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 (Lecture 1)	Introduction Secure Design Principles	• *Define/Describe/explain* some key security terms • *Describe/explain* the importance of trust, assurance and operational issues within the security area • *Explain* the secure design principles and its importance	• Chap 1: Overview of Security • Chap 12: Design Principles • **Reading Assignment**

Week 2
 	
(Lecture 2.1, Lecture 2.2)
	Access control in Unix and Windows
	
	Mathematical Review
		• *Recognize* the basic access control mechanism in OS
		• *Use* access control commands to *manipulate* permissions in the OS
		• *Quick overview of maths*
		  • *Write* a sentence in logic form and *interpret* the logic expressions
		  • *Solve* problems using mathematical induction
		  • *Interpret, analyze and construct* lattice structures
			• Unix (Garfinkel book in Text book list in main page)
			• Microsoft Reference (http://technet.microsoft.com/en-us/library/cc781716.aspx)
			• (Bishop's brown book has intro on these topics - Logic, Induction and Lattice) + Chapter 2
			
			• **Lab 1 Out (Due after 2 Weeks)**
			• **Homework 1 Out (Due after 1 week)**

Week 3 (Lecture 3)	HRU Access Control Matrix	• *Represent/Describe* formally the safety problem using ACM • *Reason* and *Demonstrate* the undecidability result related to security	• Chap 3 : HRU Access Control Model and results • **Homework 2 Out (Due after 2 Weeks)** • **Quiz 1** (for Week 1, 2, 3) (Quiz is after this week's modules)
Week 4 (Lecture 4)	Confidentiality, Integrity: (BLP, Biba models)	• *Understand/Explain* the confidentiality, integrity and *relate* them to application needs • *Employ* them to new applications and synthesize solution	• Chap 4 –7 : Security Policies, Confidentiality and Integrity Models • **Lab 2** Out (Due after: 2 Weeks)
Week 5 (Lecture 5)	Hybrid Policy Models (Clark-Wilson, Chinese Wall, RBAC)	• *Understand/Explain* the hybrid policy models and *relate* them to application needs • *Employ* them to new applications and synthesize solution	• RBAC (refer to NIST Standard paper in Reading List) • **Homework 3 (Due after 2 Weeks)**
Week 6 (Lecture 6)	Privacy Issues/Models	• *Understand/Explain* general privacy issues, models and solution approaches	• Reading (PrivacyPaper1.pdf, PrivacyPaper2.pdf, PrivacyPaper3.pdf) • **Quiz 2** (for Week 4, 5, and 6; after module 6)
Week 7 (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 • **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 (Lecture 8)	Network Security	• *Explain* and *employ* the basic network security techniques (Secure protocols, certificates, signatures, etc.)	• Chap 9, 11, 20 • **Quiz 3 (for Week 7 and 8)**
Week 9	**Midterm**	**Programming Project/Assignment** **Java programming Project** Out (Due: Last Week of the Semester)	
Week 10	**Spring Break**		
Week 11 (Lecture 11)	Security Evaluation, Legal and Ethical Issues	1. *Explain* the main idea behind common criteria 2. *Recognize*, *define/explain* legal and ethical concerns related to security	3. Legal Issues (Stallings book: Chapter 18) 4. Chap 18: Evaluation standards 5. **HW 5 (Due after 1 Week)**
Week 12 (Lectures 12.1, 12.2, 12.3)	Malicious Code, Vulnerability Analysis; Risk Management,	6. *Recognize*, *compare*/*contrast*, *explain* different types of malicious code 7. *Recognize* the importance of risk management process and *employ* it to *assess* and *solve* organizational security 8. *Recognize*, *classify* and *compare* vulnerability (taxonomy/classification)	9. Chapters: 19, 20 10. NIST Risk Management document (http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf)
Week 13 (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 13. **Quiz 4** (for Week 11, 12 and 13)
Week 14 (Lecture 14)	IDS; Auditing; Firewalls	14. *Recognize*, *explain* and *analyze* auditing/IDS/Auditing systems	15. Chap 20, 21, 22 16. **HW6 (Reading assignment): DDoSSurvey.pdf paper – write a 1 page summary**
Week 15 (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 18. *Understand*, *explain* privacy models and approaches	19. Readings: 1. NIST 800-144, "Guidelines on Security and Privacy in Public Cloud Computing" 2. H. Takabi, J. Joshi, G-J Ahn, "Security and Privacy Challenges in Cloud Computing Environments" IEEE Security and Privacy, 2010 3. http://www.isaca.org/Groups/Professional-English/big-data/GroupDocuments/Big_Data_Top_Ten_v1.pdf ~~20.~~ **Quiz 5** (for Week 14, 15)
Week 16	21. Final Exams		