INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal, Hyderabad - 500 043

COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

DEFINITION AND TERMINOLGY

Course Title	**FOUNDATIONS OF CYBER SECURITY**				
Course Code	ACCC02				
Program	B.Tech				
Semester	IV	CSE(CS)			
Course Type	Core				
Regulation	IARE - UG20				
Course Structure	Theory			Practical	
	Lecture	Tutorials	Credits	Laboratory	Credits
	3	1	4	-	-
Course Coordinator	Ms.J Alekhya, Assistant Professor				

COURSE OBJECTIVES:

The students will try to learn:

I	**The reduction of cyber-attacks and cyber-crimes**
II	**The threats and risks within context of the cyber security.**
III	**The security model and analyze them before being used in many applications**
IV	**The defensive techniques against these attacks**

COURSE OUTCOMES:

After successful completion of the course, students should be able to:

CO 1	**Explain** Basic Cyber Security Concepts to overcome the cyber-attacks.	Understand
CO 2	**Select** cyberspace and the law to offer reliable legal inclusiveness to facilitating registration of real-time records.	Apply
CO 3	**Relate** forensic investigation and challenges in computer forensics to gather and preserve evidence.	Understand
CO 4	**List out** various Organizational security Policies and Measures in security issues of mobile computing domain	Remember
CO 5	**Demonstrate** the cost of cybercrimes and IPR issues to detect and recover internal costs in an organization.	Understand

CO 6	**Recall** briefly about the cybercrime mini-cases examples to know the real world case studies.	Remember

DEFINITION AND TERMINOLOGY:

S.No	DEFINITION	CO's
MODULE I		
INTRODUCTION TO CYBER SECURITY		
1	**Define Cyber Security.** Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.	CO 1
2	**Define CIA Triad.** The CIA Triad is actually a security model that has been developed to help people think about various parts of IT security.	CO 1
3	**Define Vulnerability.** Vulnerabilities are the gaps or weaknesses in a system that make threats possible and tempt threat actors to exploit them.	CO 1
4	**Define Threat.** Cyber threats are security incidents or circumstances with the potential to have a negative outcome for your network or other data management systems.	CO 1
5	**Define Confidentiality in CIA Triad.** Confidentiality is about preventing the disclosure of data to unauthorized parties.	CO 1
6	**Define Integrity in CIA Triad.** This is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed.	CO 1
7	**Define Availability in CIA Triad.** Availability is making sure that authorized parties are able to access the information when needed.	CO 1
8	**Categorize different Layers of Security** The 7 layers of cyber security should center on the mission critical assets you are seeking to protect.	CO 1
9	**Categorize different types of cyber criminals.** The growth of the global cyber criminal network, which is largely credited to the increased opportunity for financial incentives, has created a number of different types of cyber criminals, many of which pose a major threat to governments and corporations.	CO 1

10	**Define Identity Thieves** Identity thieves are cyber criminals who try to gain access to their victims' personal information – name, address, phone number, place of employment, bank account, credit card information and social security number.	CO 1
11	**Define Internet Stalkers** Internet stalkers are individuals who maliciously monitor the online activity of their victims to terrorize and/or acquire personal information.	CO 1
12	**Define Phishing Scammers.** Phishers are cyber criminals who attempt to get a hold of personal or sensitive information through victims' computers.	CO 1
13	**Define Cyber Terrorists.** Cyber terrorism is a well-developed, politically inspired cyber-attack in which the cybercriminal attempts to steal data and/or corrupt corporate or government computer systems and networks, resulting in harm to countries, businesses, organizations, and even individuals.	CO 1
14	**Define an Asset.** An asset is any data, device or other component of an organization's systems that is valuable – often because it contains sensitive data or can be used to access such information.	CO 1
15	**Define Cyber Warfare** Cyber warfare refers to the use of digital attacks like computer viruses and hacking by one country to disrupt the vital computer systems of another, with the aim of creating damage, death and destruction.	CO 1
16	**Classify different Cyber-attacks in cyber security** Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber-attacks.	CO 1
17	**Define Cyber Crime** Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Cybercrime is committed by cybercriminals or hackers who want to make money.	CO 1
18	**Define Espionage** Cyber spying, or cyber espionage, is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from individuals.	CO 1
19	**Define Cyber Security Policy.** A security policy also considered to be a ”living document” which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.	CO 1

MODULE II		
CYBER SPACE AND THE LAW AND CYBER FORENSICS		
1	**Define Cyber space** Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services.	CO 2
2	**Define Cyber Forensics** Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence.	CO 3
3	**Classify Cyber Security Regulations** There are five predominant laws to cover when it comes to cybersecurity.	CO 2
4	**Define Indian Penal Code** Identity thefts and associated cyber frauds are embodied in the Indian Penal Code (IPC), 1860 invoked along with the Information Technology Act of 2000.	CO 2
5	**What do you mean by NIST Compliance?** NIST Cybersecurity Framework encompasses all required guidelines, standards, and best practices to manage the cyber-related risks responsibly	CO 2
6	**Define The Indian Cyber Space.** Indian cyberspace was born in 1975 with the establishment of National Informatics Centre (NIC) with an aim to provide govt with IT solutions.	CO 2
7	**What are the Roles of International Law** In various countries, areas of the computing and communication industries are regulated by governmental bodies. There are specific rules on the uses to which computers and computer networks may be put, in particular there are rules on unauthorized access, data privacy and spamming.	CO 2
8	**Define National Cyber Security Policy.** National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology. It aims at protecting the public and private infrastructure from cyberattacks.	CO 2
9	**Define Digital Forensics** Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law.	CO 3
10	**Define Computer Forensics?** Computer forensics is also important because it can save your organization money. From a Technical standpoint, the main goal of computer forensics is to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case.	CO 3

11	**Define Forensics Analysis of Email.** E-mail forensics refers to the study of source and content of e-mail as evidence to identify the actual sender and recipient of a message, data/time of transmission, detailed record of e-mail transaction, intent of the sender, etc.	CO 3
12	**Classify different Email Forensics Tools.** Emails can be forensically extracted even after deletion. Forensic tracing of e-mail is similar to traditional detective work. It is used for retrieving information from mailbox files.	CO 3
13	**What is a MiTec Mail Viewer?** This is a viewer for Outlook Express, Windows Mail/Windows Live Mail, Mozilla Thunderbird message databases, and single EML files.	CO 3
14	**What is OST and PST Viewer?** Nucleus Technologies' OST and PST viewer tools help you view OST and PST files easily without connecting to an MS Exchange server.	CO 2
15	**What is eMail TrackerPro?** eMailTrackerPro analyses the headers of an e-mail to detect the IP address of the machine that sent the message so that the sender can be tracked down.	CO 2
16	**What is Email Tracer?** EmailTracer is an Indian effort in cyber forensics by the Resource Centre for Cyber Forensics (RCCF) which is a premier centre for cyber forensics in India	CO 2
17	**Classify different challenges in Computer Forensics?** Computer forensics has been defined as the use of scientifically derived and proven methods towards the identification, collection, preservation, validation, analysis, interpretation, and presentation of digital evidence derivative from digital sources to facilitate the reconstruction of events found to be criminal.	CO 3
18	**Define Forensics Investigation.** Forensics are the scientific methods used to solve a crime. Forensic investigation is the gathering and analysis of all crime-related physical evidence in order to come to a conclusion about a suspect.	CO 3
19	**What is Digital Forensics Life Cycle?** There are many type of Cyber crimes taking place in the digital world, it is important for the investigator to collect, analyze, store and present the evidence in such a manner that court will believe in such digital evidences and give appropriate punishment to the Cyber criminal.	CO 3

MODULE III		
CYBER CRIME : MOBILE AND WIRELESS DEVICES		
1	**Define Proliferation of mobile and wireless devices.**	CO 4
	A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls. A key driver for the growth of mobile technology is the rapid growth of business solutions into hand-held devices.	
2	**Classify the trends in mobility**	CO 4
	Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking. ”iPhone” from Apple and Google-led ”Android” phones are the best examples of this trend and there are plenty of other developments that point in this direction.	
3	**Classify different Popular types of attacks against 3G mobile networks.**	CO 4
	There are numerous attacks that can be committed against mobile networks and they can originate from two primary vectors. One is from outside the mobile network and the other is within the mobile networks.	
4	**Define security challenges posed by Mobile Networks.**	CO 4
	Mobility brings two main challenges to cybersecurity: first, on the hand-held devices and another at the organizational level called macro- challenges	
5	**Describe Registry Settings for Mobile Devices**	CO 4
	Microsoft Active sync is meant for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook. ActiveSync acts as the ”gateway between Windows- powered PC and Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos and applications from a user’s desktop to his/her device.	
6	**Define Skull Trojan**	CO 4
	It targets Series 60 phones equipped with the Symbian mobile OS.	
7	**Define Cabir Worm**	CO 4
	It is the first dedicated mobile-phone worm infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology.	
8	**Define Mosquito Trojan**	CO 4
	It affects the Series 60 Smartphones and is a cracked version of ”Mosquitos” mobile phone game.	

9	**Define Brador Trojan** It affects the Windows CE OS by creating a svchost. exe file in the Windows start-up folder which allows full control of the device. This executable file is conductive to traditional worm propagation vector such as E-Mail file attachments.	CO 4
10	**Define Lasco Worm** It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir's source code and replicates over Bluetooth connection.	CO 4
11	**Define Denial-of-service (DoS)** The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable.	CO 4
12	**Define Overbilling attack** Overbilling involves an attacker hijacking a subscriber's IP address and then using it (i.e., the connection) to initiate downloads that are not "Free downloads" or simply use it for his/her own purposes.	CO 4
13	**Define Spoofed policy development process** These of attacks exploit the vulnerabilities in the GTP [General Packet Radio Service (GPRS) Tunneling Protocol].	CO 4
14	**Define Signaling-level attacks** The Session Initiation Protocol (SIP) is a signaling protocol used in IP multimedia subsystem (IMS) networks to provide Voice Over Internet Protocol (VoIP) services.	CO 4
	MODULE IV	
	CYBER SECURITY: ORGANIZATIONAL IMPLICATIONS	
1	**Define Insider Threat** An insider threat is defined as “the misuse or destruction of sensitive or confidential information, as well as IT equipment that houses this data by employees, contractors and other ‘trusted’ individuals.”	CO 5
2	**Define Flow and Connections of Cyber crime** There is certainly a paradigm shift in computing and work practices; with workforce mobility, virtual teams, social computing media, cloud computing services being offered, sharp rise is noticed in business process outsourcing (BPO) services, etc.	CO 5
3	**Define Industrial espionage?** There are several tools available for web administrators to monitor and track the various pages and objects that are accessed on their website.	CO 5
4	**What is IP-based blocking?** This process is often used for blocking the access of specific IP addresses and/or domain names.	CO 5

5	**What is IP-based “cloaking”?** Confidentiality is about preventing the disclosure of data to unauthorized parties.	CO 5
6	**What is User sphere?** In User sphere the data is stored on users’ desktops, PCs, laptops, mobile phones, Radio Frequency Identification (RFID) chips, etc. Organization’s responsibility is to provide access to users and monitor that access to ensure misuse does not happen.	CO 5
7	**What is Recipient sphere?** In Recipient sphere the data lies with recipients: servers and databases of network providers, service providers or other parties with whom data recipient shares data.	CO 5
8	**What is Joint sphere?** In Joint sphere the data lies with web service provider’s servers and databases. This is the in between sphere where it is not clear to whom does the data belong.	CO 5
MODULE V		
CYBERCRIME: EXAMPLES AND MINI-CASES EXAMPLES		
1	**Define FIR** First Information Report (FIR) is a written document prepared by the police when they receive information about the commission of a cognizable offence. It is a report of information that reaches the police first in point of time and that is why it is called the First Information Report.	CO 6
2	**Define E-mail spoofing** Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust. In spoofing attacks, the sender forges email headers so that client software displays the fraudulent sender address, which most users take at face value.	CO 6
3	**Define Industrial espionage?** There are several tools available for web administrators to monitor and track the various pages and objects that are accessed on their website.	CO 6
4	**What is anonymity** Anonymity describes situations where the acting person’s identity is unknown. Some writers have argued that namelessness, though technically correct, does not capture what is more centrally at stake in contexts of anonymity. The important idea here is that a person be non-identifiable, unreachable, or untrackable. Anonymity is seen as a technique, or a way of realizing, a certain other values, such as privacy, or liberty.	CO 6

5	**Write a short note on Trade Marks Act, 1958.**	CO 6
	The Trade Mark Act, 1958 is an earlier legislation that governed the trademarks law in India. The main intention behind the legislation was to provide registration and legal protection of trademarks and regulate the use of fraudulent marks on products. The Act provides the definition of the trademark in two different contexts.	
6	**write a short notes on Banking-Related frauds**	CO 6
	India saw more banking frauds in the first half of 2021-22 than in the same year-ago period. However, the amount involved in the frauds declined from 64,621 crore to 36,342 crore, according to the RBI's Trend and Progress of Banking in India report.	
7	**Write a short notes on credit card related frauds in cyber domain.**	CO 6
	credit card fraud, act committed by any person who, with intent to defraud, uses a credit card that has been revoked, cancelled, reported lost, or stolen to obtain anything of value. Using the credit card number without possession of the actual card is also a form of credit card fraud.	
8	**Define phishing incidence in financial frauds of cyber domain.**	CO 6
	Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.	
9	**Define skimming**	CO 6
	Skimming is an illegal practice used by identity thieves to capture credit card information from a cardholder surreptitiously. Fraudsters often use a device called a skimmer that can be installed at gas pumps or ATM machines to collect card data.	

Course Coordinator:
Ms. J Alekhya, Assistent Professor

HOD CSE(CS)