Course Curriculum

Course Code : SE 3205
Course Title : Software Security
Course Credit: 2 Credit (Theory course)
Credit Hour : 14 X 2 = 28 hours (1 class equivalent to 1 hour lecture)

Week	Topic	Content (Lesson Plan)	Reference Book & Chapter
WEEK 01	**Overview**	**Class 1:** Threats, Attacks, and Assets Security Functional Requirements Attack Surfaces and Attack Trees Computer Security Strategy	
	Authentication & Access Control	**Class 1:** Electronic User Authentication Principles Password-Based Authentication Token-Based Authentication Biometric Authentication	
WEEK 02		**Class 2:** Security Issues for User Authentication Remote User Authentication Case Study: Security Problems for ATM Systems	
		Class 3: Access Control Principles Example: UNIX File Access Control Role-Based Access Control Attribute-Based Access Control **ASSIGNMENT-01 (online)**	
WEEK 03	**Attacks and Countermeasures**	**Class 1:** SQL Injection Attacks Database Access Control Inference Database Encryption	
		Class 2: Security Requirements of Database Reliability & Integrity of Database Data Protection in the Cloud Cloud Security Risks and Countermeasures	

WEEK 04		**Class 3:** Types of Malicious Software (Malware) Advanced Persistent Threat Propagation and Payload Countermeasures	
		Class 4: Denial-of-Service (DoS) Attacks Flooding Attacks Application-Based Bandwidth Attacks Defence & Response to DoS Attack	
WEEK 05		**Class 5:** Intruders Intrusion Detection Analysis Approaches Host-Based Intrusion Detection Network-Based Intrusion Detection	
		Class 6: Firewall Characteristics and Access Policy Types of Firewalls Firewall Basing Firewall Location and Configurations Intrusion Prevention Systems **ASSIGNMENT-02 (online)**	
WEEK 06	**Distributed System Security**	**Class 1:** Security Tools and Techniques Identity Management Securing IaaS Risk Analysis & Assessment	
	Security Flaws	**Class 1:** Application Low Level Vulnerabilities Web applications Cryptographic/Access controls Networking Vulnerabilities	
WEEK 07	**Program Security**	**Class 1:** Buffer Overflows Defending Against Buffer Overflows Other Forms of Overflow Attacks	
		Class 2: Software Security Issues Writing Safe Program Code Program Input & Output **STUDENT TOPIC PRESENTATION (1):** *Taxonomy of Coding Errors*	

WEEK 08		**Class 3:** Automatic Program Repair Pre-Patch Window Security Workaround for Rapid Response Error Propagation	
		Class 4: Concurrency and Race Condition Concurrency Management Blocking Time Priority Inversion & Inheritance Countermeasure for Race Condition	
WEEK 09	**Operating System Security**	**Class 1:** System Security Planning Operating Systems Hardening Application Security Linux/Unix and/or Windows Security	
		Class 2: Security in the Design of OS: Layerd & Kernelized Design Security Maintenance Reference Monitor Correctness & Completeness Rootkit Detection & Prevention **ASSIGNMENT-03 (online)**	
WEEK 10	**Secure Software Design & Development**	**Class 1:** Program Analysis Static & Dynamic Analysis Symbolic Execution using Propositional Logic **STUDENT TOPIC PRESENTATION (2):** *Code Review*	
		Class 2: Branching Behaviour Loops & Recursion Deal with Infinite Execution Tree Security Assertions Concolic Execution	
WEEK 11		**Class 3:** Expected vs. Abnormal Execution Behaviour Control-Flow Integrity Imprecision: Call/Return Mismatch, Destination Equivalence	
		Class 4: Shadow Stack Memory Safety SoftBound **STUDENT TOPIC PRESENTATION (3):** *Architecture Risk Analysis*	

WEEK 12	**Threat Modelling**	**Class 1:** What, When, Why? Process of Modelling with DFD Identity Threats STRIDE Standards Mitigation Validation Threats	
		Class 2: **STUDENT TOPIC PRESENTATION:** *4. Risk Management Framework* *5. Software Penetration Testing* *6. Risk based Security Testing*	
WEEK 13	**Trusted Computing**	**Class 1:** The Bell-LaPadula Model for Computer Security Other Formal Models for Computer Security The Concept of Trusted Systems Application of Multilevel Security **ASSIGNMENT-04 (online)**	
	Security vs Usability	**Class 1:** Human Behaviour Analysis Usability and Authentication Human Factor: Security Principals	
WEEK 14	**Security Auditing**	**Class 1:** Security Auditing Architecture Security Audit Trail Implementing the Logging Function Audit Trail Analysis	
	Secure Development Lifecycle	**Class 1:** Training Security Requirements Define Metrics & Compliance Reporting Risk based Security Testing Safe Codes Touch-points	
		Online: Student Individual Presentation on Research Articles	
Final Examination			**All**

Reference Books:

WSL *Computer Security: Principles and Practice* (3rd Edition). William Stallings, Lawrie Brown. Pearson Education, Inc. 2015

CSJ *Security in Computing* (5th Edition). Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies. Pearson Education, Inc. 2015

GMW *Software Security: Building Security in*. Gary McGraw. Addison-Wesley Professional. 2006

JEH *Hacking: The Art of Exploitation* (2nd Edition). Jon Erickson. No Starch Press. 2008

DMH *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws* (2nd Edition). Dafydd Stuttard, Marcus Pinto. Wiley Publishing, Inc. 2007

GWP *Penetration Testing: A Hands-On Introduction to Hacking* (1st Edition). Georgia Weidman. No Starch Press. 2014