GUJARAT TECHNOLOGICAL UNIVERSITY

COMPUTER ENGINEERING (SOFTWARE ENGINEERING) (02)

INFORMATION SECURITY
SUBJECT CODE: 2710211
SEMESTER: I

Type of course: Major Elective I

Prerequisite: Mathematical concepts: Random numbers, Number theory, finite fields

Rationale: The use of the Internet for various purpose including social, business, communication and other day to day activities has been in common place. The information exchanged through Internet plays vital role for their owners and the security of such information/data is of prime importance. Knowing the concepts, principles and mechanisms for providing security to the information/data is very important for the students of Computer Engineering/Information technology. The subject covers various important topics concern to information security like symmetric and asymmetric cryptography, hashing, message and user authentication, digital signatures, key distribution and overview of the malware technologies. The subject also covers the applications of all of these in real life applications.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks						Total Marks
L	T	P	C	Theory Marks		Practical Marks				
				ESE (E)	PA (M)	PA (V)		PA (I)		
						ESE	OEP	PA	RP	
3	2	2	5	70	30	20	10	20	0	150

Content:

Sr. No.	Topics	Teaching Hrs.	Module Weightage
1	Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques	3	5
2	Stream ciphers and block ciphers, Block Cipher structure, Data Encryption standard (DES) with example, strength of DES, Design principles of block cipher, AES with structure, its transformation functions, key expansion, example and implementation	10	25
3	Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	3	5
4	Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and security, Diffie-Hillman Key Exchange algorithm, Man-in-Middle attack	7	15
5	Cryptographic Hash Functions, their applications, Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA)	4	8

6	Message Authentication Codes, its requirements and security, MACs based on Hash Functions, Macs based on Block Ciphers	3	7
7	Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm	3	8
8	Key management and distribution, symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, X.509 certificates, Public key infrastructure	4	7
9	Remote user authentication with symmetric and asymmetric encryption, Kerberos	4	5
10	Software Flaws and Malware : Introduction, Software Flaws, Buffer overflow, Incomplete Mediation, Race Conditions Malware, Brain, Morris Worm, Code red, SQL Slammer, Trojan Example, Malware Detection, The Future of Malware, Cyber Disease versus Biological diseases, Miscellaneous software-based Attacks, Salami Attacks, Linearization, Time bombs, Trusting Software Insecurity in software: Software Reverse Engineering, Anti-disassembly Techniques, Anti-Debugging Techniques Software Tamper Resistance: Guards, Obfuscation, Metamorphism Revisited	7	15

Reference Books:

1. Cryptography And Network Security, Principles And Practice Sixth Edition, William Stallings, Pearson
2. Information Security Principles and Practice By Mark Stamp, Willy India Edition
3. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGrawHill
4. Cryptography and Network Security Atul Kahate, TMH
5. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India
6. Information Systems Security, Godbole, Wiley-India
7. Information Security Principles and Practice, Deven Shah, Wiley-India
8. Security in Computing by Pfleeger and Pfleeger, PHI
9. Build Your Own Security Lab : A Field Guide for network testing, Michael Gregg, Wiley India

Course Outcome:

After learning the course the students should be able to

1. Define the concepts of Information security and their use.
2. Describe the principles of symmetric and asymmetric cryptography.
3. Understand and apply the various symmetric key algorithms.
4. Understand and apply the various asymmetric key algorithms.
5. Understand the concepts of hashing with algorithms and apply them.
6. Understand and use the message authentication and its requirement.
7. Understand the concepts of digital signature and digital certificates.
8. List and explain various digital signature algorithms.
9. Understand and use the various key management and remote authentication mechanisms.
10. Understand the concept of malware technology and its impacts.

List of Experiments:

1. Implement Caesar cipher encryption-decryption.
2. Implement Monoalphabetic cipher encryption-decryption.
3. Implement Playfair cipher encryption-decryption.
4. Implement Polyalphabetic cipher encryption-decryption.
5. Implement Hill cipher encryption-decryption.
6. To implement Simple DES or AES.
7. Implement Diffi-Hellmen Key exchange Method.
8. Implement RSA encryption-decryption algorithm.
9. Write a program to generate SHA-1 hash.
10. Implement a digital signature algorithm.
11. Perform various encryption-decryption techniques with cryptool.
12. Study and use the Wireshark for the various network protocols.
13. Study the SNORT intrusion detection system and list the operations available in it.
14. Perform the various filtering operations using firewall software.
15. Develop a with fixed size String based C or Java based Application and using buffer overflow technique show the injecting exploit in benign application
16. Reverse engineer the code by dissembling the code either using tools such as dex2jar or any API calls
17. Obfuscate the code and show the exploit protection before and after obfuscation

Open Ended Problems:

1. Study the standard document for the security policy for an organization and prepare the detailed security policy document for managing information security for your institute.
2. Develop a complete GUI based cryptography system using any symmetric key algorithm for practical use. Provide the performance analysis in terms of timing requirements.
3. Study the keytool provided by the Java to generate key pairs for public key cryptography. Design and develop your own such tool to generate the key pair and test the pair with RSA implementation for encyprion-decyprion.
4. Simulate the complete system to act as key distribution centre for the distribution of the symmetric keys.
5. Develop a system to generate a digital certificate in X.509 format.
6. Study how the browsers manage the digital certificates for various secured websites for making secured communication.
7. Develop a system that detects the SQL injection attack on your database and prevent your database for such attack.
8. Configure the Active directory and DNS server for your organization to comply with security policy of the organization.
9. Check whether your browser supports security mechanism for phishing attack. If yes, provide the details that how your browser implements it.

Major Equipments:

- Latest PCs with related software

List of Open Source Software/learning website:

- Software: cryptool (www.cryptool.org)
- Software: snort (**www.snort.org**)
- Software: Wireshark (**www.wireshark.org**)

- http://www.cryptix.org/
- http://www.cryptocd.org/
- http://www.cryptopp.com/