# IS2150/TEL2810 Information Security and Privacy

## *Tentative Course Schedule from Earlier Semester (Will try to follow this but will update)*

## *(Chapters are from Green Book)*

| ***Week #*** | ***Topic*** | ***Objective***: The students are expected to have the following capability after the lecture | ***Reading/Testing*** |
|---|---|---|---|
| Week 1<br><br>(Lecture 1) | Introduction Secure Design Principles | • *Define/Describe/explain* some key security terms<br>• *Describe/explain* the importance of trust, assurance and operational issues within the security area<br>• *Explain* the secure design principles and its importance | • Chap 1: Overview of Security<br>• Chap 12: Design Principles<br><br>• **Reading Assignment** |
| Week 2<br><br>(Lecture 2.1, Lecture 2.2) | Access control in Unix and Windows<br><br>Mathematical Review | • *Recognize* the basic access control mechanism in OS<br>• *Use* access control commands to *manipulate* permissions in the OS<br>• *Quick overview of maths*<br>  • *Write* a sentence in logic form and *interpret* the logic expressions<br>  • *Solve* problems using mathematical induction<br>  • *Interpret, analyze and construct* lattice structures | • Unix (Garfinkel book in Text book list in main page)<br>• Microsoft Reference (http://technet.microsoft.com/en-us/library/cc781716.aspx)<br>• (Bishop's brown book has intro on these topics - Logic, Induction and Lattice) + Chapter 2<br><br>• **Lab 1 Out (Due after 2 Weeks)**<br>• **Homework 1 Out (Due after 1 week)** |
| Week 3<br><br>(Lecture 3) | HRU Access Control Matrix | • *Represent/Describe* formally the safety problem using ACM<br>• *Reason* and *Demonstrate* the undecidability result related to security | • Chap 3 : HRU Access Control Model and results<br>• **Homework 2 Out (Due after 2 Weeks)**<br>• **Quiz 1** (for Week 1, 2, 3)<br>(Quiz is after this week's modules) |
| Week 4<br><br>(Lecture 4) | Confidentiality, Integrity: (BLP, Biba models) | • *Understand/Explain* the confidentiality, integrity and *relate* them to application needs<br>• *Employ* them to new applications and synthesize solution | • Chap 4 –7 : Security Policies, Confidentiality and Integrity Models<br>• **Lab 2** Out (Due after: 2 Weeks) |
| Week 5<br><br>(Lecture 5) | Hybrid Policy Models (Clark-Wilson, Chinese Wall, RBAC) | • *Understand/Explain* the hybrid policy models and *relate* them to application needs<br>• *Employ* them to new applications and synthesize solution | • RBAC (refer to NIST Standard paper in Reading List)<br>• **Homework 3 (Due after 2 Weeks)** |
| Week 6<br><br>(Lecture 6) | Privacy Issues/Models | • *Understand/Explain* general privacy issues, models and solution approaches | • Reading (PrivacyPaper1.pdf, PrivacyPaper2.pdf, PrivacyPaper3.pdf )<br>• **Quiz 2** (for Week 4, 5, and 6; after module 6) |
| Week 7<br><br>(Lecture 7) | Authentication and Identity, Basics of Cryptography | • *Recognize/explain* and use the authentication techniques, identity issues, and basic cryptographic techniques | • Chap 9: Basic Cryptography and Network Security<br>• **Homework 4 Out (Crypto/NetSec) 3 (Due after 2 Weeks)** |

**Homeworks/Labs are due by the end of the due date, i.e., by 11:59PM**

| | | | |
|---|---|---|---|
| Week 8<br><br>(Lecture 8) | Network Security | • *Explain* and *employ* the basic network security techniques (Secure protocols, certificates, signatures, etc.) | • Chap 9, 11, 20<br>• **Quiz 3 (for Week 7 and 8)** |
| Week 9 | **Midterm** | **Programming Project/Assignment**<br>**Java programming Project** Out (Due: Last Week of the Semester) | |
| Week 10 | **Spring Break** | | |
| Week 11<br><br>(Lecture 11) | Security Evaluation, Legal and Ethical Issues | 1. *Explain* the main idea behind common criteria<br>2. *Recognize*, *define/explain* legal and ethical concerns related to security | 3. Legal Issues (Stallings book: Chapter 18)<br>4. Chap 18: Evaluation standards<br>5. **HW 5 (Due after 1 Week)** |
| Week 12<br><br>(Lectures 12.1, 12.2, 12.3) | Malicious Code, Vulnerability Analysis; Risk Management, | 6. *Recognize*, *compare*/*contrast*, *explain* different types of malicious code<br>7. *Recognize* the importance of risk management process and *employ* it to *assess* and *solve* organizational security<br>8. *Recognize*, *classify* and *compare* vulnerability (taxonomy/classification) | 9. Chapters: 19, 20<br>10. NIST Risk Management document (http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf) |
| Week 13<br>(Lecture 13) | Software Security | 11. *Recognize*, *compare*/*contrast*, *explain* different types of coding related software issues (e.g., program exploits, buffer overflow, SQL Injections, etc.) | 12. Chapter on String from Seacord's "Secure Programming in C/C++" (and reading list<br>13. **Quiz 4** (for Week 11, 12 and 13) |
| Week 14<br><br>(Lecture 14) | IDS; Auditing; Firewalls | 14. *Recognize*, *explain* and *analyze* auditing/IDS/Auditing systems | 15. Chap 20, 21, 22<br>16. **HW6 (Reading assignment): DDoSSurvey.pdf paper – write a 1 page summary** |
| Week 15<br><br>(Lecture 15) | Overview of security of emerging systems/issues (Cloud, SN, BigData, ATP) | 17. *Recognize*, *explain* the basic security and privacy issues in new systems<br>18. *Understand*, *explain* privacy models and approaches | 19. Readings:<br>1. NIST 800-144, "Guidelines on Security and Privacy in Public Cloud Computing"<br>2. H. Takabi, J. Joshi, G-J Ahn, "Security and Privacy Challenges in Cloud Computing Environments" IEEE Security and Privacy, 2010<br>3. http://www.isaca.org/Groups/Professional-English/big-data/GroupDocuments/Big_Data_Top_Ten_v1.pdf<br>~~20.~~ **Quiz 5** (for Week 14, 15) |
| Week 16 | 21. Final Exams | | |