# MTCF – 301[A] Secure Software Engineering

**UNIT I**

Study of various Software life cycle models, Requirement analysis and specification, formal requirements, Fundamental issues in software design: Function-oriented design, structured analysis and design, Unified Modeling Language (UML), User interface design.

**UNIT II**

Software Static and Dynamic analysis, Software Testing Fundamentals, Software Test Process, Testing Levels, Test Criteria, Test Case Design, Test Oracles, Code inspections, Reliability models, verification and validation, Software project management, Activities covered by software project management, key objectives of effective management project planning, measurement and metrics, cost estimation.

**UNIT III**

Approach through software reliability engineering, Software reliability metrics, Software reliability specification, Reliability growth modeling, reliability concepts, software and hardware reliability. Programming for reliability, Fault avoidance, Fault tolerance, Exception handling, concurrence rate – occurrence probabilities- applying operation profiles.

**UNIT IV**

Defining failure for the product - System failure intensity objectives, common failure intensity objective, engineering software reliability strategies, Preparing for Test, Distributing new test cases among new operations, Detailing test cases, Preparing test procedures.

**UNIT V**

Using UML for Security, UM L diagrams for security requirement, physical security, security critical interaction, security state, Analyzing Model, Notation, formal semantics, security analysis, important security opportunities, Model based security engineering with UML, Design principles for secure systems, Applying security patterns.

**REFERENCES**


1. Pressman R.S. Software Engineering: A Practitioner's Approach, MGH.
2. John Musa D, "Software Reliability Engineering", 2nd Edition, Tata McGraw-Hill, 2005
3. Jan Jürjens, "Secure Systems Development with UML", Springer; 2004
4. Ian Sommerville, "Software Engineering", Fifth Editon, Pearson Education Asia.

# MTCF – 301[B] Secure Cloud Computing

**UNIT 1**

Cloud Computing Fundamentals- Definition, Evolution, Essential characteristics, Cloud Deployment Models, Cloud Service Models, Benefits, Cloud Architecture, Virtualization in Cloud, Cloud Data Centre, SLA, Cloud Applications.

**UNIT 2**

Cloud Security Challenges, Cloud Information Security Objectives, Cloud Security Services, Secure Cloud Software Requirements, Cloud Security Policy Implementation, Infrastructure Security, Data Security and Storage, Privacy in Cloud.

**UNIT 3**

Threats and Vulnerabilities to Infrastructure, Data, and Access Control; Risk Management and Risk Assessment in Cloud, Cloud Service Provider Risks, Virtualization Security Management in the Cloud, Trusted Cloud Computing, Identity Management and Access Control,

**UNIT 4**

Cloud Computing and Business Continuity Planning/Disaster Recovery, Cloud Audit and Compliance: Internal Policy Compliance, Regulatory/External Compliance, Cloud Security Alliance.

**UNIT 5**

Standards for Security: SAML OAuth, OpenID, SSL/TLS, Encrypting Data and Key Management, Creating a Cloud Security Strategy, The Future of Security in Cloud Computing.

**REFERENCES**


1. Ronald L. Krutz, Russell Dean Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, 2010.
2. Tim Mather, SubraKumaraswamy, and ShahedLatif, ” Cloud Security and Privacy", Published by O’Reilly Media, Inc., 2009.

# MTCF – 301[C] Malware Analysis And Reverse Engineering

**Unit 1**

Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM) Methodology, Brief Overview of Malware analysis lab setup and configuration, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM)

**Unit 2**

Malware taxonomy and characteristics, Understanding Malware Threats, Malware indicators, Malware Classification, Examining ClamAV Signatures, Creating Custom ClamAV Databases, Using YARA to Detect Malware Capabilities. Malware Labs, Creating a Controlled and Isolated Laboratory, Introduction to MA Sandboxes.

**Unit 3**

Malware Lab Integrity, Routing TCP/IP Connections, Capturing and Analyzing Network Traffic, Internet simulation using INetSim, Using Deep Freeze to Preserve Physical Systems, Using FOG for Cloning and Imaging Disks, Using MySQL Database to Automate FOG Tasks. Malware Analysis Tools, Introduction to Python, Introduction to x86 Intel assembly language, Scanners: VirusTotal, Jotti, and NoVirusThanks. Analyzers: ThreatExpert, CWSandbox, Anubis, Joebox, Dynamic Analysis Tools: Process Monitor, Regshot, HandleDiff, Analysis Automation Tools:

**Unit 4**

Malware Forensics, Using TSK for Network and Host Discoveries, Using Microsoft Offline API to Registry Discoveries, Identifying Packers using PEiD, Registry Forensics with RegRipper Plug-ins, Case Studies. Malware and Kernel Debugging, Opening and Attaching to Processes, Configuration of JIT Debugger for Shellcode Analysis, Controlling Program Execution, Setting and Catching Breakpoints, Debugging with Python Scripts and PyCommands, DLL Export Enumeration, Execution, and Debugging, Debugging a VMware Workstation Guest (on Windows), Debugging a Parallels Guest (on Mac OS X), Introduction to WinDbg Commands and Controls,

**Unit 5**

Memory Forensics and Volatility, Memory Dumping with MoonSols Windows Memory Toolkit, Accessing VM Memory Files, Overview of Volatility, Investigating Processes in Memory Dumps, Code Injection and Extraction. Researching and Mapping Source Domains/IPs, Using WHOIS to Research Domains, DNS Hostname Resolution. Reverse IP Search, Creating Static Maps, Creating Interactive Maps

**Reference:**


1. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code, First Edition (2010): Michael Ligh, Steven Adair, Blake Hartstein, and Matthew Richard. ISBN-10: 0470613033, ISBN-13: 978-0470613030. Wiley Publications
2. Malware: Fighting Malicious Code: Ed Skoudis and Lenny Zeltser (2003). ISBN-10: 0131014056, ISBN-13: 978-0131014053. Prentice Hall Publications.
3. Malware Forensics: Investigating and Analyzing Malicious Code: Cameron H. Malin, Eoghan Casey, and James M. Aquilina (2008). ISBN-10: 159749268X, ISBN-13: 978- 1597492683. Syngress Publications.

# MTCF – 302[A] Steganography and Digital Watermarking

**UNIT I**

Introduction to Steganography, Information Hiding, Digital Watermarking, Difference between Watermarking and Steganography, Importance of Digital Watermarking, Importance of Steganography.

**UNIT II**

Watermarking: Basic Watermarking Principles, Usage-specific requirements, Copyright protection, Annotation watermarking, Fingerprinting, Watermarking for copy protection, Digital watermarking for still images: Photographic and photorealistic images, Binary and halftoned images. Digital watermarking for audio data: Perceptual audio watermarking, Algorithms. Digital watermarking for three-dimensional data, Modification and Multiple Watermarks, Fragile watermarking for Image authentication, Perceptible versus Imperceptible, Private versus Public watermark, Watermarking for Copyright Protection, Watermarking for Image Authentication, Requirements and Algorithmic Design Issues: Imperceptibility, Robustness, Watermark Recovery with or without the Original Data.

**UNIT III**

Types of Steganography: Technical Steganography, Linguistic Steganography, Digital Steganography, Properties of Steganographic and Steganalysis Systems: Embedding, Steganographic Capacity, Embedding Capacity, Blind or Informed Extraction, False Alarm Rate, Principles of Steganography, Frameworks for Secret Communication, Information Hiding in Written Text, Substitution methods: Least Significant Bit Substitution, Pseudorandom Permutations, Image Downgrading and Covert Channels, Information Hiding in Binary Images

**UNIT IV**

Watermarking Attacks, Classification of attacks, Removal attacks and manipulations, Desynchronization attacks, Embedding attacks, Detection attacks.Steganalysis Introduction and Terminology, Detecting Hidden Information: Palette-Based Images, Image Distortion and Noise, Extracting Hidden Information, Disabling Hidden Information. Steganalysis Scenarios, Detection, Forensic Steganalysis, The Influence of the Cover Work on Steganalysis.

**UNIT V**

Applications of Watermarking, Broadcast Monitoring, Owner Identification, Proof of Ownership, Transaction Tracking, Content Authentication, Copy Control, Device Control, Legacy Enhancement, Applications of Steganography, Steganography for Dissidents, Steganography for Criminals,

**TEXT BOOKS:**


1. Stefan Katzenbeisser Fabien A. P. Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking”, 2000 ARTECH HOUSE, INC.
2. Michael Arnold, Martin Schmucker, Stephen D. Wolthusen, “Techniques and Applications of Digital Watermarking and Content Protection”, 2003 ARTECH HOUSE, INC.
3. Digital Watermarking and Steganography, Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker. 2nd Edition, Morgan Kaufmann Publishers, 2008.
4. Jessica Fridrich, “Steganography in Digital Media: Principles, Algorithms, and Applications”, Cambridge university press, 2010.
5. Peter Wayner, “Information Hiding: Steganoraphy& Watermarking”, 3rd Edition, 2009.

## MTCF – 302[B] Security Threats And Modeling

**Unit-1**

Dive In and Threat Model, Learning to Threat Model. Strategies for Threat Modeling, Brainstorming Your Threats, Structured Approaches to Threat Modeling, Models of Software,

**Unit-2**

Finding Threats, STRIDE, Spoofing Threats, Tampering Threats, Repudiation Threats, Information Disclosure Threats, Denial-of-Service Threats.Attack Trees, Working with Attack Trees, Representing a Tree, Real Attack Trees. Attack Libraries, Properties of Attack Libraries.

**Unit-3**

Managing and Addressing Threats, Processing and Managing Threats, Starting the Threat Modeling Project, Digging Deeper into Mitigations, Tracking with Tables and Lists, Scenario-Specifi c Elements ofThreat Modeling.Defensive Tactics and Technologies, Tactics and Technologies for Mitigating Threats, Addressing Threats with Patterns, Mitigating Privacy Threats.

**Unit-4**

Threat Modeling Tools, Generally Useful Tools, Open-Source Tools, Commercial Tools.Web and Cloud Threats, Web Threats, Cloud Tenant Threats, Cloud Provider Threats, Mobile Threats.

**Unit-5**

Threats to Cryptosystems, Cryptographic Primitives, Classic Threat Actors, Attacks against Cryptosystems, Building with Crypto, Things to Remember about Crypto.Experimental Approaches, Looking in the Seams, Operational Threat Models, Threats to Threat Modeling Approaches, How to Experiment.

**Text Books**


1. Adam Shostack, “Threat Modeling: Designing for Security Designing for Security” Wiley publication, Edition, 2008.

2. Frank Swiderski, Window Snyder “Threat Modeling (Microsoft Professional)” Microsoft Press, Edition, 2008.

## MTCF – 302[C] Internet Security- TCP/IP Vulnerability

**UNIT 1**

Introduction, Networking and Security Overview, Review of TCP/IP Internetworking, Attack Methods, Access Control and Site Security, Host Security.

**UNIT 2**

Security issues in Internet protocols: TCP, DNS, and routing, Web security: Web security requirements, Session management and user authentication, Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Secure Electronic Transaction (SET), HTTPS, Secure Shell (SSH), Content Security Policies (CSP).

**UNIT 3**

IP Security: IP Security overview, Architecture, Authentication, Encapsulating security payload, Combining security associations, Key management.

**UNIT 4**

E mail security- Pretty Good Privacy: Notation, Operational Description, Cryptographic Keys and Key Rings, Public-Key Management, S/MIME: RFC 5322, Multipurpose Internet Mail Extensions, S/MIME Functionality, S/MIME Messages, S/MIME Certificate Processing, Enhanced Security Services, Domain Keys Identified Mail: Internet Mail Architecture, E-mail Threats, DKIM Strategy, DKIM Functional Flow.

**UNIT 5**

Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics, Network defense tools: Firewalls, VPNs, Intrusion Detection, and filters. Criminal acts, ethics, legal frameworks and the impact on internet security.

**REFERENCES**


1. William Stallings “Cryptography and Network Security: Principles and Practice”, 5th Edition, Pearson Education. (ISBN:978-81-317-6166-3)
2. Behrouz A. Forouzan, “Cryptography and Network Security”, Tata McGraw-Hill. 2007, (ISBN: 978-00-706-6046-5).
3. William Stallings, "Network Security Essentials: Applications and Standards, Pearson, 2013. ISBN-10: 0273793365.
4. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security: Private Communication in a public world”, Prentice Hall India, 2nd Edition, 2002.