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

Week 1

Lecture 1 – 02/01/2012

• Introduction to the course
• Evaluation Guidelines
• Term paper and Term project guidelines

Lecture 2 – 03/01/2012

• Confidentiality, Integrity and Availability
• Threats
• Policy and Mechanism

Lecture 3 – 05/01/2012

• Goals of security
• Assumptions and trust
• Assurance
• Operational issues
• Organizational issues

Week 2

Lecture 4 – 09/01/2012

• Protection state of a system
• Access Control Matrix
• Various system states represented as ACM
• Access control by Boolean expression evaluation

Lecture 5 – 10/01/2012

• Own, copy and surrender of rights
• Principle of attenuation of privilege
• Introduction to HRU Model
• Components of the model
• Commands, interpretation and constraints
• Example commands
Lecture 6 – 12/01/2012

- How a primitive operation can be used to yield one configuration to another in HRU
- Generating new configurations using commands in HRU
- Example state transition in HRU

Week 3

Lecture 7 – 16/01/2012

- Leakage of right and safety in HRU
- Safety in mono-operational model
- Introduction to Take Grant protection model

Lecture 8 – 17/01/2012

- Take Grant protection model
- t and g rights
- Rules for state transition
- Sharing of rights between two subjects that are connected by t or g in either direction

Lecture 9 – 19/01/2012

- Sharing in subject only graphs
- Sharing subject-object graphs
- Blocks and bridges
- Linear time algorithm for deciding whether a subject can obtain a right
- Notion of sharing and stealing
- Characteristics of TG protection model

Week 4

Lecture 10 – 24/01/2012

- Confidentiality and integrity policies
- DAC, MAC, ORAC
- Bell-LaPadula model

Week 5

Lecture 11 – 31/01/2012

- Biba’s model
• Low water mark policy, Ring policy and complete model

Week 6

Lecture 12 – 06/02/2012
• Integrity requirements of commercial systems
• Lipner’s model

Lecture 13 – 06/02/2012 (Compensatory)
• Clark-Wilson integrity model
• Chinese Wall security model

Lecture 14 – 07/02/2012
• Class test 1 held

Lecture 15 – 09/02/2012
• Class test scripts shown and feedback given
• Introduction to authentication
• Components of an authentication system
• Password based authentication
• Length of password and alphabet size
• Time for guessing a password and counter measures
• Type 1 dictionary attack

Week 7

Lecture 16 – 13/02/2012
• Type 2 dictionary attack
• Pronounceable password
• Challenge-response and pass algorithm
• SKey one time password

Lecture 17 – 14/02/2012
• Further discussions on SKey one time password
• Kerberos

Lecture 18 – 14/02/2012 (extra lecture)
• Kerberos realms and multiple kerberi
Week 8

Mid-sem Exam.

Week 9

Lecture 19 – 27/02/2012
• Secure system design principles
• Mid sem scripts shown and feedback given

Lecture 20 – 28/02/2012
• Introduction to RBAC

Lecture 21 – 01/03/2012
• RBAC0, RBAC1, RBAC2 and RBAC3

Week 10

Lecture 22 – 05/03/2012
• Administrative RBAC
• Temporal, spatial and spatio-temporal extensions of RBAC
• Introduction to TRBAC
• Calendars, sub-calendars and Periodic expressions

Lecture 23 – 06/03/2012
• Evaluating intervals in periodic expressions, pi function
• Sol function
• Simple and prioritized event expressions, role status expressions
• Role enabling base – periodic event, role triggers
• Run time requests

Week 11

Lecture 24 – 12/03/2012
• Conflicting events
• Blocked events and Nonblocked events
• Introduction to role mining
Lecture 25 – 13/03/2012

- Boolean matrix multiplication
- Delta consistency
- Basic role mining problem
- Delta-approx RMP
- Min-noise RMP
- Nature of the RMP problems

Lecture 26 – 15/03/2012

- Mapping RMP to database tiling problem
- Minimum tiling problem
- Mapping min-noise RMP to database tiling problem

Week 12

Lecture 27 – 19/03/2012

- Mapping RMP to minimum biclique cover problem

Lecture 28 – 20/03/2012 (including compensatory lecture)

- Problems on minimum biclique cover and RBAC solved in class

Lecture 29 – 22/03/2012

- Introduction to assurance
- Sources of errors in secure systems
- Policy, design, implementation and operational assurance
- Informal, Semi-formal and formal approaches
- Evaluating systems based on assurance- TCSEC, ITSEC and CC

Week 13

Lecture 30 – 26/03/2012

- Peer review
- Defect report, review effectiveness
- Project estimation, productivity, person-month
- UCL and LCL of review effectiveness

Lecture 31 – 27/03/2012

- Other metrics – productivity, defect leakage
• Requirements traceability
• Different models for system development – fixed cost and T&M
• Internal audit and senior management review
• External audit – Certification audit and surveillance audit
• Certification based on evidence of assurance in the form of internal audit reports and other reports like defect report, etc.

Lecture 32 – 29/03/2012

• Configuration Management
• Problem report
• Detection of problem by external entities/other phase reviews
• Version numbering

Week 14

Lecture 33 – 02/04/2012

• Formal methods of assurance
• Various formal methods
• Model checking
• CTL
• Example safety, non-blocking and liveness properties and their verification on a given model

Lecture 34 – 03/04/2012

• Further examples of model checking
• Validation vs. verification
• Review of property specifications

Week 15

Lecture 35 – 09/04/2012

• Evaluating systems
• TCSEC
• ITSEC

Lecture 36 – 10/04/2012

• CC, CCRA, Indian perspective and current status
• Intrusion detection systems
• NIDS and HIDS
• Misuse based and anomaly based
• True positive, false positive, true negative and false negative

Lecture 37 – 12/04/2012

• Base rate fallacy and the problem of intrusion detection

Week 16

Lecture 38 – 13/04/2012

• Term projects demonstrated