GUJARAT TECHNOLOGICAL UNIVERSITY

COMPUTER ENGINEERING (SYSTEMS AND NETWORK SECURITY) (56)

CYBER SECURITY
SUBJECT CODE: 2725602
SEMESTER: II

Type of course: Foundation/Core

Prerequisite: Basic knowledge of Computer Networking, Web Application and File Structures.

Rationale: To understand the major concepts of Cyber Security and Forensics, and to educate the students for learning of how to avoid becoming victims of cyber crimes. The subject and the course content will help to the student who wish to take up cyber forensics as career as well as those who want to seek careers in cyber security and to gain experience of doing independent study and research in the field of cyber security and cyber forensics.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks						Total Marks
L	T	P	C	Theory Marks		Practical Marks				
				ESE (E)	PA (M)	ESE (V)		PA (I)		
						ESE	OEP	PA	RP	
3	2#	2	5	70	30	20	10	10	10	150

Course Content:

Sr. No.	Topics	Teaching Hrs.	Module Weightage
1.	Introduction to Cyber Crimes: Definition and evolution of Cyber Crimes, Cybercrime and Information Security, Classifications of Cybercrimes: – Hacking, E-Mail Spoofing, Spamming, Cracking, Forgery, Virus Attacks, Software Piracy, Intellectual property, E-Mail Bombing/Mail Bombs, Network Intrusions, Password Sniffing, Credit Card Frauds. Tools and Methods Used in Cybercrime. Case Study: Real world examples of all the crimes mentioned.	5	15
2.	Cyber Forensics : Introduction to Cyber Forensics, Cyber Security & Cyber Forensics, Cyber Forensics and Digital Forensics, Forensic Investigation process, Phases in Computer Forensics/Digital Forensics, Taxonomy of Computer Crime scene, Investigation Tools, Incident Notification Checklist	7	20
3.	**Importance of Data and Evidence Recovery in Cyber Forensics:** Role of Evidences in Cyber forensics, Evidence detection and preservation, Introduction to Deleted File Recovery, Formatted Partition Recovery, Data	8	20

	Recovery Tools, Time line analysis of file modification and file access, Recover Temporary Files or Cache Files.		
4.	**Cyber Security PART-I**: **Cyber Security Fundamentals:** Introduction to Cyber Security, Network & Security Concepts: Authentication, Authorization, NonRepudiation, Integrity, Basic Cryptography, Encryption Techniques, Firewalls, Fraud Techniques, Malicious Code, Defense and analysis techniques	10	30
5.	**Cyber Security PART-II: Cyber Security Policy:** Cyber Security Policy Taxonomy: Cyber Governance Issues, Cyber User Issues, Cyber Conflict Issues, Cyber Management Issues, Cyber Infrastructure Issues	5	15

Reference Books:

1. Nina Godbole, Sunit Belapur, “Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives”, Wiley India Publications, April, 2011
2. James Graham, Richard Howard, Ryan Olsan, “Cyber Security Essentials” CRC Press
3. Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, “Cyber Security Policy Guidebook” Wiley Publications
4. Albert J. Marcella, Jr. Doug Menendez ”CYBER FORENSICS: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes”, Auerbach Publications
5. Robert Jones, “Internet Forensics: Using Digital Evidence to Solve Computer Crime”, O’Reilly Media, October, 2005

Course Outcome:

After successful completion of the course, student will be able to

- Understand the categories of cyber crimes and to know basics of cyber forensics and security.
- Realize the activities carried using forensic technologies in detection of cyber crime.
- Introduce a novel methodology of performing cyber forensics or system forensics.
- Assess how the digital evidences will be handled in any crime scene.

List of Experiments/Tutorials:

1. Discuss the Email Based crime investigation scenario with the Investigation steps.
2. Elaborate any real world case of credit-card fraud with the applicable laws and intended users’ motivation.
3. Consider any real world case of Hacking of an Email Account with the applicable laws and sections.
4. Discuss the online scams of Foreign Country Visit Bait, Lottery Scam and Fake Job Offer Scam.

Open Ended Problems:

1. Case Study of Cyber Law: NASSCOM vs. Ajay Sood & Others.

2. Case Study of any real world scenario of Theft of Confidential Information like source code of software or password etc.
3. Case Study of : “Justice” vs. “Justice”: Software Developer Arrested for Launching Website Attacks

Major Equipments:
Desktop, Laptop

Review Presentation (RP): The concerned faculty member shall provide the list of peer reviewed Journals and Tier-I and Tier-II Conferences relating to the subject (or relating to the area of thesis for seminar) to the students in the beginning of the semester. The same list will be uploaded on GTU website during the first two weeks of the start of the semester. Every student or a group of students shall critically study 2 papers, integrate the details and make presentation in the last two weeks of the semester. The GTU marks entry portal will allow entry of marks only after uploading of the best 3 presentations. A unique id number will be generated only after uploading the presentations. Thereafter the entry of marks will be allowed. The best 3 presentations of each college will be uploaded on GTU website.