DR. A P J ABDUL KALAM UNIVERSITY, INDORE

SYLLABUS

of

MASTER OF TECHNOLOGY (CYBER SECURITY)

Department of Information Technology

(Second Year)

(Session July- December 2017)

College of Engineering

Dr. A P J Abdul Kalam University, Indore

DR. A P J ABDUL KALAM UNIVERSITY, INDORE

Syllabus for Master of Technology (Cyber Security)

Department of Information Technology

List of Subject (Second Year)

Unit 1: 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 2: 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 3: 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 4: 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 5: 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.

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

Sub Code : MTCYS 302-1 Sub Name : Security Threats And Modeling 4 Credits

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-Specific Elements of Threat 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.

References/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.

Sub Code : MTCYS 302-2 Sub Name : Internet Security - TCP/IP Vulnerability 4 Credits

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.