Uka Tarsadia University

BCA

Introduction to Cyber Security (030010504)

5th Semester

EFFECTIVE FROM JUNE-2013

UKA TARSADIA UNIVERSITY			
BCA (5th Semester) Syllabus, 2014-2015			
Course Code: 030010504		Course Title: Introduction to Cyber Security	
Course Credits: 04	Total Hours: 48	[Lectures: 04, Tutorial: 00, Practical: 00]	
Prerequisites:	030010305 – Foundations of computer security		
Prerequisites By Topics:	Vulnerabilities and backup strategies, password and its failures		
Objectives:	To understand the fundamentals of cyber security and cyber offenses, be familiar with cybercrime techniques and prevention through cyber laws, gain knowledge of cyber forensics and the security mechanisms		

1	Introduction		[06 Hours]
	1.1.	Terminologies : Cyberspace, Cybercrime, Cybersecurity, Cybersquatting, Cyberpunk, Cyberwarfare, Cyberterorrism	
	1.2.	Cybersecurity Needs	
	1.3.	Cyber Criminals : Introduction, Cybercriminals Groups	
	1.4.	Classification Of Cyber Crimes	
	1.5.	Cybercrime Categories	
	1.6.	Cybercrime : The Legal Perspective	
2	Cyberoffenses		[08 Hours]
	2.1.	Hackers, crackers, phreakers : Introduction	
	2.2.	Planning cybercrime	
	2.3.	Social engineering	
	2.4.	Cyberstalking	
	2.5.	Cybercafe and cybercrime	
	2.6.	Attack vector	
	2.7.	Botnets	
3	Cybercrime Techniques		[10 Hours]
	3.1.	Proxy servers and Anonymizers, phishing	
	3.2.	Password cracking	
	3.3.	Keyloggers and spywares	
	3.4.	Virus and worms	
	3.5.	Trojan horse and backdoors	
	3.6.	Steganography	
	3.7.	Dos and DDos attacks	
	3.8.	SQL injection	
	3.9.	Buffer overflow	
4	Phishing and Identity Theft		[09 Hours]
	4.1.	Phishing : Introduction	
	4.2.	Phishing methods : Dragnet, Rod-and-reel , Lobsterpot, Gillnet	
	4.3.	Techniques of phishing	
	4.4.	Phishing Toolkits and Spy Phishing	
	4.5.	Phishing countermeasures	
	4.6.	Personally Identifiable Information (PII)	
	4.7.	Types of Identity theft	
	4.8.	Techniques of Identity theft	
	4.9.	Identity Theft Countermeasures	
5	Legal Perspectives of Cyber Security & Forensic Fundamentals		[08 Hours]
	5.1.	Need for cyber laws: The Indian context	
	5.2.	Indian IT Act 2000	
	5.3.	Changes made in IT Act 2000	
	5.4.	Digital signatures and the Indian IT Act	
	5.5.	Cybercrime and punishment	
	5.6.	Cyberforensics : introduction,types	
	5.7.	Needs of cyberforensics	

	5.8.	Cyberforensicsand digital evidence	
6	Cyber Security: Organization Implications		[07 Hours]
	6.1.	Search Breach: PI Collecting by Organization, Insiders threats in Organization	
	6.2.	Privacy Dimension	
	6.3.	Key-challenges in Organization	
	6.4.	Cost of cyber crimes and IPR issues	
	6.5.	Organizational guidelines for Internet usage, safe computing guidelines and computer usage policy	
	6.6.	Forensics best practices for organization	

Course Outcomes:

CO1:	Understand the basic concept of cybersecurity
CO2:	Understand cyberoffenses
CO3:	Aware of cybercrime techniques and preventive measures
CO4:	Recognize cyber laws in India
CO5:	Know about cyber forensics
CO6:	Analyse impact of cybercrime

Course Objectives and Course Outcomes Mapping:

Fundamentals of cybersecurityand cyberoffenses: CO1,CO2

Explore cybercrime techniques and prevention : CO2, CO3

Familiarize cyber laws, cyberforensics and the security mechanisms: CO4, CO5,CO6

Course Units and Course Outcomes Mapping:

Unit No.	Unit	Course Outcome					
		CO1	CO2	CO3	CO4	CO5	CO6
1	Introduction to cybersecurity	✓					
2	Cyberoffenses	✓	✓				
3	Cybercrime techniques		✓	✓			
4	Phishing and Identity theft		✓	✓			
5	Legal Perspective of Cybersecurity& Forensics fundamentals		✓	✓	✓	✓	
6	Cyber Security: Organization Implications		✓	✓	✓	✓	✓

Modes of Transaction (Delivery):

❖ **Lecture method** shall use along withdiscussion method. It shall be supplemented with appropriate audio-visual aids.

Activities/Practicum:

The following activities shall be carried out by the students.

❖ Give seminar on assigned topics

- ❑ Teacher shall form the groups of students during the 4th week.
- ❑ Seminar titles and respective student groups shall be placed on website after approval of Course Coordinator on website in the 5thweek of the semester.
- ❑ Students shall work in team and following points shall be followed:
  - o Each team shall have different seminar topics.
  - o A team shall consist of at the most 5 and not less than 3 members.
  - o After6th week, student give seminarof given topic.
- ❑ Seminar topic shall be related to cyber security and approved by teacher. Seminar topic can be like

listed but not restricted to:

- Email spoofing
- Spamming
- cyber defamation
- Internet time theft
- Salami attack
- Data diddling
- Forgery
- Web jacking
- Newsgroup spam
- Industrial spying
- Hacking
- Online fraud
- Pornographic offenses
- Software piracy
- Computer sabotage
- Email bombing
- Usenet newsgroup
- Computer network intrusions
- Password sniffing
- Credit card frauds
- Identity theft

The following activities shall be carried out by the teacher.

- ❖ Demonstration regarding proxy servers and anonymizers, phishing, keyloggers and spywares, steganography, SQL injection.

Text Book:

1. Nina Godhbole, SunitBelapure - Cyber Security understanding Cyber Crimes, Computer Forensics and Legal Perspectives - Wiley India

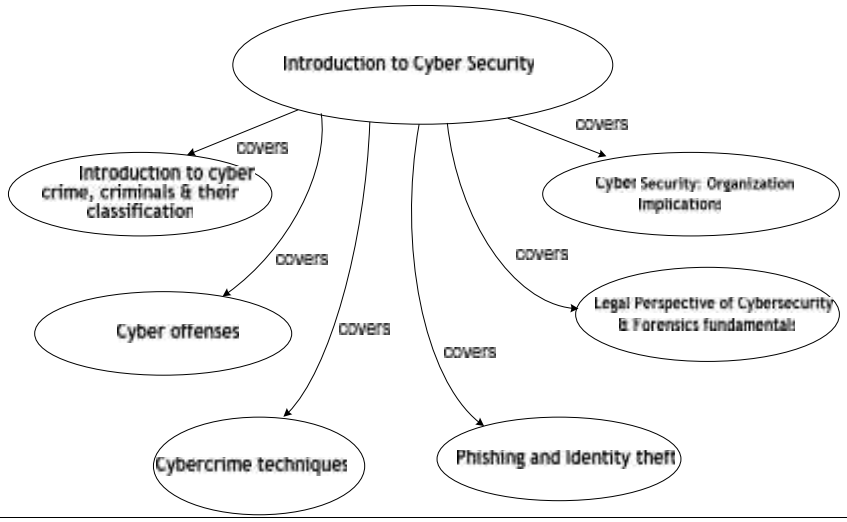
Reference Books:

1. Marjie T. Britz - Computer Forensics and Cyber Crime: An Introduction - Pearson
2. Alfared Basta and Wolf Holten - Computer Security Concepts, Issues and Implementation - CENGAGE learning
3. Raghu Santanam, M. Sethumadhavan, Mohit Virendra - Cyber Security, Cyber Crime and Cyber Forensics - IGI Global
4. George M. Mohay, Alison Anderson - Computer and Intrusion Forensics - Artech House

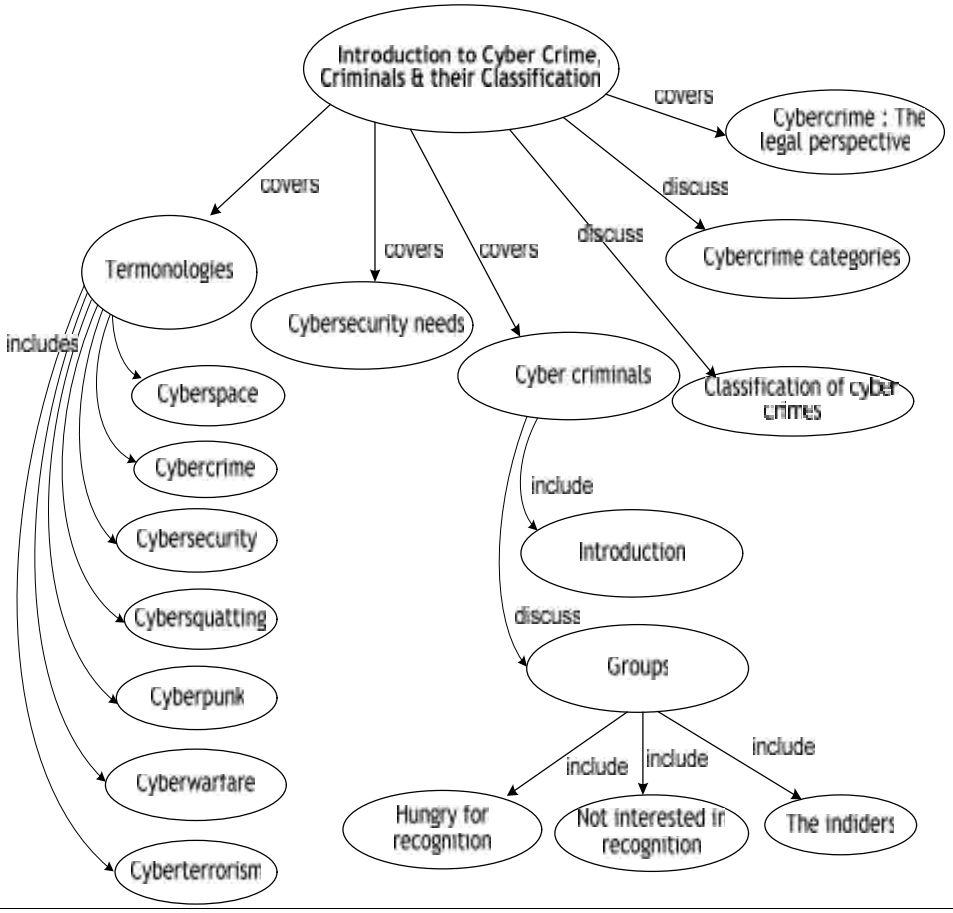
Concept Map:

It is a hierarchical / tree based representation of all topics covered under the course. This gives direct / indirect relationship /association among topics as well as subtopics.

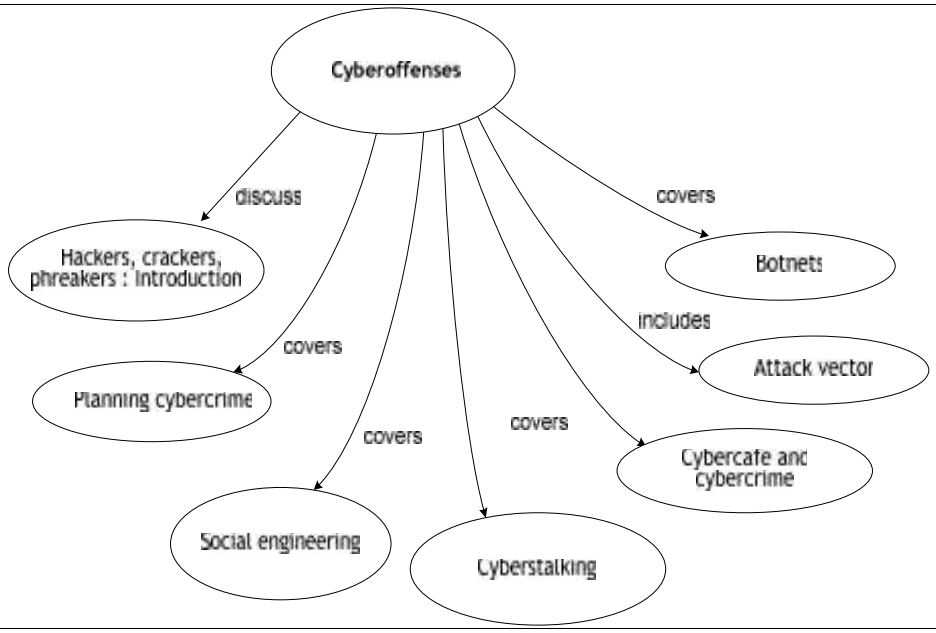
Introduction to Cyber Security



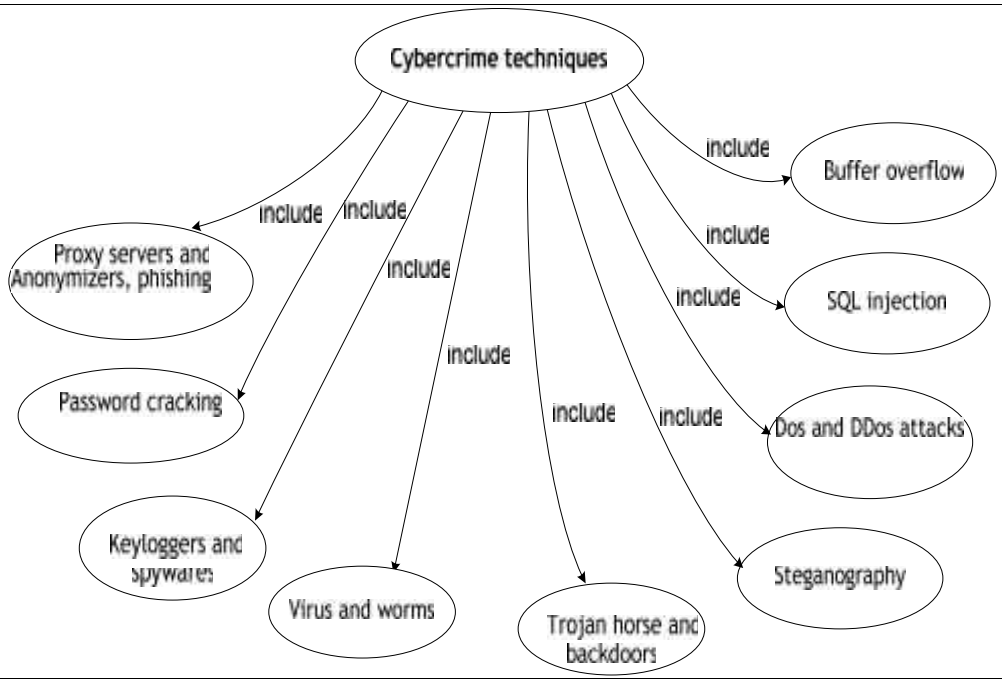
Unit-1: Introduction to Cyber Security



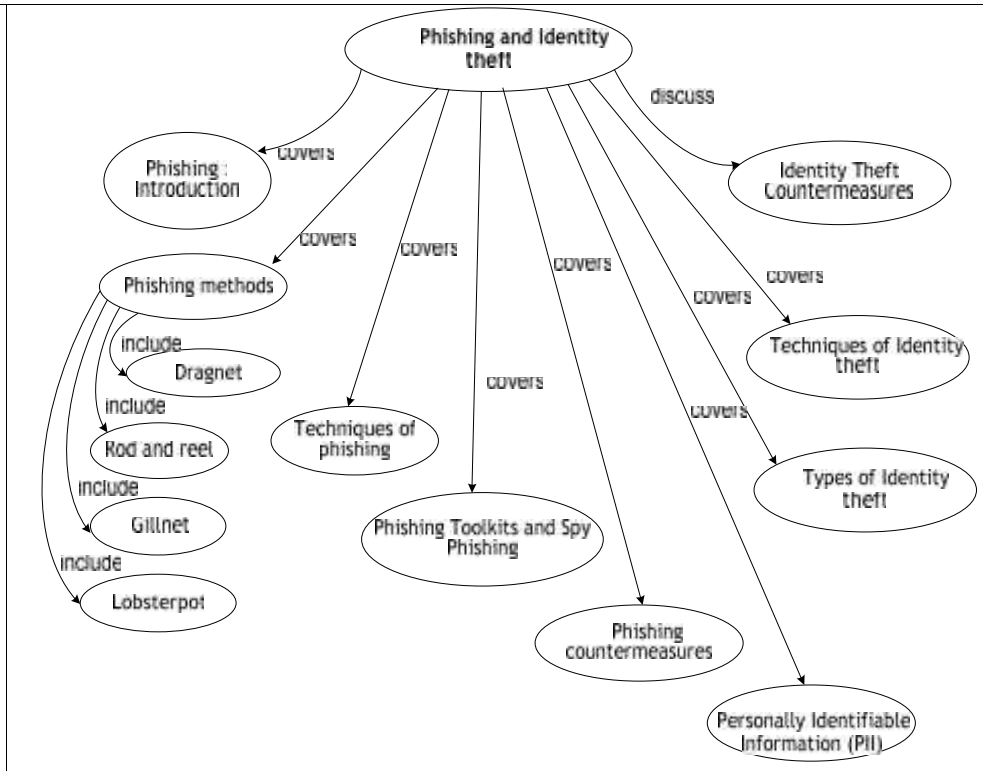
Unit-2: Cyberoffenses



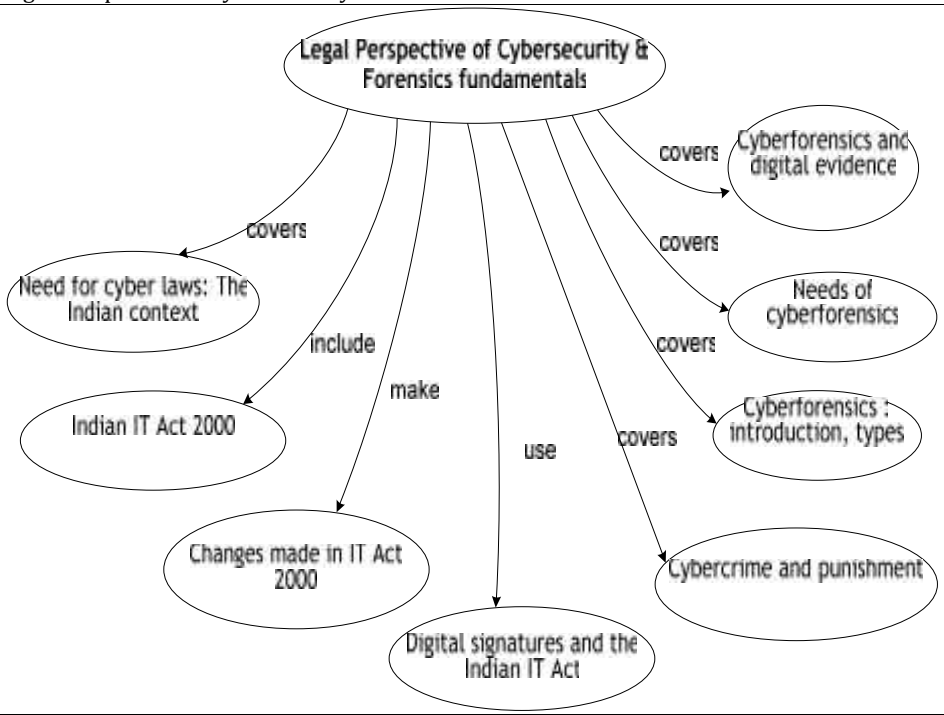
Unit-3: Cybercrime Techniques



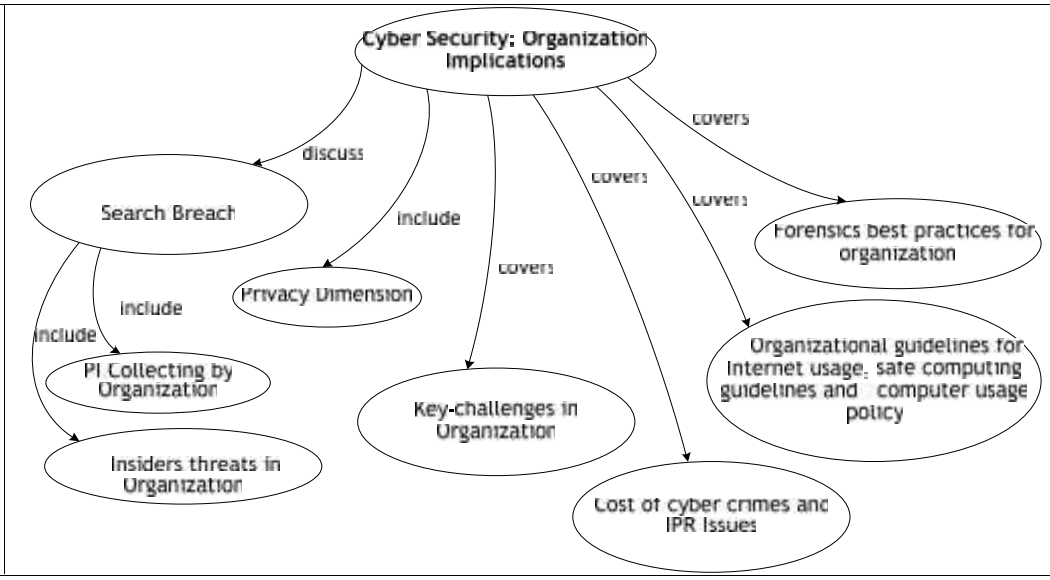
Unit-4: Phishing and Identity Theft



Unit-5: Legal Perspective of Cybersecurity & Forensics fundamentals



Unit-6: Cyber Security : Organization Implications



Assessment:

The weightage of CIE and University examination shall be as per the University regulations.

Composition of CIE shall be

Assessment Code	Assessment Type	Duration of each	Occurrence	Each of marks	Weightage in CIE of 40 marks	Remarks
A1	Quiz	45mins	2	20	4X2 = 8	Taken at the end of unit 1,5,6
A2	Unit Test	45mins	3	25	4X3 = 12	Taken at the end of unit 2,3,4
A3	Seminar(including viva)	15 mins	1	10	5 X 1 = 5	Give seminar after 6th week
A4	Internal Exam	2 hrs.	1	50	15 X 1 = 15	Before completion of the term

- ❖ The teams shall be allowed to give seminar of typically minimum 10 minutes and maximum 15 minutes followed by Question – Answer session.
- ❖ Syllabus for each CIE parameter shall be covered by the date of the corresponding test.
- ❖ No make-up work shall be accepted for missed or failed tests.
- ❖ Student may receive 5% bonus points for active participation during the seminar.
- ❖ Late seminar shall be penalized as 5% of full marks per day for maximum two days after the cut-off date. No seminar shall be accepted thereafter with the corresponding mark set to 0.

Course Assessment with Course Outcomes Mapping

Assessment	Course Outcomes				
	CO1	CO2	CO3	CO4	CO5
A1	✓		✓	✓	✓
A2		✓			
A3	✓	✓			
A4	✓	✓	✓	✓	✓

Question Bank:

Question Bank shall be prepared which consists ofMultiple Choice Questions, fill in the blanks, short type

	questions,long type questions.
Academic Honesty:	
	Coursework is assumed to be accomplished individually (otherwise stated). Any portion of submission taken directly from anywhere (like statements in assignment/report etc.) without modification shall be accompanied with the properly formatted reference giving credit to the author and to the source.
UFM:	
	❖ Any ascertained fact of breaking institute policy shall be associated with one or all of the following: (i) zero marks for the work; (ii) report to the Course coordinator; (iii) report to the Director; (iv) report to parents.
Discussion Group:	
	Students are welcome to post on the Course Discussion Board available on SRIMCA View Course Webpage. It is responsibility of the concern subject teacher to maintain Discussion Board.
Attendance:	
	❖ Attendance means being present for the entire class session. Those arriving significant late or leaving significantly early without prior permission shall be counted as ABSENT for the entire class session. ❖ Concern teacher shall clearly state his/her attendance policies at the first class meeting.