10M1WCI131: System and Network Security Techniques

Course Credit: 3

Semester: I

Introduction

In today's Internet-dependent business environment, organizations must link their systems across enterprise-wide and virtual private networks as well as connect mobile users. In this course, you learn how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to network threats.

Course Objectives (Post-conditions)

Knowledge objectives:

- Analyze your exposure to security threats and protect your organization's systems and data
- Deploy data encryption to minimize threats
- Assess alternative user and host authentication mechanisms
- Manage risks emanating from inside the organization and from the Internet

Application objectives:

- To deploy the security devices in network.
- To configure the devices for better security
- To know about various security approaches and learn R&D basics in the field.

Expected Student Background (Preconditions)

Knowledge about computer network is required. In addition, some of the programming knowledge/tool knowledge of C/C++/JAVA, Mat LAB, NS2, NS3, OMNET++ is required for the execution of course projects.

Topics Outline:

S NO	Topics	Hrs
1	SYSTEM PROTECTION AND SECURITY Goals of Protection, Revocation of Access Rights, Principles of Protection, Capability-Based Systems, Domain of Protection, Language-Based Protection, Access Matrix, Implementation of Access Matrix, Access Control; The Security Problem, Computer-Security, Program Threats and Classifications; System and Network Threats, An Example: Windows XP; Cryptography as a Security Tool; User Authentication; Implementing Security Defenses; Firewalling to Protect Systems.	5
2	NETWORK ARCHITECTURE Network Design Considerations; Network Device Security; Firewalls, Virtual Private Network security; Wireless Network Security; Intrusion Detection Systems; Integrity and Availability Architecture;	13

	Network Role-based Security	
3	APPLICATION SECURITY Principle of Application Security; Writing Secure Software; J2EE Security; Windows .NET security; Database Security	10
4	STATE-OF-ART PART 1 BASICS: Control hijacking attacks: exploits and defenses; Dealing with legacy code: sandboxing and isolation; Tools for writing robust application code; Principle of least privilege, access control, and operating systems security; Exploitation techniques and fuzzing PART 2 WEB SECURITY: Basic web security model; Web application security; Content Security Policies (CSP), Web workers, and extensions; Session management and user authentication; Overview of cryptography; HTTPS: goals and pitfalls PART 3 NETWORK SECURITY: Security issues in Internet protocols: TCP, DNS, and routing; Network defense tools: Firewalls, VPNs, Intrusion Detection, and filters; Unwanted traffic: denial of service attacks PART 4 SECURITY OF MOBILE PLATFORMS: Mobile platform security models: Android and iOS; Mobile threats and malware; More on malware: viruses, Spyware and key-loggers; PART 5 CYBER FORENSICS, CYBER CRIME AND CYBER LAWS	14
Total		42

References

1. Roberta Bragg, Mark Phodes-Ousley and Keith Strassberg, Network Security: The Complete Reference, 7th Reprint, TMH Publishing
2. ABRAHAM SILBERSCHATZ, PETER BAER GALVIN and GREG GAGNE, Operating System Concepts, 7th Edition, JOHN WILEY & SONS. INC.
3. http://crypto.stanford.edu/cs155/syllabus.html

Evaluation Scheme:

S.No	Examination	Marks
1	T-1	15
2	T-2	25
3	T-3	35
4	*Internal Marks	25

*Internal Marks Breakdown:

Assignments 9 marks (3x3)

Quizzes 12 marks (3x4)

Regularity 4 Marks