Five Years Integrated M.Sc. (IT)
Semester 7

060010708 – Network Security

Objective: To help the students design and develop secure solution to provide confidentiality and integrity, user authentication, secure network and transport layer communication, secure wireless communication, defeat vulnerabilities and electronic payment.

Course Outcomes:

Upon the completion of the course, students will be able to

CO1: Identify and inspect vulnerabilities and defense strategies of attacks on a network
CO2: Describe protocols at network layer and application layer
CO3: Comprehend and categorize authentication measures.
CO4: Identify and compare mechanisms for secure communications at network and transport layer
CO5: Describe security measures for wireless and cell phone communications
CO6: Define the basics of RFID, E-passport and electronic payment

UNIT	Sub Unit	No. of Lecture	Topics	Reference Chapter/ Additional Reading	Methodology to be used	Planned Date	Actual Date	Evaluation Parameters
1		**7**	**Introduction of Network Security**			**7/7/14**		
	1.1	2	Cyber Attacks	BM#1, Page no. 1-5	PowerPoint Presentation	**9/7/14 – 10/7/14**		
	1.2	1	Defense Strategies and Techniques	BM#1, Page no. 5-7	PowerPoint Presentation	**11/7/14**		
	1.3		Guiding Principles	BM#1, Page no. 8-11	PowerPoint Presentation			**Quiz 1**
	1.4	1	Local Area Networks	BM#2, Page no. 14-16	PowerPoint Presentation + Discussion	**14/7/14**		
	1.5	2	Network Layer Protocols	BM#, Page no. 16-19	PowerPoint	**16/7/14 –**		

					Presentation Discussion	**17/7/14**		
	1.6	1	The Transport Layer	BM#1, Page no. 19-23	Discussion + Chalk and Talk	**18/7/14**		
	1.7	1	Application Layer Protocols	BM#1, Page no. 23-26	PowerPoint Presentation	**21/7/14**		
2		**8**	**Authentication**					
	2.1	3	One-way Authentication	BM#11, Page no. 154-157	PowerPoint Presentation	**23/7/14-24/7/14**		**Unit Test 1**
	2.2		Mutual Authentication	BM#11, Page no. 157 - 161	PowerPoint Presentation + Chalk and Talk	**28/7/14**		
	2.3	1	Dictionary Attacks	BM#11, Page no. 161-163	PowerPoint Presentation	**30/7/14**		
	2.4		Centralized Authentication	BM#12, Page no. 167-168	PowerPoint Presentation			
	2.5	2	The Needham-Schroeder Protocol	BM#12, Page no. 168-172	Chalk and Talk + discussion	**31/7/14 – 1/8/14**		
	2.6	1	Kerberos	BM#12, Page no. 172-174	PowerPoint Presentation	**7/8/14**		
	2.7	1	Biometric	BM#12, Page no. 175-183	PowerPoint Presentation	**8/8/14**		
3		**9**	**Security at Network Layer and Transport Layer**					
	3.1	2	Security at Different Layers: Pros and Cons	BM#13, Page no. 187	PowerPoint Presentation	**11/8/14**		**Quiz 2**
	3.2		IPSec in Action	BM#13, Page no. 188-191	Chalk and Talk + Video Demonstration	**13/8/14**		
	3.3	3	Internet Key Exchange (IKE) Protocol	BM#13, Page no. 192-197	Chalk and Talk + PowerPoint Presentation + Video Demonstration	**14/8/14, 18/8/14-20/8/14**		

	3.4	1	Security Policy and IPSec	BM#13, Page no. 197-198	PowerPoint Presentation	**21/8/14**		
	3.5		Virtual Private Networks	BM#13, Page no. 198	PowerPoint Presentation			
	3.6	2	SSL Handshake Protocol	BM#14, Page no. 201-204	PowerPoint Presentation + Chalk and Talk	**22/8/14 – 25/8/14**		
	3.7	1	SSL Record Protocol	BM#14, Page no. 205	PowerPoint Presentation	**27/8/14**		
	3.8		OpenSSL	BM#14, Page no. 205	PowerPoint Presentation			
4		**7**	**Wireless and Cell Phone Security**					
	4.1	1	IEEE 802.11 Wireless LAN	BM#15, Page no. 208-211	PowerPoint Presentation	**28/8/14**		**Unit Test 2**
	4.2	1	Authentication	BM#15, Page no. 211-214	PowerPoint Presentation + Chalk and Talk	**1/9/14**		
	4.3	2	Confidentiality and Authentication	BM#15, Page no. 215-219	PowerPoint Presentation + Chalk and Talk	**3/9/14 - 4/9/14**		
	4.4	1	Cellphone Security	BM#16, Page no. 222-224	PowerPoint Presentation	**11/9/14**		
	4.5		GSM (2G) Security	BM#16, Page no. 224-226	PowerPoint Presentation			
	4.6	2	Security in UMTS (3G)	BM#16, Page no. 227-230	Discussion + Chalk and Talk	**12/9/14**		
5		**8**	**Vulnerabilities**					
	5.1	1	DoS and DDoS	BM#17, Page no. 233-236	Demonstration	**15/9/14**		**Group Activity –Assignment on summary report of network security toolkits**
	5.2		Session Hijacking and Spoofing	BM#17, Page no. 236-239	Chalk and Talk + Demonstration			
	5.3	2	Pharming Attacks	BM#17, Page no. 239-243	PowerPoint Presentation + Discussion	**17/9/14 - 18/9/14**		

	5.4	1	Wireless LAN Vulnerabilities	BM#17, Page no. 243-246	PowerPoint Presentation	**19/9/14**		
	5.5		Phishing	BM#18, Page no. 251-252	PowerPoint Presentation			
	5.6	2	Buffer Overflow	BM#18, Page no. 252-260	Chalk and Talk + Demonstration	**22/9/14, 24/9/14**		
	5.7	1	Format String Attacks	BM#18, Page no. 260-262	PowerPoint Presentation + Chalk and Talk	**25/9/14**		
	5.8		Cross-site Scripting (XSS)	BM#18, Page no. 262-264	PowerPoint Presentation + Chalk and Talk			
	5.9	1	SQL Injection	BM#18, Page no. 264-268	PowerPoint Presentation	**26/9/14**		
6		**9**	**RFID, E-Passport and Electronic Payment**					
	6.1	1	RFID and Its Applications	BM#23, Page no. 356-358	PowerPoint Presentation	**29/9/14**		
	6.2		Security Issues	BM#23, Page no. 358-359	PowerPoint Presentation			
	6.3	2	Generation 2 Tags: A Case Study	BM#23, Page no. 359-363	PowerPoint Presentation + Discussion	**1/10/14, 8/10/14**		
	6.4	1	Addressing RFID Privacy Concerns	BM#23, Page no. 363-367	Chalk and Talk	**9/10/14**		
	6.5	1	Electronic Passports	BM#23, Page no. 367-371	PowerPoint Presentation	**10/9/14**		
	6.6	1	Electronic Payment	BM#24, Page no. 374-375	PowerPoint Presentation	**13/10/14**		
	6.7		Enabling Technologies	BM#24, Page no. 375-377	PowerPoint Presentation			
	6.8	1	Cardholder Present E-Transactions	BM#24, Page no. 378-381	PowerPoint Presentation + Chalk and Talk	**20/10/14**		
	6.9	1	Payment Over the Internet	BM#24, Page no. 381-	PowerPoint	**22/10/14**		

				386	Presentation + Chalk and Talk			
	6.10	1	Mobile Payment and Electronic Cash	BM#24, Page no. 387-390	PowerPoint Presentation	**27/10/14**		
		Text Book						
1.		Bernard Menezes - Network Security and Cryptography- Cengage Learning.						
		Reference Book						
1.		Straub, Detmar W., Goodman, Seymour, Baskerville, Richard L. - Information Security : Policy, Processes, and Practices – PHI						
2.		Eric Cole - Network Security Bible - Wiley.						
3.		Behrouz A. Forouzan, Debdeep Mukhopadhyay - Cryptography and Network Security - McGraw Hill						
4.		William Stallings - Cryptography and Network Security - Pearson Education						

Course Objectives and Course Outcomes Mapping:

To provide confidentiality and integrity and authentication: CO1, CO3
To provide basic understanding of protocols and mechanisms for secure communications: CO2, CO4
To recognize techniques for secure wireless communication: CO5
To defeat vulnerabilities and secure electronic payment: CO6

Course Units and Course Outcomes Mapping:

Unit No.	Unit	Course Outcome					
		CO1	CO2	CO3	CO4	CO5	CO6
1	Introduction to Network Security	✓	✓				
2	Authentication			✓			
3	Security at Network Layer and Transport Layer		✓		✓		
4	Wireless and Cellphone Security					✓	
5	Vulnerabilities	✓					
6	RFID, E-Passport and Electronic						✓

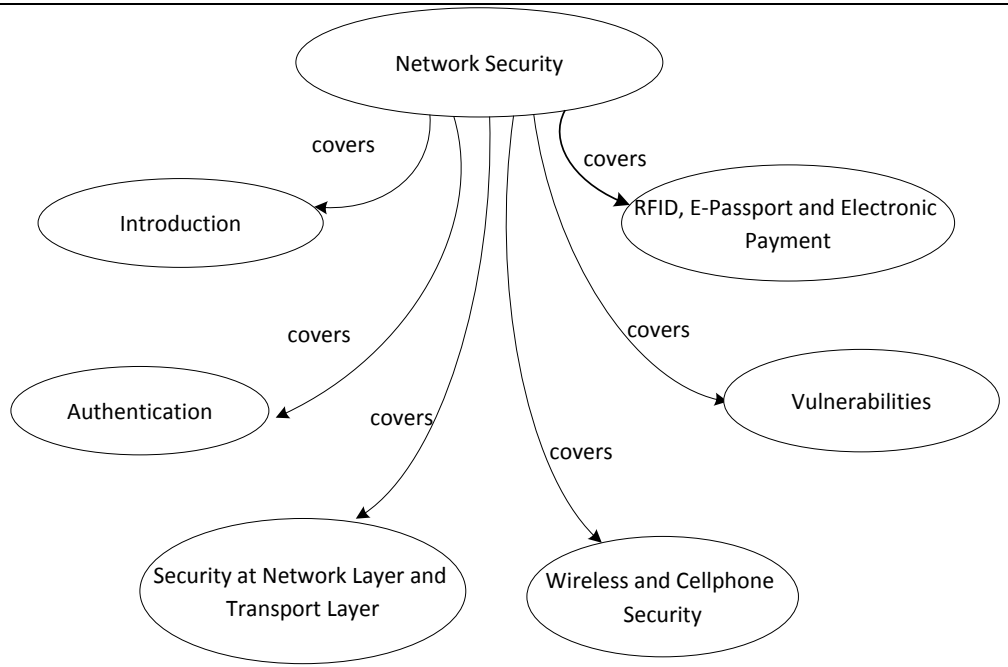
	Payment						

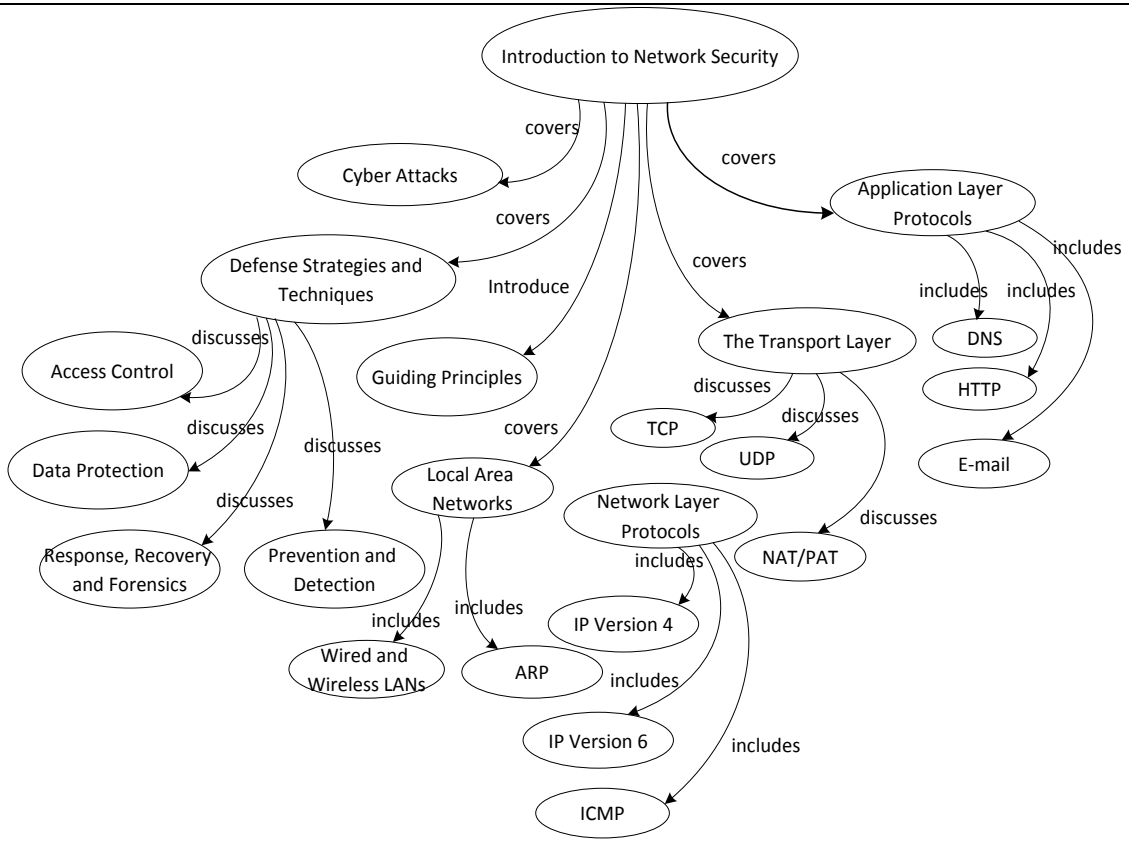
Course Outcomes and Program Outcomes Mapping:

Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6
CO1	✓		✓	✓	✓	
CO2	✓			✓		
CO3	✓	✓		✓		
CO4	✓	✓		✓		
CO5		✓		✓	✓	
CO6	✓		✓		✓	

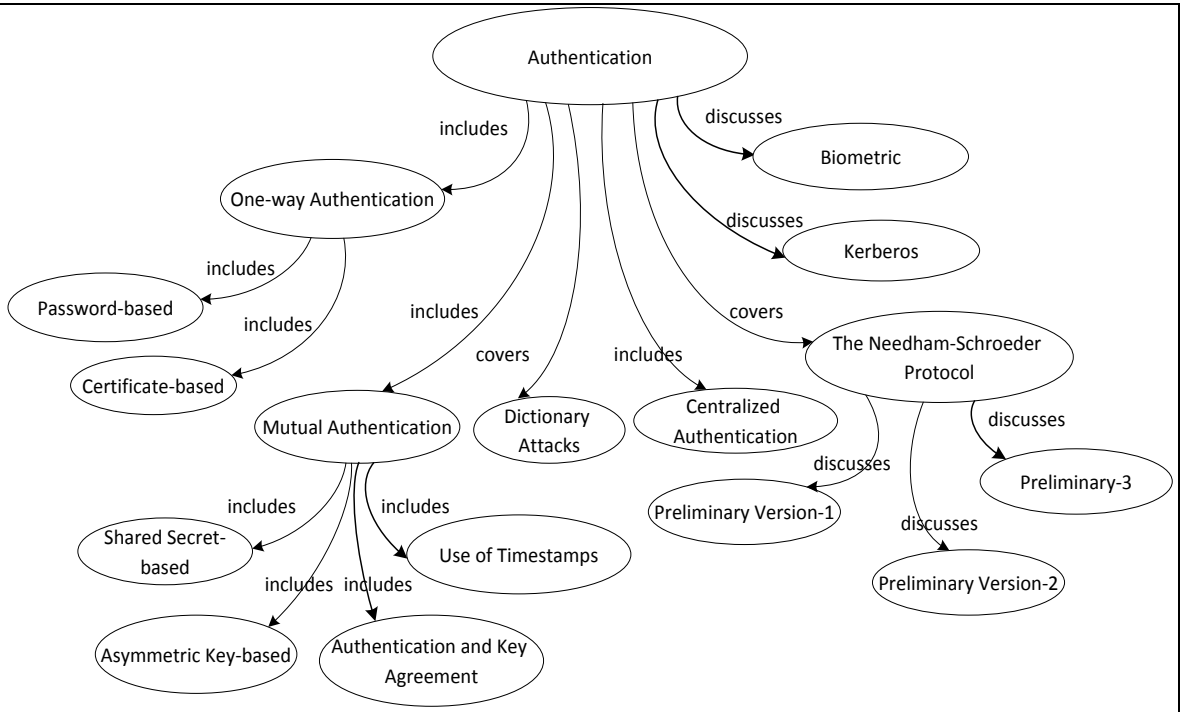
Activities/Practicum:

	The following activities shall be carried out by the students.	
	❖	Study cyber attacks such as : Email bombing ,Salami attack ,Logic bomb
	❖	Students will install WireShark on their laptops and analyse packets on the internet, after completion of the 1st unit.
	The following activities shall be carried out by the teacher.	
	❖	Demonstration on Wireshark Toolkit
	❖	Demonstration of Metasploit Toolkit
Hands-on Experience Activity:		
	❖	The students shall be working on security toolkit – Wireshark on their individual laptops.
Modes of Transaction (Delivery):		
Lecture methods will be used for most of the topics in all the units. Demonstration method will be used for IPSec in action(unit 3), IKE protocol(unit 3), Dos and DDOS attacks (unit 5) , session hijacking (unit 5) and buffer overflow(unit 5),		
Text Book:		

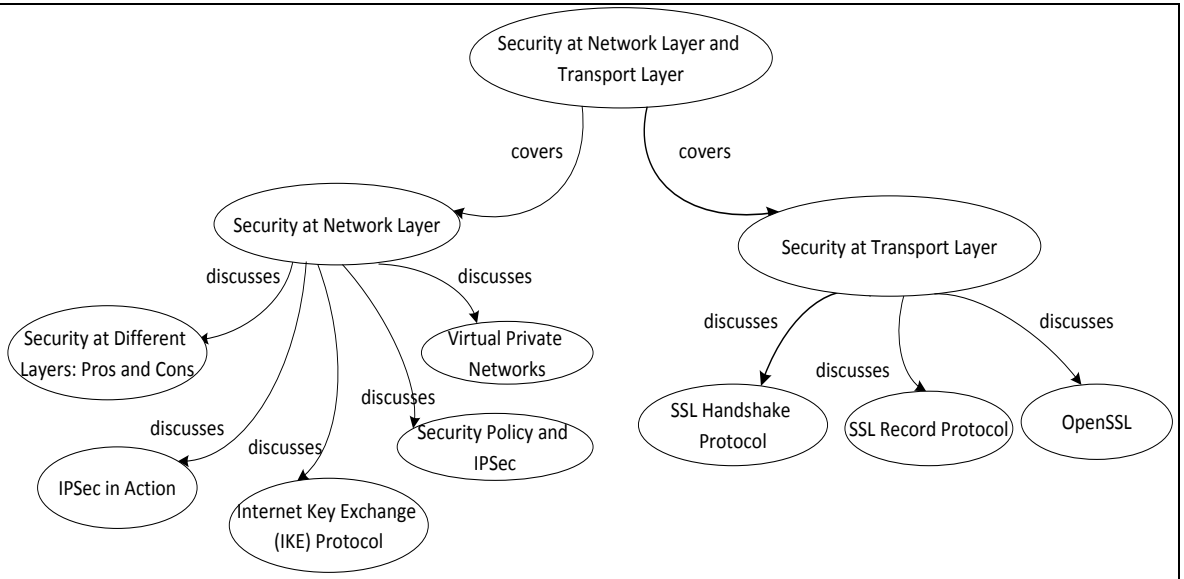
	1.	Bernard Menezes - Network Security and Cryptography- Cengage Learning.
Reference Books:		
	5.	Straub, Detmar W., Goodman, Seymour, Baskerville, Richard L. - Information Security : Policy, Processes, and Practices – PHI
	6.	Eric Cole - Network Security Bible - Wiley.
	7.	Behrouz A. Forouzan, Debdeep Mukhopadhyay - Cryptography and Network Security - McGraw Hill
	8.	William Stallings - Cryptography and Network Security - Pearson Education
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.	
	Network Security	
		
	Unit-1: Introduction to Network Security	



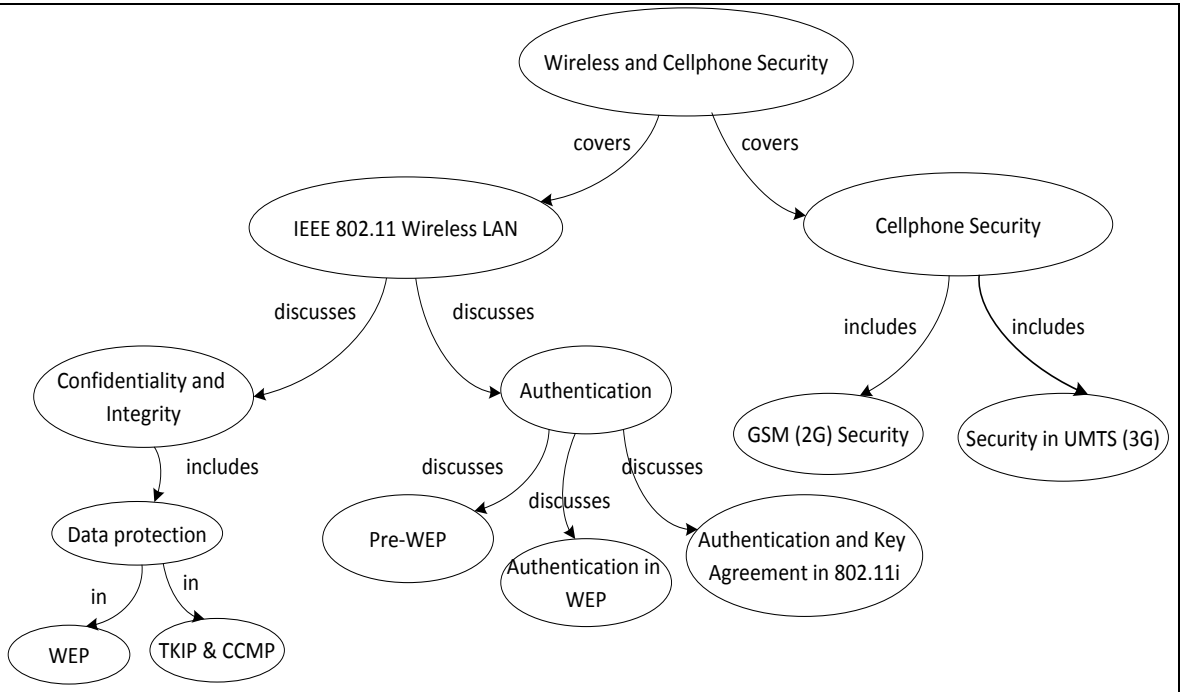
Unit-2: Authentication



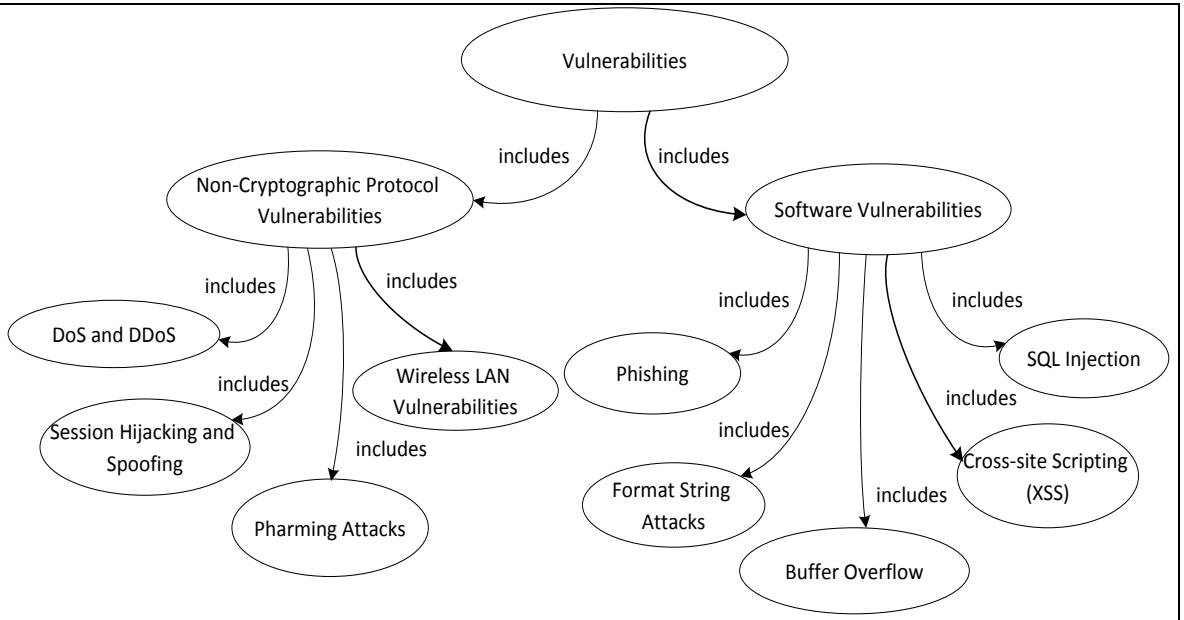
Unit-3: Security at Network Layer and Transport Layer



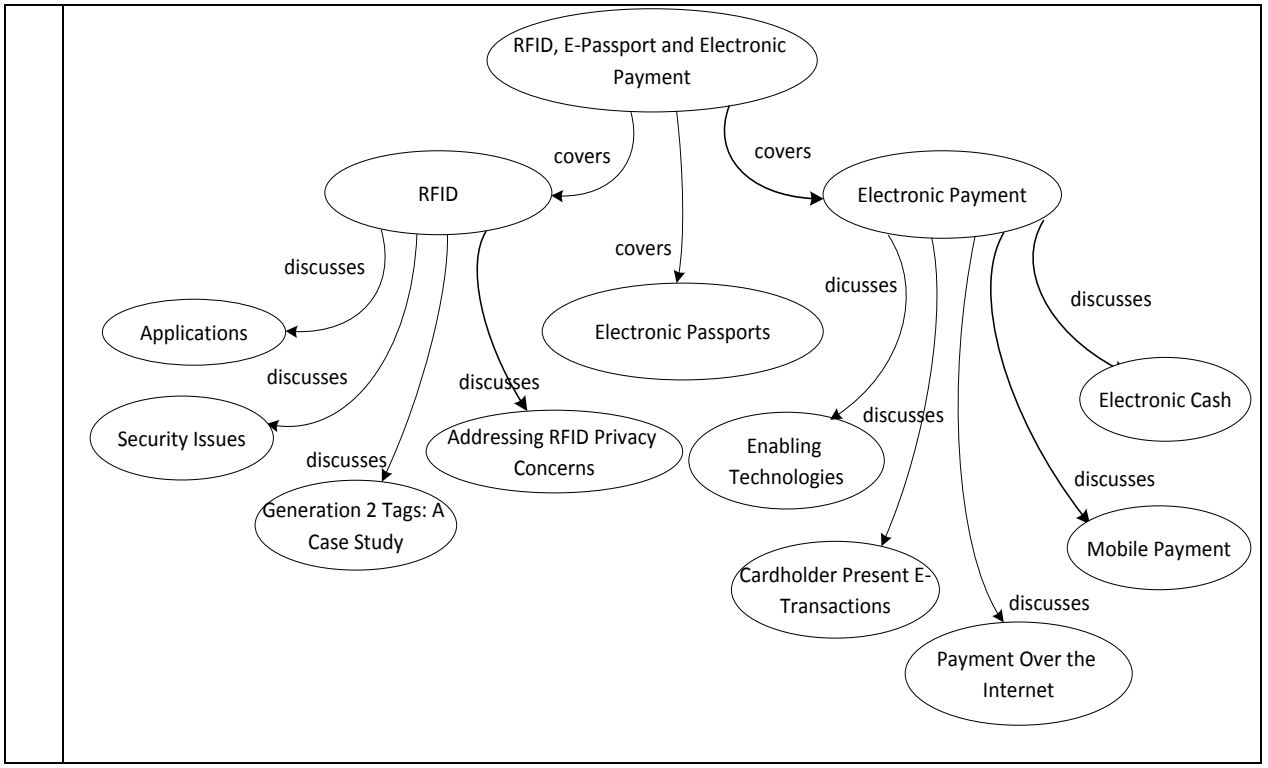
Unit-4: Wireless and Cellphone Security



Unit-5: Vulnerabilities



Unit-6: RFID, E-Passport and Electronic Payment


RFID, E-Passport and Electronic Payment
covers
covers
RFID
Electronic Payment
covers
discusses
dicusses
discusses
Applications
Electronic Passports
discusses
discusses
discusses
discusses
Security Issues
Addressing RFID Privacy Concerns
Enabling Technologies
Electronic Cash
discusses
discusses
Generation 2 Tags: A Case Study
Mobile Payment
Cardholder Present E-Transactions
discusses
Payment Over the Internet