

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

Week 1

Lecture 1 – 29/12/2010

- Introduction to the course
- Evaluation guidelines
- Attendance requirement

Lecture 2 – 30/12/2010

- Security Fundamentals – Confidentiality, Integrity, Availability
- Threats and their classification
- Some types of attacks

Lecture 3 – 31/12/2010

- Policy and mechanism
- Assumptions and trust
- Assurance
- Legal, organization and people issues

Week 2

Lecture 4 – 5/01/2011

- Protection system and protection states
- Access Control Matrix model
- ACM to represent protection state
- Copy right, own right

Lecture 5 – 6/01/2011

- Access control by Boolean expression evaluation
- HRU Model - Introduction

Lecture 6+7 – 7/01/2011

- HRU Model – Details
- Model, State transition, reachability
- Undecidability results

Week 3

Lecture 8 – 12/01/2011

- Recap of HRU Model
- Relation between richness and ability to analyze models
- Take Grant Protection Model
- Graph rewriting rules
- Safety in Subject only graph

Lecture 9 – 13/01/2011

- Further discussions on Take Grant Protection Model
- Safety in Subject-object graph

Lecture 10+11 – 14/01/2011

- Bell-LaPadula Model
- Preliminary version and full version
- Current security level and original security level

Week 4

Lecture 12 – 19/01/2011

- Integrity policies
- Biba's model – three versions
- Information transfer path

Lecture 13 – 20/01/2011

- Requirements of commercial systems as suggested by Lipner
- Separation of duty and other general characteristics of commercial systems
- Lipner' model

Lecture 14 – 21/01/2011

- Clark Wilson Model

Week 5

Lecture 15 – 27/01/2011

- Chinese Wall security policy

Lecture 16 – 31/01/2011

- Introduction to authentication
- Components of an authentication system
- Password based authentication
- System generated password
- Dictionary attacks and minimum length of password
- User selected password
- Password aging

Week 6

Lecture 17 – 02/02/2011

- Guessing through authentication function
- S/Keys one time password

Lecture 18 – 03/02/2011

- Kerberos

Lecture 19+20 – 04/02/2011

- Class Test 1

Week 7

Lecture 21 – 10/02/2011

- Kerberos realms and multiple Kerber
- Class test script shown and feedback given

Lecture 22 – 11/02/2011

- Secure system design principles

Week 8

Mid Sem Exam

Week 9

Lecture 23 – 02/03/2011

- Introduction to RBAC

- Mid-sem test script shown and feedback given

Lecture 24 – 03/03/2011

- RBAC0 and RBAC1

Lecture 25 – 04/03/2011

- RBAC2 and RBAC3
- ARBAC

Week 10

Lecture 26 – 09/03/2011

- New directions in research on RBAC
- Possibilities of temporal, spatial and spatio-temporal extensions
- Introduction to Temporal RBAC
- Notion of calendar and sub-calendar
- Periodic expression
- Representation of time

Lecture 27 – 10/03/2011

- TRBAC Model syntax
- Event expressions, REB
- Run time request expression

Lecture 28 – 11/03/2011

- Other possible temporal extensions to RBAC
- Capturing location information for Spatial and Spatio-temporal RBAC
- Introduction to role engineering
- Top down and bottom up approaches
- Role mining
- Basic role mining problem
- Delta-consistency
- Delta-approx RMP

Week 11

Lecture 29 – 16/03/2011

- Minimal Noise RMP

- Mapping RMP to Database Tiling Problem

Lecture 30 – 17/03/2011

- Greedy approach to database tiling problem
- Mapping tiles to roles
- Mapping basic RMP to Minimum Biclique Cover problem

Lecture 31 – 18/03/2011

- Finding Biclique Covers to generate roles
- Comparison between RMP, Database Tiling and MBC problems
- Research directions – Other objective functions, Constrained Role mining, Mining temporal roles

Week 12

Lecture 32 – 23/03/2011

- Introduction to assurance
- Trust and assurance
- Relation between Policy, Model and System
- Policy assurance, design assurance, development/implementation assurance, operational and administrative assurance
- Role of certification

Lecture 33 – 24/03/2011

- Informal, Semi-formal and Formal methods for security assurance
- Role of peer review in assurance
- Defect report, Upper Control Limit and Lower Control Limit
- Controlling process
- Quantitative measurement of quality

Lecture 34 – 25/03/2011

- Class Test 2 held

Week 13

Lecture 35 – 30/03/2011

- Quantitative process management
- Other metrics like productivity, defect leakage
- Assurance based on quantitative measure of quality

Lecture 36 – 31/03/2011

- Class test 2 scripts shown and feedback given
- Practical demonstration of peer review

Lecture 37 – 01/04/2011

- Configuration management
- Process audit

Week 14

Lecture 38 – 06/04/2011

- Formal methods for assurance
- Model checking approach
- CTL

Lecture 39 – 07/04/2011

- Further clarifications on model checking
- Introduction to Evaluating Systems
- TCSEC overview

Lecture 40+41 – 08/04/2011

- TCSEC details
- ITSEC
- Highlights of CC

Week 15

Lecture 42 – 13/04/2011

- Intrusion detection systems
- Misuse based and anomaly based
- Network, host and hybrid IDSs
- Base rate fallacy and difficulty in anomaly detection

Lecture 43 – 15/04/2011

- Summary and conclusion