SUBJECT DESCRIPTION FORM

Subject Title: Information Security: Technologies and Systems

Subject Code: COMP5525

Credit Value: 3

Pre-requisite:

Nil

Recommended background knowledge:

Number System, Programming, Image Processing, Internet and Computer System

Mutual Exclusions:

Information Security: Technologies and Systems (COMP559)

Learning Approach:

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

Assessment:

Continuous Assessment	45%
Test, and Examination	55%

Objectives:

1. To understand the problems with current security technologies and systems; and
2. To introduce biometric computing knowledge and methods.

Learning Outcomes:

After completing this subject, students should be able to:

1. apply both classical and conventional encryption algorithms for information coding;
2. understand the differences between secret key and public-key approaches for information security and their applications;

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.

3. use watermarking techniques for information hiding and authentication; and
4. apply pattern recognition techniques for biometric classification with various applications.

Keyword Syllabus:

Introduction to Information Security
Why information security? Some definitions of security technologies and systems. Software and hardware security and networks security. Access control.

Applied Cryptography
Classical systems. Secret key. Public key. Data encryption standard. Conventional encryption. Substitution and transposition encryption technologies. Encryption algorithms.

Best Privacy Tool: Biometrics
Current privacy tools: password and key. Advantage of using personal features. Biometrics in living body, including human head & face, the mechanism of human eye, hand & skin characteristics, personal voice & sound, and habitual behaviors.

Privacy Biometrics Techniques
Biometrics data acquisition and biometrics database. The related image processing and pattern recognition technologies, including digital image and signal representation, pattern extraction and classification. Basic approaches of automated biometrics identification and verification.

Typical Physical & Behavial Biometrics
Basic security systems using physical and behavial characteristics of biometrics. Some basic introduction of physical and behavial biometrics systems (such as fingerprint, palm-print, finger, hand, face, iris, and face, as well as dental, DNA, retina recognition, voice, signature, gesture recognition, knowledge-based recognition, and keyboard-input-based recognition).

Security Applications
Internet/Intranet. E-Commerce. Banking services. Immigration and Naturalization Service. Benefit Systems. Computer Systems. National Identity. Physical Access. Telephone Systems. Time, Attendance and Monitoring.

Indicative reading list and references:

Books

Stallings, W., 2003, *Cryptography and Network Security, Principles and Practices,* (3rd Edition), Prentice Hall.

Stallings, W., 2000, *Network Security Essentials: Applications and Standard*, Prentice Hall.

Jain, et al., (eds), 1998, *Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publisher.

Sid-Ahmed, M.A., 1995, *Image Processing, Theory, Algorithms, & Architectures*, McGraw-Hill.

Awcock, G.W., 1996, *Applied Image Processing*, McGraw-Hill.

Zhang, D., 2000, *Automated Biometrics: Technologies & Systems*, Kluwer Academic Publishers.

Zhang, D. (ed), 2002, *Biometrics Solutions for Authentication in an E-World*, Kluwer Academic Publishers.