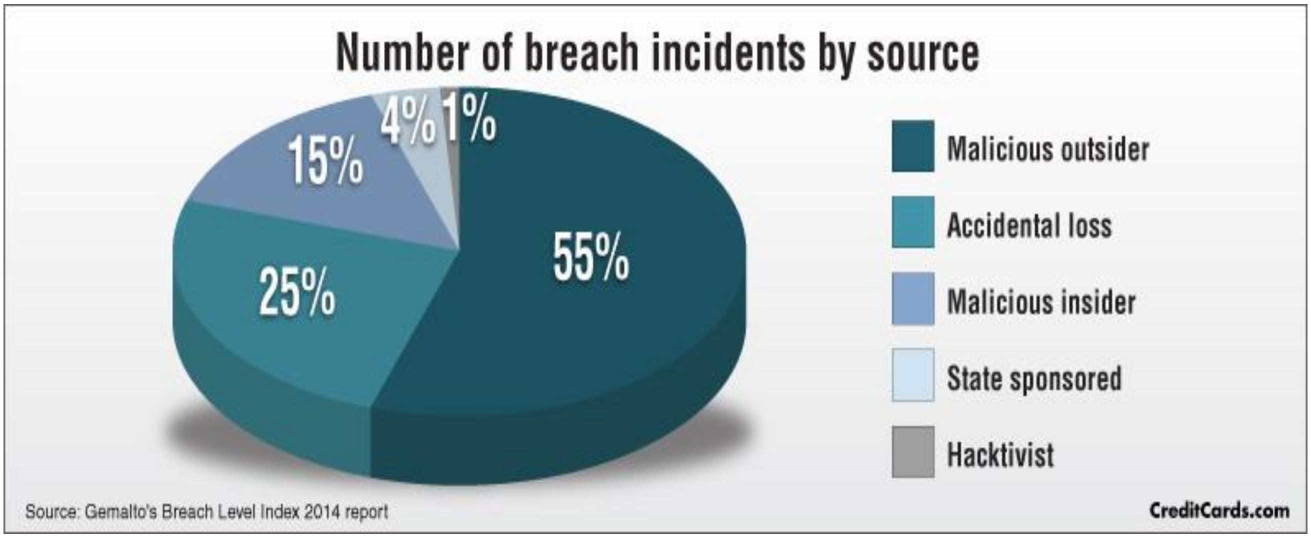
TYPES & TECHNIQUES OF CREDIT CARD FRAUDS:

Credit card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. Credit card fraud is also an adjunct to identity theft. According to the United States Federal Trade Commission, while the rate of identity theft had been holding steady during the mid 2000s, it increased by 21 percent in 2008. However, credit card fraud, that crime which most people associate with ID theft, decreased as a percentage of all ID theft complaints for the sixth year in a row.

Credit card fraud comes in many different shapes and forms, including fraud that involves using a payment card of some description, and more. The reasons for credit card fraud also vary. Some are designed to obtain funds from accounts, while others wish to obtain goods for free. Furthermore, it is very important to understand that credit card fraud is linked closely to identity theft. According to the Federal Trade Commission, some 5% of all people over 16 in this country have been or will be the victim of identity theft. Additionally, at the last count in 2008, it was found that there had been a 21% growth in prevalence of identity theft. On the other hand, the percentage of identity theft cases related to credit card fraud decreased, which is a positive thing and a credit to law enforcement professionals and the general public as a whole.

It seems that about 0.1% of all credit card transactions are fraudulent, which equates to a huge financial loss. Some 12 billion credit card transactions were conducted in 2009, of which about 10 million were fraudulent. Additionally, it was found that 0.04% of all accounts that were active monthly were fraudulent. These proportions have not changed much over time. It is a positive thing to know, however, that there are now more sophisticated methods of detecting fraud and stopping it. Unfortunately, the actual amount in losses continues to be in the billions.

Featured Graphic:



Source: Gemalto's Breach Level Index 2014 report

According to CreditCards.com, data breaches totaled 1,540 worldwide in 2014 — up 46 percent from the year before — and led to the compromise of more than one billion data records. Twelve percent of breaches occurred in the financial services sector; 11 percent happened in the retail sector. Malicious outsiders were the culprits in 55 percent of data breaches, while malicious insiders accounted for 15 percent.

But credit card fraud is not just one single action. In fact, there are many different forms out there. It is important to remember that there are more, particularly as hackers and identity thieves are becoming more proficient at taking people's financial data online.

Below are the 11 most common forms of credit card fraud.

1. Application Fraud

Application fraud generally happens in conjunction with identity theft. It happens when other people apply for credit or a new credit card in your name. They will usually first steal supporting documents, which are then used to substantiate their fraudulent application. Banks have various safeguarding measures in place to stop this type of fraud from happening. The most important one is requiring original documentation only. Additionally, they will often telephone employers to confirm identity. Unfortunately, criminals will frequently forge documents and provide false telephone numbers for places of employment. Unfortunately, there are always ways around certain safeguarding measures.

2. Electronic or Manual Credit Card Imprints

A second form of credit card fraud is experienced through credit card imprints This means that somebody skims information that is placed on the magnetic strip of the card. This is then used to encode a fake card or to complete fraudulent transactions.

3. CNP (Card Not Present) Fraud

If somebody knows the expiry date and account number of your card, they can commit CNP fraud against you. This can be done through phone, mail or internet. It essentially means that somebody uses your card without actually being in physical possession of it. More and more and often, merchants will require the card verification code, making CNP fraud slightly more difficult, but if a fraudster can get your account number, they probably know that number too. Additionally, there are only 999 possible combinations for the verification code. As such, many criminals attempt to order items of very low amounts until they figure out the right number. Be on the lookout, therefore, for small payments on your statements.

4. Counterfeit Card Fraud

Counterfeit card fraud is usually committed through skimming. This means that a fake magnetic swipe card holds all your card details. This fake strip is then used to create a fraudulent card that is fully functional. Essentially, it is an exact copy, which means fraudsters can simply swipe it in a machine to pay for certain goods. This type of fraud can also be committed by someone who knows your card details. They can use this information to create a so-called 'fake plastic'. Here, the magnetic strip or the chip on the card doesn't actually work. However, it is often easy enough to convince a merchant that there is something wrong with the card, at which point they will enter the transaction by hand.

5. Lost and Stolen Card Fraud

The next possible type is lost and stolen card fraud. Here, your card will be taken from your possession, either through theft or because you lost it. The criminals who get their hands on it will then use it to make payments. It is difficult to do this through machines, as they will require a pin number. However, it is easy enough to use a found or stolen card to make online purchases. It is for this reason that it is vital that you cancel your cards as soon as you realize they are missing.

6. Card ID Theft

Card ID theft happens when the details of your card become known to a criminal, and this information is then used to take over a card account or open a new one. Your name will be used for this. This is one of the most difficult types of fraud to identify and to recover from, because it can take a long time before you even know that it has happened.

7. Mail Non-Receipt Card Fraud

This type of fraud is also known as never received issue or intercept fraud. In this case, you were expecting a new card or replacement one and a criminal is able to intercept these. The criminal will then register the card and they will use it to make purchases and more.

8. Assumed Identity

With assumed identity fraud, a criminal will use a temporary address and a false name to obtain a credit card. There are a number of systems in place with banks for protection against this type of fraud. For instance, they will ask new customers to provide account references and these will be check to ascertain that they are genuine. Additionally, they could ask for such things as birth certificates, original copies of driver's license or passports and so on. They often ask for these things before they will send a card out.

9. Doctored Cards

A doctored card is a card whereby a strong magnet has erased its metallic stripe. Criminals do this and then manage to change the details on the card itself so that they match those of valid cards. Naturally, this card won't work when a criminal tries to pay for something. However, they will then use their charm to convince a merchant to just enter the details of the card manually.

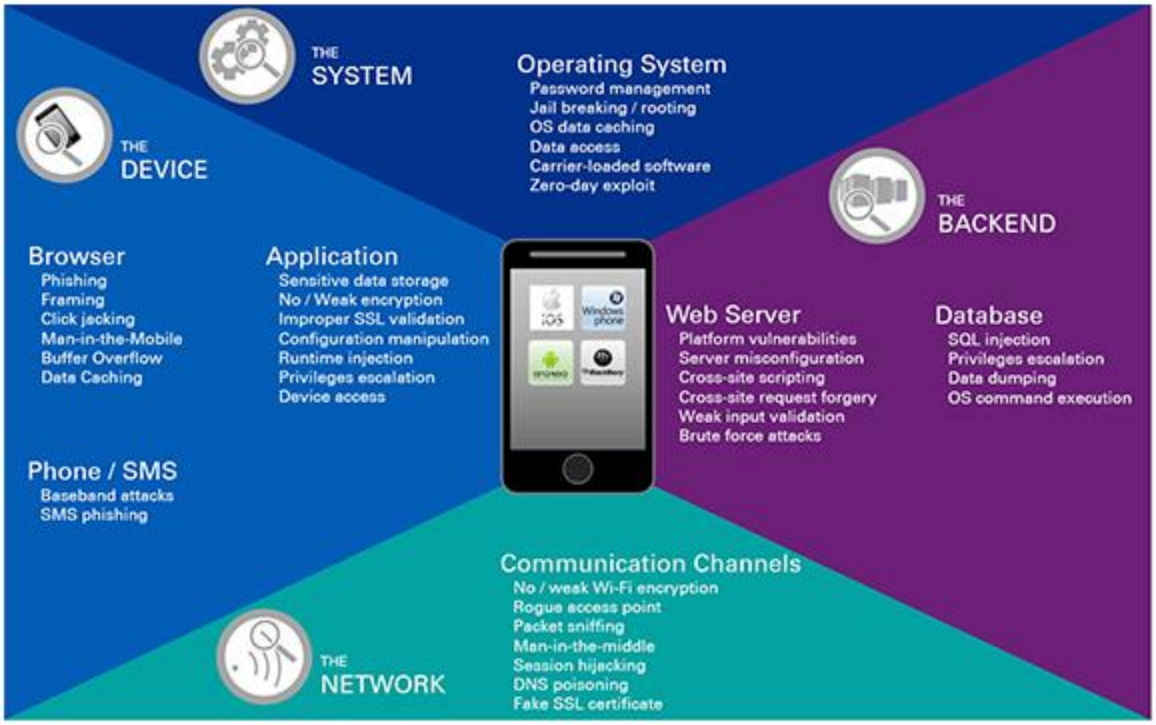
10. Fake Cards

It takes a lot of time, skill and effort to create fake credit cards, but that doesn't stop a determine criminal. A card has to meet certain complex security features and cards are becoming increasingly advanced, meaning this is much harder to do. There is the magnetic strip, the chip and, often, holograms. However, someone who is skilled can forge this type of cards using fake names and numbers and will make transactions with the card. The card isn't actually linked to an account, so the credit card company will not pay for the transaction since they cannot link it to a specific user. By that time, however, the criminal will be long gone with their purchases.

11. Account Takeover

Account takeover is actually one of the most common forms of credit card fraud. Basically, a criminal will somehow manage to get hold of all of your information and relevant documents. This is usually done online. They will then contact the credit card company and pretend to be you, asking them to change the address. They will provide 'proof' of identity, since they have hacked through or otherwise obtained, your personal details. A replacement card will then be sent to the fake address, and the criminal will be able to make charges.

Security challenges Posed by Mobile Devices: If mobile applications are provided to customers, secure coding best practices for online applications need to be followed for mobile development. Specific additional aspects need to be considered such as inter-application communication, storage of data in the cache of the device itself, certificate management between the application and the device, information leakage through screenshot capabilities, etc.



The device and its operating systems typically come with vulnerabilities and those need to be taken into account in the application architecture. Although more demanding, ensuring that the application acts as a safe encrypted container on the phone prevents unauthorized access to information from malicious third party application or mobile Trojans and malwares.

Increasing need for mobile security Expertise:

Mobile applications and mobile devices are great business enablers and business opportunities. They however come with new risks and new challenges. Facing these challenges will require more and more expertise to ensure that a well architected cyber defense strategy is deployed for secure connectivity of BYOD devices and to ensure that mobile applications are secure by design. Taking the specific challenges of mobile devices into account from the beginning of the application and device deployment lifecycle, as well as ensuring that mobile devices are regularly assessed and tested for security vulnerabilities are key steps for a successful business investment in a fast growing mobile environment.

Registry Settings for Mobile Devices:

MSDN contains information on the Default Security Policy settings for both Windows Mobile Pocket PC's and Windows Mobile-based Smart phones. Check them out! Of interest is the section referring to the Grant Manager settings. The several comments on the Windows Mobile team blog that referred to changing the registry key value in HKLM\Security\Policies\Policies\00001017 from the default of 128 to 144 and that this would aid in being able to install certificates, but didn't quite understand why that would make a difference until I read the MSDN documentation.

The MSDN article indicates that the registry key 00001017 is the setting for the Grant Manager Policy, which basically defines which roles are granted system administrative authority. The different roles are (there are actually a few more which are listed in the link below, they are particularly relevant):

Security Role	**Registry Key Value (Decimal)**
SECROLE_OPERATOR_TPS	128
SECROLE_PPG_TRUSTED	2048

SECROLE_PPG_AUTH	1024
SECROLE_TRUSTED_PPG	512
SECROLE_USER_AUTH	16
SECROLE_MANAGER	8
SECROLE_OPERATOR	4

The thing to understand about registry settings such as these is that they can be used singularly, or in combination. When you look at the value of the key, it represents all settings that are enabled.

By default, on non-phone based devices (Pocket PC only), the default setting (outlined in the MSDN article) is actually set to Decimal 16 (Hex of 0x000010), which equates to SECROLE_USER_AUTH. On phone-based devices (Pocket PC Phone edition and Smart phones), however, it defaults to Decimal 128 (Hex 0x000080), which is SECROLE_OPERATOR_TPS. By changing the value to Decimal 144 (Hex 0x000090), what you are actually doing is enabling both SECROLE_OPERATOR_TPS and SECROLE_USER_AUTH (128+16 = 144). In the same section of the MSDN site, another page describes the various security roles.

The only bit of advice I feel compelled to share here is to make sure that you document any settings when you make changes. There is nothing worse than knowing you changed something, but forgetting where it was you made the change, and what the default value was, especially when it is causing problems.

Authentication Service Security:

Modern computer systems provide service to multiple users and require the ability to accurately identify the user making a request. Password based authentication is not suitable for use on computer network – as it can be easily intercepted by the eavesdropper to impersonate the user.

There are 2 components of security in mobile computing:

1. **Security of Devices** : – A secure network access involves mutual authentication between the device and the base station or web servers. So that authenticated devices can be connected to the network to get requested services. In this regard Authentication Service Security is important due to typical attacks on mobile devices through WAN:

- DoS attacks.
- Traffic analysis
- Eavesdropping
- Man-in-the-middle attacks

2. **Security in network**: – Security measures in this regard come from

  - Wireless Application Protocol (WAP)
  - use of Virtual Private Networks (VPN)
  - MAC address filtering

CRYPTOGRAPHIC SECURITY FOR MOBILE DEVICES:

Encryption and Security on Mobile Devices:

Information security is associated with attributes they wish to preserve data, systems, or any other resources that have some value to the individual. Broadly, information security involves requirements directed to the guarantee of origin, transit and use of information, in order to ensure all steps that make up their life cycle.

The development of an application, security should not be treated as a process, but as part of the whole development. Practice safety comes down to providing confidentiality, integrity, availability and, according to some literature, authenticity and irreversibility. As you increase the number of applications in the market, there is growing concern about the vulnerability and the occurrence of malicious attacks.

It is motivating the implementation of techniques aimed at ensuring the information and the quality of services offered by applications, and help developers to incorporate such safety practices, are these: authenticity, confidentiality, integrity, availability and irrevocability. Malicious attacks the mobile devices According to a study conducted by Juniper.

Cryptographic software, intended to protect sensitive data on mobile phones, uses a digital signature algorithm, called ECDSA. This algorithm unintentionally exposes the cryptographic keys through physical side channels when used on a mobile device. The device experiences changes in its electromagnetic radiation, as well as in its power consumption, in accordance with the data it's encrypting.

This means a cyber criminal could circumvent cryptographic security for mobile devices using a non-invasive attack method to steal sensitive information by using a simple probe that measures electromagnetic radiation. An additional attack vector could be connecting an improvised adapter to the phone's USB cable. Both vectors do not require the attacker to write any code or to do anything aside from being in proximity to the device.

Researchers managed to extract signing keys successfully from OpenSSL and CoreBitcoin running on iOS devices. They have also witnessed a partial key leakage from OpenSSL running on Android and from iOS's CommonCrypto. This could potentially put users using Bitcoin wallets or even Apple Pay accounts at risk.

LDAP Security FOR HAND-HELD MOBILE COMPUTING DEVICES:

LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.

LDAP is lighter because in its initial version it did not include security features. LDAP originated at the University of Michigan and has been endorsed by at least 40 companies. Netscape includes it in its latest Communicator suite of products. Microsoft includes it as part of what it calls Active Directory in a number of products including Outlook Express. Novell's NetWare Directory Services interoperates with LDAP. Cisco also supports it in its networking products.

RAS SECURITY FOR MOBILE DEVICES:

A **remote access services** (**RAS**) is any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.

A remote access service connects a client to a host computer, known as a remote access server. The most common approach to this service is remote control of a computer by using another device which needs internet or any other network connection.

Here are the connection steps:

1. User dials into a PC at the office.
2. Then the office PC logs into a file server where the needed information is stored.
3. The remote PC takes control of the office PC's monitor and keyboard, allowing the remote user to view and manipulate information, execute commands, and exchange files.

Many computer manufacturers and large businesses' help desks use this service widely for technical troubleshooting of their customers' problems. Therefore you can find various professional first-party, third-party, open source, and freeware **remote desktop applications.** Which some of those are cross-platform across various versions of Windows, macOS, UNIX, and Linux. Remote desktop programs may include LogMeIn or TeamViewer.

To use RAS from a remote node, a RAS client program is needed, or any PPP client software. Most remote control programs work with RAS. PPP is a set of industry standard framing and authentication protocols that enable remote access.

Microsoft Remote Access Server (RAS) is the predecessor to Microsoft Routing and Remote Access Server (RRAS). RRAS is a Microsoft Windows Server feature that allows Microsoft Windows clients to remotely access a Microsoft Windows network.

MEDIA PLAYER CONTROL SECURITY:

Windows Media Player Control
Windows CE .NET

The Microsoft® Windows Media® Player control is a Microsoft ActiveX® control used by developers to add multimedia playback capabilities to Web pages or applications. It allows you to embed Windows Media content in applications such as Internet Explorer. It also provides a programming interface for rendering a variety of network streaming and non-streaming multimedia formats.

The Windows Media Player control is built on Microsoft DirectShow® technology. DirectShow is based on Component Object Model (COM) architecture, which employs components called *filters* that can be plugged in to process multimedia data. Each filter is designed to receive digital input, process the data, and pass the results on to the next filter. The filters are arranged in a configuration called a filter graph. The Windows Media Player controls use an appropriate DirectShow filter graph to parse, decode, and render the media stream. The Windows Media Player controls are implemented through the DirectShow Filter Graph Manager (FGM).

NETWORKING API SECURITY:

What is an API:

An API is a set of functions or routines that accomplish specific tasks or provide a simplified method of interacting with a software component, often allowing the automation of common processes that interact with services running on other machines.

APIs can be in the form of a library that includes specifications for routines, data structures, object classes and variables, or simply a specification of remote calls exposed to the API consumer. Some APIs are based on international standards such as POSIX (Portable Operating

System Interface), while others are made public in open source or vendor documentation. For example, Microsoft's Windows API enables developers to create software for the Windows platform.

To generate potential revenue streams and business opportunities, enterprises are increasingly making their business applications and data available through APIs. Additionally, Web 2.0 has created a surge in Web API usage, allowing users and programs to interact with the core data behind online applications. Amazon Web Services is the most prolific example, as it uses APIs to provide customers with access to its various services, such as EC2.

By making APIs publicly available, enterprises can improve partner connectivity, cloud integration and services to customers. Third parties can also develop applications that offer additional capabilities to users and help grow the awareness and use of an enterprise's services and products.

API security mistakes and How to avoid them

During development and certainly prior to release API code should be manually checked by a security expert to test whether it could be abused or misused by an attacker. Documentation is also critical. Clearly documented code allows reviewers to see exactly what the APIs should and should not do, and lets those incorporating the APIs into an application understand how to implement them correctly.

In documentation, developers should state how to call the API, what data will be returned and in what format, and what error messages can be expected. Internal records should also note who can access the API and what information will be logged to capture who, what and when resources have been accessed for audit purposes. While on the topic of access, machine IDs should supplement authentication checks where appropriate. Each API call should also be checked to ensure that the user or device has the correct permissions to view, edit or delete the requested data. Unfortunately, many developers omit secondary access control checks once a user has been authenticated.

POSSIBLE QUESTIONS

PART-B

1. Write about proliferation of mobile and wireless devices.

2. Write short notes on authentication service security.

   (i) LDAP security

   (ii). RAS security

3. Illustrate the trends in mobility.

4. Write about cryptographic security for mobile devices in service security.

5. Write about credit card frauds in mobile and wireless computing era?

6. Write about types and techniques of credit card frauds?

7. Discuss the security challenges posed by mobile devices.

8. Illustrate the trends in mobility

KARPAGAM ACADEMY OF HIGHER EDUCATION

COIMBATORE - 21

DEPARTMENT OF COMPUTER SCIENCE,CA & IT

CLASS : III B.Sc COMPUTER SCIENCE

BATCH : 2015-2018

Part -A Online Examinations **(1 mark questions)**

SUBJECT: Cyber Security **SUBJECT CODE: 15CSU603B**

S.NO	Questions	Opt1	Opt2	Opt3	Opt4	Answer
1	PII stands for-------------------------	Personally Identifiable Information	Personally Identifiable Interchange	Personally Identifiable Intermediate	None of these	Personally Identifiable Information
2	The first Palm OS virus was seen after the number of Palm OS device reached-----------------	20 million	15 million	10 million	30 million	15 million
3	Smartphone offer-----------------communication protocols	Single	Double	Multiple	None of these	Multiple
4	A ------------------------ is similar to conputer virus that targets mobile phone data or	Mobile attack	Virus attack	Trojan virus	Mobile virus	Mobile Virus
5	Mobile virus get spread through two dominant communication protocol----------------------	Bluetooth and MMS	Bluetooth only	MMS only	None of these	Bluetooth and MMS
6	Bluetooth virus can easily spread within a distance of ---------------	15-30m	20-30m	10-30m	5-30m	10-30m
7	Combination of mobile phone and phishing is-----------------------	Smishing	Vishing	Hacking Bluetooth	Mishing	Mishing
8	Mishing attacks are attempted using------------------ technology	Internet	Mobile phone	Information	none of these	Mobile phone
9	The criminal practice of using social engineering over the telephone system most facilitated by VOIP-------------------	Smishing	Vishing	Hacking Bluetooth	Smishing	Vishing

10	Mobile virus get spread through ------------------------------ dominant communication protocol-----------------------	2	3	4	5	2
11	Internet E-mail is also called -------------------------	Smishing mail	Vishing mail	Phishing mail	Mishing mail	Phishing mail
12	An open wireless technology standard used for communication over short distance is ------------------------	LAN	Bluetooth	WAN	MAN	Bluetooth
13	A criminal offense conducted by social engineering technique similar to phishing is --------------------------------	Smishing	Mishing	Hacking Bluetooth	Vishing	Smishing
14	A GUI based utility for finding discoverable and hidden bluetooth enabled device is ----------------------	BlueBugger	Bluesnarfer	BlueDiving	BlueSniff	BlueSniff
15	Exploit the vulnerability of the device and access the images,phone book,messages,personal information is---------------	BlueBugger	Bluesnarfer	BlueDiving	BlueSniff	BlueBugger
16	Testing Bluetooth penetration and attacks like BlueBugger and Bluesnarf is -----------------	BlueDiving	BlueSniff	BLueBugger	Bluesnarfer	BlueDiving
17	A tool enables to search for Bluetooth enable device and try to extract as much information as is------------------------	Bluesnarfer	BlueBugger	BlueSniff	BlueScanner	BlueScanner
18	Sending unsolicited messages over Bluetooth to Bluetooth enabled device such as mobile phone,PDA is-------------------	Car Whisperer	BlueBugging	Bluejacking	Bluesnarfing	Bluejacking
19	A piece of software that allows attackers to send audio to and receive audio from a Bluetooth-enabled cae stereo is-----	Bluejacking	Car whisperer	Bluesnarfing	BlueBugging	Car Whisperer

20	SMS is an abbrevation of ----------------------------	Speed Message Service	Short Message Service	Small Message Service	None of these	Short Message Service
21	how many types are introduced of mobile computers in 1990______________	5	3	8	9	8
22	how many types are mobility and its implications______________	4	3	8	9	4
23	distributed life cycle management security is strong issue__________	user mobility	device mobility	session mobility	service mobility	service mobility
24	service mobility other name ______________	user mobility	device mobility	session mobility	code mobility	code mobility
25	now a day's using mobile network ____________	3G	4G	2G	2G/3G	3G
26	GPS stands for ____________	global positioning system	goal positing system	game professional system	a only	global positioning system
27	the numerous attackers that can be committed in____ primary vectors	5	2	4	4	2
28	Popular types of attacks against in 3G mobile networks____________	3	4	5	7	3
29	IPS stands for	internet service provider	intranet service provider	idle service provider	a only	internet service providers
30	In 60 smart phones and its cracked in ______mobile phone game	mosquitoes	butterfly	angry bird	a only	mosquiotes
31	DoS for _______	denial of service	demo of service	detail of service	dental of service	denial of techniques
32	Ddos for ______	distributed denail of service	denail of service	distributed dos domain	a only	distributed denial of service

33	SIP stands for ______________	session initiation protocol	service identify protocol	service initation protocol	session identify protocal	session initiation protocol
34	credit card frauds using __________	m-commerce	m-banking	a and b	b only	m-banking
35	______ types and techniques of credit card frauds	3	2	5	4	2
36	traditional techniques are called _________	proper based fraud	application fraud	a and b	b only	proper
37	application divided into ____parts	2	3	5	7	2
38	Modern techniques are ____ types	7	3	2	4	2
39	credit card generators comes under the________ type of technique	modern technique	traditional technique	a and b	a only	modern technique
40	public and private internet using ____ the mobile network	inside	outside	inside/outside	b only	outside
41	what are the two components of security in mobile computing ------------ and ----------------	security of devices and security in network	devices and network	secure network and devices	none of these	security of devices and security in network
42	_______ is palm 035 is a system wide suite of cryptographic services	CPM	CGA	IP SEC	SPM	CPM
43	____________controls or deployed on some devices	cybersecurity	cryptographic security	CPM	CGA	cryptographic security
44	trust comes from the practise of _____________	remote scanning	finger scanning	port scanning	system scanning	port scanning
45	A _________ is a collection of sits that are related in some sense	domain	system	name	service	doamin
46	______ stack to see what communiation ports are unprotected by firewalls	TCP	UDP	Both a and b	none of the above	UDP
47	___________is a software protocal for enabling anyone to located in individuals	ALDAP	LADP	LDAP	RAS	LDAP
48	An _____________ server is called directory systems agent	ALDAP	LDAP	LDAP	RAS	LDAP

49	_______ transmission are typically assigned to port 21	FTP	UDP	both a and b	none o these	FTP
50	________ is misused to open new credit account, take new loan, etc	privately identified information	privately identifiable informtion	personally identified information	Personally identifiable information	Personally identifiable information
51	A _____ firewall on a packet PC are smartphone devices can be an effective productice screen	personnel	personal	a only	b only	Personal
52	Deployiong secure assess methods that implement _______ keys	strong authentication	weak authentication	medium authentication	none of these	strong authentication
53	_______ is responsible for the LAN	IT professional	IT personal	IT personnel	others	IT personnel
54	_________ is a important consideration of protecting the business sensitive data	RAS	LDAP	LADP	SAS	RAS
55	In term of cybersecurity, mobile devices are _________	random	sensitive	touch	none of these	sensitive
56	DAP means __________	directory access protocol	dictionary access protocol	device access protocol	detail access protocol	directory access protocvol
57	RAS is an important consideration for protecting the ___ sensitive data	organisation	business	personal	office	business
58	There are ______ components of security in mobile computing	1	2	3	4	2
59	CGA is internal protocol version is	IPV4	IPV6	IPV7	IPV8	IPV6
60	PKI means _______	public key infrastructure	private key infrastructure	personal key distribution	protocol key infrastructure	public key infrastructure

UNIT-IV

SYLLABUS

Mobile Devices: Security Implication for Organizations – Managing Diversity and Proliferation of Hand-Held Devices, Unconventional/ Steath 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

Mobile Devices: Security Implication for Organizations:

- Managing diversity and proliferation of Hand-Held devices
- Unconventional/ stealth storage devices
- Threat through lost and stolen devices
- Protecting data on lost devices
- Educating the laptop users

Managing diversity and proliferation of Hand-Held Devices:

- Employees aren't just bringing their mobile devices to the workplace—they're *living* on them
- As smart phones and tablets become constant companions, cyber attackers are using every avenue available to break into them.
- With the right (inexpensive) equipment, hackers can gain access to a nearby mobile device in less than 30 seconds and either mirror the device and see everything on it, or install malware that will enable them to siphon data from it at their leisure.
- Analysts predict that by 2018, 25 percent of corporate data will completely bypass perimeter security and flow directly from mobile devices to the cloud.
- Chief information security officers (CISOs) and other security executives are finding that the proliferation of mobile devices and cloud services are their biggest barriers to effective breach response.
- In order to secure the corporate data passing through or residing on mobile devices, it is imperative to fully understand the issues they present.

5 Security Risks and a Surprising Challenge:

1. Physical access
2. Malicious Code
3. Device Attacks
4. Communication Interception
5. Insider Threats

Physical access:

- Mobile devices are small, easily portable and extremely lightweight.
- hence easy to steal or leave behind in airports, airplanes or taxicabs.
- As with more traditional devices, physical access to a mobile device equals "game over."
- The cleverest intrusion-detection system and best anti-virus software are useless against a malicious person with physical access.
- Circumventing a password or lock is a trivial task for a seasoned attacker, and even encrypted data can be accessed.
- This may include not only corporate data found in the device, but also passwords residing in places like the iPhone Keychain, which could grant access to corporate services such as email and virtual private network (VPN).

Malicious Code:

- Mobile malware threats are typically socially engineered and focus on tricking the user into accepting what the hacker is selling.
- The most prolific include spam, weaponries links on social networking sites and rogue applications.
- Android devices are the biggest targets, as they are widely used and easy to develop software for.
- Mobile malware Trojans designed to steal data can operate over either the mobile phone network or any connected Wi-Fi network.
- They are often sent via SMS (text message); once the user clicks on a link in the message, the Trojan is delivered by way of an application, where it is then free to spread to other devices.
- When these applications transmit their information over mobile phone networks, they present a large information gap that is difficult to overcome in a corporate environment.

Device Attacks:

- Attacks targeted at the device itself are similar to the PC attacks of the past.
- Browser-based attacks, buffer overflow exploitations and other attacks are possible.
- The short message service (SMS) and multimedia message service (MMS) offered on mobile devices afford additional avenues to hackers.
- Device attacks are typically designed to either gain control of the device and access data, or to attempt a distributed denial of service (DDoS).

Communication Interception:

- Wi-Fi-enabled smartphones are susceptible to the same attacks that affect other Wi-Fi-capable devices.

- The technology to hack into wireless networks is readily available, and much of it is accessible online, making Wi-Fi hacking and man-in-the-middle (MITM) attacks easy to perform.
- Cellular data transmission can also be intercepted and decrypted.
- Hackers can exploit weaknesses in these Wi-Fi and cellular data protocols to eavesdrop on data transmission, or to hijack users' sessions for online services, including web-based email.
- For companies with workers who use free Wi-Fi hot spot services, the stakes are high.
- While losing a personal social networking login may be inconvenient, people logging on to enterprise systems may be giving hackers access to an entire corporate database.
-

Insider Threats:

- Mobile devices can also facilitate threats from employees and other insiders.
- Malicious insiders can use a smartphone to misuse or misappropriate data by downloading large amounts of corporate information to the device's secure digital (SD) flash memory card, or by using the device to transmit data via email services to external accounts.
- The downloading of applications can also lead to unintentional threats.
- The misuse of personal cloud services through mobile applications is another issue; when used to convey enterprise data, these applications can lead to data leaks that the organization remains entirely unaware of.
- Many device users remain unaware of threats, and the devices themselves tend to lack basic tools that are readily available for other platforms, such as anti-virus, anti-spam, and endpoint firewalls.

Policy making efforts:

- Organization needs to establish security practice subject to legal and external constraints
- Policy making effort starts with the commitment of CEO, president or Director who takes cyber security seriously
- Mobile devices of the employees should be registered in the corporate asset register
- Close monitoring of these devices
- Physical access to corporate resources must be removed from mobile devices before the employee leaves
- Employees register their device with the IT department: to control the access

Unconventional/ Stealth Storage devices:

- Secondary storage devices
  - CDs
  - USBs
  - Portable external hard disks
  - Portable storage devices can be easily lost or stolen.

- Decrease in size and emerge in new shape and sizes – difficult to detect
- Prime challenge for organizational security
- Firewalls and antivirus software are no defense against the open USB ports
- Remedy- block these ports, but Windows OS do not support
- Disgruntled employee can use these to download confidential data or upload harmful virus.

Device lock software:

- Device Lock provides network administrators the ability to set and enforce contextual policies for how, when, where to, and by whom data can or can't be moved to or from company laptops or desktop PCs via devices like phones, digital cameras, USB sticks, CD/DVD-R, tablets, printers or MP3 players.
- In addition, policies can be set and enforced for copy operations via the Windows Clipboard, as well as screenshot operations on the endpoint computer.

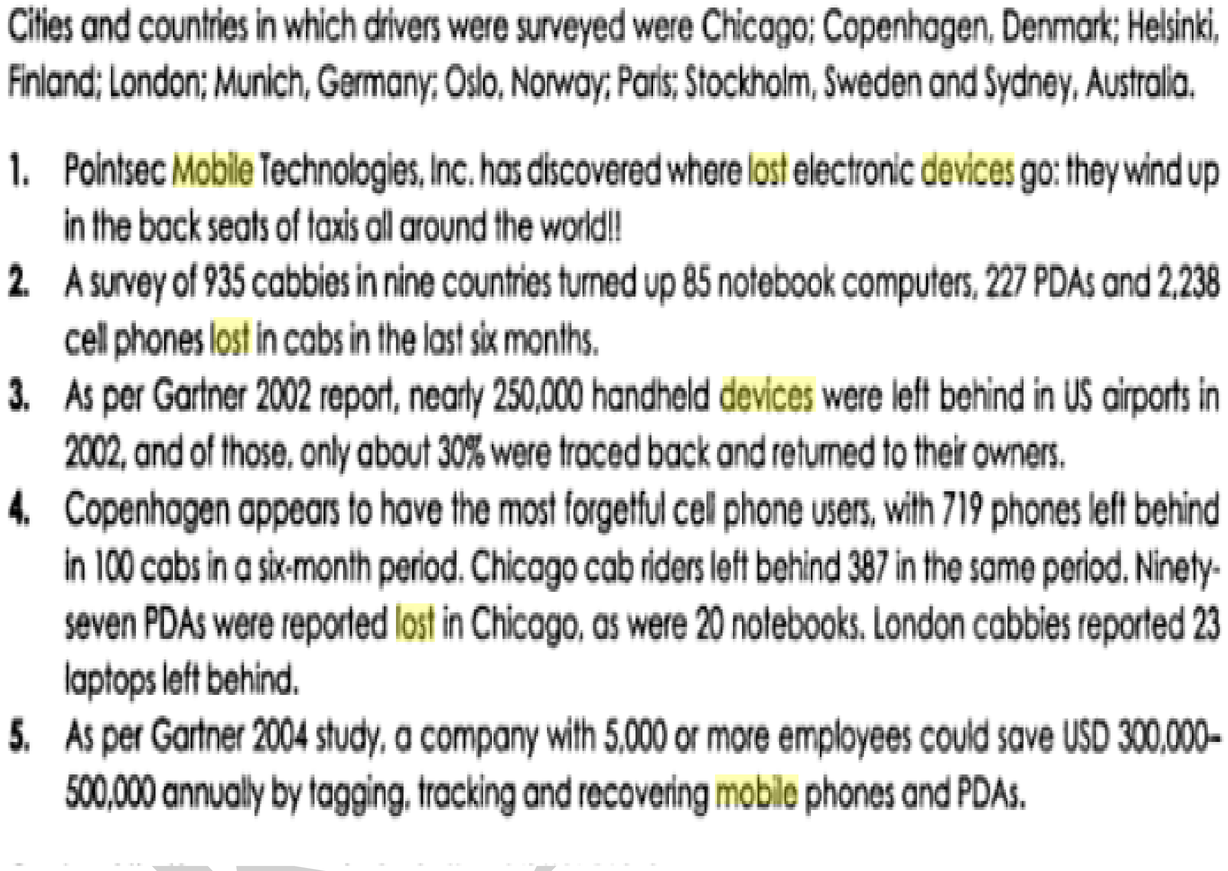
Stealth storage devices:

A computer storage device is any type of hardware that stores data. The most common type of storage device, which nearly all computers have, is a hard drive. The computer's primary hard drive stores the operating system, applications, and files and folders for users of the computer.

While the hard drive is the most ubiquitous of all storage devices, several other types are common as well. Flash memory devices, such as USB keychain drives and iPod nanos are popular ways to store data in a small, mobile format. Other types of flash memory, such as compact flash and SD cards are popular ways to store images taken by digital cameras.

External hard drives that connect via Firewire and USB are also common. These types of drives are often used for backing up internal hard drives, storing video or photo libraries, or for simply adding extra storage. Finally, tape drives, which use reels of tape to store data, are another type of storage device and are typically used for backing up data.

Threats through lost and stolen devices:



Cities and countries in which drivers were surveyed were Chicago; Copenhagen, Denmark; Helsinki, Finland; London; Munich, Germany; Oslo, Norway; Paris; Stockholm, Sweden and Sydney, Australia.

1. Pointsec Mobile Technologies, Inc. has discovered where lost electronic devices go: they wind up in the back seats of taxis all around the world!!
2. A survey of 935 cabbies in nine countries turned up 85 notebook computers, 227 PDAs and 2,238 cell phones lost in cabs in the last six months.
3. As per Gartner 2002 report, nearly 250,000 handheld devices were left behind in US airports in 2002, and of those, only about 30% were traced back and returned to their owners.
4. Copenhagen appears to have the most forgetful cell phone users, with 719 phones left behind in 100 cabs in a six-month period. Chicago cab riders left behind 387 in the same period. Ninety-seven PDAs were reported lost in Chicago, as were 20 notebooks. London cabbies reported 23 laptops left behind.
5. As per Gartner 2004 study, a company with 5,000 or more employees could save USD 300,000–500,000 annually by tagging, tracking and recovering mobile phones and PDAs.

Protecting data on lost devices:

- Encrypting sensitive data
- Encrypting entire file system
- Encrypting servers: third party solutions
- Create a database action to delete the entire data on the user's device

Educating the Laptop users:

As instructors, we may wonder if laptop use helps or hinders learning in our classrooms. We may find ourselves on the fence—understanding that some students prefer to type their notes, but then wondering whether students are paying attention and staying engaged, and whether their laptop use may be distracting others.

Two classroom-based studies suggest that students' use of laptops can have a positive effect on their attention and learning—*if* these tools are used for course-related, instructional purposes. In contrast, one of the two studies found a negative correlation between use of laptops in class and course grade when laptop use was not yoked to course-related purposes. Moreover, when in-class laptop-use was not a required part of the class, the students in these studies reported lower levels of engagement and learning.

While these results suggest some good news, they also suggest that laptop use in class significantly increases distractions for students, which can diminish attention and learning. The studies found that students often find the presence of these devices to be distracting—whether because having the devices in class makes it more likely that students will engage in activities such as texting or online social networking, or because students find themselves distracted by their peers' use of devices to type, text, play games, or surf the internet.

POSSIBLE QUESTIONS

PART-B

1. Explain about managing diversity and proliferation of Hand-Held devices?
2. Explain in mobile devices:
   (i) Unconventional/stealth storage devices.

   (ii) Threats thru lost and stolen devices
3. Discuss about organizational measures for handling mobile devices.
4. Explain in mobile devices:
   (i) Protecting data on lost devices

   (ii) Educating the laptop users

KARPAGAM ACADEMY OF HIGHER EDUCATION
COIMBATORE - 21
DEPARTMENT OF COMPUTER SCIENCE,CA & IT
CLASS : III B.Sc COMPUTER SCIENCE
BATCH : 2015-2018

Part -A Online Examinations (1 mark questions)

SUBJECT: Cyber Security SUBJECT CODE: 15CSU603B

S.NO	QUESTIONS	OPT1	OPT2	OPT3	OPT4	ANSWER
1	The first step in securing mobile device is creating ___________ that address the unique issues.	company policies	standards	platform	onlyb	company policies
2	The employees who use mobile devices more than ____________of the time will have different requirements than less frequent users.	20%	30%	50%	10%	20%
3	The owner of the laptops has a _________device that communicates wih laptops alarm device.	clockring	key ring	a only	a and b only	key ring

4	________cards that act as a motion detector,an alarm and also have the capability to lockdown the laptop.	PCMCIA	only b	PSVIA	only a	PCMCIA
5	Warning labels contain tracking __________and __________details can be fixed onto the laptops to deter aspiring thieves	information,identifictaion	batteries,number	identity,cards	locks,system	information,identification
6	Companies may new to the mobiledevices may adopt an _____________mobile policy	device	data sycing	umbrella	system	umbrella
7	As the price of the computing technology is steadily ___________useage of devices such as laptps is becoming more common	decreasing	increasing	moderate	simple	decreasing
8	The theft of laptops have been always major issue,according to the _________________________and ____________________	cybersecurity and inusrance company statistics	cybercafe and cyber fraud	only b	only a	cybersecurity and inusrance company statistics

9	The ideal solution to safe guard any mobile devices is securing with ______________	locks and memory	only b	cards and locks	only c	cards and locks
10	The labels cannot be removed easily and are__________solution to a laptop.	low-cost	high cost	moderate cost	rich cost	low-cost
11	PCMCIA also secures the ____________and ____________ to prevent access to the os.	encryption keys and integrity	password and encryption keys	availability and encryption keys	authenticity and passwords	availability and encryption keys
12	PCMCIA have ________________that keep them powered on when the system is shut down.	batteries	wireless connectivity	remote sensor	alarm set up	batteries
13	the survey asked the participants about the likelihood of _____seperate scenarios for the use of cell phone s to communicate sensitive.	8	10	6	4	6

14	________and __________ should clearly define what sort of data may bestored on the mobile devices.	information classification and handling	only a	system passwords and policies	only a and c	information classification and handling policy
15	most laptops conatin personal and corporate information that could be _____________	available	sensitive	hidden	authenticity and passwords	sensitive
16	The labels have an identification number that is stored in a ________database for verification	universal	national	international	country	universal
17	when control cannot be implemented to protect the date in the even they are _________	over ridden	copied	stolen	theft	stolen
18	one should give a deep thought about the _______________ for a public company	potential legal troubles	troubles and policies	sytem theft and troubles	virus legal and troubles	potential legal troubles

19	The importanc eof security policies is related to ______________	mobile computing devices	wireless connectivity	company policies	authenticity and passwords	mobile computing devices
20	______to information system through usage of mobile device	organisation	mobile	threats	security	threats
21	Cyber Security is always a ___________________	primary concern	threat reduction	mobile device	both a and b	primary concern
22	_________ is a sowtware solution one can have control over unauthorized access to plug and play device	system lock	device lock	application lock	only b	only b
23	Mobile hand-held device are provided by the __________________________	users	organistion	employee	none of these	organization

24	Data that are stored on hard disk in_________________________________	persistent memory	device memory	both a and b	removable memory	both a and b
25	Mobile phones and media players used by ________________________________	organstions	users	employee	none of these	organizations
26	Gen-Y also called to as ________________________________	young workers	younger work	young work	none of these	a only
27	Old worker Sometime __________________________________ the Younger worker to progrees	spoiled	congradulate	none of these	only a	only a
28	Hand Helds were________________________	expensive	specialized	none of these	both a and b	both a and b

29	________european business laptop users such as spyware and viruses	600	200	400	500	500
30	____________________ is used to discribe the technologies in contract to the simple encryption	multi dimensional space rotation	strong encryption	encryption standards	only b	only b
31	Security policies relating to____________________	cyber	organistional	mobile	users	mobile
32	SSN____________________	social security numbers	social secret number	only b	none of these	social security numbers
33	_________________________are targetting laptops thet are expensive to enable them to fetch a quick profit	cyber criminals	theft	hackers	none of these	cybercriminals

34	PCMCIA______________________ ______	personal computer memory card industry	personal compute memory card inadustry	only b	only a	only a
35	__________________can be used to carry and safeguard laptops	laptop sales	cables	motion sensor and alarms	hard disk	motion sensor and alarms
36	__________________cantaining tracking information and identification details	motion sensors	warning cables	stamps	both b and c	both b and c
37	___________________are annoying owing their false alarms and sound level in security lap	motion sensors	alarms	laptop safes	cables	motion sensor and alarms
38	MSDR _________________________	multi dimensional space rotation	multi data space rotation	multi dimensional spam rotation	multi driven space rotation	multi dimensional space rotation

39	CRM ________________________	customer relationship management	consumer relationship management	coherent relationship management	only b	customer relationship management
40	IT department can have the server send a ____________to destroy privileged data on the device	device	security	mechanism	policy	device
41	CRM Means ______________	Customer Relation Management	Customer Relationship Management	Customer Reading Management	Customer Requirement Message	customer relationship management
42	Database file encryption techniligy using either the ______ or _____ algorithm	AES or DES	DES or MDSR	AES or MDSR	DES or RSA	AES or MDSR
43	Strong encryption means that it is much ______________	Harder to break	Harder to stop	Harder to continue	Harder to device	Harder to break

44	USB Means	Universal system Bus	Unit security Bus	Universal Serial Bit	Universal serial Bus	Universal serial Bus
45	The cybersecurity threat under this _______________	Viruses	Scenario is seary	worms	Trojans	Scenario is seary
46	cybersecurity is always a ________________ concern	key	security	Primary	Secondary	Primary
47	NIST Means ________________	National Institute of studies & Technology	National Institute of Standards &	National Information of students &	National Information of studies &	National Institute of Standards & Technology
48	_______ lawyer asks for proprietary and confidential information using his cellphone	Internal	External	Physical	Network	External

49	USB drives another names called ____________________	Zip drive	Memory disk	Memory sticks	A & B	A & B
50	Proteching data types are _________	4	2	1	3	2
51	Proteching data types are _________	129	127	128	130	128
52	Data protection especially whwn it resides on a _________ device	Mobile hand-held device	hand-held device	USB hand-held device	Network hand-held device	Mobile hand-held device
53	SSNs Means ________________	Social Security Nodes	System Security Numbers	System Security Node	Social Security Numbers	Social Security Numbers

54	which users or groups can access USB ports ___________________	Wifi &Bluetooth adapters	Wifi & Datacable	Wifi & Pendrive	Wifi & USB	Wifi &Bluetooth adapters
55	Cybercriminals are why targeting laptops ________________	Quick Profit in White Market	Quick Profit in Black Money	Quick Profit in White Money	Quick Profit in Black Market	Quick Profit in Black Market
56	____________ softwaer is control over unauthorized access to plug nd play devices	DeviceLock	Device Security	Antivirus	Firewall	DeviceLock
57	Data that are stored on hard disks in _____________Memory	Package	Hard ware	DataBase	Persistent	Persistent
58	Proteching data two types are _________	Encrypting sensitive data & Encrypting the entire	Decrypting sensitive data & Decryptin	Encrypting sensitive data & Decryptin	Decrypting sensitive data & Encrypti	Encrypting sensitive data & Encrypting the entire file system

59	MDSR Means	Multi-Dimensional Space Rotation	Multi-Diamand Space Rotation	Multi-Dimensional space Right	Multi-dimensional system Rotaion	Multi-Dimensional Space Rotation
60	Greater security there is an option available that instructs the __________ server to disply a dialogbox	Database	Datastore	DataSystem	DataConection	Database

UNIT-V

SYLLABUS

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.

Organizational Measures for Handling Mobile

Devices Related Security Issues:

Encrypting Organization Databases:

Organizations take a lot of steps to protect their confidential data. Almost all security measures including encryption are considered only while transferring information on the wire not while storing it in the database. More often than not, it is stored as clear text in the database. In this article we see how database encryption can enhance the security of our data.

The need to encrypt

These days information security has become essential for all organizations. Organizations take a lot of steps to protect their confidential data. Almost all security measures including encryption are considered while transferring information on the wire. More often than not, it is stored as clear text in the database. Databases may contain a lot of sensitive data; loss of which can cause great damage to any organization. Also, database is the place where data resides most of the time. Hence, database encryption needs to be given high priority.

Defense in depth

Organizations feel that they have more than enough access control mechanisms in place making it almost impossible for attackers to reach to the database. In reality these controls make it difficult for the attacker to reach the database but not impossible. Another important point that they overlook is, even if the attacker is not able to break through, the database administrator has access to all the clear text data stored. This definitely harms the confidentiality of information. If data is encrypted, we are safeguarding it against administrators and attackers who are able to break the access controls & get into the database. Thus, encrypting critical data residing in database will add one more layer to an organization’s IT security. It is always better to store data in some not-easily-guessable format.

The issues involved in encryption

1. **Encrypting whole DB Vs Specific Columns**: Encrypting the whole database may not be a good solution. Consider indexed fields getting encrypted in this process. The database software will sort the indexed fields in the order that will not match the real un-encrypted form. Also, it will defeat the purpose of speeding up the access by preordering it.

   Consider one more scenario when you are searching a particular row in a table which is full encrypted. Suppose, the table has three columns Employee ‘ID’, ‘Name’ and ‘Salary’. Now if we search by ‘Name’, each time a row is fetched, the name needs to be decrypted first and then compared to the input. The overhead of decryption is considerable when the table is having thousands of rows. Moreover, there is actually no need to encrypt employee name and hide it from others. Instead, encrypting only the ‘Salary’ column will not cause any performance overhead and still will protect the employee salary information.

2. **Where to handle decryption, client side or server side**: A better place to handle decryption is the client side, because even when the data is transmitted on the network, it will be transferred encrypted and anybody sniffing on the network will not be able to break it easily.

   For this, client applications should be capable enough and the existing ones may need to be modified. This may not always be realistic. This approach can be used for applications in the development phase. For existing applications, it may better to encrypt at server and use techniques like SSL for transferring it on the network.
3. **Securing Encryption Keys**: The next important issue is protecting the encryption keys. One simple solution is to store all the keys in one flat file and let the related applications pick those up from the file. Apply NTFS permissions on this file and restrict access to needed applications only. One disadvantage of this approach is, if the administrator account is compromised, then the attacker will have easy access to the keys.

Second approach is to store all the keys encrypted in a table in the database itself. Oracle database provides this facility. It decrypts the keys for authenticated users and returns it back. These decrypted keys can then be used to decrypt the actual data.

4. **Extra Disk space and CPU cycles required**: Encrypted data will be much more voluminous than the normal one. A 4 byte integer might become a 16 byte long character sequence. Thus, while using encryption, the required disk space and logical memory capacity needs to be ensured. Also, the extra CPU cycles consumed during the process of encryption/decryption should be considered.

Pros and Cons of DB Encryption

Encrypting the data in a database may not be a very good option if we look at the following considerations-

1. Performance parameters
2. Disk space requirements
3. Application level development complexities
4. Extra CPU cycles required to encrypt/decrypt data

On the other hand, if we consider the following parameters, we may be persuaded to go for database encryption

1. Confidentiality of data
2. The security risks the data is exposed to
3. The damage that can be done to the organization

Some DB encryption tools

1. Ingrian Networks, DataSecure Platforms.
2. Application Security, DbEncrypt.
3. Ncipher, CipherTools.

Including Mobile Devices in Security Strategy:

With a security strategy that includes device discovery and impact assessment, you can protect your corporate network from some mobile device dangers.

Wi-Fi-enabled consumer electronics have triggered an explosion in the number of devices connecting to the corporate network and requiring some kind of mobile device security strategy. A recent Cisco IBSG Horizons survey (PDF) found that the average number of devices per knowledge worker will jump from 2.2 in 2012 to 3.3 by 2014, increasing IT spending on mobility initiatives to 20% by 2014.

Laptops, smart phones and tablets have a direct effect on the total cost of ownership of the corporate network. WLAN infrastructure must be added to satisfy growing bandwidth demands. Security systems must spot and block non-business traffic, such as streaming video and back channels for Trojan horses.

Bring your own device (BYOD) policies should include Quality-of-Service mechanisms to ensure performance. IT must create diagnostic tools and mobile management processes to deal with diverse and often cranky consumer devices.

Furthermore, every new employee-owned device represents an opportunity to leak corporate data. BYOD challenges include lost or stolen devices with data that cannot be remotely wiped, malware infections, and sensitive data that's too easily forwarded outside the workplace.

To avoid these pitfalls, businesses must implement BYOD safeguards and monitor mobile device usage to detect -- and preferably prevent -- such leaks.

Organizational Security Policies and Measures in mobile Computing Era:

Importance of Security polices relating to mobile Computing Devices:

Mobile security policies are important for maintaining the health of a quality mobile corporate environment.

A mobile device security policy should define which types of the organization's resources may be accessed via mobile devices, which types of mobile devices are permitted to access the organization's resources, the degree of access that various classes of mobile devices may have—for example, organization-issued devices versus personally-owned (bring your own device) devices—and how provisioning should be handled.

It should also cover how the organization's centralized mobile device management servers are administered, how policies in those servers are updated, and all other requirements for mobile device management technologies. The mobile device security policy should be documented in the system security plan. To the extent feasible and appropriate, the mobile device security policy should be consistent with and complement security policy for non-mobile systems.

Operating Guidelines for Implementing Mobile Devices Security Polices:

Most organizations do not need all of the possible security services provided by mobile device solutions. Categories of services to be considered include the following:

General policy: enforcing enterprise security policies on the mobile device, such as restricting< access to hardware and software, managing wireless network interfaces, and automatically monitoring, detecting, and reporting when policy violations occur. **Data communication and storage**: supporting strongly encrypted data communications and data< storage, wiping the device before reissuing it, and remotely wiping the device if it is lost or stolen and is at risk of having its data recovered by an untrusted party.

User and device authentication: requiring device authentication and/or other authentication< before accessing organization resources, resetting forgotten passwords remotely, automatically locking idle devices, and remotely locking devices suspected of being left unlocked in an unsecured location**.**

Applications: restricting which app stores may be used and which applications may be installed,< restricting the permissions assigned to each application, installing and updating applications, restricting the use of synchronization services, verifying digital signatures on applications, and distributing the organization's applications from a dedicated mobile application store.

Organizations should implement the following guidelines to improve the security of their mobile devices.

Organizations should have a mobile device security policy.

A mobile device security policy should define which types of the organization's resources may be accessed via mobile devices, which types of mobile devices are permitted to access the organization’s resources, the degree of access that various classes of mobile devices may have—for example, organization-issued devices versus personally-owned (bring your own device) devices—and how provisioning should be handled. It should also cover how the organization's centralized mobile device management servers are administered, how policies in those servers are updated, and all other requirements for mobile device management technologies. The mobile device security policy should be documented in the system security plan. To the extent feasible and appropriate, the mobile device security policy should be consistent with and complement security policy for non-mobile systems.

Organizations should develop system threat models for mobile devices and the resources that are accessed through the mobile devices.

Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other client devices (for example, desktop and laptop devices only used within the organization’s facilities and on the organization’s networks). Before designing and deploying mobile device solutions, organizations should develop system threat models.

Threat modeling helps organizations to identify security requirements and to design the mobile device solution to incorporate the controls needed to meet the security requirements. Threat modeling involves identifying resources of interest and the feasible threats, vulnerabilities, and security controls related to these resources, then quantifying the likelihood of successful attacks and their impacts, and finally analyzing this information to determine where security controls need to be improved or added.

Organizations should implement and test a pilot of their mobile device solution before putting the solution into production.

Aspects of the solution that should be evaluated for each type of mobile device include connectivity, protection, authentication, application functionality, solution management, logging, and performance. Another important consideration is the security of the mobile device implementation itself; at a minimum, all components should be updated with the latest patches and configured following sound security practices. Also, use of jail broken or rooted mobile devices should be automatically detected when feasible. Finally, implementers should ensure that the mobile device solution does not unexpectedly “fall back” to default settings for interoperability or other reasons.

Organizations should fully secure each organization-issued mobile device before allowing a user to access it.

This ensures a basic level of trust in the device before it is exposed to threats. For any already-deployed organization-issued mobile device with an unknown security profile (e.g., unmanaged device), organizations should fully secure them to a known good state (for example, through deployment and use of enterprise mobile device management technologies). Supplemental security controls should be deployed as risk merits, such as antivirus software and data loss prevention (DLP) technologies.

Organizations should regularly maintain mobile device security.

Helpful operational processes for maintenance include checking for upgrades and patches, and acquiring, testing, and deploying them; ensuring that each mobile device infrastructure component has its clock synced to a common time source; reconfiguring access control features as needed; and detecting and documenting anomalies within the mobile device infrastructure, including unauthorized configuration changes to mobile devices.

Other helpful maintenance processes are keeping an active inventory of each mobile device, its user, and its applications; revoking access to or deleting an application that has already been installed but has subsequently been assessed as too risky to use; and scrubbing sensitive data from mobile devices before reissuing them to other users. Also, organizations should periodically perform assessments to confirm that their mobile device policies, processes, and procedures are being followed properly. Assessment activities may be passive, such as reviewing logs, or active, such as performing vulnerability scans and penetration testing.

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

Mobile Security for BYOD Settings

With so many people using mobile devices, including more and more employees working remotely, the need for enhanced mobile security has never been greater. Additionally, the growth of enterprise mobility solutions is slowly reducing the need for traditional office settings. Companies are also implementing bring your own device or BYOD programs and even moving to mobile-first environments. In fact, the majority of IT decision makers support BYOD and mobility programs. However, as the number of mobile devices connected to both enterprise and public networks increases, companies need to be acutely aware of mobile security, including these important aspects:

1. **Mobile Device Management**. Because it’s so difficult to accurately monitor how employees use their mobile devices, especially personally owned devices, mobile device management is vital to maintain your organization’s mobile security. This can be easier said than done since it could violate employees’ privacy rights. However, there are several viable systems and applications that can help improve enterprise mobile security and offer effective mobile management and support.

2. **Mobile Application Management**. While the ever-increasing access to mobile apps is great, when you operate in a BYOD environment, managing those apps can be a serious security issue for your organization. This makes robust mobile application management (MAM) more important than ever.

   Essentially, MAM is the delivery and administration of enterprise software to the end users' personal and corporate mobile devices. Implementing effective MAM not only helps with software delivery and application life cycle management, but it also tracks usage. Furthermore, many MAMs can also match mobile devices and their owners to specific IT policies and better control how company data is shared via mobile applications.

3. **Antivirus for Devices**. In addition to mobile device and app management, it's imperative that companies and organizations implement the appropriate level of antivirus protection. Hackers and malware are a constant threat. This means any employee using the Internet on a personal mobile device must install and update to the latest antivirus and anti-malware software properly to ensure device security is maintained.

4. **Encryption**. An important part of any organization's security plan needs to include encryption, which is the process of converting information or data into a secure code to prevent unauthorized access. Companies should also encrypt mobile device network communication while at work to prevent outside snooping. There are various steps you can take to implement proper encryption, including requiring all mobile devices to use approved encryption protocol before access is granted to corporate email accounts and files.

Additional Mobile Device Security

To help you improve your company's mobile device security even more, here are some additional important measures to consider.

1. **Create a Mobility Policy.** Every company should create and enforce a mobility policy. This policy will be different for each company, but should include some primary guiding principles, align with your company culture and provide flexibility without compromising security.

2. **Be Transparent with Employees.** As with any company policy, employees appreciate transparency. Your mobile security policy should be open and clear, without hidden features and rules. Let your employees know up front what they can and cannot do with their devices, whether it's company or personally owned. A clear policy will also help eliminate confusion and enhance the effectiveness of your company's security policy.

3. **Mixing Personal and Professional Use.** When your employees use their own personal devices for business, it’s imperative that your mobile security policies are clear and flexible. More importantly, it must protect your company’s and customers’ private information. Therefore, you must create a proper balance between your employees’, company’s and customers’ security and privacy.

Secure Your Mobility

In this evolving world of mobile computing and communication, maintaining proper mobile security is vital for any company or organization to succeed and ultimately thrive. Want to learn more about our mobile security solutions? Please contact New Era Tech for more information and discover how we can help manage and protect your BYOD environment from hackers and other security threats.

Laptops:

A **laptop**, often called a **notebook** or "notebook computer", is a small, portable personal computer with a "clamshell" form factor, an alphanumeric on the lower part of the "clamshell" and a thin LCD or LED computer screen on the upper part, which is opened up to use the computer. Laptops are folded shut for transportation, and thus are suitable for mobile use. Although originally there was a distinction between laptops and notebooks, the former being bigger and heavier than the latter, as of 2014, there is often no longer any difference. Laptops are commonly used in a variety of settings, such as at work, in education, in playing games, Internet surfing, for personal multimedia and general home computer use.

Physical Security Countermeasures:

Physical Security for Laptop Computers

- Never leave your laptop in a public place. If you take your laptop into libraries or classrooms, do not leave it alone, even just "for a minute" while you go to the restroom or talk with a friend. Thieves look for such opportunities. If you do leave your laptop in a public place, lock it up with a notebook lock (such as those made by Kensington and Belkin), there are even options for devices without security slots, but they can be bulky, Searching Amazon for "adhesive laptop security plate" will provide you with a few options.

- Always lock your door, even if you are just heading to the bathroom. Arrange this with your suitemates as well. If you leave your door open, you are providing thieves easy access to steal your belongings.

- Never leave your laptop unattended, even for a moment, even in your office or dorm room. Most laptops are stolen from their owner's *office*, while the owner is on a quick break or at a meeting.

- If you must leave your laptop in a car, stow your bag in the trunk before you reach your destination so potential thieves don't see you. Make sure your car is locked.

- Avoid setting your laptop on the floor Putting your laptop on the floor is an easy way to forget or lose track of it. If you have to set it down, try to place it between your feet or against your leg (so you're always aware it's there).

- Use a low-key shoulder bag, briefcase, or backpack for your laptop. Avoid expensive bags that scream, "Laptop inside!"

- If you are going out for coffee or lunch, lock your gear in a desk or an office that can be locked. Or, at least purchase and use a laptop cable lock.

- All laptops should be set to require a password to log on to the computer. Never leave access numbers or passwords in your carrying case.

- Configure your screen saver to require a password.

- Never allow your web browser to automatically supply a password for you. If you do, it means that anyone at your computer can access that site under your account.

- Enroll your computer in the STOP Program. This program attaches serialized security plates to laptop computers for a small charge ($25 for three years). With this prominent plate, your computer is less desirable to thieves. You can enroll your computer in the STOP program by visiting the Yale Security Office at Phelps Gate.

- Purchase CompuTrace for your computer. If your computer is stolent, CompuTrace will alert the proper authorities to retrieve your computer. The computer bundles that we have configured for you come with CompuTrace already activated.

Physical restraints and locks

Physical locks are the best means to prevent your laptop from being stolen. Most stolen laptops are grabbed and gone before their owners know what happened. Laptop thieves look for quick easy hits, and will not risk the delay or commotion of trying to break a lock.

Computer supplies, software and equipment can be purchased online viaSciQuest.

Protecting the privacy and security of your data and identity

If you ever store Yale confidential 2-Lock data on your laptop or other mobile computing device, you should use file or whole disk encryption techniques to keep the data secure and private in case the laptop is lost or stolen.

Use a screen guard. These guards help prevent people from peeking over your shoulder as you work on sensitive information in a public place. This is especially helpful when you're traveling or need to work in a crowded area.

POSSIBLE QUESTIONS

PART-B

1. Describe devices – related security issues?
2. Discuss about organizational policies for the use of mobile Hand-Held devices.
3. Discuss about importance of security policies related to mobile computing devices.
4. Illustrate laptops in detail?
5. What are the Operating Guidelines for Implementing Mobile Devices Security Polices

KARPAGAM ACADEMY OF HIGHER EDUCATION
COIMBATORE - 21

DEPARTMENT OF COMPUTER SCIENCE,CA & IT

CLASS : III B.Sc COMPUTER SCIENCE

BATCH : 2015-2018

Part -A Online Examinations **(1 mark questions)**

SUBJECT: Cyber Security **SUBJECT CODE: 15CSU603B**

S.NO	Questions	Opt1	Opt2	Opt3	Opt4	Answer
1	Expand OFDM _________________.	Origin frequency division multiplexing	Original frequent divide multiplex	Orthogonal frequency division multiplexing	Orthogonal frequent divide multiplexing.	Orthogonal frequency division multiplexing
2	Expand MIMO ____________________.	Multiple input Multiple output	Multiple interact multiple origin	More input more output	Multiple interact more output	Multiple input Multiple output
3	_________changes the settings of existing firmware that helps an attacker to engage in malicious configuration of firmware settings.	WAPjacking	WAPkitting	WARjacking	WARkitting	WAPjacking
4	__________the attacker injects the frame whose content is carefully spoofed and which are valid as per 802.11 specification.	MAC address spoofing	IPspoofing	Frame spoofing	email spoofing	Frame spoofing
5	The "strack –smashing protector " is also known as	Libsafe	propolice	stackguard	all the three	Propolice
6	__________ is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.	blind injection	SQL injection	piggy backed quer	both (a) and (b)	SQL injection
7	Which one is a packet flooding attack and the client controls the size of the flooding packets and the duration of the attack.	Trinoo	Tribe flood	MStream	Shaft	Shaft
8	A _____attack damages a system so badly that it requires replacement and reinstallation of hardware.	DDoS	PDoS	DoS	EDoS	PDoS

9	Which attack can crash various OS due to bug in their TCP/IP fragmentation reassembly code.	SYN attack	Teardrop	Nuke	Flood attack	Teardrop
10	__________is mainly used by networked computers OS to send error messages indicating datagrams to the victims.	Flood attack	Smurf attack	Ping of death atta	Nuke	Ping of death attack
11	________is a harmful program in which malicious or harmful code is contained inside apparently harmless programming or data.	Backdoors	Trojan horse	Trojan war	SAP doors	Trojan horse
12	The most popular online attack is a man in the middle (MITM) attack also termed as ______.	Bucket brigade attack	Janus attack	Non electronic attack	Both (a) and (b)	Both (a) and (b)
13	__________is a process of recovering passwords from data that have been stored in or transmitted by a computer system.	Strong passwor	Random passw	Password crackin	Weak password	Strong password
14	__________ is a computer on a network which acts as an intermediary for connections with other computers on that network.	Anonymizers	Proxy servers	Network probe	E-crime	Proxy servers
15	_______ is the simple process of intercepting wireless data that is being broadcasted on an unsecured network.	Spoofing	DoS	MITM attack.	Sniffing	Sniffing
16	___________ is the unique identifier of each code of th	MAC	NIC	WAP	WAP2	MAC
17	Warwalking is also known as _______.	Warbiking	Warjagging	Warkitting	Warjacking	Warjagging
18	______ is an old DoS attack against computer networks consisting of fragmented or otherwise invalid ICMP packets sent to the target.	Flood attack	Ping of death at	SYN attack	Nuke	Nuke
19	_____is the art and science of detecting of messages that are hidden in images, audio/video files using stenography.	Steganalysis	Stegnology	Stenography	Stegnometer	Steganalysis
20	A ______ is a means of access to a computer program that bypasses security mechanisms.	Trojan horse	Backdoors	Back orifice	SAP backdoors	Backdoors
21	Computer viruses can be categorized into ________	5	6	7	8	7
22	________is a tool that can detect the keylogger installed on the computer system and also can remove the tool.	Spywares	Hardware keylo	Antikeylogger	Keylogger	Antikeylogger

23	Stegnography in digital media is very similar to __	Watermarking	Digital waterma	Redundant bits	Trademark	Digital watermarking
24	Morris worm is also known as ______.	Great worm	Internet worm	Both (a) and (b)	Nimda	Both (a) and (b)
25	Once the program files get infected ,the virus makes copies of itself and infects the other programs on the computer system____.	Multipartite vir	Polymorphic vi	Program viruses	Stealth viruses	Program viruses
26	It infects the storage media on which OS is stored and which is used to start the computer system	Program viruses	Boot sector viru	Macroviruses	Multipartite viruse	Boot sector viruses
27	_______is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker.	SQL injection	Blind injection	Piggy backed queries	Injection	Blind injection
28	The _______are responsible for storing informatio	CPU	Hard disk	Peer	Memory disk	Peer
29	_________is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message.	Cryptography	Steganography	Steganalysis	Cryptanalysis	Steganography
30	The term ____or_____is used to describe the original,innocent message,data,audio,still,video and so on.	Cover or cover medium	Covers or cover medium	Cover or covers medium	Covers or covers medium	Cover or cover medium
31	The factors that contribute to overcome exploits are____.	Null bytes in addresses	Variability in the location of shellcode	Differences between environments	All the three	All the three
32	_____is an open database connectivity driver that acts as an SQL injection protection feature.	SQL injection	SQL statements	SQL block	SQL	SQL block
33	_____is different from the memory space allocated for stack and code.	Heap	Buffer	Heap buffer	Both (a) and (b)	Heap
34	Expand SSID_______	Service set identification	Server set ident	Service set identif	Server set identif	Service set identifier
35	The payment can be made using debit/credit card through the payment gatewayssuch as____	PayPal	Commercial ho	PalPay	Wifi hotspot	PayPal
36	__________is also known as WiMax	802.11	802.12	802.15	802.16	802.16

37	_________combines the benefits of broadband and wireless and it provides high speed wireless internet over very long distance and provides access to large areas.	802.12	802.16	802.14	802.15	802.16
38	The attacker usually installs the sniffers remotely on victims system and conducts activities such as _______	Passive scanning of wireless network	Detection of SS	Collecting the MAC address	Collecting the frame to crack WEP	All the above
39	It is a computer malware that holds a computer system ,or the data it contains,hostage against its user by demanding a ransom for its restoration.	Scareware	Malvertising	Clickjacking	Ransomware	Ransomware
40	_____is a tool enables to erase event records selectively from security log in Windows NT 4.0 and Windows 2000.	ELSave	WinZapper	Traceless	Track Eraser Pro	WinZapper
41	________is a scenario where a website ends up denied not due to a deliberate attack by a single individual or group of individuals.	Logic attacks	Bandwidth atta	Protocol attacks	Unintentional Dos attack	Unintentional Dos attack
42	__________ is a central server that keeps information about the network.	Mixed P2P	Hybrid P2P	Pure P2P	Only (a)	Hybrid P2P
43	________can detect Trinoo,Stachedraht and Tribe Fllod Network programs running with their default settings.	DDoSPing	Dspoofing	Ddosping	Only (a)	Only (a)
44	Numeric value sholud be checked while accepting a query ______value.	String	Character	NULL	All the above	String
45	______ is a malicous technique of tricking netizens into revealing confidential information.	Scareware	Malvertising	Clickjacking	Ransomware	Clickjacking
46	________is a hybrid of a boot sector and program virus	Program viruses	Boot sector viru	Stealth viruses	Multipartite viruse	Multipartite viruses
47	A________ is a self-replicating malware computer prog	Morris worm	Computer worn	Great worm	Both (a) and (b)	Computer worm
48	_______ viruses become active when the program file i	Program viruses	Boot sector viru	Stealth viruses	Multipartite viruse	Program viruses
49	Wireless networks are generally composed of _______ basic elements.	2	3	4	5	2
50	The cover media are digital ,the alterable parts are calle	Redundant bits	Redundancy bit	Redundant bytes	Redundancy bits and bytes	Redundant bits

51	According to a study by Jupiter Research,__________ of wireless network owners have accessed their neighbor's connection.	20%	15%	14%	18%	14%
52	The practice of noting the keys struck on a keyboard that are often called _________.	Keylogger	Spywares	Antikeylogger	Hardware keylogging	Keylogger
53	SYN attack is also termed as _________.	SYN and ACK	TCP SYN Flodd	Both (a)and (b)	SYN AND TCP	TCP SYN Flodding
54	______ is a memory space in which automatic variables	Register	Stack	Buffer	Buffer overflows	Stack
55	_________ is a way of generating significant computer network traffic on a victim network.	Nuke	Teardrop attack	Smurf attack	Flood attack	Smurf Attack
56	______ is the ultimate mobile user and spends little time in the office.	Remote worker	Roaming user	Nomad	Road warrior	Road Warrior
57	Most people associate __________with E-mail messages that spoof or mimic banks,credit cards companies or others.	Proxy server	Phishing	Anonymizers	Hacking	Phishing
58	___________uses poofed TCP packets.	Mstream	Shaft	Trinoo	Stachedraht	Mstream
59	_____________ is also known as Downup,Downadup a	Autorun	Conficker	Agent	Flystudio	Conficker
60	Execute the ------------- statement may enable selling politically incorrect items on an e-commerce website	SELECT	INSERT	UPDATE	MODIFY	INSERT

Register Number____________

[15CSU603B]

KARPAGAM ACADEMY OF HIGHER EDUCATION

Coimbatore-641021.

B.Sc COMPUTER SCIENCE

FIRST INTERNAL EXAMINATION - JANUARY 2018

Sixth Semester

CYBER SECURITY

Class : III B.Sc (CS) **Duration : 2 Hours**

Date & Session : 19.1.2018 **Maximum : 50 Marks**

SECTION A – (20 X 1 = 20 Marks)

ANSWER ALL THE QUESTIONS

1. People who create electronic spam are called ____________

a) Cybercrime b) Cyberfraud c) Spammers d)Criminals

2. Salami attack are used for committing _______________crimes.

a) Rawdata b) Financial c) Social media d) Cyber fraud

3. NCRB is a________________

a) National Crime Record Bureau b) Netizen Crime Record Bureau

c) Nationalism Crime Record Bureau d) Network Crime Record Bureau

4. In 2006 how many percentage of financial fraud crimes occur_____________

a)12% b)38% c)55% d) 9%

5. Who break into computer system?

a)Hackers b) Crackers c)Cyberfraud d)Cybercriminals

6. "Power of controller to give direction" is under the category of ____________ section.

a) Section 43 b) Section 67 c) Section 68 d) Section 72

7. _________ is where users mentally travel through metrics of data.

a) Cybersquatting b) Cyberpunk c) Cyberspace d) Cyberwarfare

8. Cybercrimes are punishable under two categories_____________

a) ITA 2000 and IPC b) ITA 2000 c) IPC d) Only A

9. ____________ is a event depend program create to do something only when a certain event occurs.

a) Logic bomb b) Computer sabotage

c) Identity theft d) Software piracy

10. ____________ is a fraud involving another person identity for an illicit purpose.

a) Software piracy b) Identity theft c) Spamming d) Spoofing

11.Cybercrime is divided into _______ and _______

a) Technology and technocrime b) cyber terrorist and cyber terrorism

c) crime and criminals d) Technocrime and Techno vandalism

12.The unwanted information are created in _________

a) Technocrime b) Technovandalism c) Cyberspace d) Cybercrime

13.You will using a other person facebook id is called _______

a) Spamming b) Spoofing c) Hacking d) Internet Time Theft

14. Technology is a ___________ as it can be used for both good and bad purposes.

a) single-edged sword b) double-edged sword

c) No-edged sword d) None of the above

15. The objectives of scanning is of ____________

a) Two types b) Three types c) Four types d) Five types

16. ____________ understand the existing weakness in the system.

a) Port scanning b) Network scanning c) Vulnerability scanning d) URL scanning

17. The scrutinizing phase is always called ____________ in the hacking world.

a) Privileges b) Enumeration c) Malicious d) Cracking

18.Cybercrimes such as stealing of bank passwords are happened through ____________

a) Internet b) Shoulder sniffing c) Dumpster diving d) Cybercafes

19. ________ is another means of passive attack to yield information.

a) Network sniffing b) E-mail spoofing c) only A d) Both A and B

20. An active attack involves the risk of detection and is also called as ___________

a) Rattling the door nobs b) Active reconnaissance c) Door nobs d) Both A and B

PART-B (3 X10 = 30Marks)

(Answer ALL the Questions)

21. a) Define Cybercrime. What are the two types of Attack in Cybercrime?

(or)

b) Explain about Global Perspective on Cybercrimes.

22. a) What is Information Security in Cybercrimes & Who are Cybercriminals?

(or)

b) How Criminals Plan the Attacks?

23. a)How are Cybercrimes Classified? Explain any 10 briefly.

(or)

b) Define Social Engineering. What are the Classification of Social Engineering?

Register Number____________

[15CSU603B]

KARPAGAM ACADEMY OF HIGHER EDUCATION

Coimbatore-641021.

B.Sc COMPUTER SCIENCE

FIRST INTERNAL EXAMINATION - JANUARY 2018

Sixth Semester

ANSWER KEY-CYBER SECURITY

Class	**: III B.Sc (CS)**	**Duration**	**: 2 Hours**
Date & Session :	**19.1.2018**	**Maximum**	**: 50 Marks**

SECTION A – (20 X 1 = 20 Marks)

ANSWER ALL THE QUESTIONS

1. People who create electronic spam are called ____________

a) Cybercrime b) Cyberfraud c) **Spammers** d)Criminals

2. Salami attack are used for committing _______________crimes.

a) Rawdata b) **Financial** c) Social media d) Cyber fraud

3. NCRB is a________________

a) **National Crime Record Bureau** b) Netizen Crime Record Bureau

c) Nationalism Crime Record Bureau d) Network Crime Record Bureau

4. In 2006 how many percentage of financial fraud crimes occur_____________

a)12% b)38% c)55% d) **9%**

5. Who break into computer system?

a)Hackers b) **Crackers** c)Cyberfraud d)Cybercriminals

6. "Power of controller to give direction" is under the category of ____________ section.

a) Section 43 b) Section 67 c) **Section 68** d) Section 72

7. _________ is where users mentally travel through metrics of data.

a) Cybersquatting b) Cyberpunk c) **Cyberspace** d) Cyberwarfare

8. Cybercrimes are punishable under two categories_____________

a) ITA 2000 and IPC b) ITA 2000 c) IPC d) **Only A**

9. ____________ is a event depend program create to do something only when a certain event occurs.

a) **Logic bomb** b) Computer sabotage

c) Identity theft d) Software piracy

10. ____________ is a fraud involving another person identity for an illicit purpose.

a) Software piracy b) **Identity theft** c) Spamming d) Spoofing

11.Cybercrime is divided into _______ and _______

a) Technology and technocrime b) cyber terrorist and cyber terrorism

c) crime and criminals d) **Technocrime and Techno vandalism**

12.The unwanted information are created in _________

a) Technocrime b) **Technovandalism** c) Cyberspace d) Cybercrime

13.You will using a other person facebook id is called _______

a) Spamming b) Spoofing c) Hacking d) **Internet Time Theft**

14. Technology is a ___________ as it can be used for both good and bad purposes.

a) single-edged sword b) **double-edged sword**

c) No-edged sword d) None of the above

15. The objectives of scanning is of ____________

a) Two types b) **Three types** c) Four types d) Five types

16. ____________ understand the existing weakness in the system.

a) Port scanning b) Network scanning c) **Vulnerability scanning** d) URL scanning

17. The scrutinizing phase is always called ____________ in the hacking world.

a) Privileges b) **Enumeration** c) Malicious d) Cracking

18.Cybercrimes such as stealing of bank passwords are happened through ____________

a) Internet b) Shoulder sniffing c) Dumpster diving d) **Cybercafes**

19. ________ is another means of passive attack to yield information.

a) Network sniffing b) E-mail spoofing c) **only A** d) Both A and B

20. An active attack involves the risk of detection and is also called as ___________

a) Rattling the door nobs b) Active reconnaissance c) Door nobs d) **Both A and B**

PART-B (3 X10 = 30Marks)

(Answer ALL the Questions)

21. a) Define Cybercrime. What are the two types of Attack in Cybercrime?

DEFINING CYBER CRIME:

- Crime committed using a computer and the internet to steal data or information.
- Illegal imports.
- Malicious programs.

What is Cyber Crime?

- Cybercrime is not a new phenomena
- The first recorded cybercrime took place in the year 1820.
- In 1820, JosephMarie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new echnology. **This is the first recorded cyber crime!**

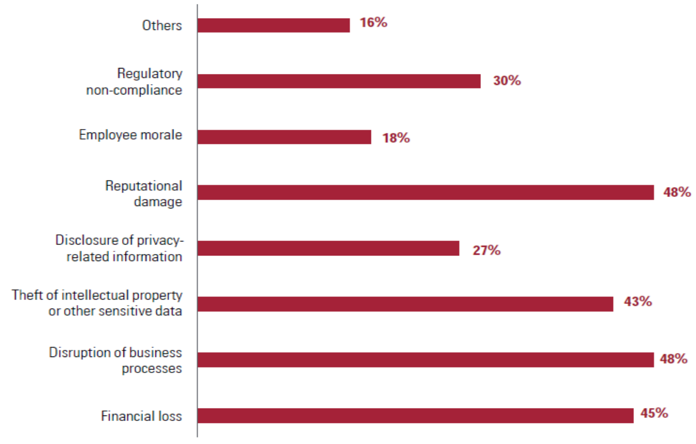
Alternative definitions for cybercrime:

- Any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation or prosecution
- Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers
- Any financial dishonesty that takes place in a computer environment.
- Any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom
- **"*Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that target the security of computer systems and the data processed by them*".**
- Hence cybercrime can sometimes be called as ***computer-related crime, computer crime, E-crime, Internet crime, High-tech crime….***

Cybercrime specifically can be defined in number of ways…

- A crime committed using a computer and the internet to steal a person's identity (identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs.
- Crimes completed either on or with a computer
- Any illegal activity through the Internet or on the computer.
- All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW.
- Cybercrime refers to the act of performing a criminal act using cyberspace as communication vehicle.
- **Two types of attacks are common:**
    - **Techno- crime : *Active attack***
        - Techno Crime is the term used by law enforcement agencies to denote criminal activity which uses (computer) technology, not as a tool to commit the crime, but as the subject of the crime itself. Techno Crime is usually pre-meditated and results in the *deletion, corruption, alteration, theft or copying of data on an organization's systems*.
        - Techno Criminals will usually probe their prey system for weaknesses and will almost always leave an electronic 'calling card' to ensure that their pseudonym identity is known.
    - **Techno – vandalism: *Passive attack***
        - Techno Vandalism is a term used to describe *a hacker or cracker* who breaks into a computer system with the *sole intent of defacing and or destroying its contents*.
        - Techno Vandals can deploy *'sniffers'* on the Internet to locate soft (insecure) targets and then execute a range of commands using a variety of protocols towards a range of ports. If this sounds complex - it is! The best weapon against such attacks is a firewall which will hide and disguise your organization's presence on the Internet.

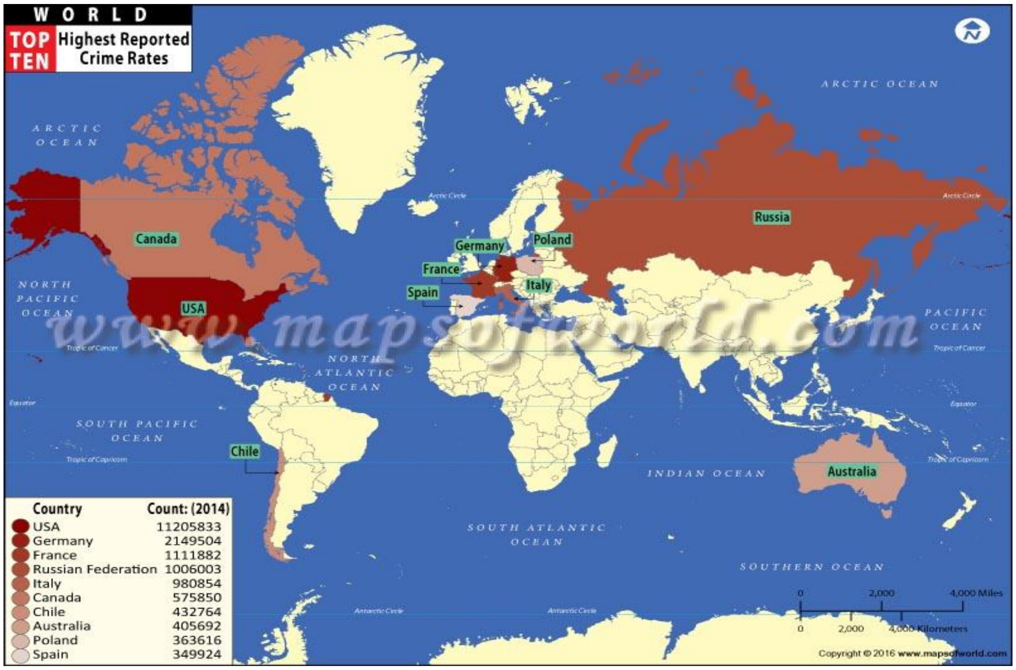
Survey result - Impact of cybercrime in India



Source: Cybercrime survey report 2014, KPMG in India

b) Explain about Global Perspective on Cybercrimes.

A Global Perspective on cybercrimes:



It refers to illegal internet-mediated activities that often take place in global electronic networks. Cybercrime is "international" or "transnational" – there are ‘no cyber-borders between countries'.

International cybercrimes often challenge the effectiveness of domestic and international law and law enforcement. Because existing laws in many countries are not tailored to deal with cybercrime, criminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments or difficulties of being traced.

No matter in developing or developed countries, governments and industries have gradually realized the colossal threats of cybercrime on economic and political security and public interests. However, complexity in types and forms of cybercrime increases the difficulty to fight back. In this sense, fighting cybercrime calls for international cooperation.

Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale.

U.S.-China's cooperation is one of the most striking progress recently because they are the top two source countries of cybercrime.

22. a) What is Information Security in Cybercrimes & Who are Cybercriminals?

Cybercrime and information security:

- Lack of information security give rise to cybercrime
- Cybersecurity: means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

Challenges for securing data in business perspective:

- Cybercrime occupy an important space in information security due to their impact.
- Most organizations do not incorporate the cost of the vast majority of computer security incidents into their accounting
- The difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost
- Financial losses may not be detected by the victimized organization in case of Insider attacks : such as leaking customer data

Cybercrime trends over years

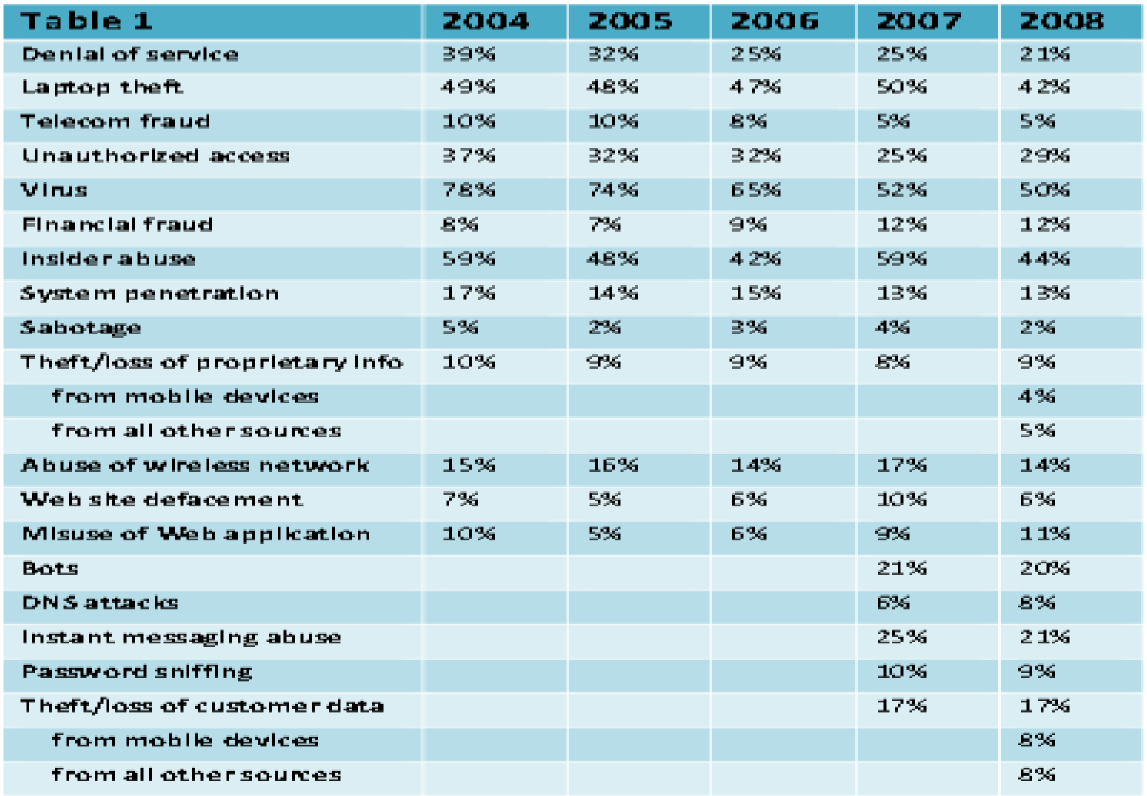


Table 1	2004	2005	2006	2007	2008
Denial of service	39%	32%	25%	25%	21%
Laptop theft	49%	48%	47%	50%	42%
Telecom fraud	10%	10%	8%	5%	5%
Unauthorized access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial fraud	8%	7%	9%	12%	12%
Insider abuse	59%	48%	42%	59%	44%
System penetration	17%	14%	15%	13%	13%
Sabotage	5%	2%	3%	4%	2%
Theft/loss of proprietary info	10%	9%	9%	8%	9%
from mobile devices					4%
from all other sources					5%
Abuse of wireless network	15%	16%	14%	17%	14%
Web site defacement	7%	5%	6%	10%	6%
Misuse of Web application	10%	5%	6%	9%	11%
Bots				21%	20%
DNS attacks				6%	8%
Instant messaging abuse				25%	21%
Password sniffing				10%	9%
Theft/loss of customer data				17%	17%
from mobile devices					8%
from all other sources					8%

Who are Cybercriminals:

- Are those who conduct acts such as:
  - Child pornography
  - Credit card fraud
  - Cyberstalking
  - Defaming another online
  - Gaining unauthorized access to computer systems

  - Ignoring copyrights
  - Software licensing and trademark protection
  - Overriding encryption to make illegal copies
  - Software piracy

Stealing another's identity to perform criminal acts.

Categorization of Cybercriminals:

- **Type 1: Cybercriminals- hungry for recognition**
  - **Hobby hackers**
    - A person who enjoys exploring the limits of what is possible, in a spirit of playful cleverness. May modify hardware/ software
  - **IT professional(social engineering):**
    - **Ethical hacker**
  - **Politically motivated hackers :**
    - promotes the objectives of individuals, groups or nations supporting a variety of causes such as : Anti globalization, transnational conflicts and protest
  - **Terrorist organizations**
    - Cyberterrorism
    - Use the internet attacks in terrorist activity
    - Large scale disruption of computer networks , personal computers attached to internet via viruses

Type 2: Cybercriminals- not interested in recognition:

  - **Psychological perverts**
    - Express sexual desires, deviates from normal behavior
    - Poonam panday
  - **Financially motivated hackers**
    - Make money from cyber attacks
    - Bots-for-hire : fraud through phishing, information theft, spam and extortion
  - **State-sponsored hacking**
    - Hacktivists
    - Extremely professional groups working for governments
    - Have ability to worm into the networks of the media, major corporations, defense departments

Type 3: Cybercriminals- the insiders:

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

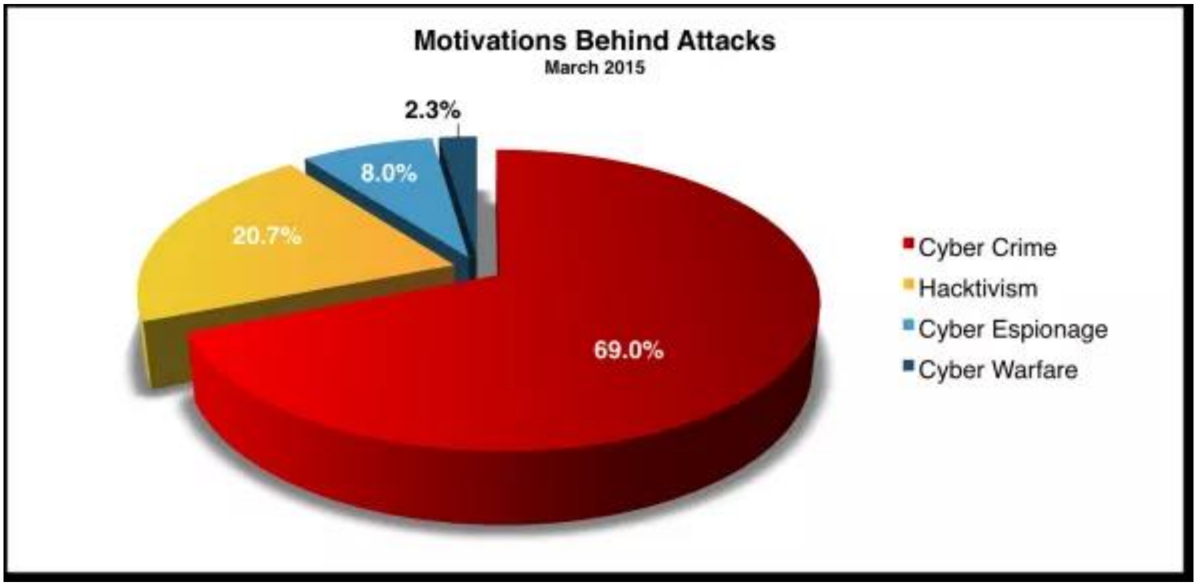
Motives behind cybercrime:

- Greed
- Desire to gain power
- Publicity
- Desire for revenge
- A sense of adventure
- Looking for thrill to access forbidden information
- Destructive mindset

(or)

b) How Criminals Plan the Attacks?

HOW CYBER CRIMINALS PLAN CYBER ATTACKS:



Cyber Attacks statistics India image source : hackmageddon

How Cyber Criminals Plan cyber Attacks

Cyber Criminals use many tool and methods to locate vulnerability of their victim. Criminal mostly categorized as.

1. Passive attacks
2. Active Attacks

Attackers can be categorized as inside attacker or outside attacker. Attacks perform within the organization is called inside attack whereas attacker get information from outside is called outside attack. Inside attack are always more dangerous than outside, because inside attackers has get more resources than outsider.Following are three major phases are involved in planning of cyber crime.

1. **RECONNAISSANCE**

This is first step towards cyber attacks, it is one kind of passive attack. “Reconnaissance” means an act of reconnoitering. In this phase attacker try explore and gain every possible information about target.

In hacking world, Hacking start with “foot printing”. Foot printing provide overall system structure, loop holes and exploration of those vulnerability. Attacker utilize this phase is to understand system, personal information, networking ports and services.

CYBER ATTACKER USE TWO STEPS TO GATHER THIS INFORMATION.

Passive Attacks: Passive attacks used to gain information about individual or organization. It exploit confidential information. Passive attacks involve gaining data about a target without target knowledge. Now day’s passive attack are much easier

- Use Google or other search engine: Gather information by searching on Google.
- Social Media: Search on social media like Facebook, Twitter, and LinkedIn.
- Use properly privacy setting in social media to avoid
- Organization Website: Attacker may get employee information using organizational website.
- Blog or press release: This are new source where attacker easily get company or individual information. Company.
- Job Posting: Search job profile provide valuable information about person an Job profile for technical person can give data about type of technology that is, software, server, database or network devices a company using on its network.
- Network Sniffing: This attack use to gather information such as IP address, network range, hidden server and other valuable services on network.

Active attacks: Active attack mostly used to manipulate or alter the system. It may effect on integrity, authenticity and availability of data. Information from passive phase is act as input to active phase. In this phase attacker verify gather information (IP address, network range, hidden server, personal information). This is very important as cyber attacker point of view, it provide security measure.

2. SCANNING AND SCRUTINIZING : In this phase attacker collect validity of information as well as find out existing vulnerability. It is key phase before actual attack happen.

- Port scanning: Identify all ports and services (open / closed)
- Network scanning: Verify IP address and network information before cyber attacks.
- Vulnerability scanning: Checking loop hole in system.

Scrutinizing phase is also called enumeration.

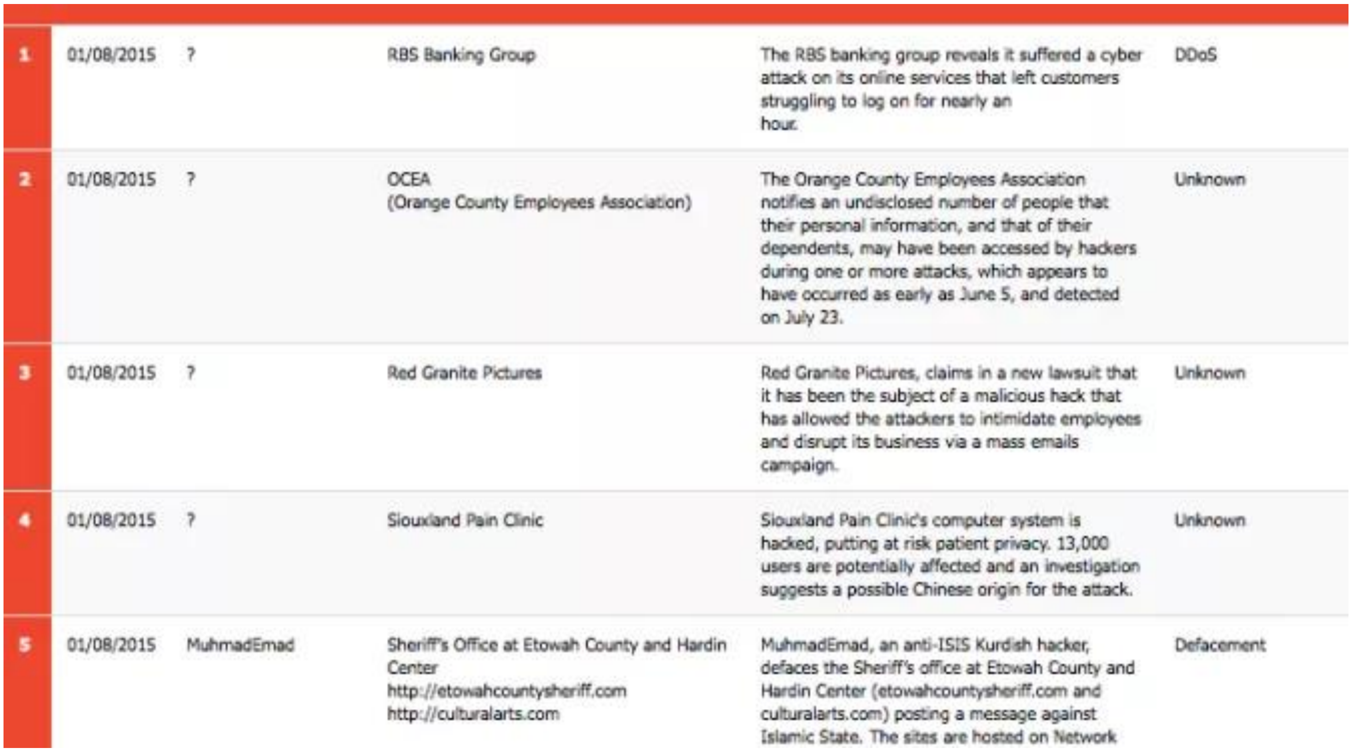
- Validate user accounts and groups
- Find out list of network resource and how many network devices are shared?
- Different types of OS and application.

3. LAUNCHING AN ATTACK

Using step two information actual launching attack to gain system information. Once step two complete cyber attacker ready to launch attack.

1. Crack the password.
2. Exploit the privilege
3. Execute malicious command
4. Hide the files
5. Final but most important is cover the track.

Recent cyber attacks



1	01/08/2015	?	RBS Banking Group	The RBS banking group reveals it suffered a cyber attack on its online services that left customers struggling to log on for nearly an hour.	DDoS
2	01/08/2015	?	OCEA (Orange County Employees Association)	The Orange County Employees Association notifies an undisclosed number of people that their personal information, and that of their dependents, may have been accessed by hackers during one or more attacks, which appears to have occurred as early as June 5, and detected on July 23.	Unknown
3	01/08/2015	?	Red Granite Pictures	Red Granite Pictures, claims in a new lawsuit that it has been the subject of a malicious hack that has allowed the attackers to intimidate employees and disrupt its business via a mass emails campaign.	Unknown
4	01/08/2015	?	Siouxland Pain Clinic	Siouxland Pain Clinic's computer system is hacked, putting at risk patient privacy. 13,000 users are potentially affected and an investigation suggests a possible Chinese origin for the attack.	Unknown
5	01/08/2015	MuhmadEmad	Sheriff's Office at Etowah County and Hardin Center http://etowahcountysheriff.com http://culturalarts.com	MuhmadEmad, an anti-ISIS Kurdish hacker, defaces the Sheriff's office at Etowah County and Hardin Center (etowahcountysheriff.com and culturalarts.com) posting a message against Islamic State. The sites are hosted on Network	Defacement

Cyber Attack News

23. a)How are Cybercrimes Classified? Explain any 10 briefly.

Classification of cybercrimes:

1. Cybercrime against an individual
2. Cybercrime against property
3. Cybercrime against organization
4. Cybercrime against Society
5. Crimes emanating from Usenet newsgroup

1. Cybercrime against an individual:

- Electronic mail spoofing and other online frauds
- Phishing, spear phishing
- spamming
- Cyberdefamation
- Cyberstalking and harassment
- Computer sabotage
- Pornographic offenses
- passwordsniffing

2.Cybercrime against property:

- Credit card frauds
- Intellectual property(IP) crimes
- Internet time theft

3.Cybercrime against organization:

- Unauthorized accessing of computer
- Password sniffing
- Denial-of-service attacks
- Virus attack/dissemination of viruses
- E-Mail bombing/mail bombs
- Salami attack/ Salami technique
- Logic bomb
- Trojan Horse
- Data diddling
- Industrial spying/ industrial espionage
- Computer network intrusions
- Software piracy

4.Cybercrime against Society:

- Forgery
- Cyberterrorism
- Web jacking

5.Crimes emanating from Usenet newsgroup:

- Usenet groups may carry very offensive, harmful, inaccurate material
- Postings that have been mislabeled or are deceptive in another way
- Hence service at your own risk

History of Usenet groups:

- In 1979 it was developed by two graduate student
- s from Duke University in North Carolina (UNC) as a network that allowed users to exchange quantities of information too large for mailboxes
- Usenet was designed to facilitate textual exchanges between scholars.
- Slowly, the network structure adapted to allow the exchange of larger files such as videos or images.

Usenet groups as a "safe" place?

- Usenet newsgroups constitute one o the largest source of child pornography available in cyberspace
- This source useful for observing other types of criminal or particular activities: online interaction between pedophiles, adult pornographers and writers of pornographic stories.
- Usenet for sharing illegal content

Criminal activity on Oracle USENET Newsgroups:

- This interesting SearchOracle article on Oracle security bloopers, we see the risks with engaging the unsavory inhabitants of the Oracle USENET newsgroup, a forum laced with profanity, pornography and, according to this note, criminal Oracle hackers:
- “I subscribe to several Usenet groups so I can keep my skills current. Well, a few years ago a DBA needed some assistance and posted a question in which he shared his tnsnames.ora file and wondered why he could not connect to SQL*Plus with the following syntax:
- sqlplus system/SecurePswd@prod
- Almost immediately several people connected to this person’s production system and was able to fish around the system. Numerous people emailed the DBA back and pointed out that he just broadcasted to the world his production connection string and password. How crazy is that?”

E-Mail Spoofing:

- E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.
- To send spoofed e-mail, senders insert commands in headers that will alter message information.
- It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say.
- Thus, someone could send spoofed e-mail that appears to be from you with a message that you didn't write.
- Classic examples of senders who might prefer to disguise the source of the e-mail include a sender reporting mistreatment by a spouse to a welfare agency
- Although most spoofed e-mail falls into the "nuisance" category and requires little action other than deletion, the more malicious varieties can cause serious problems and security risks.
- For example, spoofed e-mail may purport to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information -- any of which can be used for a variety of criminal purposes.
- The Bank of America, eBay, and Wells Fargo are among the companies recently spoofed in mass spam mailings.
- One type of e-mail spoofing, self-sending spam, involves messages that appear to be both to and from the recipient.

Spamming:

- People who create electronic spam : spammers
- Spam is abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately
- Spamming may be
    - E-Mail Spam
    - Instant messaging spam
    - Usenet group spam
    - Web search engine spam
    - Spam in blogs, wiki spam
    - Online classified ads spam
    - Mobile phone messaging spam

  - Internet forum spam
  - Junk fax spam
  - Social networking spam.
- Spamming is difficult to control
- Advertisers have no operating costs beyond the management of their mailing lists
- It is difficult to hold senders accountable for their mass mailings
- Spammers are numerous

Search engine spamming:

- Alteration or creation of a document with the intent to deceive an electronic catalog or a filing system
- some web authors use “subversive techniques” to ensure that their site appears more frequently or higher number in returned search results.
- remedy: permanently exclude from the search index

Avoid the following web publishing techniques:

- Repeating keywords
- Use of keywords that do not relate to the content on the site
- Use of fast meta refresh
  - change to the new page in few seconds.
- Redirection
- IP cloaking:
  - including related links, information, and terms.
- Use of colored text on the same color background
- Tiny text usage
- Duplication of pages with different URLs
- Hidden links

Cyber defamation:

- The tort of cyber defamation is considered to be the act of defaming, insulting, offending or otherwise causing harm through false statements pertaining to an individual in cyberspace.
- Example: someone publishes defamatory matter about someone on a website or sends an E-mail containing defamatory information to all friends of that person.

It may amount to defamation when

- If imputation to a deceased person would harm the reputation of that person, and is intended to be hurtful to the feelings of his family or other near relatives
- An imputation is made concerning a company or an association or collection of people as such.
- An imputation in the form of an alternative or expressed ironically
- An imputation that directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person.

Types of defamation:

- **Libel** : written defamation
- **Slander**: oral defamation
- The plaintiff must have to show that the defamatory statements were unlawful and would indeed injure the person’s or organization’s reputation.

- When failed to prove, the person who made the allegations may still be held responsible for defamation.

Cyber defamation cases:

- In first case of cyber defamation in India (14 dec 2009),
    - the employee of a corporate defamed its reputation was sending derogatory and defamatory emails against the company.
    - In this case the Court(delhi court) had restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails.
    - The court passed as important ex-parte injunction.
- In another case, accused posted obscene, defamatory and annoying message about a divorcee woman and also sent emails to the victim.
    - The offender was traced and was held guilty of offences under section 469, 509 IPC and 67 of IT Act, 2000.
- Other defamation cases:
    - A malicious customer review by a competitor could destroy a small business.
    - A false accusation of adultery on a social networking site could destroy a marriage.
    - An allegation that someone is a “crook” could be read by a potential employer or business partner

Internet Time Theft:

- Occurs when an unauthorized person uses the Internet hours paid for by another person
- Comes under hacking
- The person get access to someone else’s ISP user ID and password, either by hacking or by gaining access to it by illegal means
- And uses the internet without the other person’s knowledge
- This theft can be identified when Internet time is recharged often, despite infrequent usage.
- This comes under “identity theft”.

Salami attack/ salami technique:

- Are used for committing financial crimes.
- The alterations made are so insignificant that in a single case it would go completely unnoticed.
- Example: a bank employee inserts a program, into the bank’s serve, that deduces a small amount from the account of every customer every month,
- The unauthorised debit goes unnoticed by the customers, but the employee will make a sizable amount every month.

Salami attack: real life examples:

- Small “shavings” for Big gains!
- The petrol pump fraud

Data diddling:

- Data diddling involves changing data input in a computer.
- In other words, information is changed from the way it should be entered by a person typing in the data.
- Usually, a virus that changes data or a programmer of the database or application has pre-

programmed it to be changed.

- For example, a person entering accounting may change data to show their account, or that or a friend or family member, is paid in full. By changing or failing to enter the information, they are able to steal from the company.
- To deal with this type of crime, a company must implement policies and internal controls.
- This may include performing regular audits, using software with built-in features to combat such problems, and supervising employees.

Real life example:

Doodle me Diddle:

- Electricity board in India have been victims to data diddling programs inserted when private parties computerized their systems.

Forgery :

- The act of forging something, especially the unlawful act of counterfeiting a document or object for the purposes of fraud or deception.
- Something that has been forged, especially a document that has been copied or remade to look like the original.
- Counterfeit currency notes, postage, revenue stamps, marksheets, etc., can be forged using sophisticated computers, printers and scanners.

(or)

b) Define Social Engineering. What are the Classification of Social Engineering?

Social Engineering:

Definition(s) of Social Engineering

- The term "Social Engineering" can be defined in various ways, relating to both physical and cyber aspects of that activity. Wikipedia defines social engineering as:
- "...the art of manipulating people into performing actions or divulging confidential information".

Other authors have provided the following definitions:

- "An outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system".
- "The practice of deceiving someone, either in person, over the phone, or using a computer, with the express intent of breaching some level of security either personal or professional".
- "Social Engineering is a non-technical kind of intrusion relying heavily on human interaction which often involves tricking other people into breaking normal security procedures" the attacker uses social skills and human interaction to obtain information about an organization or their computer systems.
- In reality Social Engineering can be any of these definitions depending on the circumstances that surround the attack.
- Social Engineering is actually a hackers manipulation of the natural human tendency to trust so as to get sensitive information needed to gain access to a system. Social
- Engineering does not require high level of technical expertise but requires the individual to have decent social skills.

Many people, for several decades have used social engineering as a method to research and collect data. These early social engineers would use the gathered information as a form of blackmail against the other organizations. Social engineering has been used to gain unauthorized access into several huge organizations. A hacker who spends several hours trying to break passwords could save a great deal of time by calling up an employee of the organization, posing as a helpdesk or IT employee, and can just asking for it.

Out of the blue you receive an email informing you about a large sum of money that is trapped in a foreign bank account a wealthy politician has died leaving a large sum of money. The sender is asking your help to transfer the money out of the country. You will receive a huge reward as well. The sender asks you to give them your bank account details to transfer the money then asks you to pay transfer fee/tax to transfer money out of the country. This fee may start with a small amount but will increase. The criminal will make up new fees that is necessary to be paid to receive your reward. It does not matter how much you pay, you will never receive your reward. This is a “scam” a type of social engineering and this particular scam is commonly known as “419 scam” an advanced fee fraud.

Criminals can use sophisticated attacks to gain access to your computer or trick you and obtain money. But they have another easier and non sophisticated tool in their arsenal called “social engineering”. Social engineering uses human interaction(social skills) and obtains confidential information. The obtained information is then used in accessing the user accounts or according to the above example the user is tricked in obtaining money.

Classification of Social Engineering:

Social engineering attacks may be divided into two categories.

1. Computer based social engineering.
2. Human based social engineering.

Computer based social engineering attacks may include the below.

- Email attachments
- Fake websites
- Pop-up windows

On-line Scams

Emails sent by scammers may have attachments that include malicious code inside the attachment. Those attachments may include Keyloggers to capture users passwords,Viruses, Trojans, or worms.

Worm attacks

Attackers will trick users to click on a link or download a file then click on it, the executable file is a worm and will propagate from computer to computer copying itself.

The email requests the user to open an attachment in an email. When the users opens the attachment the worm copies itself to all the contacts in the users address book. This worm overloaded a huge number of email servers in the year 2000.

Sometimes pop-up windows can also be used in social engineering attacks. pop-up windows that advertise special offers may tempt users to unintentionally install malicious software.

Phishing attacks
This type of social engineering attack commonly uses emails to trick users in getting credentials to their bank accounts or maybe email accounts. The email mostly claims to be from a well known source, a highly reputed organization, and asks the user to click on a link that takes the users to a site similar to the organizations web site but this site is a fraudulent website that harvests users credentials. The fraudsters use these credentials to gain access to bank or email accounts and steal important information and money.

How to avoid being a victim

- Do not input confidential information into websites without checking the website security.
- Make sure the site is legitimate by checking the URL of the web site.
- Do not click on links inside suspicious emails.
- Fraudsters may even use events such as natural disasters(Asian Tsunami, Hurricane Katrina) or popular events(Olympics) for their benefit, be aware.
- If you are unsure of the legitimacy of an email try calling the company directly with the use of contact information used previously.
- Do not click or download suspicious attachments from email senders that you have not heard before.
- Use email filters, firewalls, virus guards to reduce the threat.
- When you are on the web, be aware that pop-ups that advertise bargains may request you to install malicious software to claim prices.

What can you do if you are a victim

- If you think you have entered your user id and password to a fraudulent website change your password as soon as possible.
- Inform the necessary authorities of the fraudulent object.
- If financial information have been compromised, close down or lock account to prevent harm.

In human-based social engineering attacks, the social engineer interacts directly with the target to get information.

An example of this type of attack would be where the attacker calls the database administrator asking to reset the password for the targets account from a remote location by gathering the user information from any remote social networking site of the XYZ company.

Human-based social engineering can be categorized as follows:

- **Piggybacking**: In this type of attack the attacker takes advantage by tricking authorized personnel to get inside a restricted area of the targeted company, such as the server room. For example, attacker X enters the ABC company as a candidate for an interview but later enters a restricted area by tricking an authorized person, claiming that he is a new employee of the company and so doesn’t have an employee ID, and using the targets ID card.

- **Impersonating**: In this type of attack, a social engineer pretends to be a valid employee of the organization and gains physical access. This can be perfectly carried out in the real world by wearing a suit or duplicate ID for the company. Once inside the premises, the social engineer can gain valuable information from a desktop computer.

- **Eavesdropping**: This is the unauthorized listening to of communication between two people or the reading of private messages. It can be performed using communication channels such as telephone lines and e-mails.

- **Reverse social engineering**: This is when the attacker creates a persona that appears to be in a position of authority. In such a situation, the target will ask for the information that they want. Reverse engineering attacks usually occur in areas of marketing and technical support.

- **Dumpster diving**: Dumpster diving involves looking in the trash can for information written on pieces of paper or computer printouts. The hacker can often find passwords, filenames, or other pieces of confidential information in trash cans.

- **Posing as a legitimate end user**: In this type of attack, the social engineer assumes the identity of a legitimate user and tries to get the information, for example, calling the helpdesk and saying, “Hi, I am Mary from the X department. I do not remember my account password; can you help me out?”