SUBJECT DESCRIPTION FORM

Subject Title : Internet Infrastructure Security

Subject Code : COMP5351

Credit Value: 3

Pre-requisite: (Subject title and code no, if any)

Internetworking Protocols and Software I (COMP526) or
Internet Infrastructure & Protocols (COMP5311) or equivalent

Recommended background knowledge: Nil

Mutual Exclusions: Nil

Learning Approach:

42 hours of Class activities including - lecture, tutorial, lab, workshop seminar where applicable

Assessment:

Continuous Assessment	30%
Class Project	35%
Test, and Examination	35%

Objectives:

The overall objective of this course is to build up a foundational understanding on the security issues relevant to the current Internet infrastructure. Specifically,

1. Understand the principles of the three cryptographic functions: secret key, public key, and hash;
2. Understand the four main network security services: secrecy, message integrity, authentication, and nonrepudiation;
3. Understand the major components in today's network security infrastructure, such as public key infrastructure, IPSec, IKE, and SSL/TLS; and
4. Understand the inherent vulnerabilitiies of network protocols, such as TCP and application protocols, and other attacks, such as, buffer-flow attacks and denial-of-service attacks, and their countermeasures.

The Department reserves the right to update the syllabus contents. Please note that the learning approach for the same subject could vary slightly due to different delivery modes.

Learning Outcomes:

After completing this subject, students should be able to:

1. read some articles in a professional computer and network security magazine, such as IEEE Security & Privacy and SC Magazine;
2. use various network diagnosis tools, such as wireshark, to study network security protocols, and educational tools, such as CrypTool, to study cryptographic algorithms; and
3. take on a self-study on more advanced network security topics that require foundational understanding of cryptographic algorithms and network security protocols.

Keyword Syllabus :

1. Cryptographic preliminaries: threat analysis, security goals, security verses privacy, basic cryptographic functions, public key infrastructure and digital signatures

2. Application layer security: DNS and email security, end-to-end security, examples of designing secure application protocols, e.g., Secure Shell, Kerberos, and Pretty Good Privacy

3. Transport layer security: TCP security (initial sequence number attack, SYN flooding attacks, etc), Transport Layer Security protocols and vulnerability analysis

4. IP layer security: IP security associations, authenticated Diffie-Hellman exchange, IPSec, and IKE protocols, routing security

5. Wireless data-link and mobile network security: IEEE 802.11 security, mobile network security (e.g., redirection attacks)

6. Network access control and Internet-wide attacks: firewalls and proxies, intrusion detection, denial-of-service attacks and Internet worms (e.g., Snapper and Code Red)

Indicative reading list and references:

1. C. Kaufman, R. Perlman and M. Speciner, *Network Security: Private Communication in a Public World*, Second Edition, Prentice Hall PTR, 2002.
2. M. Bishop, *Introduction to Computer Security*, Addison Wesley, 2005.
3. B. Schneier. *Applied Cryptography*, Second Edition, Wiley, 1996.
4. N. Ferguson and B. Schneier. *Practical Cryptography*, Wiley, 2003.
5. D. Stinson. *Cryptography: Theory and Practice, Chapman & Hall/CRC*, Second Edition, 2002.
6. A. Menezes and P. van Oorschot. *Handbook of Applied Cryptography*, CRC Press, 1996.
7. D. B. Chapman and E. D. Zwicky, *Building Internet Firewalls*. Second Edition, O'Reilly & Associates, 2000.
8. B. Schneier, *Secrets and Lies*, Wiley, 2000.
9. S. Flannery, *In Code: A Mathematical Journey*, Workman Publishing, 2000.

Supplementary articles from IEEE/ACM publications