Course Code	CSE552
Course Name	Security Engineering
Credits	4
Course Offered to	Btech 3rd / 4th year, M.Tech, PhD
Course Description	This course is designed to present the students a “host” centric approach to various aspects of computer software security. Broadly, the course would cover: Traditional multi-level security models (Bell La-Padula, Biba etc.), access controls, security in traditional computer programs and attacks against them (buffer/heap overflow attacks), defences against such attacks, writing secure programs (Secure Coding), Viruses/Malware and Trojans, OS level hardening, application and system level security primitives and APIs, cryptographic system primitives and APIs (how to (not) use (and break) them), system level authentication frameworks, introduction to allied topics – IDS, network security etc.

Pre-requisites

Pre-requisite (Mandatory)	**Pre-requisite (Desirable)**	**Pre-requisite(other)**
C/C++, Operating Systems	Foundations of Computer Security (FCS)	

*Please insert more rows if required

Post Conditions

CO1	**CO2**	**CO3**	**CO4**
Able to comprehend and put to practice different forms of access control primitives in different software systems	Able to identify software vulnerabilities especially those related to buffer overflows, and ways to overcome such vulnerabilities.	Have hands on experience with different security primitives in modern Oses and platforms,	Able to use various libraries to achieve various security postures – e.g. confidentiality, integrity protection and authentication

Weekly Lecture Plan

Week Number	**Lecture Topic**	**COs Met**	**Assignment/Labs/Tutorial**
1	Introductions - Basics of Computer Systems Security, thinking wrt security, traditional security models -- their applicability and their drawbacks		Assignment – Basic file system – tests the basic systems’ programming skills of students
2	Access controls -- implementations in various OSes, usage, vulnerabilities and defenses	CO1	Assignment – Basic DAC
3	Introduction to Buffer Overflow Vulnerabilities	CO2	
4	Stack Smashing Attack	CO2	
5	Stack Smashing Demo, formatted output	CO2	Assignment – Basic buffer overflow vulnerabilities
6	Formatted output wrap-up, Dynamic memory allocation	CO2	Lab – formatted output vulnerability
7	Dynamic memory allocation vulnerabilities wrap-up. Mid-term review	CO2	
8	Return2Libc attacks,	CO2	Assignment – Return 2 Libc
9	Crash course in applied cryptography -- history, stream ciphers, block ciphers -- DES, AES, modes of operation. Encryption using OpenSSL.	CO3, CO4	Lab – using crypto programs
10	Message authentication and integrity, Public Key Cryptography. Generating hashes and digests using OpenSSL	CO3, CO4	Lab – using GPG for signatures
11	Miscellaneous -- Key Derivation Function, PBKDF, Disk Encryption DH Key Exchange, Web of Trust (GPG)	CO3, CO4	Assignment – Confidentiality and authentication using libraries
12	Authentication: Needham Schroeder Protocol, Kerberos, PKI	CO3, CO4	
13	X.509 Certificates, OpenSSL Certificates, Introduction to Linux PAM	CO3, CO4	Assignment – Public private crypto libraries – using X.509 cetificates

*Please insert more rows if required

Weekly Lab Plan

Week Number	**Laboratory Exercise**	**COs Met**	**Platform (Hardware/Software)**
6	Lab – formatted output vulnerability	CO2	Linux / gcc
9	Lab – using crypto programs	CO3,CO4	Linux / openssl
10	Lab – using GPG for signatures	CO3,CO4	Linux / GPG

*Please insert more rows if required

Assessment Plan

Type of Evaluation	**% Contribution in Grade**
Assignments	0.55
Midterms	0.15
Final + Quiz	20% + 10%

Resource Material

Type	**Title**
Textbook	Craft of Systems Security, S. Smith and J. Marchesini, Addison-Wesley, 2007, ISBN 0-32143483-8
Textbook	Secure Coding in C/C++, Second Edition, Robert C. Seacord, ISBN-13: 978-0321822130
Textbook	Computer Security: Principles and Practices, Second Edition, W. Stallings and L. Browne, 2011, ISBN-13: 978-0312775069