

1. Network programming & security basics 9

TCP/IP protocol architecture; user datagram protocol (UDP); multicasting; transmission control protocol (TCP); standard Internet services, and protocol usage by common Internet applications. Sockets programming; client/server; peer-to-peer; Internet addressing; TCP sockets; UDP sockets; raw sockets. Multithreading and exception handling. Finger, DNS, HTTP, and ping clients and servers. Routers and architectures, routing protocols.

Introduction – Primer on a Networking – Active and Passive Attacks – Layers and Cryptography – authorization – Viruses, worms. The Multi level Model of Security – Cryptography – Breaking an Encryption Scheme – Types of Cryptographic functions – secret key Cryptography – Public key Cryptography – Hash algorithms.

2. Cryptography 9

Secret key cryptography – Data encryption standard – International Data Encryption Algorithm (IDEA) Modes 4 Operations – Encrypting a Large message – Electronic code book, cipher block chaining, OFB, CFB, CTR – Generating MACs – Multiple Encryption DES.

Introduction to public key algorithms – Model of arithmetic – Modular addition, Multiplication, Exponentiation. RSA – RSA Algorithm – RSA Security – Efficiency of RSA – Public Key cryptography Standard (PKCS) - Digital Signature Standard – DSS Algorithm – Working of Verification procedure – Security and DSS – DSS controversy – Zero Knowledge proof systems.

3. Authentication 9

Authentication – Overview of authentication systems – password based authentication – Add nets based authentication – cryptographic authentication protocols – who is seeing authenticate – passwords as cryptographic keys – Eaves dropping and server database reading – Trusted intermediaries – Session key establishment.

Authentication of people – passwords – online – off line password of using – Eavesdropping – passwords and careless users – Initial Password distribution – Authentication tokens

4. IP security 9

Standards and IP security – Introduction to Kerberos – Tickets and Ticket granting tickets. Configuration - logging into the network – replicated KDCs. Overview of IP security – security associations – security association database - security policy database, AH and ESP – Tunnel Transport mode why protect - IP Header IPV4 and IPV6, NAT, Firewalls, IPV4, IPV6 Authentication Header – ESP - reason for having Authentication Header.

5. Management & firewalls 9

Network management architecture, ISO network management model including performance management, configuration management, accounting management, fault management, security management. Network Monitoring & Control - SNMP, V2, V3, RMON, RMON2.

Firewalls – packet filters – application level gateway – encrypted tunnels – comparisons why firewalls don't work – denial of service attacks. Web security – Introduction – URLs/URIs – HTTP – HTTP digest authentication. Cookies – other web security problems

TOTAL = 45

References

1. J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, Addison-Wesley Publishing, 2nd edition, 2002
2. Charlie Kaufman, Radia Perlman and Mike Speciner “Network Security : Private Communication in a Public Work”, Second Edition, Pearson Education, 2002.
3. Blawchart and Fabrycky , “Systems Engineering and Analysis”, Prentice Hall, 1998.
4. William Stallings, SNMP, SNMPV2, SNMPV3, RMON1 and 2, 3rd Edition , Addison Wesley - 1999.
5. Hans, “Information and Communication Security”, Springer Verlag, 1998.