



GUJARAT TECHNOLOGICAL UNIVERSITY

Master of Engineering

Subject Code: 3725910

Semester II

Operating system and Host Security

Type of course:

Prerequisite:

- Operating System fundamental
- Digital logic and Fundamentals

Rationale:

- The aim of this course is to study, learn, and understand the main concepts of secure operating systems design and Hardware as well as software features that support these systems.
- To understand BIOS boot environments and how they interact with the platform architecture.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks	
L	T	P		C	Theory Marks		Practical Marks		
					ESE (E)	PA (M)	ESE (V)		PA (I)
3	0	2	4	70	30	30	20	150	

Content:

Sr. No	Course Content	No of Hrs	% Weight
Part-I Operating System			
1	OS Processes, Synchronization, Memory Management, File Systems	2	5
2	Trusted Operating Systems, Assurance in Trusted Operating Systems, Virtualization Techniques.	3	6
3	Secure operating systems, Security goals, Trust model, Threat model	4	9
4	Access Control Fundamentals – Protection system – Lampson's Access Matrix, Mandatory protection systems, Reference monitor.	4	9
5	Multics – Multics system, Multics security, Multics vulnerability analysis	3	6
6	Security in Ordinary OS – Unix, Windows	3	6
7	Verifiable security goals – Information flow, Denning's Lattice model, Bell-Lapadula model, Biba integrity model, Covert channels.	4	9
8	Security Kernels – Secure Communications processor, Securing Commercial OS	3	6
9	Secure Capability Systems – Fundamentals, Security, Challenges Secure Virtual Machine Systems	3	6
10	Case study – Windows, Linux kernel, Android, DVL, Solaris Trusted Extensions	4	8
Part-II Host Security			



GUJARAT TECHNOLOGICAL UNIVERSITY

Master of Engineering

Subject Code: 3725910

1	Introduction of BIOS and identification of trusted platform	1	2
2	Techniques for Recording Platform State	1	2
3	Can We Use Platform Information Locally?	2	4
4	Can We Use Platform Information Remotely?	2	4
5	How Do We Make Sense of Platform State?	2	4
6	Roots of Trust	2	4
7	Challenges in Bootstrapping Trust in Secure Hardware.	2	4
8	Validating the Process, Implementing Trust Bootstrapping: Open Source Tools	2	4
9	Human Factors & Usability	1	2

Reference Books:

1. Trent Jaeger, Operating System Security, Morgan & Claypool Publishers, 2008.
2. Bryan Parno, Jonathan M. McCune, Adrian Perrig, Bootstrapping Trust in Modern Computers, Springer Science & Business Media, 2011.
3. BRAGG, Network Security: The Complete Reference, McGraw Hill Professional, 2012.

Course Outcome:

Sr. No.	CO statement	Marks % weightage
CO-1	Understand the concept of secure operating system & virtualization	25
CO-2	Compare various security features in Multics, Windows and Linux OS.	15
CO-3	Analyze different models for securing commercial OS	25
CO-4	Understand the System Management Mode (SMM), chip-set architecture	20
CO-5	Understand how the BIOS interacts with the Trusted Platform Module (TPM) and the measured boot process	15

Suggested List of Experiments:

- Implement inter process communication using semaphore
- Implement inter process communication using monitor
- Implement inter process communication using shared memory
- Implement inter process communication using message queue
- Develop any client-server based program and demonstrate covert channel
- Using fork and Join, show the trace of any boot sequence
- Download the root kits and using any system call library shows the demonstration of login into root account.
- Boot the Raspberry pi using Ubuntu and develop the client server program using JAVA/C and test it on Raspberry pi.
- In the above program, hook and inject any small payload during run time and test it again.



GUJARAT TECHNOLOGICAL UNIVERSITY

Master of Engineering

Subject Code: 3725910

Major Equipments:

- Computer systems with firewall card
- Firewall and IDS system
- Raspberry pi kit
- VPN Router
- Hardware based packet analyzer tool

List of Open Source Software/learning website:

- GnuPG
- Truecrypt
- Application security
- Host security
- OWASP
- AxCrypt