SUBJECT DESCRIPTION FORM

Subject title : Internet Security: Principles and Practice

Subject code : COMP 5353

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: COMP5351 Internet Infrastructure Security

Learning approach:

42 hours of class activities, including lectures, tutorials, workshops, and guest seminars

Assessment:

Continuous Assessment	30%
Examination	70%
(Practicum 35%; Written 35%)	

Objectives:

The overall objective of this course is to equip students with foundational principles and practical skills on security issues relevant to the current Internet infrastructure, such as

1. The three main cryptographic functions: secret key, public key, and hash;
2. The four main network security services: secrecy, message integrity, authentication, and nonrepudiation; and
3. Public key infrastructure, IP network security, SSL/TLS, web server and browser security, system security, and network intrusion and defense.

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:

Upon successful completion of this course, students should be able to:

1. Read and understand articles in professional computer and network security magazines, such as IEEE Security & Privacy and SC Magazine.
2. Use Wireshark to analyze network attacks; build, design, and test the security of web applications and web services; and perform basic site penetration tests.
3. Take on a self-study on more advanced network security topics that require foundational understanding of cryptographic algorithms and security of network protocols.

Keyword syllabus :

1. Cryptographic preliminaries: threat analysis, security goals, security verses privacy, basic cryptographic functions, public key infrastructure, and digital signatures
2. IP network and end-to-end security: IP Security, Internet Key Exchange, routing security, SSL/TLS, and TCP security
3. Web and system security: Windows and Linux systems security, web server security, and OWASP top 10 vulnerability for web services
4. Network intrusions: Intrusion detection and prevention, site penetration tests, firewalls, stateful inspection

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.

Indicative reading list and references:

1. R. Anderson. *Security Engineering*, Second Edition, Wiley, 2008.
2. M. Bishop. *Introduction to Computer Security*, Addison Wesley, 2005.
3. B. Chapman and E. Zwicky. *Building Internet Firewalls*. Second Edition, O'Reilly & Associates, 2000.
4. N. Ferguson, B. Schneier, and T. Kohno. *Cryptography Engineering*, Wiley, 2010.
5. C. Kaufman, R. Perlman, and M. Speciner. *Network Security: Private Communication in a Public World*, Second Edition, Prentice Hall PTR, 2002.
6. A. Menezes and P. van Oorschot. *Handbook of Applied Cryptography*, CRC Press, 1996.
7. B. Schneier. *Secrets and Lies*, Wiley, 2000.
8. B. Schneier. *Applied Cryptography*, Second Edition, Wiley, 1996.
9. D. Stinson. *Cryptography: Theory and Practice*, Third Edition, Chapman and Hall/CRC, 2006.

Supplementary articles from IEEE/ACM publications