Information security and Cryptography Course Syllabus

Ref. comp560u.tex
Vers. Code : 20140401

Overview

Course Title : Information security and Cryptography

Course code :

Credit hours :

Duration : 45 class hours

Course Type : Core course. Graduate level.

Syllabus Prepared by : Prof. S. Parthasarathy (drpartha@gmail.com)

Syllabus Reviewed by : ? ? ? ?

Syllabus Maintained by : Prof. S. Parthasarathy (drpartha@gmail.com)

Course objectives : The objective of the course is to provide a basic understanding of the various issues related to information systems security (e-security). The course will present an overview of the risks encountered in information systems security, and the tools used for resolving these risks.

Prerequisites :: Participants will be expected to have a fairly good background in discrete mathematics. Since the tools used in this course will be based on Linux/FOSS, participants will need to be comfortable working with Linux/FOSS.

Course delivery and methodology :: Will be announced in the class.

Course outline :

1. **Overview of e-security**
   - (a) Threats, risks, consequences
   - (b) Sources of threats
   - (c) Attacks classification
   - (d) Preventive measures, remedial measures
2. **Cryptography for e-security**
   - (a) Historical perspective
   - (b) Confusion vs. diffusion
   - (c) Stream ciphers vs. block ciphers
   - (d) Keys and key management
   - (e) Key exchange (peer to peer, peer - keyserver - peer)
   - (f) Diffie Helman key sharing scheme
   - (g) Symmetric key cryptography vs asymmetric key cryptography
   - (h) Trapdoor functions
3. **Hash digests**
   - (a) Properties of cryptographic hash functions
   - (b) Merkle Damgard construction
   - (c) md family
   - (d) sha family
   - (e) Digital signatures
   - (f) sha3
4. **GPG**
   - (a) Overview of GPG
   - (b) Commands and CLI
   - (c) GPG trust model
   - (d) GUI – KGPG, Seahorse
   - (e) Frontends – Kleopatra, enigmail

5. **Block ciphers**

   (a) Block cipher principles
   (b) Feistel networks
   (c) S boxes and P boxes
   (d) Block cipher modes of operation
   (e) DES
   (f) 3DES
   (g) AES

6. **Elementary number thoery**

   (a) Prime numbers, Factoring
   (b) Modular arithmetic
   (c) Fermat's & Euler's theorems
   (d) gcd, Euclid's algorithm
   (e) Discrete logarithm problem

7. **Public key encryption**

   (a) Public key crypto systems
   (b) RSA algorithm
   (c) Elliptic Curve cryptography

8. **Practical applications**

   (a) PKI, CA. X509 certificates
   (b) SSL/TLS, HTTPS
   (c) IPV6 and IPSEC
   (d) Proxies and Firewalls

9. **Misc. techniques**

   (a) Encryption using non-cryptographic tools (vi, zip)
   (b) Authentication principles and methods
   (c) Passwords, two-factor authentication
   (d) One-way encryption

   (e) Steganography

   (f) Hamming

   (g) Chaffing and Winnowing

10. **Management aspects**

    (a) System Administration policies

    (b) Security audit

    (c) Penetration testing and ethical hacking

    (d) Mandatory Access control, Discretionary Access Control

    (e) Monitoring and logging tools

    (f) Legal aspects

Laboratory sessions

1. Creation of key pairs using GPG
2. Encryption, decryption, signing, verification using GPG
3. Key signing party. Creation of a web of trust
4. Computation of hash digests (md5, sha1)
5. Building a fortress
6. Encryption of a whole drive/partition

Carry-home assignments and exercises

1. Exercises announced by email
2. Mini projects

Recommended Books

1. William Stallings, *Cryptography and network security*, Pearson Education.
2. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone , *Handbook of Applied Cryptography*, CRC Press.
3. Margaret Cozzens, Steven J Miller, *The mathematics of encryption*, American Mathematical Society

4. Bruce Schneier *Applied Cryptography*, John Wiley and Sons

5. Mark Stamp, *Information Security: Principles and Practice*, John Wiley and Sons

6. Matt Bishop, *Computer Security, Art and Science*, Pearson Education

Supplementary study material

1. Tutorial material prepared by Prof.Partha, available in Prof.Partha's website

2. Papers and articles to be suggested by Prof.Partha in the class

3. Material published on the w-w-web, to be suggested by Prof.Partha in the class

4. Material available on the course DVD

* * * * *