CMR
INSTITUTE OF
TECHNOLOGY

USN □□□□□□□□□□

Internal Assessment Test 1 – March 2017

Sub:	Cyber Crime and Digital Forensics							**Code:**	**14SCN424**
Date:		Duration:	90 mins	Max Marks:	50	**Sem:**	IV	**Branch:**	M.Tech(CNE)

NOTE: Answer any five full questions. Total marks: 50

1. What is cybercrime? How do we classify cybercrime? Explain each one in detail. [10 Marks]

2. Write a short note on Indian legal perspective on cybercrime and IT Act 2000. [10 Marks]

3. Explain how botnets can be used as fuel to cybercrime. [10 Marks]

4. What is cyberstalking? How stalking works? As per your understanding is it a crime under the Indian IT Act? [10 Marks]

5. Explain the online environment for credit card transactions. Discuss the type of techniques of credit card frauds. [10 Marks]

6. a) Explain the challenges in registry settings for mobile devices. [5 Marks]
   b) Mention organizational security policies and measures in mobile computing era. [5 Marks]

7. Differentiate between virus and worm. Explain the various categories of virus. [10 Marks]

8. What do you understand by SQL injection? What are the different counter measures to prevent the attack? [10 Marks]

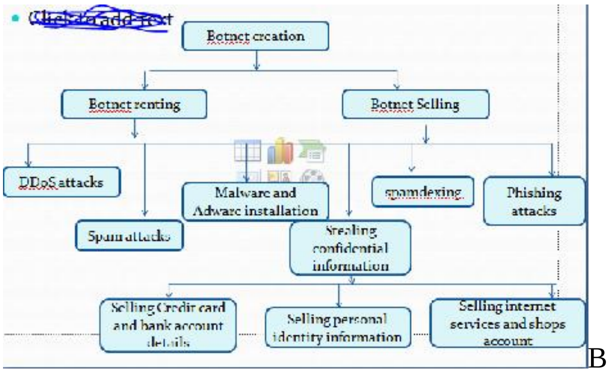
Scheme & Solution

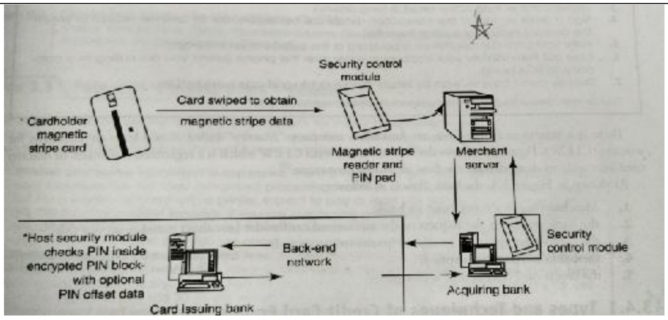
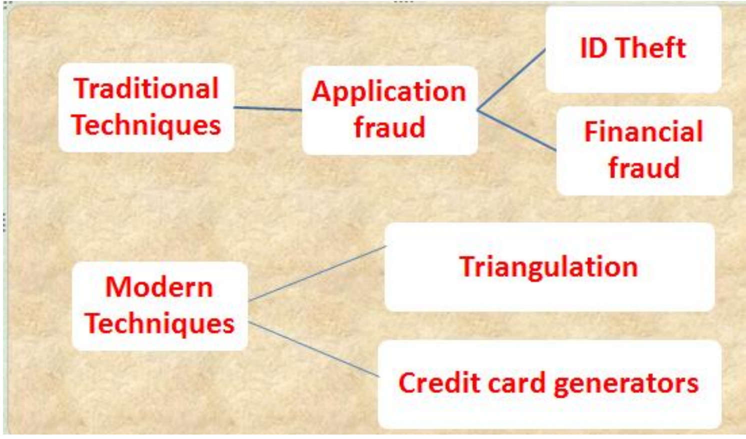
Internal Assessment Test 1 – March 2017

Sub:	Cyber Crime and Digital Forensics					**Code:**	**14SCN424**
Date:		Duration: 90 mins	Max Marks: 50	**Sem:**	IV	**Branch:**	M.Tech(CNE)

Total marks: 50

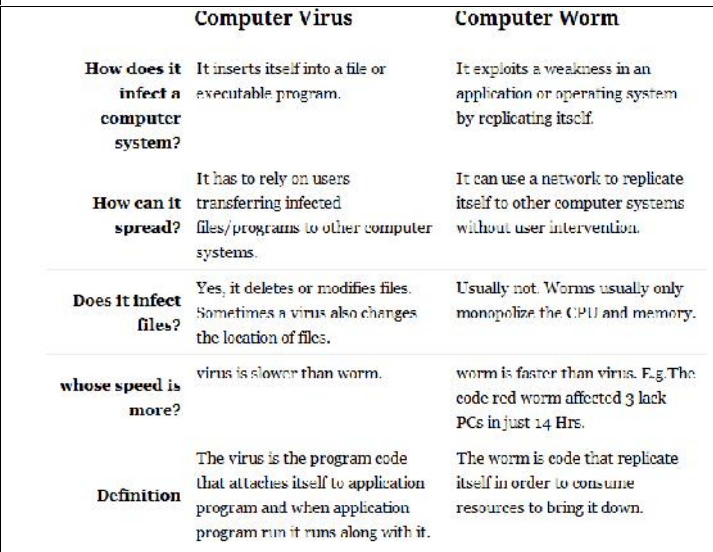
1a)	Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that target the security of computer systems and the data processed by them.- **1 Mark** Classification of cybercrimes: 1. Cybercrime against an individual • Electronic mail spoofing and other online 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 Explain the classification in detail------------------------------------- **9 Marks(2.5+1.5+2.5+1.5+1)**
2.	• 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).** • **List out few cases registered under IT Act 2000 ------ 1 Mark for each point (10 marks)**
3.	• Bot: “ an automated program for doing some particular task, often over a network” • A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. • Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator. • Most computers compromised in this way are home-based. According to a report from Russian-based Kaspersky Labs, botnets -- not spam, viruses, or worms -- currently pose the biggest threat to the Internet ---**5 Marks**  Botnet creation Botnet renting Botnet Selling DDoS attacks Malware and Adware installation spamdexing Phishing attacks Spam attacks Stealing confidential information Selling Credit card and bank account details Selling personal identity information Selling internet services and shops account Botnets for gainful purposes – **2 Marks** Ways to secure system: • Use antivirus and anti-spyware • Install updates • Use firewall • Disconnect internet when not in use • Don’t trust free downloads • Check regularly inbox and sent items • Take immediate action if system is infected ------------------------------**3 Marks**
4.	• **Cyberstalking** is the use of the Internet or other electronic means to stalk or harass an individual, a group, or an 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 or harass. • Cyberstalking is sometimes referred to as Internet stalking, e-stalking or online stalking. - Online and offline stalkers----------------------------------- **2 Marks** - How stalking works? 1. Personal information gathering about the victim. 2. Establish a contact with the victim through telephone/ cell phone. – start threatening or harassing 3. Establish a contact with the victim through E-mail. 4. Keep sending repeated E-mails asking for various kinds of favors or threaten the victim.

	5. Post victim’s personal information on any website related to illicit services. 6. Whosoever comes across the information, start calling the victim on the given contact details, asking for sexual services. 7. Some stalkers may subscribe/ register E-Mail account of the victim to innumerable pornographic and sex sites, bez of which victim start receiving such kind of unsolicited E-Mails -- **7 Marks** - Crime under Indian IT Act -- **1 Mark**
5.	 Cardholder magnetic stripe card Card swiped to obtain magnetic stripe data Security control module Magnetic stripe reader and PIN pad Merchant server Security control module Acquiring bank Back-end network *Host security module checks PIN inside encrypted PIN block with optional PIN offset data Card issuing bank Online environment for credit card transactions (**5 Marks**)  Traditional Techniques Application fraud ID Theft Financial fraud Modern Techniques Triangulation Credit card generators Explain each of these types of techniques **(5 Marks).**
6.a)	• Microsoft Active Sync : synchronize PCs and MS Outlook • Gateway between Windows-Powered PC and Windows mobile-Powered device • Enables transfer of Outlook information, MS Office documents, pictures, music, videos and applications • Active sync can synchronize directly with MS Exchange Sever so that the user can keep their E-Mails, calendar, notes and contacts updated wirelessly. • If you use an Active Directory® environment to administer the computers in your network, Group Policy provides a comprehensive set of policy settings to manage Windows® Internet Explorer® 8 after you have deployed it to your users' computers. • You can use the Administrative Template policy settings to establish and lock registry-based policies for hundreds of Internet Explorer 8 options, including security options. 1700 settings in a standard group policy • Even if the user go through every control panel setting and group policy option- no desired baseline security • So make additional registry changes that are not exposed to any interface: avoid “registry hacks” -- **(5 Marks).**
b)	Elaborate following points: - Importance of security policies of mobile computational devices

- Guidelines of security policies of mobile devices
- Organizational policies of mobile devices ------------------------**(5 Marks).**

7.



	Computer Virus	Computer Worm
How does it infect a computer system?	It inserts itself into a file or executable program.	It exploits a weakness in an application or operating system by replicating itself.
How can it spread?	It has to rely on users transferring infected files/programs to other computer systems.	It can use a network to replicate itself to other computer systems without user intervention.
Does it infect files?	Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.	Usually not. Worms usually only monopolize the CPU and memory.
whose speed is more?	virus is slower than worm.	worm is faster than virus. E.g.The code red worm affected 3 lack PCs in just 14 Hrs.
Definition	The virus is the program code that attaches itself to application program and when application program run it runs along with it.	The worm is code that replicate itself in order to consume resources to bring it down.

--- **4 Marks**

- Boot sector viruses
- Program viruses
- Multipartite viruses
- Stealth viruses
- Polymorphic viruses
- Macroviruses
- Active X and Java control **------------------------------ 6 Marks**

8.

- **SQL injection** is a code **injection** technique, used to attack data-driven applications, in which malicious **SQL** statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

It is the type of attack that takes advantage of improper coding of your web applications that allows hacker to inject SQL commands into say a login form to allow them to gain access to the data held within your database. ----------------------------------- **(3Marks).**

Measures to prevent:

- Input validation
  - Replace all single quotes to two single quotes
  - Sanitize the input: clean characters like ;, --, select, etc
  - Numeric values should be checked while accepting a query string value
  - Keep all text boxes and form fields short
- Modify error reports
  - SQL errors should not be displayed to the outside world
- Other preventions
  - Never use default system accounts for SQL server 2000
  - Isolate database server and webserver: different machines
  - Extended stored procedures, user defined functions should be moved to an isolated server. **---(7 Marks).**