**NUST Institute of Information Technology (NIIT)**
**Department of Information Systems Engineering**

| **EC848** | **Data Security & Privacy** | **Spring 2008** |
|---|---|---|

Credit Hours : 3+0

Instructor: **Dr. Fauzan Mirza** Email: fauzan@niit.edu.pk
Office: **Academic Block 4 (House #164)** Office Hours: Mon-Fri 2pm – 5pm
Extension: AB-4 ext. 13

## Course Objective

The aim of the course is to help the students understand important concepts in various areas of data privacy and protection, including cryptography, operating systems security and software security.Upon completing this course, the students should be able to describe the applications and limitations of several significant cryptographic mechanisms, demonstrate an understanding of why vulnerabilities exist in software and how they are exploited, describe the features and security mechanisms that are generally used to implement security policies, and understand properties of malicious software and how they are detected.

## Preliminary Syllabus

- *Classical cryptology:* Transposition ciphers, Simple substitution ciphers, Polyalphabetic substitution ciphers, Cryptanalysis methods (frequency analysis, Kasiski analysis, Index of Coincidence), Kerckhoffs' principle.
- *Encryption algorithms:* Block ciphers (DES, AES), Stream ciphers (LFSR-based stream ciphers, RC4), Modes of operation (ECB, CBC, CFB, OFB).
- *Public-key cryptography:* Key agreement (Diffie-Hellman), Data encryption (RSA), Digital signatures (RSA), Secret sharing.
- *Integrity and authentication:* Hash functions (MD5, SHA-1), Message-authentication codes, Digital signatures, Identification protocols.
- *Software security:* Database security, File security, Program security, Malicious software, Operating System security, Application security, Secure programming
- *Software protection*: Copy protection techniques, Watermarking, Anti-debugging, Obfuscation.
- *Software vulnerabilities and exploits:* Buffer overflows, format strings, Web application security, SQL injections.
- *Malicious software*: Trojans, Worms, Viruses, Spyware, Scanning and detection techniques.

## Recommended Text Books

The course is mostly based on the following text books:

- M. Bishop, *Computer Security: Art and Science*, Addison Wesley, 2002.
- C.P. Pfleeger, *Security in Computing*, Prentice-Hall, 2002 (third edition).
- D.E. Denning, *Cryptography and Data Security*, Addison-Wesley, 1983.

The following text books are recommended for supplementary reading:

- A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997. (Online at *http://www.cacr.math.uwaterloo.ca/hac/*)
- F. Piper and S. Murphy, *A Very Short Introduction to Cryptography*, Oxford University Press, 2002.
- S. Singh, *The Code Book*, Fourth Estate 1999.
- B. Schneier, *Applied Cryptography*, 2nd Edition, Wiley (1996).
- D. Gollmann, *Computer Security*, John Wiley & Sons, 1999.
- S. Castano, M. Fugini, G. Martella, P. Samarati, *Database Security*, Addison Wesley, 1994.

## Grading / Mark Scheme

- 10/15-Minute Quizzes: 10%
- Assignments: 5%
- Term Project: 15%
- Mid-Term Exam: 30%
- Final Exam: 40%

## Policy Matters

- Assignments will be issued which will be due one week from the issue date.
- Quizzes may be conducted in class during the first 5-10 minutes, and late-comers will suffer.
- Missed quizzes cannot be retaken under any circumstances.
- Anyone found assisting or committing plagiarism in any assignment or quiz will have all their assignment and quiz marks cancelled.
- Project reports due in week 12 and presentation given in weeks 13-15.
- Exams during 8th week and 16th week.
- At least 75% attendance needs to be maintained in order to be allowed to sit the Final Exam.