IT 225: Computer Security and Cyber Law

Credits: 3
Lecture Hours: 48

Course Objectives

This module aims to introduce the fundamental knowledge of computer security and the recent development in the enactment of cyber laws.

Course Description

Introduction to Computer Security, Cryptography and Cryptographic Algorithms, Introduction to Network Security, Digital Signatures and Authentication Protocols, Design Principles and Common Security related programming problems, Malicious Logic and protection, Intrusion Detection System(IDS), Web security and Email Security, Database Security, Policy and Procedures, Issues with Internet in college.

Course Details

Unit 1: Introduction to computer security LH 5

Basic components of security (Confidentiality, Integrity and Availability), Security threats (Snooping, Modification, Masquerading, repudiation of origin, denial of receipt, Delay, Denial of service), Issues with security (Operational issues, human issues), Security Policies, Type of security policy, Access control, Type of access control (Introduction to MAC, DAC, Originator Controlled Access Control, Role Based Access Control) Overview of the Bell-LaPadula Model and Biba integrity model.

Unit 2: Cryptography and Cryptographic Algorithms LH 4

Cryptography, Data Encryption Standard, Symmetric key Cryptography(Block and stream ciphers), Asymmetric key Cryptography, Public key Cryptography (RSA), Message Digest 5, Hash Function, Message Authentication Code (MAC).

Unit 3: Introduction to Network Security LH 4

Fundamentals of Network security, Principal methods of protecting Network (Encryption, Decryption, Encryption in network), Network organization (Firewalls and proxies, Analysis of the network infrastructure), DMZ, Types of Firewalls(Packet Filtering, State-full Packet Filtering Circuit Level Gateway, Application level/proxy), IPSec, VPN.

Unit 4: Digital Signature and Authentication Protocols LH 5

Authentication Basic , Password (Attacking a password system, countering password guessing, Password aging), Challenge Response, Biometrics, Location, Multiple Methods, ,Mutual (Symmetric, Public Key), One-way (Symmetric, Public Key) Digital

Signature, Direct Digital Signature, Arbitrated Digital Signature, Digital Certificate, X.509 Certificate, Authentication Protocols, Authentication Services, Kerberos V4, Digital Signature Standards (DSS) , DSS approach Vs RSA approach.

Unit 5: Design Principles and Common Security related programming problems LH 4

Eight principles for the design and implementation of security mechanisms, Common Security related programming problems (Improper choice of initial protection domain, Improper Isolation of implementation detail, Improper change, Improper Naming, Improper de-allocation or deletion, Improper validation, Improper indivisibility, Improper Sequencing, Improper choice of operand or operation).

Unit 6: Malicious programs and Protection LH 4

Computer Viruses and Worms, Rabbits and Bacteria Defenses (Sandboxing, Information flow metrics, reducing the rights, malicious logic altering files, proof carrying code and notion of trust). Antivirus and features.

Unit 7: Intrusion Detection LH 4

Intruders, Intrusion techniques, Intrusion detection (Anomaly modeling, misuse modeling, specification modeling), Architecture (Agent (Host based information gathering, Network based information gathering, combining sources), Director, Notifier), Organization of intrusion detection system (Monitoring Network traffic for Intrusions(NSM), combining host and network monitoring (DIDS), Autonomous Agents(AAFID)), Intrusion Response (Incident prevention, Intrusion Handling (Containment Phase, Eradication Phase, Follow-up Phase).

Unit 8: Web security and Email Security LH 5

Web security, Threats, SSL (Architecture, Handshake protocol, Handshake protocol action), overview of TLS and HTTPS, Secure Electronic Transaction overview, Dual Signature, Payment Processing, E-Mail, SMTP, PEM, PGP, Concept of Secure Email.

Unit 9: Database Security LH 5

Issues regarding the right to access information, system related issues: system levels: physical hardware, Operating system, DBMS level, Multiple security level and categorization of data and users, Loss of integrity, Loss of availability, Loss of confidentiality, Access control, Inference control, flow control, data encryption.

Unit 10: Policy and Procedures LH 3

Computer Crime and Categories, Cyber Crime, Digital Forensics (overview of (Digital Evidence, Investigation Procedures, Categories of evidence (Impressions, Bioforensics, Trace evidence, Material evidence)), Intellectual Property Rights, Copyrights, Trademarks, Patents Licenses, Agreements, Plagiarism, Digital rights management, Privacy protection, Cyber Law, Electronic Transaction Act, Electronics Transaction Rules, IT Policy, Information Security and policies.

Unit 11: Issues with Internet in college LH 5

Cyberbullying: Curbing student use of technology to intimidate and harass others; Student use of the Internet: Reducing inappropriate Internet behaviors; Staff use of the Internet: Drawing a Line between teachers' public and private lives; Privacy and security: Protecting student information; The school as an Internet service provider: Providing access and protecting students; Copyright law in the classroom: steering clear of legal liability; Policies, procedures and contracts: communicating expectations to teachers, students and parents; Ethical Issues: Developing responsible internet citizens

References

Bishop M, Venkatramanayya S. S, Introduction to Computer Security

Stallings W. Cryptography and Network Security

Bishop M, Computer Security Art and Science

Pfleeger C. P., Pfleegar S. L., Security in computing.

Kaufman C., Perlman R., Speciner M.: Network Security: Private Communication in a Public World.

Electronic Transaction Act(ETA), Government of Nepal.

Electronic transaction Rule (ETR), Government of Nepal.

IT policy Of Nepal.

Copyrights Acts, Government of Nepal.

Eoghan Casey Handbook of Digital Forensics and Investigation, Academic Press, 2010, 2e.

Katz J., Lindell Y. Introduction to Modern Cryptography. CRC Press, 2007.

Cyber Law: Maximizing safety and Minimizing risk in classrooms, Aimee M. Bissonette, Worwin