

UNIT II NP-complete problems: Search problems, Class NP, NP-hard problem, Reduction, NP-complete problems, Coping with NP-completeness: Intelligent exhaustive search, Approximation algorithms, Local search heuristics, SAT solvers, Implications on Information security : P vs NP Problem, Reasons for $P \neq NP$ (the foundation and the assumption of modern cryptography), Implications of $P = NP$ on Information security
(16 Hours)
UNIT III Complexity Analysis of algorithms used in Modern Cryptography namely, Integer Factorization Problem, Discrete log problem, primality testing, Modular exponentiation, Hashing Algorithms, Qualitative Introduction to Quantum Computing Algorithms : Peter Shor's quantum algorithm for factoring and Grover's Searching algorithm and their Implications on Information security
(16 Hours)
Textbooks : 1. Algorithms - Sanjoy Dasgupta, Christos Papadimitriou and Umesh Vazirani, TMH-2008 2. Introduction to Algorithms – Thomas H.Cormen, Charles E. Leiserson, Ronald L Rivest, Clifford Stein, third edition, The MIT Press, 2009 3. Combinatorial Optimization : Algorithms and Complexity, Christos H. Papadimitriou, Kenneth Steiglitz 4. “A Course in Cryptography”, Heiko Knospe, American Mathematical Society, 2019 5. “Introduction to Modern Cryptography”, Jonathan Katz, Yehuda Lindell, Chapman & Hall/CRC, 2008 6. “Foundations of Cryptography - Basic Tools”, Oded Goldreich, Cambridge University Press, 2004 7. “Foundations of Cryptography - Basic Applications”, Oded Goldreich, Cambridge University Press, 2009
CSCH 452 - NETWORK SECURITY
Course Objectives : 1. To make the student aware of the security needs of the computer network which works on protocols and how the weakness in these protocols be exploited 2. To make the student aware of the wrong practices of the employees which lead to cyber attacks

Course Outcomes :

1. Student gets the knowledge of the security loopholes in the existing network topologies and the ways to safeguard them
2. Student gets the knowledge to patch the networks with security patches whenever they are available from vendors

UNIT I

Secure Network Design : Introduction to Secure Network Design: Acceptable Risk, Designing Security into a Network, Designing an Appropriate Network, The Cost of Security, Performance, Availability, Security: Wireless Impact on the Perimeter, Remote Access Considerations, Internal Security Practices, Intranets, Extranets, and DMZs, Outbound Filtering, Compliance with Standards: NIST, ISO 27002, COBIT, Network Device Security : Switch and Router Basics: MAC Addresses, IP Addresses, and ARP, TCP/IP, Hubs, Switches, Routers, Network Hardening: Patching, Switch Security Practices, Access Control Lists, Disabling Unused Services, Administrative Practices, Internet Control Message Protocol (ICMP), Anti-Spoofing and Source Routing, Logging

(16 Hours)

UNIT II

Firewalls: Overview: The Evolution of Firewalls, Application Control, Must have Firewall features, Core Firewall Functions, Network Address Translation (NAT), Auditing and Logging, Additional Firewall Capabilities: Application and Website Malware Execution Blocking, Antivirus, Intrusion Detection and Intrusion Prevention, Web Content (URL) Filtering and Caching, E-Mail (Spam) Filtering, Enhance Network Performance, Firewall Design: Firewall Strengths and Weaknesses, Firewall Placement, Firewall Configuration, Virtual Private Networks: How a VPN Works, VPN Protocols: IPSec, PPTP, L2TP over IPSec, SSL VPNs, Remote Access VPN Security: Authentication Process, Client Configuration, Client Networking Environment, Offline Client Activity, Site-to-Site VPN Security, Wireless Network Security: Radio Frequency Security Basics: Security Benefits of RF Knowledge, Layer One Security Solutions, Data-Link Layer Wireless Security Features, Flaws, and Threats: 802.11 and 802.15 Data-Link Layer in a Nutshell, 802.11 and 802.15 Data-Link Layer Vulnerabilities and Threats, Closed-System SSIDs, MAC Filtering, and Protocol Filtering, Built-in Bluetooth Network Data-Link Security and Threats, Wireless Vulnerabilities and Mitigations: Wired Side Leakage, Rogue Access Points, Misconfigured Access Points, Wireless Phishing, Client Isolation, Wireless Network Hardening Practices and Recommendations: Wireless Security Standards, Temporal Key Integrity Protocol and Counter Mode with CBC-MAC Protocol, 802.1x-Based Authentication and EAP Methods, Wireless Intrusion Detection and Prevention: Wireless IPS and IDS, Bluetooth IPS, Wireless Network Positioning and Secure Gateways

(16 Hours)

UNIT III

Intrusion Detection and Prevention Systems: IDS Concepts, Threat Types, First-Generation IDS, Second-Generation IDS, IDS Types and Detection Models: Host-Based IDS, Network-Based IDS (NIDS), Anomaly-Detection (AD) Model, Signature-Detection Model, the type of IDS to Use, IDS Features: IDS End-User Interfaces, Intrusion-Prevention Systems (IPS), IDS Management, IDS Logging and Alerting, IDS Deployment Considerations: IDS Fine-Tuning, IPS Deployment Plan, Security Information and Event Management (SIEM): Data Aggregation, Analysis, Operational Interface, Additional SIEM Features, Voice over IP (VoIP) and PBX Security: Background, VoIP Components, Call Control, Voice and Media Gateways and Gatekeepers, MCUs, Hardware Endpoints, Software Endpoints, Call and Contact Center Components, Voicemail Systems, VoIP Vulnerabilities and Countermeasures: Old Dogs, Old Tricks: The Original Hacks, Vulnerabilities and Exploits, The Protocols, Security Posture: System Integrators and Hosted VoIP, PBX: Hacking a PBX, Securing a PBX, TEM: Telecom Expense Management

(16 Hours)

Textbooks :

1. "Information Security - The Complete Reference", Mark Rhodes-Ousley, Roberta Bragg, Keith Strassberg McGraw Hill Education; Second Edition
2. Network Security For Dummies – a book by Chey Cobb, CISSP, Publisher- John Wiley & Sons, 2011
3. Network Security: A Practical Approach- a book by Jan L. Harrington Morgan Kaufmann publications
4. Convery, Sean. Network Security Architectures. Cisco Press, 2004.
5. Ghosh, Sumit, and H. Lawson. Principles of Secure Network Systems Design. Springer, 2001.
6. Northcutt, Stephen, et al. Inside Network Perimeter Security. New Riders Publishing, 2005.
7. Strassberg, Keith, Richard Gondek, and Gary Rollie. Firewalls: The Complete Reference. McGraw-Hill/Osborne, 2002.
8. Zwicky, Elizabeth, Simon Cooper, and D. Brent Chapman. Building Internet Firewalls. 2nd ed. O'Reilly & Associates, Inc., 2000.
9. Akin, Thomas. Hardening Cisco Routers. O'Reilly, 2002.
10. Davis, Peter. Securing and Controlling Cisco Routers. Auerbach, 2002.
11. Hogg, Scott, and Eric Vyncke. IPv6 Security. Cisco Press, 2008.

CSCH 453 : DATA COMMUNICATIONS

Course Objectives :

1. To make the student aware of the different protocols and devices used in computer network for data communication
2. To make the student aware of the new technologies which are emerging in the market