EE 518: Network Security

Lecture Schedule		ay,Thursday 7:30 pm	Semester		Fall 2018		
Credit Hours	Three	<u> </u>	Pre-requisite		Computer Networks (UG)		
Instructor	Muhammad Ali		Contact		m.ali@uet.edu.pk		
Office	Room		Office Hours		Tuesday, Thursday		
omee	EE De	epartment			4:00 – 6:00 pm		
		UET, Lahore					
Course		The course aims to provide overview of the main concepts and					
Description		mathematics behind most of the cryptographic algorithms. It gives					
		the theoretical knowledge concerning the architectures of symmetric					
		and asymmetric cryptosystems. The course describes key					
	management and message authentication. It also outlines some of						
	the well known security standards as IPsec, Kerberos, Secure Socket						
	Layer (SSL)/Public Key Infrastructure (PKI).						
	CLOs	CLOs Description			PLOs	Level	
	CLO1	Symmetric-key cryptography and protocols using symmetric-key encipherment		PLO1	High		
Measurable Learning Outcomes	CLO2	Asymmetric-key protocols us encipherment	cryptograpl sing asym	ny and metric-key		High	
ole Le	CLO3	Become familiar with integrity authentication and key distribution		PLO1	High		
surak	CLO4	Become familiar with network and system security		PLO1	High		
Mea	protocois in 1 ython/1 en				PLO5	High	
Textbooks	•	EQUIRED:					
		Lecture notes, Avinash Kak, Purdue University OPTIONAL:					
	Cryptography and Network Security by Behrouz A. Forouzan and Debdeep						
	Mukhopadhyay, 2 nd Edition, McGraw Hill.						
		Network Security: PRIVATE Communication in PUBLIC World by Charlie					
		Kaufman, Radia Perlman and Mike Speciner, 2 nd Edition, Pearson Education.					
Grading		Assignments/Quizzes 30% CLO1 to CLO5					
Policy	Midterm Final						
			1070	3238 10 0			

Lecture Plan

Classical Encryption Techniques	Weeks	Topics	Lecture notes				
CLO1-2 & Cl			& CLOs				
1.5* Finite Fields	0.5*	Classical Encryption Techniques	Lec2				
CLO1-2 & CLO1			CLO1-2 & CLO5				
1* AES: The Advanced Encryption Standard Lec8 CLO1 & CL 0.5* Block and Stream Ciphers Lec9 CLO1-2 & Cl 0.5* Key Distribution Lec10 CLO3 & CL 1* Prime Numbers and Discrete Logarithms Lec11 CLO2 1* Public-Key Cryptography and the RSA Algorithm Lec12 CLO2 & CL 0.5* Certificates, Certificate Authorities, and Digital Signatures Lec13 CLO2 & CL 1.5* Elliptic Curve Cryptography Lec14 CLO2 & CL 1* Hashing for Message Authentication Lec15 CLO3 & CL 0.5* TCP/IP Vulnerabilities: IP Spoofing and Denial-of-Service Attacks Lec16 CLO4 & CL 0.5* DNS and the DNS Cache Poisoning Attack Lec17 CLO4 & CL 1* Firewalls Lec18,19 CLO4 1* PGP, IPSec, SSL/TLS, and Tor Protocols Lec20 CLO4 0.5* The Buffer Overflow Attack Lec21 CLO4 & CL	1.5*	Finite Fields	Lec4-7				
CLO1 & CL O.5* Block and Stream Ciphers			CLO1-2 & CLO5				
D.5* Block and Stream Ciphers Lec9 CLO1-2 & Cl	1*	AES: The Advanced Encryption Standard					
CLO1-2 & CL 0.5* Key Distribution Lec10 CLO3 & CL 1* Prime Numbers and Discrete Logarithms Lec11 CLO2 1* Public-Key Cryptography and the RSA Algorithm Lec12 CLO2 & CL 0.5* Certificates, Certificate Authorities, and Digital Signatures Lec13 CLO2 & CL 1.5* Elliptic Curve Cryptography Lec14 CLO2 & CL MIDTERM 1* Hashing for Message Authentication Lec15 CLO3 & CL 0.5* TCP/IP Vulnerabilities: IP Spoofing and Denial-of- Service Attacks CLO4 & CL 0.5* DNS and the DNS Cache Poisoning Attack Lec17 CLO4 & CL 1* Firewalls Lec18,19 CLO4 1* PGP, IPSec, SSL/TLS, and Tor Protocols Lec20 CLO4 0.5* The Buffer Overflow Attack Lec21 CLO4 & CL			CLO1 & CLO5				
CLO3 & CL	0.5*	Block and Stream Ciphers					
CLO3 & CL			CLO1-2 & CLO5				
1* Prime Numbers and Discrete Logarithms Lec11 CLO2 1* Public-Key Cryptography and the RSA Algorithm Lec12 CLO2 & CL 0.5* Certificates, Certificate Authorities, and Digital Signatures Lec13 CLO2 & CL 1.5* Elliptic Curve Cryptography Lec14 CLO2 & CL MIDTERM 1* Hashing for Message Authentication Lec15 CLO3 & CL 0.5* TCP/IP Vulnerabilities: IP Spoofing and Denial-of-Service Attacks CLO4 & CL 0.5* DNS and the DNS Cache Poisoning Attack Lec17 CLO4 & CL 1* Firewalls Lec18,19 CLO4 1* PGP, IPSec, SSL/TLS, and Tor Protocols Lec20 CLO4 0.5* The Buffer Overflow Attack Lec21 CLO4 & CL	0.5*	Key Distribution	Lec10				
CLO2			CLO3 & CLO5				
1* Public-Key Cryptography and the RSA Algorithm Lec12 CLO2 & CL 0.5* Certificates, Certificate Authorities, and Digital Signatures Lec13 CLO2 & CL 1.5* Elliptic Curve Cryptography Lec14 CLO2 & CL MIDTERM 1* Hashing for Message Authentication Lec15 CLO3 & CL 0.5* TCP/IP Vulnerabilities: IP Spoofing and Denial-of- Service Attacks CLO4 & CL 0.5* DNS and the DNS Cache Poisoning Attack Lec17 CLO4 & CL 1* Firewalls Lec18,19 CLO4 1* PGP, IPSec, SSL/TLS, and Tor Protocols Lec20 CLO4 0.5* The Buffer Overflow Attack Lec21 CLO4 & CL	1*	Prime Numbers and Discrete Logarithms	Lec11				
CLO2 & CL O.5* Certificates, Certificate Authorities, and Digital Signatures Lec13 CLO2 & CL 1.5* Elliptic Curve Cryptography Lec14 CLO2 & CL MIDTERM 1* Hashing for Message Authentication Lec15 CLO3 & CL 0.5* TCP/IP Vulnerabilities: IP Spoofing and Denial-of- Service Attacks CLO4 & CL 0.5* DNS and the DNS Cache Poisoning Attack Lec17 CLO4 & CL 1* Firewalls CLO4 1* PGP, IPSec, SSL/TLS, and Tor Protocols Lec20 CLO4 0.5* The Buffer Overflow Attack Lec21 CLO4 & CL							
O.5* Certificates, Certificate Authorities, and Digital Signatures CLO2 & CL	1*	Public-Key Cryptography and the RSA Algorithm	Lec12				
CLO2 & CL 1.5* Elliptic Curve Cryptography Lec14 CLO2 & CL MIDTERM			CLO2 & CLO5				
1.5* Elliptic Curve Cryptography Lec14 CLO2 & CL MIDTERM 1* Hashing for Message Authentication 1* TCP/IP Vulnerabilities: IP Spoofing and Denial-of-Service Attacks DNS and the DNS Cache Poisoning Attack Lec17 CLO4 & CL 1* Firewalls Lec18,19 CLO4 1* PGP, IPSec, SSL/TLS, and Tor Protocols Lec20 CLO4 0.5* The Buffer Overflow Attack Lec17 CLO4 & CL Lec20 CLO4	0.5*	Certificates, Certificate Authorities, and Digital Signatures	Lec13				
MIDTERM 1* Hashing for Message Authentication Lec15 CLO3 & CL 0.5* TCP/IP Vulnerabilities: IP Spoofing and Denial-of- Service Attacks CLO4 & CL 0.5* DNS and the DNS Cache Poisoning Attack Lec17 CLO4 & CL 1* Firewalls Lec18,19 CLO4 1* PGP, IPSec, SSL/TLS, and Tor Protocols Lec20 CLO4 0.5* The Buffer Overflow Attack Lec21 CLO4 & CL			CLO2 & CLO5				
MIDTERM 1* Hashing for Message Authentication 1. Lec15 CLO3 & CL CLO3 & CL CLO3 & CL CLO4 & CL CLO4 & CL CLO4 & CL CLO4 & CL 1* Firewalls 1* PGP, IPSec, SSL/TLS, and Tor Protocols 1. Lec20 CLO4 CLO4 CLO4 CLO4 CLO4 CLO4 CLO4 CLO4	1.5*	Elliptic Curve Cryptography	Lec14				
1*Hashing for Message AuthenticationLec15 CLO3 & CL0.5*TCP/IP Vulnerabilities: IP Spoofing and Denial-of- Service AttacksLec16 CLO4 & CL0.5*DNS and the DNS Cache Poisoning AttackLec17 CLO4 & CL1*FirewallsLec18,19 CLO41*PGP, IPSec, SSL/TLS, and Tor ProtocolsLec20 CLO40.5*The Buffer Overflow AttackLec21 CLO4 & CL			CLO2 & CLO5				
CLO3 & CL O.5* TCP/IP Vulnerabilities: IP Spoofing and Denial-of- Service Attacks O.5* DNS and the DNS Cache Poisoning Attack Lec17 CLO4 & CL 1* Firewalls Lec18,19 CLO4 1* PGP, IPSec, SSL/TLS, and Tor Protocols CLO4 O.5* The Buffer Overflow Attack CLO3 & CL Lec16 CLO4 & CL Lec17 CLO4 & CL Lec18,19 CLO4 Lec20 CLO4 CLO4 CLO4	MIDTERM						
0.5*TCP/IP Vulnerabilities: IP Spoofing and Denial-of-Service AttacksLec16 CLO4 & CL0.5*DNS and the DNS Cache Poisoning AttackLec17 CLO4 & CL1*FirewallsLec18,19 CLO41*PGP, IPSec, SSL/TLS, and Tor ProtocolsLec20 CLO40.5*The Buffer Overflow AttackLec21 CLO4 & CL	1*	Hashing for Message Authentication	Lec15				
Service Attacks O.5* DNS and the DNS Cache Poisoning Attack Lec17 CLO4 & CL 1* Firewalls Lec18,19 CLO4 1* PGP, IPSec, SSL/TLS, and Tor Protocols Lec20 CLO4 O.5* The Buffer Overflow Attack Lec21 CLO4 & CL			CLO3 & CLO5				
0.5* DNS and the DNS Cache Poisoning Attack Lec17 CLO4 & CL 1* Firewalls Lec18,19 CLO4 1* PGP, IPSec, SSL/TLS, and Tor Protocols Lec20 CLO4 0.5* The Buffer Overflow Attack Lec21 CLO4 & CL	0.5*	TCP/IP Vulnerabilities: IP Spoofing and Denial-of-	Lec16				
CLO4 & CL		Service Attacks	CLO4 & CLO5				
1*FirewallsLec18,19 CLO41*PGP, IPSec, SSL/TLS, and Tor ProtocolsLec20 CLO40.5*The Buffer Overflow AttackLec21 CLO4 & CL	0.5*	DNS and the DNS Cache Poisoning Attack	Lec17				
1* PGP, IPSec, SSL/TLS, and Tor Protocols Lec20 CLO4 0.5* The Buffer Overflow Attack Lec21 CLO4 & CL			CLO4 & CLO5				
1*PGP, IPSec, SSL/TLS, and Tor ProtocolsLec20 CLO40.5*The Buffer Overflow AttackLec21 CLO4 & CL	1*	Firewalls	Lec18,19				
0.5* The Buffer Overflow Attack CLO4 & CLO4 & CL			CLO4				
0.5* The Buffer Overflow Attack Lec21 CLO4 & CL	1*	PGP, IPSec, SSL/TLS, and Tor Protocols	Lec20				
CLO4 & CL			CLO4				
	0.5*	The Buffer Overflow Attack	Lec21				
0.5* Malware: Viruses and Worms Lec22			CLO4 & CLO5				
	0.5*	Malware: Viruses and Worms	Lec22				
CLO4 & CL			CLO4 & CLO5				
0.5* Port and Vulnerability Scanning, Packet Sniffing, Lec23	0.5*	Port and Vulnerability Scanning, Packet Sniffing,	Lec23				
Intrusion Detection, and Penetration Testing CLO4			CLO4				
0.5* Dictionary Attacks and Rainbow-Table Attacks on Lec24	0.5*		Lec24				
Password Protected Systems CLO3			CLO3				
1* Security Vulnerabilities of Mobile Devices Lec32	1*	Security Vulnerabilities of Mobile Devices	Lec32				
			CLO4 & CLO5				
FINAL							

^{* -} Tentative