M.Sc.(CA)(3rd Semester)

040020315: Network Security

Lesson Plan

Objective: Design and develop secure solution to provide confidentiality and integrity, user authentication, secure web and email communication, secure wireless communication, secure IP communication, attack tolerance using Intrusion Detection System and firewall.

Course Outcomes: Upon completion of the course, students shall be able to

CO1: Design solutions to provide confidentiality and integrity.
CO2: Develop solutions to provide user authentication.
CO3: Design secure web and email communication.
CO4: Create secure wireless communication.
CO5: Develop solutions based on secure IP communication.
CO6: Design secure network using Intrusion Detection System and firewall.

Unit	Sub Unit	No. of Lecture(s)	Topics	Reference Chapter/Additional Reading	Teaching Methodology to be used	Evaluation Parameters
Introduction to Network Security						
1	1.1	1	Computer Security Concepts	NE - #1 Page No. 3 – 8	Power Point Presentation	UNIT TEST-1
	1.2	1	The OSI Security Architecture	NE - #1 Page No. 8 – 9		
	1.3	1	Security Attacks, Services, and Mechanisms	NE - #1 Page No. 9 – 18		
	1.4	1	A Model for Network Security	NE - #1 Page No. 19 – 21		
	1.5	1	Standards	NE - #1 Page No. 21		
	1.6	2	Symmetric Encryption Principles	NE - #2 Page No. 28 – 34		
	1.7	1	Public-Key Cryptography Principles	NE - #3 Page No. 79 – 82		
	1.8	1	Introduction to Secure Hash Function and Digital Signature	NE - #3 Page No. 67 – 73, 90		

Key Distribution and User Authentication						
2	2.1	1	Symmetric Key Distribution Using Symmetric Encryption	NE - #4 Page No. 98 – 99	Power Point Presentation	QUIZ-1, UNIT TEST-1
	2.2	1	Kerberos	NE - #4 Page No. 98 – 114		
	2.3	1	Key Distribution Using Asymmetric Encryption	NE - #4 Page No. 114 – 116		
	2.4	1	X.509 Certificates	NE - #4 Page No. 116 – 124		
	2.5	1	Public-Key Infrastructure	NE - #4 Page No. 124 – 126		
	2.6	1	Federated Identity Management	NE - #4 Page No. 126 – 132		
Transport-Level Security and Email Security						
3	3.1	1	Web Security Considerations	NE - #5 Page No. 140 – 142	Power Point Presentation	QUIZ-1
	3.2	2	Secure Socket Layer and Transport Layer Security	NE - #5 Page No. 143 – 160		
	3.3	1	HTTPS	NE - #5 Page No. 160-162		
	3.4	1	Secure Shell (SSH)	NE - #5 Page No. 162-172		
	3.5	2	Pretty Good Privacy	NE - #7 Page No. 222-241		
	3.6	1	S/MIME	NE - #7 Page No. 241 – 257		
	3.7	1	Domain Keys Identified Mail	NE - #7 Page No. 257 – 264		
Wireless Network Security						
4	4.1	1	IEEE 802.11 Wireless LAN Overview	NE - #6 Page No. 177 – 182		

	4.2	2	IEEE 802.11i Wireless LAN Security	NE - #6 Page No. 182 –197	Power Point Presentation	UNIT TEST-2
	4.3	1	Wireless Application Protocol Overview	NE - #6 Page No. 197 – 204		
	4.4	2	Wireless Transport Layer Security	NE - #6 Page No. 204 – 214		
	4.5	1	WAP End-to-End Security	NE - #6 Page No. 214 – 217		
IP Security						
5	5.1	1	IP Security Overview	NE - #8 Page No. 270 – 276	Power Point Presentation	UNIT TEST-2
	5.2	1	IP Security Policy	NE - #8 Page No. 276 – 281		
	5.3	1	Encapsulating Security Payload	NE - #8 Page No. 281 – 288		
	5.4	1	Combining Security Associations	NE - #8 Page No. 288 – 292		
	5.5	2	Internet Key Exchange	NE - #8 Page No. 292 – 300		
	5.6	1	Cryptographic Suites	NE - #8 Page No. 301 – 302		
Intruders and Firewalls						
6	6.1	1	Intruders	NE - #9 Page No. 307 – 311	Power Point Presentation	
	6.2	1	Intrusion Detection	NE - #9 Page No. 312 – 323		
	6.3	1	Password Management	NE - #9 Page No. 323 – 332		
	6.4	1	The Need for Firewalls	NE - #11 Page No. 375 – 376		
	6.5	1	Firewall Characteristics	NE - #11 Page No.		

				376 – 377		
	6.6	2	Types of Firewalls	NE - #11 Page No. 378 – 385		
	6.7	1	Firewall Basing	NE - #11 Page No. 385 – 388		
	6.8	2	Firewall Location and Configurations	NE - #11 Page No. 388 – 392		

References:

1. William Stallings (2011). Network Security Essentials: Applications and Standards, Pearson Education. [NE]
2. AtulKahate (2010). Cryptography and Network Security, McGraw Hill [CNM]

Course objectives and Course outcomes mapping:

To design and develop secure solution to provide confidentiality and integrity, user authentication : CO1, CO2
Secure web and email communication, secure wireless communication : CO3,CO4
Secure IP communication, attack tolerance using Intrusion Detection System and firewall : CO5,CO6

Course units and Course outcomes mapping:

Unit No.	Unit	Course outcome					
		CO1	CO2	CO3	CO4	CO5	CO6
1	Introduction to Network Security	✓					
2	Key Distribution and User Authentication	✓	✓				
3	Transport-Level Security and EmailSecurity	✓	✓	✓			
4	Wireless Network Security	✓	✓	✓	✓		
5	IP Security	✓	✓	✓	✓	✓	
6	Intruders and Firewalls		✓	✓	✓	✓	✓

Course outcomes and Programme outcomes mapping:

Course	Program Outcomes

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

Computing Environment:
A student shall implement any cryptography algorithm which is covered in the course in any programming language on their personal laptop.

Modes of Transaction (Delivery)
Appropriate methods of teaching shall be decided depending on the objectives of the content taught.

- ❑ Lecture method is generally used but along with it, as and when required, discussion method shall be fruitful. It shall be supplemented with various appropriate audio-visual aids.
- ❑ Seminar topics shall be used to teach in-depth view of unit 2, 3, 4 and 5.

Activities/Practicum:

The following activities shall be carried out by the students.

The following activities shall be carried out by the students.

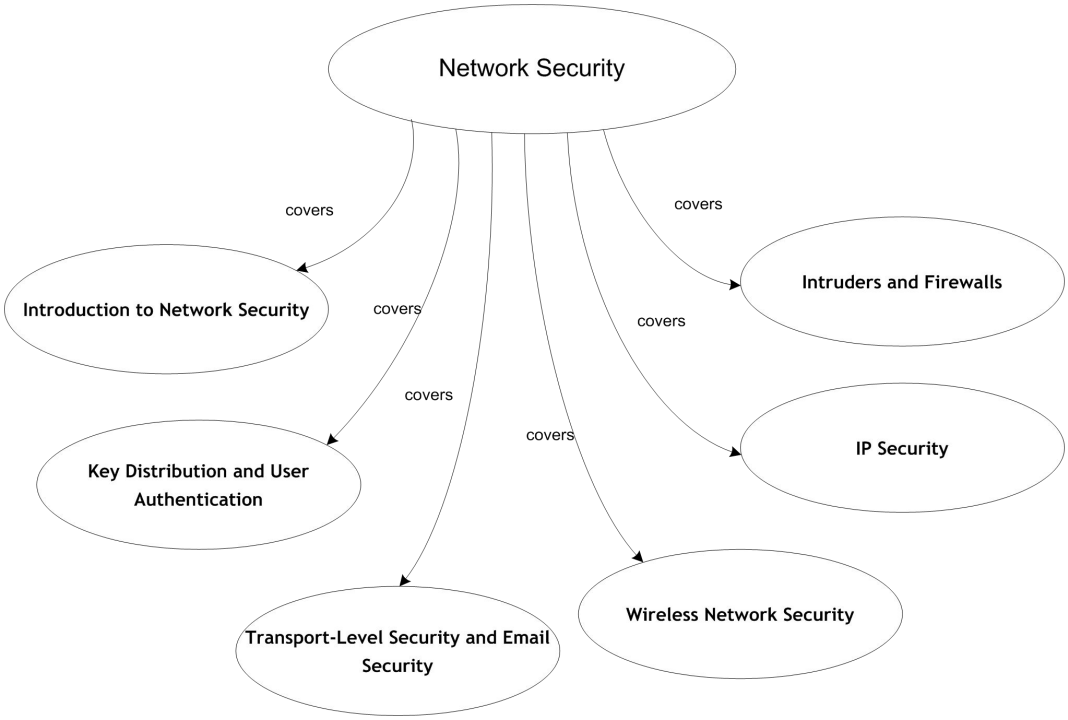
1. Study of history and recent trend in network security.
2. Symmetric key cryptography case analysis.
3. WAP, WEP hands on.
4. Firewall configuration.

The following activities shall be carried out by the teachers.

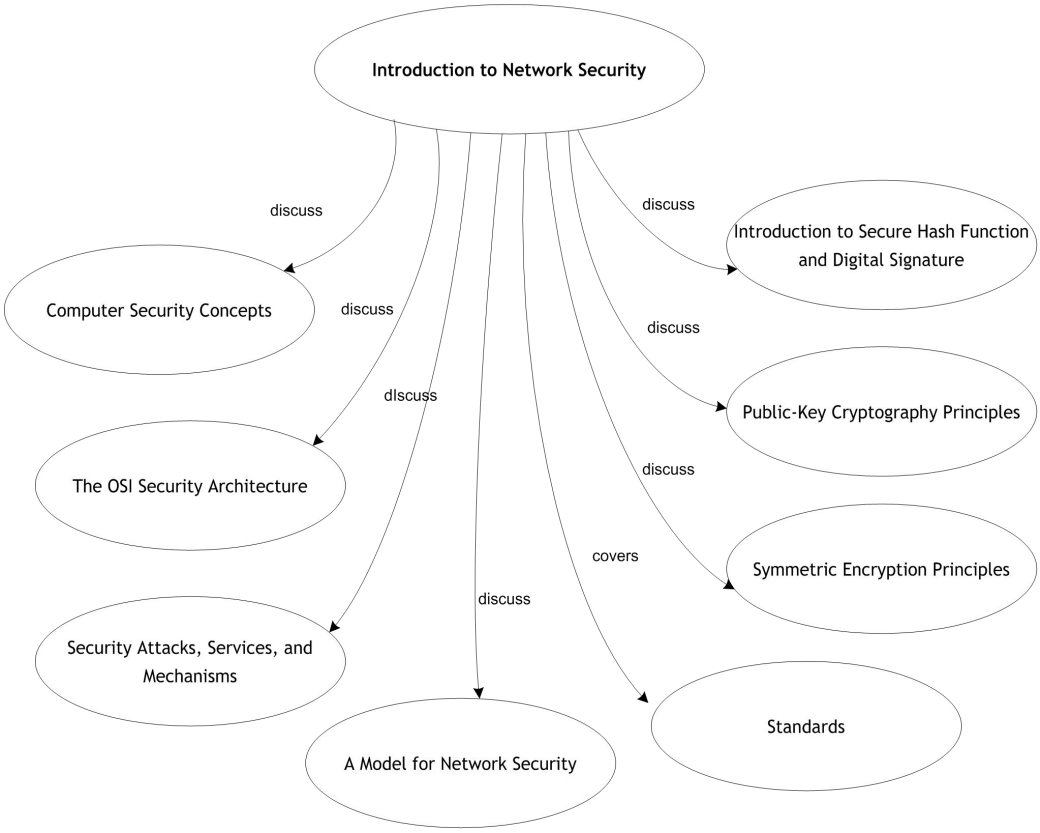
1. Simulation/experiment with SSL and SSH.
2. Wireless and IP Security related demonstration.

Concept map:

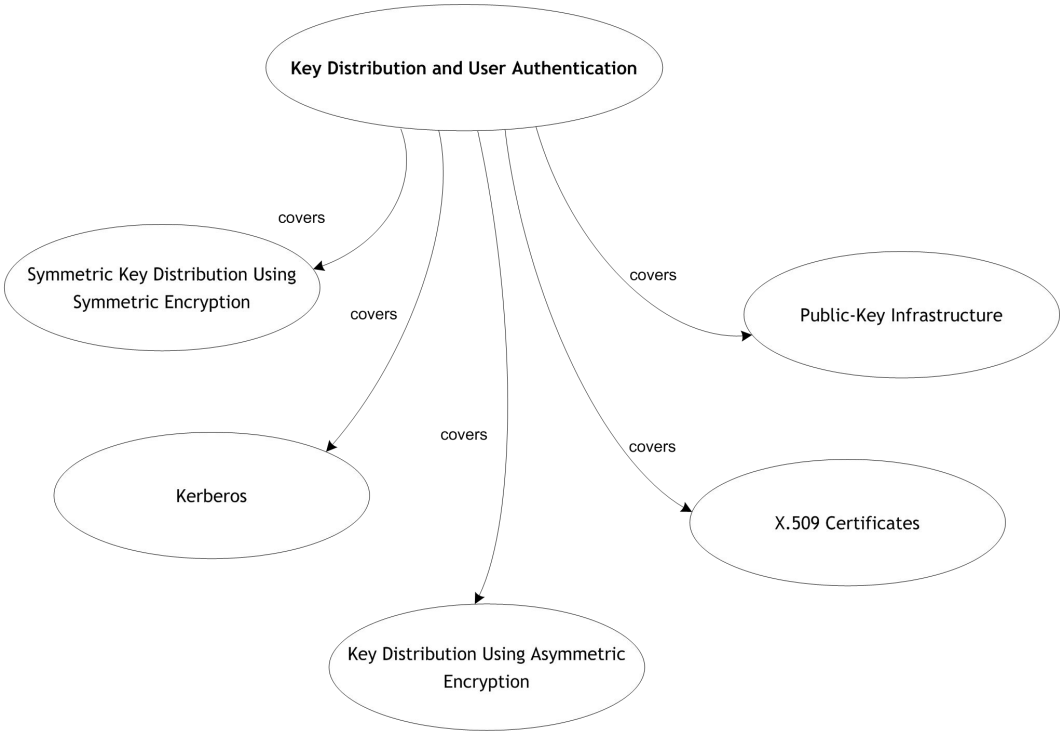
Network Security Course



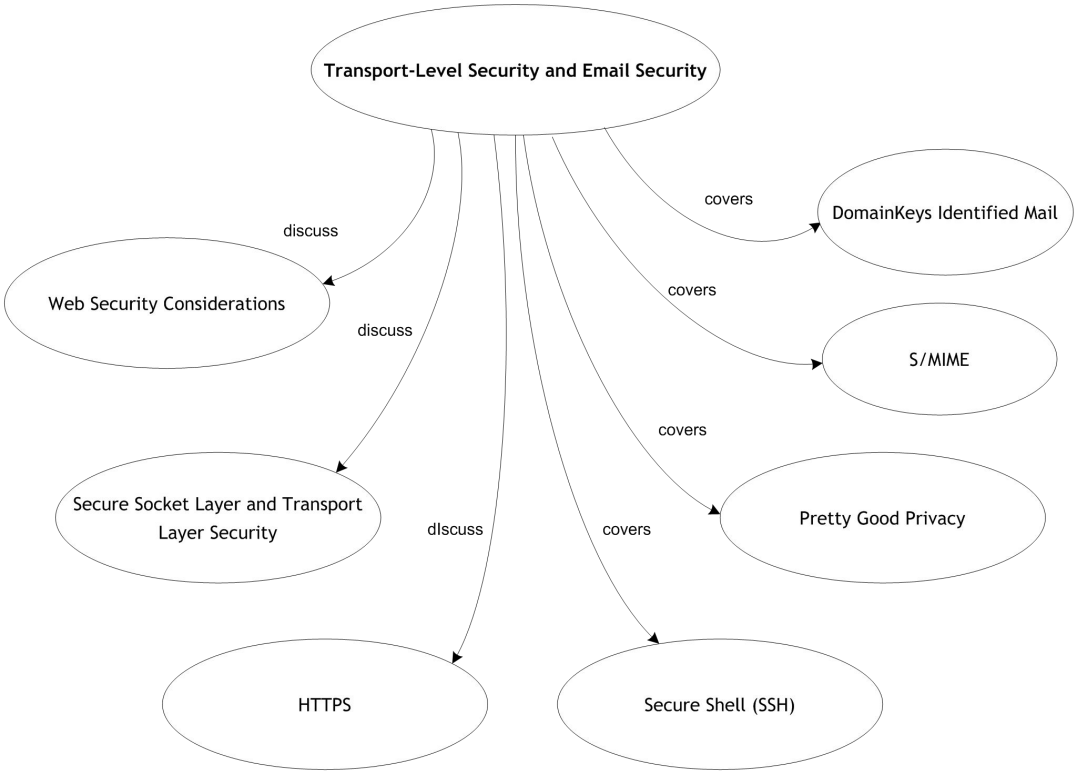
Unit-1


Introduction to Network Security
discuss
Computer Security Concepts
discuss
The OSI Security Architecture
dIscuss
Security Attacks, Services, and Mechanisms
discuss
A Model for Network Security
covers
Standards
discuss
Symmetric Encryption Principles
discuss
Public-Key Cryptography Principles
discuss
Introduction to Secure Hash Function and Digital Signature

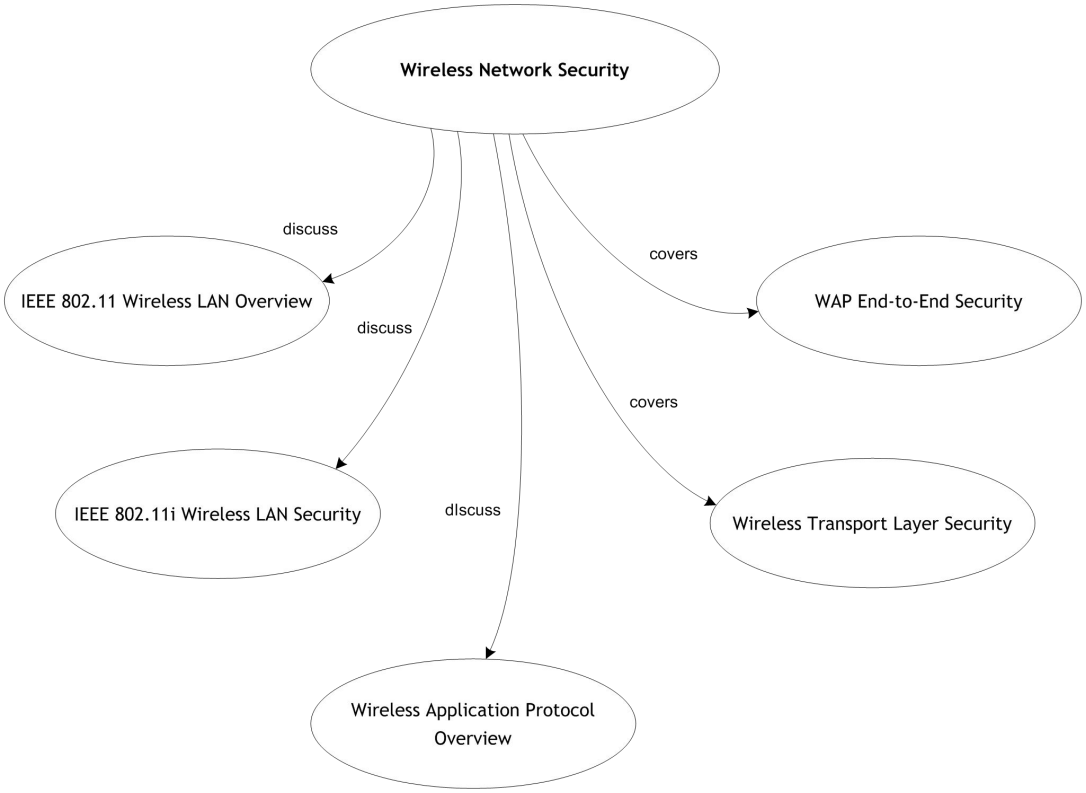
Unit-2


Key Distribution and User Authentication
covers
Symmetric Key Distribution Using Symmetric Encryption
covers
Kerberos
covers
Key Distribution Using Asymmetric Encryption
covers
X.509 Certificates
covers
Public-Key Infrastructure

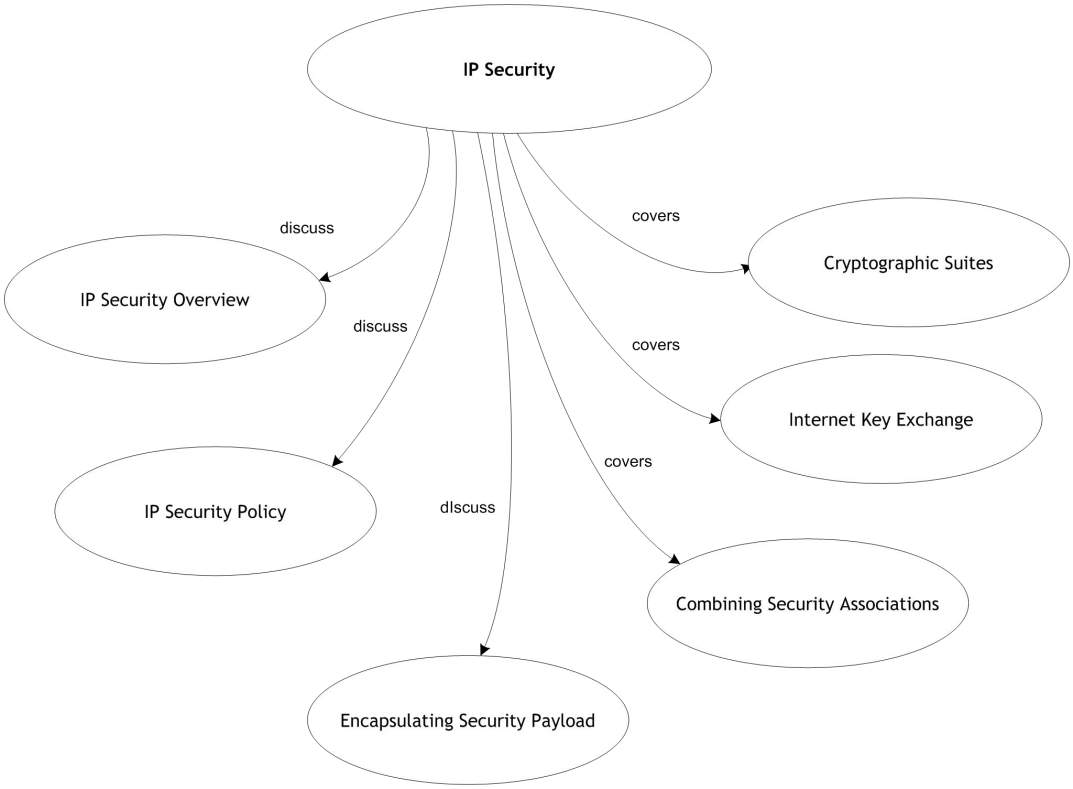
Unit-3


Transport-Level Security and Email Security
discuss
Web Security Considerations
discuss
Secure Socket Layer and Transport Layer Security
dIscuss
HTTPS
covers
DomainKeys Identified Mail
covers
S/MIME
covers
Pretty Good Privacy
covers
Secure Shell (SSH)

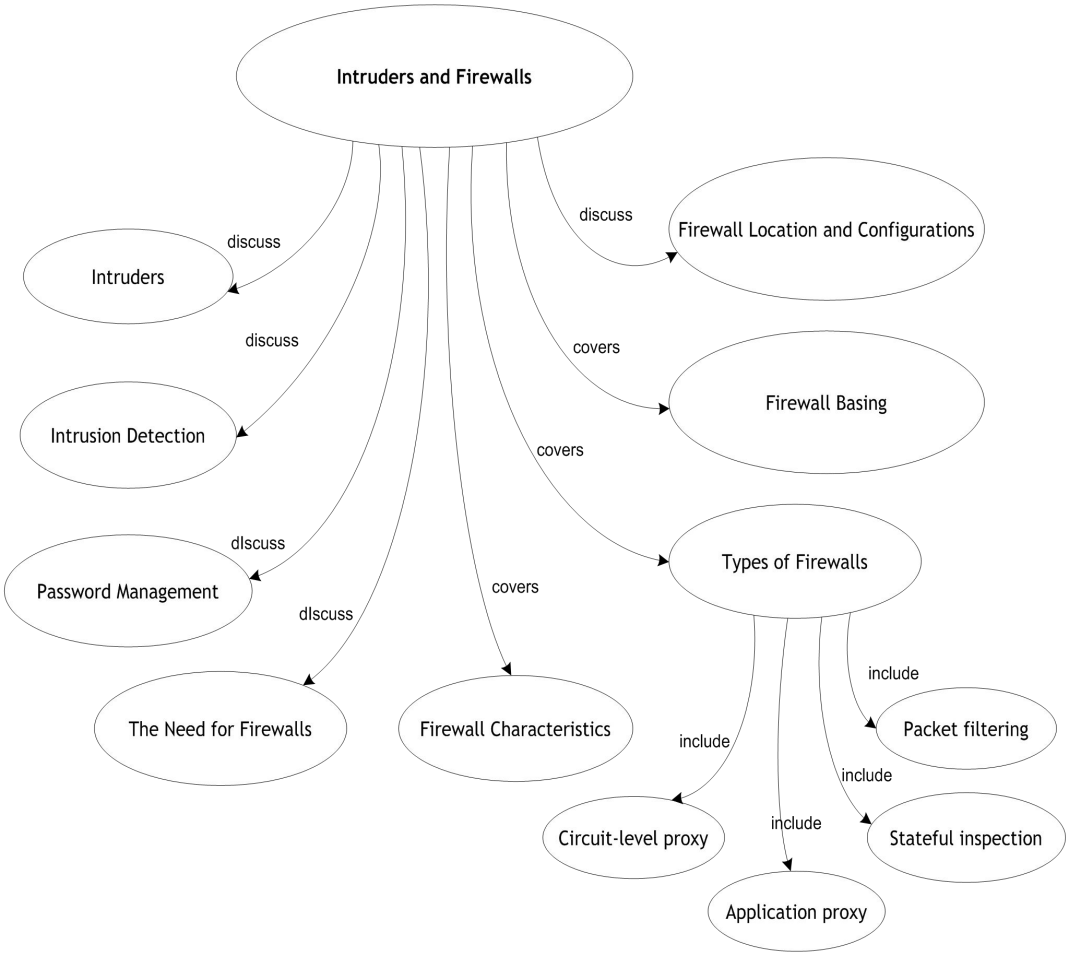
Unit-4


Wireless Network Security
discuss
IEEE 802.11 Wireless LAN Overview
discuss
IEEE 802.11i Wireless LAN Security
dIscuss
Wireless Application Protocol Overview
covers
WAP End-to-End Security
covers
Wireless Transport Layer Security

Unit-5


IP Security
discuss
IP Security Overview
discuss
IP Security Policy
dIscuss
Encapsulating Security Payload
covers
Cryptographic Suites
covers
Internet Key Exchange
covers
Combining Security Associations

Unit-6


Intruders and Firewalls
discuss
Intruders
discuss
Intrusion Detection
dIscuss
Password Management
dIscuss
The Need for Firewalls
covers
Firewall Characteristics
discuss
Firewall Location and Configurations
covers
Firewall Basing
covers
Types of Firewalls
include
Packet filtering
include
Stateful inspection
include
Application proxy
include
Circuit-level proxy