APPLIED CRYPTOGRAPHY AND NETWORK SECURITY

Course Code : CSC 401 **Credit Units: 03**
Total Hours: 45

Course Objective:

The Internet is changing life as we know it – bringing new economic and social opportunities to communities throughout the world and increasing the global demand for information and communication technology (ICT) skills. Security and risk management skills are among the most highly sought-after skills in networking, and demand continues to grow. Organizations around the world are experiencing a shortage of qualified ICT candidates with the specialized knowledge and skills needed to administer devices and applications in a secure infrastructure, recognize
network vulnerabilities and mitigate security threats.

- Understanding about the fundamental concepts of Network Security and role of cryptography.
- To transfer a message securely over insecure channel.
- To be able to maintain the confidentiality, Integrity and Availability of a data transferred over a Network.

Course Contents:

Module I: Introduction to Applied Cryptosystems: (7 Hours)

Protocols for identification and login: Interactive protocols, ID protocols, Password protocols, Challenge-response protocols, Schnorr's identification protocol, Proving properties in zero knowledge, One-sided authenticated key exchange, Security of protocol AKE1, Protocol PAKE0, Protocol PAKE1, Protocol PAKE2.

Module II: Fundamentals of Security Protocols and usage: (9 Hours)

Security Protocols and Standards, SCP, SSH, SSL, TLS, STARTTLS, IPSec, VPN, HTTPS; Encrypting and Signing Emails: PGP- GPG/open PGP, DKIM and SPF; Single Sign On (SSO)-OAUTH and OPENID, Signature and Anomaly based detection, Honeypots and Honeynets, Network Log management-syslog or SPLUNK; RBAC: Role mining; DNS-Dig tool: DNSSEC-DS and NSEC records

Module III: Implementation of Cryptosystems: (7 Hours)

Authenticated Key Exchange: Goals for authentication and Key Establishment, encryption-based protocol and its attacks, Perfect forward secrecy, Protocol based on ephemeral encryption, Attacks on Insecure variations, Identity protection, Password authenticated key exchange – Phishing attacks, Explicit key confirmation.

Module IV: Network Security Primitives (7 Hours)

Classes of Key Agreement protocols, Pairing based cryptographic protocol, ID based encryption schemes, Conference Key protocols, Security goals, Static and dynamic groups, Key exchange protocol, Techniques for Network Protection, Monitoring and Detection, Firewalls, packet filter and stateful firewalls, application aware firewalls, personal firewalls, Proxies, NAT, ACL.

Module V: Security issues and solutions: (8 Hours)

Intrusion Detection System-Snort, Attack Techniques: Network reconnaissance-Nmap and vulnerability audits-openVAS; DNS based attacks, Phishing-DNSTwist; Network based malware attacks: Remote access Trojan Poison Ivy and Domain name generation algorithm based Botnets; LAN attacks: ARP Cache poisoning-Ettercap/arp spoof, MAC flooding, Man in the middle attacks, Port Stealing, DHCP attacks, VLAN hopping; Network Sniffing - Wireshark and Password Cracking-John the Ripper; Attacks on SSL/TLS: SSL stripping, Drown and Poodle attack; Network packet creation and Manipulation using scapy and dpkt libraries.

Module VI: Protecting the Network Infrastructure: (7 Hours)

Network Services such as NTP, SNMP are used to provide facilities such as time synchronization among all devices, health status, etc. If these Services are not configured properly, these become vulnerable to attacks, VPN, IPSec, RADIUS and TACACS+, Intrusion Prevention System, Operation of Host-Based and Network-Based Intrusion Prevention Systems, Content and Endpoint Security.

Course Outcomes:

The student will learn

- Understand various techniques for Network Protection and explore new tools and attacks in network security domain
- Exploring DNS, DNS based attacks and DNSSEC
- Familiarize the LAN based attacks and its mitigations
- Exploring Secure Network Communication protocols and attacks

Examination Scheme:

Components	A	CT	S/V/Q/HA	EE
Weightage (%)	5	15	10	70

A: Attendance, CT: Class Test, S/V/Q/HA: Seminar/Viva/Quiz/ Home Assignment, EE: End Semester Examination.

Text & References:

- William Stallings, Cryptography and Network Security: Principles and Practice,8th Edition, Pearson edition, 2020.
- Behrouz A. Forouzan, Cryptography & Network Security, McGraw-Hill.
- W. Stallings, Network Security Essentials: Applications and Standards, Pearson Prentice Hall.
- Bryan Sullivan and Vincent Liu, Web Application Security, A Beginner's Guide, McGraw-Hill Education.
- C. Kaufman, R. Perlman and M. Speciner, Network Security: Private Communication in a Public World, 2nd Edition, Prentice Hall PTR, 2002.
- Boyd, Colin, Anish Mathuria, and Douglas Stebila. Introduction to Authentication and Key Establishment. Protocols for Authentication and Key Establishment. Springer, Berlin, Heidelberg; 2020
- Boneh, Dan, and Victor Shoup. A graduate course in applied cryptography.

APPLIED CRYPTOGRAPHY AND NETWORK SECURITY LAB

Course Code : CSC 421 **Credit Unit: 01**
Total Hours: 30

Course Objective:
IoT Fundamentals curriculum provides students with a comprehensive understanding of the Internet of Things (IoT). It develops foundational skills using hands-on lab activities that stimulate the students in applying creative problem-solving and rapid prototyping in the interdisciplinary domain of electronics, networking, security, data analytics, and business.

Program List:
1. Describe the security threats facing modern network infrastructures**: (3 Hours)**
2. Secure network device access and Administer effective security policies**: (3 Hours)**
3. Implement AAA on network devices**: (3 Hours)**
4. Mitigate threats to networks using ACLs**: (3 Hours)**
5. Implement secure network management and reporting**: (3 Hours)**
6. Mitigate common Layer 2 attacks**: (3 Hours)**
7. Implement the Cisco IOS firewall feature set**: (3 Hours)**
8. Implement an ASA**: (3 Hours)**
9. Implement the Cisco IOS IPS feature set**: (3 Hours)**
10. Implement site-to-site IPSec VPNs**: (3 Hours)**

Course Outcomes:
The student will learn
- Understand key IoT concepts with Big Data.
- Understand Data Analytics and Machine Learning.
- How IOT work with Big Data.

Examination Scheme:

IA			EE			
A	**PR**	**Practical Based Test**	**Major Experiment**	**Minor Experiment**	**LR**	**Viva**
5	10	15	35	15	10	10

Note: IA –Internal Assessment, EE- External Exam, A- Attendance PR- Performance, LR – Lab Record, V – Viva.

Text & References:

- W. Stallings, Network Security Essentials: Applications and Standards, Pearson Prentice Hall.
- Bryan Sullivan and Vincent Liu, Web Application Security, A Beginner's Guide, McGraw-Hill Education.
- C. Kaufman, R. Perlman and M. Speciner, Network Security: Private Communication in a Public World, 2nd Edition, Prentice Hall PTR, 2002.