Subject Code: 01CT1515

Subject Name: Information and Web Security

B. Tech. Year – III (Semester V)

Objective: To provide knowledge regarding working of information and web security mechanisms with by considering security issues and to learn the insights of information assurance techniques in area of information and web security.

Credits Earned: 04 Credits

Course Outcomes: After completion of this course, student will be able to:

1. Analyze common threats, attack and mechanism, deal with them (Analyze).
2. Apply various Symmetric and asymmetric key Algorithms (Apply).
3. Apply the concepts of Hash function, digital signature and digital certificates (Apply).
4. Understand security concepts for web development (Understand).
5. Identify the various security hazards related to web applications and need of security measures (Analyze).

Pre-requisite of course: Internet & Web Technology

Teaching and Examination Scheme:

Teaching Scheme (Hours)			Credits	Theory Marks			Tutorial / Practical Marks		Total Marks
				E	I		V	T	
Theory	Tutorial	Practical		ESE	IA	CSE	Viva	Term Work	
03	00	02	04	50	30	20	25	25	150

Contents:

Unit	Topics	Hours
1	**Introduction To Information Security:** Overview of internet security, Firewalls, Internet security, Management concepts and information privacy and copyright issues, Basics of asymmetric cryptosystems.	02
2	**Conventional Encryption & Number Theory:** Conventional encryption model, Steganography, Classical encryption techniques (Substitution and Transposition techniques), Prime and relative prime numbers, Modular arithmetic, Euler's theorem, Euclid's algorithm, Discrete logarithmic, Modular arithmetic, The Euclidean algorithm, Finite field of the form.	06

3	**Block Cipher Method:** Stream ciphers and block ciphers, Block cipher structure, Data encryption standard (DES) with example, Strength of DES, Blowfish, RC5, Cast-128, RC2, AES with structure, Traffic confidentiality, Random number generation, Key distribution	06
4	**Advanced symmetric cipher:** Multiple encryption and triple DES, Electronic code book, Cipher block chaining mode, Cipher feedback mode	04
5	**Public Key Cryptography:** Public key cryptosystems with applications, Requirements and cryptanalysis, RSA algorithm, Diffie-hillman key exchange algorithm, Man-in-Middle attack	04
6	**Message authentication and hash functions:** Authentication requirement, Message authentication code, Hash functions, Security of hash functions and macs, MD5 message digest algorithm, Secure hash algorithm	04
7	**Introduction to Web Security:** IP security overview, Architecture, Authenticationheader, Key management, pretty good privacy, S/Mime and types, Web security requirement, SSL and transport layer security, Secure electronic transactions, Firewall design principles, Types of firewalls. Web Threat Model, Authenticated Sessions, Cross-site Scripting, JavaScript Hijacking, Web Service Security, Website Vulnerability Scanner.	04
8	**Web Application Security &Vulnerability:** Web Application Security, How Does Web Application Security Work, Web Application Lifecycle Maintenance, Importance of Web Application Security, Web Application Vulnerabilities, Broken Access Control, Broken Authentication and Session Management, Buffer Overflows, Cross Site Scripting Flaws, Denial of Service, Improper Error Handling, Insecure Configuration Management, Insecure Storage, SQL Injection Flaws, Unvalidated Input, Defensive Measures	08
9	**E-Commerce Security:** Overview of online Security issues, Security for client computers, Communication channel security, Security for server computers	04
	Total Hours	**42**

Suggested Text books / Reference books:

1. William Stallings, “Cryptography and Network Principles and Practice”, Third and FourthEdition, Pearson Publication.
2. Faiyaz Ahamad, “Cyber Law and Information Security”, Dreamtech Publications.
3. Mukhopadhyay and Forouzan, “Cryptography & Network Security”, McGraw-Hill.
4. Atul Kahate, “Cryptography and Network Security”, 2nd Edition, TMH.

Suggested Theory distribution:

The suggested theory distribution as per Bloom's taxonomy is as per follows. This distribution servesas guidelines for teachers and students to achieve effective teaching- learning process.

Distribution of Theory for course delivery and evaluation					
Remember	Understand	Apply	Analyze	Evaluate	Create
5%	25%	30%	25%	10%	5%

Suggested List of Experiments: Minimum 14 experiments to be performed during the semester

1. Write code to implement Substitution cipher and Transposition cipher.
2. Write code to implement DES.
3. Write code to implement AES.
4. Write code to implement Diffie-hillman key exchange algorithm
5. Write code to implement RSA algorithm.
6. Write code to implement MD5 message digest algorithm
7. Write code to implement Dictionary Attack and Brute Force Attack.
8. Installation of Wire shark, tcpdump, etc and observe data transferred in client servercommunication using UDP/TCP and identify the UDP/TCP datagram.
9. Installation of rootkits and study about the variety of options.
10. Perform an Experiment to Sniff Traffic using ARP Poisoning.
11. Demonstrate intrusion detection system using any tool (snort or any other s/w).
12. Demonstrate how to provide secure data storage, secure data transmission and for creating digitalsignatures.
13. Installation and overview of Burpsuite Tools in Kali Linux.
14. Perform SQL injection
15. Perform Cross-site scripting and Cross-site request forgery (CSRF)
16. Demonstrate Information disclosure vulnerabilities
17. Configure NGINX and Apache webserver in Linux with https protocol
18. Configure Fail2ban with NGINX to protect the web server.

Supplementary Resources:

1. Black Book, "Web Technologies", Dreamtech Press (2012).
2. Black Book, "HTML 5", Dreamtech Press.
3. Developing Web Applications in PHP and AJAX, McGraw-Hill (2010).
4. P.J. Deitel & H.M. Deitel, "Internet and World Wide Web How to program", Pearson, 4thEdition.
5. https://portswigger.net/web-security/all-labs#sql-injection
6. https://portswigger.net/web-security/all-labs#cross-site-scripting
7. https://portswigger.net/web-security/all-labs#cross-site-request-forgery-csrf
8. https://portswigger.net/web-security/all-labs#information-disclosure