Lectures for the course: Information and System Security (IT 60112)

Week 1

Lecture 1 – 04/01/2005

- Introduction to the course
- Evaluation Criteria Explained
- Text Books and Research Materials to form part of the syllabus
- Class Test dates announced

Lecture 2 – 06/01/2005

- Computer Security Fundamentals – Confidentiality, Integrity and Availability
- Threats and Attacks
- Policy and Mechanism

Week 2

Lecture 3 – 10/01/2005

- Assumptions and Trust
- Assurance
- Introduction to access Control Matrix

Lecture 4 – 11/01/2005

- Own, Control and Copy rights
- Principle of Attenuation of privileges
- Access Control by Boolean Expression evaluation

Class on 13/01/2005 missed due to pre-occupation – to be compensated on 18/01/2005

Week 3

Lecture 5 – 17/01/2005

- Access Control by History
- Query-set Overlap based access control
- Introduction to protection state transition

Lecture 6 (A+B) – 18/01/2005

- Protection Systems
- Protection State – Representation, Commands, Primitive operators
- State representations and transitions

Lecture 7 – 20/01/2005

- Security Policies
- Confidentiality and Integrity Policy – Precise Definitions
- Precise and Broad security mechanisms
- Secure Systems
- Military and Commercial Policies
- Security mechanism
- Types of Access Control – Mandatory, Discretionary and Originator Controlled

Week 4

Lecture 8 – 24/01/2005

- Policy Language – High Level Policy Language – Java

Lecture 9 (A+B) – 25/01/2005

- Class Test 1 was held here

Lecture 10 – 27/01/2005

- Work by Jones and Lipton on Security and Precision
- Observability Postulate
- Secure Policy
- Precise Policy
- Union of policies to form new policies

Week 5

Lecture 11 – 31/01/2005

- Bell-LaPadula Model
- Classification and Categories
- Security Levels
- Simple Security Condition
- * Property

Lecture 12 – 01/02/2005

- Bell-LaPadula Model
- Basic Security Theorem
- Principle of Strong and Weak Tranquility
- Class Test 1 scripts were shown

Lecture 13 – 03/02/2005

- Information Transfer Path
- Biba's Integrity Model
- Low Water Mark
- Ring Policy
- Biba's Strict Integrity Model

<u>Week 6</u>

Lecture 14 – 07/02/2005

- Lipner's Requirements of commercial applications
- Lipner's Integrity Matrix Model

Lecture 15 – 08/02/2005

- Clark Wilson's Model

Lecture 16 – 10/02/2005

- Chinese Wall Security Policy
- Summary of the portions covered so far

<u>Week 7</u>

Lecture 17 – 14/02/2005

- Authentication Systems
- Security issues
- Dictionary attacks on passwords
- Countering Password Guessing

Lecture 18 – 15/02/2005

- Random Passwords
- Pronounceable Passwords
- Password Aging
- User specified Passwords

- Proactive Password Checking
- Attacks using authentication function – Ways to counter them

Week 8

Beak for Mid-Semester Examination

Week 9

Lecture 19 – 28/02/2005

- Mid-sem script were shown

Lecture 20 – 01/03/2005

- Challenge-Response
- Pass Algorithms
- Introduction to one-time passwords

Lecture 21 – 03/03/2005

- One-time Passwords – S/Key

Week 10

Lecture 22 – 07/03/2005

- Kerberos - Introduction

Lecture 23 – 08/03/2005

- Kerberos Version 4
- Overview of Version 5
- Realms and Multiple Kerberi

Lecture 24 – 10/03/2005

- Introduction to cryptography and cryptanalysis
- Stream Ciphers and Block Ciphers
- Public Key Cryptography and Private Key Cryptography
- Substitution and Transposition
- Types of Attack
- Caesar Cipher

Week 11

Lecture 25 – 14/03/2005

- Vigenere Cipher
- Vernam Cipher
- One time Pad
- Transposition Ciphers

Lecture 26 – 15/03/2005

- Simplified DES
- Key Generation and Encryption

Lecture 27 – 17/03/2005

- DES
- Introduction to Public Key Cryptosystems

Week 12

Lecture 28 – 21/03/2005

- Diffie-Hellman Key Exchange

Lecture 29 – 22/03/2005

- Class Test 2 was held here

Lecture 30 – 24/03/2005

- RSA
- Digital Certificate and X.509

Week 13

Lecture 31 – 28/03/2005

- Plan for the rest of the semester
- Eight Secure System Design Principles

Lecture 32 – 29/03/2005

- Assurance – Introduction
- Assurance during life cycle of a project

Lecture 33 – 31/03/2005

- Evaluation Criteria
- TCSEC
- ITSEC
- CC
- SSE-CMM

Week 13

Lecture 34 – 04/04/2005

- Malicious Logic
- Trojan Horse
- Virus – Boot sector, File Virus, Encrypted, Macro
- Worms and Bacteria

Lecture 35 – 05/04/2005

- Detection of Virus
- Avoidance of file contamination by virus

Lecture 36 – 07/04/2005

- Mandatory Access Control for prevention of Virus
- Watchdog Programs
- Signature blocks
- N-Version Programming
- Programmer Characteristics

Week 14

Lecture 37 – 11/04/2005

- Vulnerability Analysis
- Penetration Testing
- Layers of Testing
- Flaw Testing Methodology
- Penetration of a Burroughs System

Lecture 38 – 12/04/2005

- Social Engineering
- Secure Document Control
- Vulnerability Classifications and Frameworks
- NRL Taxonomy

Lecture 39 – 14/04/2005

- Holiday Declared

Week 15

Lecture 40 – 18/04/2005

- Holiday Declared

Lecture 41 – 19/04/2005

- Summary and Feedback

Lecture 42 – 20/04/2005

- Preparatory Leave

End of the Course