Savitribai Phule Pune University
Department of Technology
Information Security
Curriculum Structure for M.Tech. Program effective from A.Y. 2015-16 (GP10)

| Sr. No. | Subject Code | Subject Name | Credits | Semester |
|---|---|---|---|---|
| 1 | IS – 1 | Algorithms and Programming | 4 | I |
| 2 | IS – 2 | Systems and Network Security | 4 | I |
| 3 | IS – 3 | Cryptography | 4 | I |
| 4 | IS – 4 | Internet Technologies and Protocols | 4 | I |
| 5 | IS – 5 | Security Architecture | 4 | I |
| | | | | |
| 6 | IS – 6 | Vulnerability Assessment and Penetration Testing | 4 | II |
| 7 | IS – 7 | Operating Systems Security | 4 | II |
| 8 | IS – 8 | Cryptography Advanced | 4 | II |
| 9 | IS – 9 | Mobile Security | 4 | II |
| 10 | IS – 10 | Development - I | 4 | II |
| | | | | |
| 11 | IS – 11 | Vulnerability Management | 4 | III |
| 12 | IS – 12 | Security Monitoring | 4 | III |
| 13 | IS – 13 | Forensics – I | 4 | III |
| 14 | IS – 14 | Development - II | 4 | III |
| 15 | IS – 15 | Malware and Reverse Engineering | 4 | III |
| 16 | IS – 16 | Cyber Law | 4 | III |
| | | | | |
| 17 | IS – 17 | Governance, Risk and Compliance | 4 | IV |
| 18 | IS – 18 | Forensics - II | 4 | IV |
| 19 | IS – 19 | Development - III | 4 | IV |
| 20 | IS – 20 | Security Management | 4 | IV |
| | | Dissertation | 20 | IV |
| | | | | |

## IS – 1: Algorithms and Programming

Algorithms, data structures, Boolean algebra, programming, buffer overflows, Software design goals (Correctness, Efficiency, Robustness, Adaptability, Reusability), OO vs Procedural vs Functional programming, Abstraction, Encapsulation, Modularity Classes & Objects, Interfaces & strong typing, Inheritance & polymorphism, Discrete maths, Sets & set operations, Arrays & array operations, Basic combinatorics, Big 'O' complexity notation, Arrays, Lists (Single & Doubly linked), Stacks, operations like push(), pop(), Recursive-ness, Searching, Sorting(Quick, insertion, bubble etc.), Selection & their complexity, Buffer overflow & memory safety, Stack Overflows, understanding & writing Shellcode, Defending Against Buffer Overflows, Compiler-time & run-time defences, replacement stack frame, return-to-system call, heap overflows, global data area overflows, Other Forms of Overflow Attacks, sandboxing, exploiting buffer overflows.

Reference Books:


1. Data Structure and Algorithmic Thinking with Python by Narasimha Karumanchi.
2. Problem Solving in Data Structure & Algorithms Using C by Hemant Jain

## IS – 2: Systems and Network Security

Design principles for secure systems, host based security, systems security, server security, authentication, authorization, access control, network layer security, TCP security issues; DDoS attacks; end-to-end security, link encryption, and secure network communication, IPSEC, network authentication, firewalls, intrusion detection and prevention.

Design principles, least privilege, fail-safe defaults, economy of mechanisms, complete mediation, open design, separation of privilege, least common mechanisms, and psychological acceptability.

Electronic User Authentication Principles, Password-Based Authentication, Token-Based Authentication, Biometric Authentication, Remote User Authentication, and Security Issues for User Authentication, Practical Application: An Iris Biometric System, Case Study: Security Problems for ATM Systems

Access Control Principles, Subjects, Objects, and Access Rights, Discretionary Access Control, Example: UNIX File Access Control, Role-Based Access Control, Attribute-Based Access Control, Identity, Credential, and Access Management, Trust Frameworks, Case Study: RBAC System for a Bank

Denial-of-Service Attacks, Flooding Attacks, Distributed Denial-of-Service Attacks, Application-Based Bandwidth Attacks, Reflector and Amplifier Attacks, Defenses against Denial-of-Service Attacks, Responding to a Denial-of-Service Attack

The Need for Firewalls, Firewall Characteristics and Access Policy, Types of Firewalls, Firewall Basing, Firewall Location and Configurations, Intrusion Prevention Systems, Example: Unified Threat Management Products.

Intruders, Intrusion Detection, Analysis Approaches, Host-Based Intrusion Detection, Network-Based Intrusion Detection, Distributed or Hybrid Intrusion Detection, Intrusion Detection Exchange Format, Honeypots, Example System: Snort

Security at transport & network layers, SSL, IPsec, Authentication header, encapsulating security payload protocol.

Reference Books:

1. Network Security: The Complete Reference by Roberta Bragg, Mark Phodes –Ousley, Keith Strassberg Tata McGraw-Hill.

## IS – 3: Cryptography

Security definition, correctness of protocols, crypto primitives, building high level secure protocols, symmetric cryptography, hash and message authentication codes, asymmetric cryptography, public key infrastructure; network

Confidentiality, Integrity & availability issues, Classical Cryptosystems, transposition & substitution ciphers, block & stream ciphers, One-time pad, Public Key Cryptography, Cryptographic Checksums, HMAC, Cryptographic Tools, Confidentiality with Symmetric Encryption, Message Authentication and Hash Functions, Public-Key Encryption, DH & RSA, Digital Signatures and Key Management, Random and Pseudorandom Numbers, Practical Application: Encryption of Stored Data

Elementary Number Theory, Time estimates for doing arithmetic, Divisibility and the Euclidean algorithm, Congruences, Some applications to factoring, finite fields, Quadratic residues and reciprocity, simple cryptosystems. Enciphering matrices, public key cryptography. RSA. Discrete log. Basics of Elliptic curve cryptosystems.

Reference Books:


1. Cryptanalysis of number theoretic Cyphers, Samuel S. Wagstaff Jr.
2. Cryptography and Network Security by William Stallings

## IS – 4: Internet Technologies and Protocols

Internet Security Protocols and Standards, Secure Email and S/MIME, DomainKeys Identified Mail, Secure Sockets Layer (SSL) and Transport Layer Security (TLS), HTTPSIPv4 and IPv6 Security, Internet Authentication Applications, Kerberos, X.509, Public-Key Infrastructure, Federated Identity Management, Protocols – http, https, ssl, tls, email protocols, snmp, ldap, routing protocols, Modbus, Vpn protocols, Ipv6, Soap, Dns, dhcp, arp

Reference Books:

1. Computer Networking with Internet Protocols and Technology by Stallings.

## IS – 5: Security Architecture

Intro to security architecture, Objectives of Security - DiD, CIA, Developing security policy, Structured monitoring, Security planning for businesses, Implementing security (DLP, UTM), Virtualization, Tools for protocol disassembly, reassembly – wireshark / tcpdump / netcat, Netflow

Reference Books:


1. Information Security Architecture: An integrated Approach to Security in the organization by Jan Killmeyer.
2. Enterprise Security Architecture by Nicholas Sherwood.

## IS – 6: Vulnerability Assessment and Penetration Testing

Vulnerability analysis & Penetration testing, Vulnerability Classification, Frameworks, Offensive and defensive measures – OS, DB, Network (wired & wireless), Web Apps (owasp top 10, sans 25), Web Server, Infrastructure (Mail, AD, database, proxy, erp), Web client side, Thick clients – web / nonweb, Mobile – android, ios, windows, (owasp mobile top 10), Firewalls, IDS /IPS, Routers, Vulnerability, threat, exploit, Malware, Payload, Fuzz testing, Critical infrastructure

Reference Books:


1. Penetration Testing by Georgia Weidman
2. Mobile Application Penetration Testing by Vijay Kumar Velu
3. Kali Linux Web Penetration Testing Cookbook by Gilberto Najera-Gutierrez

## IS – 7: Operating Systems Security

Mandatory access control, trusted computing, security models, security kernel, covert channel, distributed computing, cloud computing, Windows and Linux; Web Security, App Security; hardening OS; Assurance and Trust, Building Secure and Trusted Systems, Building Security In or Adding Security Later, DAC & MAC. Introduction to Operating System Security, System Security Planning, Operating Systems Hardening, Application Security, Security Maintenance, Linux/UNIX Security, Windows Security, Virtualization Security, Designing Trusted Operating Systems, What Is a Trusted System? Security Policies & Models of Security, Trusted Operating System Design, Assurance in Trusted Operating Systems , Security in Operating Systems, Cloud Computing, Cloud Security Risks and Countermeasures, Data Protection in the Cloud, Cloud Security as a Service, Protection in General-Purpose Operating Systems, Protected Objects and Methods of Protection, Memory and Address Protection, Control of Access to General Objects, File Protection Mechanisms, User Authentication, Linux's Security Model, The Linux DAC in Depth: Filesystem Security, Linux Vulnerabilities, Linux System Hardening, Application Security, Mandatory Access Controls, Windows Security Architecture, Windows Vulnerabilities, Windows Security Defenses, Browser Defenses, Cryptographic Services, Common Criteria, Mobile OS (Android & iOS; both Unix derivative)

Reference Books:

Operating System Security by Trent Jaegar, Ravi Sandhu

## IS – 8: Cryptography Advanced

Cryptographic algorithms, Symmetric Encryption and Message Confidentiality, Symmetric Encryption and Message Confidentiality, Data Encryption Standard, Advanced Encryption Standard, Stream Ciphers and RC4, Cipher Block Modes of Operation, Location of Symmetric Encryption Devices, Key Distribution, Public-Key Cryptography and Message Authentication, Secure Hash Functions, HMAC, The RSA Public-Key Encryption Algorithm, Diffie-Hellman and Other Asymmetric Algorithms, Integers & finite group theory, RSA and ElGamal ciphers, cyclic groups and the discrete log problem, Baby-step Giant-step and the Index Calculus probabilistic algorithms to compute discrete logs in cyclic groups, Naor – Reingold and Blum – Blum – Shub Random Number Generators, Fermat, Euler and Miller-Rabin primality tests, Pollard's and Quadratic Sieve factorization algorithms, transfer protocols and zero-knowledge proofs, Commutative rings, finite fields, rings of polynomials, and finding of the greatest common divisor in the ring of polynomial, Irreducible polynomials, Field extensions, elliptic curves the ElGamal cipher on elliptic curves, Block ciphers DES and double and triple DES, AES block ciphers and modes of operation, message integrity and message authentication, cryptographic hash functions SHA-512 as well as various digital signatures, entity authentication and key management issues, Quantum cryptography

Reference Books:


1. Cryptanalysis of number theoretic Cyphers, Samuel S. Wagstaff Jr.
2. Cryptography and Network Security by William Stallings

## IS – 9: Mobile Security

Android vulnerability and security, iOS vulnerability and security, Windows vulnerability and security, Mobile application security, mobile communication security, mobile infrastructure, architecture and security

Reference Books:


1. Android Forensics by Andrew Hoog
2. Mobile Security and Privacy by Man Ho Au and Kim-Kwang Raymond Choo

## IS – 10: Development – I

Bash, Batch, Assembly, Intel platform, C, C++, Java programming, others

Reference Books:


1. Guide to Assembly Language Programming in Linux by Sivarama Dandamudi
2. Learning the bash shell: Unix Shell Programming by Cameron Newham
3. Practical C Programming by Steve Oualline
4. Practical C++ Programming by Steve Oulline
5. Java 6 Programming Black Book, New ed

## IS – 11: Vulnerability Management

Vulnerability research cycle, Idea and Importance of VM, Threat points, Preparing for VM, Vulnerability assessment, Vulnerability scanning tools, Practical approach to VM, Metasploit and others, Types of Malicious Software, Advanced Persistent Threat, Propagation – Infected Content - Viruses, Propagation – Vulnerability Exploit - Worms, Propagation – Social Engineering – SPAM E-Mail, Trojans, Payload – System Corruption, Payload – Attack Agent – Zombie, Bots, Payload – Information Theft – Keyloggers, Phishing, Spyware, Payload – Stealthing – Backdoors, Rootkits, Countermeasures.

Reference Books:


1. Integrating Risk and Vulnerability Management by Adrian V. Gheorghe
2. Vulnerability Management by Park Foreman.

## IS – 12: Security Monitoring

SOC & Security monitoring, Current state assessments, SoC, Security architecture, Network security architecture, Network security monitoring, Endpoint security architecture, Automation and daily security monitoring

Reference Books:

1. The Practice of Network Security Monitoring- Understanding Incident Detection and Response by Richard Bejtlich

## IS – 13: Forensics – I

Introduction to Forensics, Introduction to Cyber Crime Investigation, Imaging, Data Acquisition, Types of Evidence, Types of Cases, Storage Devices, File systems, Windows forensics, Linux forensics, Network analysis – Local area

Reference Books:


1. macintosh-forensic-analysis-os-26_SANS
2. facebook_forensics-finalized_fbiic.gov
3. Investigations Involving the Internet and Computer Networks, by National Institute of Justice, U.S. Department of Justice

## IS – 14: Development – II

Python, Powershell, SSDLC, Secure Coding, CERT secure coding standards

Reference Books:


1. Think Python by Allen Downey.
2. Windows Powershell Cookbook

## IS – 15: Malware and Reverse Engineering

Reverse engineering, File System, Registry, Process, Memory and Networking, File Format- Portable Executable (PE), Debuggers- OllyDbg, IDA Pro, Monitoring Tools, Reverse Engineering Tools, Malware Categories, Malware Analysis

Reference Books:


1. Practical Malware Analysis- Hands on Guide to Dissecting Malicious Software by Michael Sikorski
2. Android Malware Analysis by Ken Dunham

## IS – 16: Cyber Law

The Information Technology Act, Introduction to Cyber Law, Ecommerce & E-governance, Electronic Signature & Digital Signature, Types of Cyber Crime, IPR in Cyber Space - the Indian Perspective, Authorities under the Information Technology Act, Investigation & Adjudication, Critical Infrastructure, Cyber Law – International, Laws of Singapore Japan, China, Germany, France, Estonia, US,UK & EU, IPR in Cyber Space - the International Perspective, Case Studies

Reference Books:


1. Textbook in Cyber Law by Pavan Duggal.
2. Data Protection Law in India by Pavan Duggal
3. Legal Framework on Electronic Commerce and IPR in Cyberspace by Pavan Duggal.

## IS – 17: Governance, Risk and Compliance

Security Policy, enforcement; Security standards, ISO 27001 standard, ISMS and PDCA Aproach; ISO 27013 changes; Security controls, implementation; patch control issues, measurement of controls; automated approaches; security auditing; other frameworks, SANS Controls, Economics of security, cyber risks, compliance, National policies, Computer Security Concepts, Threats, Attacks, and Assets, Security Functional Requirements, Fundamental Security Design Principles, Attack Surfaces and Attack Trees, Computer Security Strategy, IT Security Management, Organizational Context and Security Policy, Security Risk Assessment, Detailed Security Risk Analysis, IT Security Management Implementation, Security Controls or Safeguards, IT Security Plan, Implementation of Controls, Monitoring Risks, Security Policies & their goal, The Role of Trust, Confidentiality Policies (Bell-LaPadula Model), Integrity Policies (Biba & Clark-Wilson), Hybrid Policies (Chinese wall model), Other Formal Models for Computer Security, The Concept of Trusted Systems, Application of Multilevel Security, Trusted Computing and the Trusted Platform Module, Common Criteria for Information Technology Security Evaluation, Assurance and Evaluation, Security Auditing Architecture, The Security Audit Trail, Implementing the Logging Function, Audit Trail Analysis, Example: An Integrated Approach, The Economics of Cyber security , Making a Business Case, Quantifying Security, Modeling Cybersecurity

Reference Books:


1. NIST Special Publication 800-39 Managing Information Security Risk
2. Managing Information Security Risk_nistspecialpublication800-39
3. Guide for Conducting Risk Assessments_nistspecialpublication800-30r1

## IS – 18: Forensics – II

Mac systems, network devices, hardware forensics, mobile forensics, steganography, internet forensics, OSINT, social media forensics, e-discovery

Reference Books:


1. Forensic Examination of Digital Evidence- A Guide for Law Enforcement by National Institute of Justice, U.S. Department of Justice
2. Electronic Crime Scene Investigation- A Guide for First Responders, Second Edition, by National Institute of Justice, U.S. Department of Justice

## IS – 19: BCP / DRP

Concept, Business Risk Assessment, Defining BCP, Testing BCP, Implementing BCP, Incident Response, Management, DLP

Reference Books:

1. Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference by Jamie Watters, Janet Watters.

## IS – 20: Security Management

IT Security governance, IT security organization, Role of CISO and others, Relationship with others, inter/intra organization, Designing Secure IT environment, National Cyber security eco-system – CCA, CERT-In, DEITY, CII, NTRO, NCIIPC, etc, international Cyber security eco-system – ICAAN, NSA, hackers, ENISA, Crime Technology Forecast, Effect of specific industries – Banking / Airlines / Insurance / Manufacturing / IT / etc., Security / Prevention Economics / Cost-Benefit Models., Risk Management models, Actuarial Sciences and Cyber Insurance, Effect on Economy, Cyber Security, privacy and human rights

Reference Books:


1. Guide to General Server Security_nistspecialpublication800-123
2. NIST.SP.800-61r_Computer Security Incident Handling Guide