GMR INSTITUTE OF TECHNOLOGY (AUTONOMOUS)

B.Tech- 6th Semester

COURSE HANDOUT

SYLLABUS
(Applicable for 2012-13 admitted batch)

Course Title : INFORMATION SECURITY

Course Code : CSE 3414

Course Structure : 3-1-0-4

Course coordinator : Dr R Priya Vaijayanthi

Instructor(s) : Dr R Priya Vaijayanthi

Course Description

This course describes network security applications and standards. The emphasis is on applications that are widely used on the internet for corporate networks, and on standards, especially internet standards, that have been widely deployed.

Course objectives:

Students undergoing this course are expected to:

1. Understand about various Conventional Encryption Principles designed for providing security.
2. Learn public key cryptography, key management principles and Learn Pretty Good Privacy (PGP) which is a computer program that provides cryptographic privacy and authentication.
3. Learn IP Security fundamentals, architecture and identifying the key features IP security system.
4. Understand about general requirements for Web security, which focus on standardized schemes.

TEXT BOOKS:

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.
2. Hack Proofing your network by Ryan Russell, Dan Kaminsky, Rain Forest Puppy, Joe Grand, David Ahmad, Hal Flynn IdoDubrawsky, Steve W.Manzuik and Ryan Permeh, wileyDreamtech.

REFERENCE BOOKS :

1. AtulKahate, "Cryptography and Network Security", Tata McGraw-Hill, 2003.
2. William Stallings, "Cryptography and Network Security – Principles and Practices", PrenticeHallofIndia,ThirdEdition,2003
3. Charles B. Pfleeger, Shari LawrencePfleeger, "Security in Computing", Third Edition, Pearson Education, 2003.

SYLLABUS:

UNIT- I (15 Hours)

Introduction: Security Attacks (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability), TCP session hijacking, UDP hijacking, ARP attacks, & Man-in-the-Middle Attacks. OSI Security Architecture - Classical Encryption techniques – Cipher Principles.
Conventional Encryption Principles:
Conventional encryption algorithms - Data Encryption Standard (DES), Blowfish, CAST-128, Block Cipher Design Principles and cipher block Modes of Operation, Evaluation criteria for AES Cipher

UNIT- II (15 Hours)

Public Key Cryptography: Public key cryptography principles, public key cryptography algorithms, digital signatures. Digital Certificates, Certificate Authority and key managementAuthentication & Hash Function: Authentication requirements – Authentication functions –Message Authentication Codes – Hash Functions – Security of Hash Functions and MACs – MD5message Digest algorithm - Secure Hash Algorithm – RIPEMD-HMAC Digital Signatures –Authentication Protocols – Digital Signature

UNIT- III (15 Hours)

Network Security Authentication Applications: Kerberos – X.509 Authentication Service –Electronic Mail Security – PGP – S/MIME
IP Security: IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management

UNIT-IV (15 Hours)

Web Security: Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET).System Level Security Intrusion detection – password management – Viruses and related Threats – Virus Counter measures – Firewall Design Principles – Trusted Systems

Course Outcomes:

After undergoing the course, students will be able to

1.To analyze a given system with respect to security of the system.
2.To create an understanding of Authentication functions the manner in which Message Authentication Codes and Hash Functions works.
3.To examine the issues and structure of Authentication Service and Electronic Mail Security
4.Understand conventional and public key cryptographic approaches used in message encryption.
5.Able to identify various types of attacks and its effect over the networks

Course Plan:

| Lecture No. | Learning Objectives | Topics to be covered | Reference |
|---|---|---|---|
| | Unit – I | | |
| 1 | To understand what is security | Introduction to security attacks, with attacks | T1 |
| 2 | To understand what are security services | Security Services | T1 |
| 3 | To learn TCP session hijacking and UDP hijacking | TCP session hijacking, UDP hijacking T1 | |
| 4 | Tutorial-1 | | |
| 5 | To differentiate the attacks | ARP attacks, & Man-in-the-Middle T1 Attacks.. | |
| 6 | To understand OSI security architecture | OSI Security Architecture | T1 |
| 7 | To know about different substitution techniques in IS | Classical Encryption techniques – Substitution techniques | |
| 8 | Tutorial-2 | | |
| 9 | To study about Transposition | Classical Encryption techniques Transposition techniques, rotor techniques | |
| 10 | To Know the principles of Conventional Encryption | Principles, conventional Encryption | T1 |
| 11 | To Know the symmetric encryption techniques like DES | Data Encryption Standard (DES) | T1 |
| 12 | Tutorial-3 | | |
| 13 | To understand the symmetric Encryption techniques like Blowfish and CAST-128 | Blowfish, CAST-128 | T1 |
| 14 | To understand the different modes of operation and Cipher Design principles | Block Cipher Design Principles and Block cipher block Modes of Operation | T1 |
| 15 | To understand and compare AES & DES | Evaluation criteria for AES Cipher | T1 |
| UNIT-II | | | |

| | | | |
|---|---|---|---|
| 16 | To understand Public key cryptography | Public key cryptography principles basic principles | T1 |
| 17 | To know the different algorithms of public key cryptography | public key cryptography algorithms | T1 |
| 18 | To understand how signatures are useful | digital signatures | T1 |
| 19 | Tutorial-4 | | |
| 20 | To know about the role of Digital Certificates and CA | Digital Certificates, Certificate Authority and key management | T1 |
| 21 | To understand Authentication Requirements | Authentication requirements, Message Authentication Code | T1 |
| 22 | Tutorial-5 | | |
| 23 | To understand how Hash functions are useful in IS | Hash Functions | T1 |
| 24 | To know the Security of Hash Functions and MAC | Security of Hash Functions and MAC | T1 |
| 25 | Tutorial-6 | | |
| 26 | To understand the strength of MD5 MD5 | Message Digest algorithm | T1 |
| 27 | To understand the role of RIPEMD algorithm in IS | RIPEMD | T1 |
| 28 | To know about the technique of HMAC algorithm | HMAC Digital Signatures | T1 |
| 29 | To know about the Signatures | Digital Authentication Protocols – Signature | T1 |
| 30 | Tutorial-7 | | |
| UNIT-III | | | |
| 31 | To know the role of Authentication Protocols | Introduction to Kerberos | T1 |
| 32 | To understand the different types of Kerberos algorithms | Different types of Kerberos algorithms | T1 |
| 33 | To Know the usage of X.509 Certification. | X.509 Authentication Service | T1 |

| | | | |
|---|---|---|---|
| 34 | To learn the importance of E-Mail Security | Introduction to Electronic Mail Security | T1 |
| 35 | Tutorial-8 | | |
| 36 | To understand the procedure for PGP | PGP | T1 |
| 37 | To know the procedure of S/MIME | S/MIME | T1 |
| 38 | To know procedure of HMAC | HMAC | T1 |
| 39 | Tutorial-9 | | |
| 40 | To learn the role of IP security | IP Security Overview, Authentication protocols | T1 |
| 41 | To learn about IP security architecture | IPSecurity Architecture, Authentication Header | T1 |
| 42 | Tutorial-10 | | |
| 43 | To know the usage of ESP in IP security | Encapsulating Security Payload | T1 |
| 44 | To know the role of key management | Combining Security Associations, Key Management | T1 |
| 45 | Tutorial-11 | | |
| UNIT-IV | | | |
| 47 | To understand the role of web security | Web Security Requirements | T1 |
| 48 | To understand the functionality of SSL | Secure Socket Layer (SSL) | T1 |
| 49 | To understand TLS | Transport Layer Security (TLS) | T1 |
| 50 | To understand SET | Secure Electronic Transaction (SET) | T1 |
| 51 | Tutorials-12 | | |
| 52 | To understand SSL | Introduction to System Level Security | T1 |
| 53 | To understand Intrusion Detection | Intrusion detection | T1 |
| 54 | To know about password | password management | T1 |

| | | | |
|---|---|---|---|
| | management | | |
| 55 | Tutorial-13 | | |
| 56 | To understand intruders, viruses | Viruses and related Threats | T1 |
| 57 | To know the details of Virus Counter measures | Virus Counter measures | T1 |
| 58 | Tutorial-14 | | |
| 59 | To know firewall principles | Firewall Design Principles – Trusted Systems | T1 |
| 60 | Tutorial-15 | | |

Evaluation scheme:

| Component | Duration (minutes) | % of weightage | Marks | Date & Time | Venue |
|---|---|---|---|---|---|
| Sessional Test – 1 | 90 | 20% | 20 | 01.01.2018 to 06.01.2018, 3.00 PM to 4.30PM | Admin Block |
| Sessional Test – 2 | 90 | 20% | | 19.02.2018 to 24.02.2018, 3.00 PM to 4.30 PM | |
| Sessional Test – 3 | 90 | 20% | | 02.04.2018 to 07.04.2018, 3.00 PM to 4.30 PM | |
| Online exam | 20 | 10% | 10 | 02.04.2018 to 07.04.2018, 10.00 AM to 12.30 AM | |
| Semester End Examination | 180 | 70% | 70 | 16.04.2018 to 24.04.2018 | |

Chamber Consultation Hour: 4 PM to 5PM

Venue: Second Floor staff room (Block-5)

Notices: Main notice board

Signature of the Instructor

Signature of the course-coordinator