IS2150/TEL2810 Information Security and Privacy

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

(updated on Jan 8, 2026)

- *This is tentative schedule and changes (on weekly topic and content) are expected*
- *Key content are from Chapters from Green Book; but other sources will be used.*
- *Expect Quiz in each class based on the content covered after last quiz (or as announced).*
- *Attendance will be randomly taken at any time during the class*

Week #	***Topic***	***Objective***: The students are expected to have the following capability after the lecture	***Reading/Testing***
Week 1 (Lecture 1) **Jan 14**	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
Week 2 (Lecture 2) **Jan 21**	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 background* • *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 (Due after 2/3 Weeks)**
Week 3 (Lecture 3) **Jan 29**	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 • **Quiz 1**
Week 4 (Lecture 4) **Feb 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 • **HW 1**
Week 5 (Lecture 5) **Feb 11**	Hybrid Policy Models (Clark-Wilson, Chinese Wall, RBAC, ABAC)	• *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) • **Lab 2** (Due after: 2/3 Weeks) • **Quiz 2**
Week 6 (Lecture 6) **Feb 18**	Privacy Issues/Models	• *Understand/Explain* general privacy issues, models and solution approaches	• Reading • **HW 2 (due in two weeks)**
Week 7 (Lecture 7) **Feb 25**	Basics of Cryptography	• *Recognize/explain* and use the authentication techniques, identity issues, and basic cryptographic techniques	• Chap 9: Basic Cryptography and Network Security • **Quiz 3**

Week 8 **March 4**	**Midterm**		
Fall Break: March 8-15			
Week 9 (Lecture 8) **March 18**	Network Security	- *Explain* and *employ* the basic network security techniques (Secure protocols, certificates, signatures, etc.)	- Chap 9, 11, 20 - **Lab 3** (Due after: 2/3 Weeks) - **Focus on project starts**
Week 10 (Lecture 9) **March 25**	Authentication; IDS; Auditing; Firewalls	- *Recognize*, *explain* and *analyze* auditing/IDS/Auditing systems	- Chap 20, 21, 22
Week 11 (Lectures 10) **April 1**	Malicious Code, Vulnerability Analysis; Risk Management,	- *Recognize*, *compare/contrast*, *explain* different types of malicious code - *Recognize* the importance of risk management process and *employ* it to *assess* and *solve* organizational security - *Recognize*, *classify* and *compare* vulnerability (taxonomy/classification)	- Chapters: 19, 20 - NIST Risk Management document (http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf) - **Quiz 4** - **Project (proposal due)**
Week 12 (Lecture 11) **April 8**	Software Security	- *Recognize*, *compare/contrast*, *explain* different types of coding related software issues (e.g., program exploits, buffer overflow, SQL Injections, etc.)	- Chapter on String from Seacord's "Secure Programming in C/C++" (and reading list
Week 13 (Lecture 12) **April 15**	AI Security and privacy; Blockchain	- *Recognize*, *explain* the basic security and privacy issues in new systems (AI/ML, LLM, etc.) - *Understand, explain B*lockchain and Distributed Ledger Technologies	- Reading papers (will be updated) - **Quiz 5**
Week 14 (Lecture 13) **April 22**	Security Evaluation, Legal and Ethical Issues	- *Explain* the main idea behind common criteria - *Recognize, define/explain* legal and ethical concerns related to security	- Legal Issues (Stallings book: Chapter 18) - Chap 18: Evaluation standards
Week 15 **April 29**	Final Exams		