10B1WCI735: Network Security and Cryptography Techniques

Course Credit: 2
Semester: VI

Introduction

We will study security from multiple perspectives. We will consider a variety of security policies, authentication before access, integrity of information, and confidentiality of information. The course will focus on the models, the tools, and the techniques for enforcement of security policies, with some emphasis on the use of cryptography. And because today's implementation approaches are typically flawed, we will also address the penetration and disruption of information systems in the context of operating systems and networks. We will discus national regulatory policy in the cyber-security area.

Course Objectives (Post-conditions)
Knowledge objectives:

1. You will understand the basic security services e.g.Authentication, Access Control, Confidentiality, Integrity, and Non repudiation).[Familiarity]
2. You will understand the concepts of risk, threats, vulnerabilities and attack. [Familiarity]
3. You will know the important ethical and legal issues to consider in computer security. [Familiarity]
4. You will know the goals of end-to-end data security. [Familiarity]
5. You will understand the role of random numbers and prime numbers in security. [Assessment]
You will learn standard symmetric encryption algorithms[Assessment]
6. You will learn the architecture for public and private key cryptography and how public key infrastructure (PKI)
supports network security. [Assessment]
7. You will learn the methods of digital signature and encryption. [Assessment]
8. You will learn key management and how key exchange protocols work. [Familiarity]
9. You will learn security protocols at different layers of Network layer heirachy. [Assessment]
10. You will learn futuristic cryptographic techniques like Eliptic Curve and quantum cryptography.[Assessment]
11. You will learn the concept of trusted computing. [Assessment]
12. You will learn the Web security Protocol.[Assessment]

Application objectives:

1. Apply appropriate known cryptographic techniques for a given scenario. [Usage]
2. You will be able to analyze the tradeoffs of balancing key security properties.[Usage]
3 You will be able to design a security solution and do the cryptanalysis. .[Usage]

Expected Student Background (Preconditions)

1. Introduction to Computers(CI101)
2. Knowledge of Computer Networks

Topics Outline:

S NO	Topics	Hrs
1	Foundation of Security & Cryptography: OSI security architecture, Security Policy,Classical encryption techniques(Substitution Techniques, Transposition Techniques and Staganography)	3
2	Mathematical Tools for Cryptography: Finite fields, number theory	3
3	Design Principle of Block Ciphers:DES	4
4	Block Cipher Algorithms: AES	3
5	Pseudo Random Numbers & Stream Ciphers: Multiple Encryption, Block Cipher modes of operation, stream ciphers, Confidentiality	4
6	Public Key Cryptography: RSA, Key management	4
7	Hashes & Message Digest:Authentication functions,Message authentication codes,Hash functions and their security	4
8	Digital Signature, Certificates & standards	3
9	Authentication:X.509 Authentication service	3
10	Electronic Mail Security:S/MIME	3
11	IP and Web Security Protocols:IPsec, Secure socket layer and transport layer security, secure e-transaction.	4
12	System Security : Computer Virus, Firewall & Intrusion Detection , Trusted systems, Security Investigation/Audit	4
	Total	42

References

"Cryptography & Network Security" by Stallings, William (Fourth Edition or later) will be used as the main text book; however the inputs will be supplemented with information from elsewhere wherever the same is required.

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