

## 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	<i>Objective:</i> The students are expected to have the following capability after the lecture	<i>Reading/Testing</i>
Week 1  (Lecture 1)	Introduction Secure Design Principles	<ul style="list-style-type: none"> <li>• <i>Define/Describe/explain</i> some key security terms</li> <li>• <i>Describe/explain</i> the importance of trust, assurance and operational issues within the security area</li> <li>• <i>Explain</i> the secure design principles and its importance</li> </ul>	<ul style="list-style-type: none"> <li>• Chap 1: Overview of Security</li> <li>• Chap 12: Design Principles</li> <li>• <b>Reading Assignment</b></li> </ul>
Week 2  (Lecture 2.1, Lecture 2.2)	Access control in Unix and Windows  Mathematical Review	<ul style="list-style-type: none"> <li>• <i>Recognize</i> the basic access control mechanism in OS</li> <li>• <i>Use</i> access control commands to <i>manipulate</i> permissions in the OS</li> <li>• <i>Quick overview of maths</i> <ul style="list-style-type: none"> <li>• <i>Write</i> a sentence in logic form and <i>interpret</i> the logic expressions</li> <li>• <i>Solve</i> problems using mathematical induction</li> <li>• <i>Interpret, analyze and construct</i> lattice structures</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Unix (Garfinkel book in Text book list in main page)</li> <li>• Microsoft Reference (<a href="http://technet.microsoft.com/en-us/library/cc781716.aspx">http://technet.microsoft.com/en-us/library/cc781716.aspx</a>)</li> <li>• (Bishop's brown book has intro on these topics - Logic, Induction and Lattice) + Chapter 2</li> <li>• <b>Lab 1 Out (Due after 2 Weeks)</b></li> <li>• <b>Homework 1 Out (Due after 1 week)</b></li> </ul>
Week 3  (Lecture 3)	HRU Access Control Matrix	<ul style="list-style-type: none"> <li>• <i>Represent/Describe</i> formally the safety problem using ACM</li> <li>• <i>Reason and Demonstrate</i> the undecidability result related to security</li> </ul>	<ul style="list-style-type: none"> <li>• Chap 3 : HRU Access Control Model and results</li> <li>• <b>Homework 2 Out (Due after 2 Weeks)</b></li> <li>• <b>Quiz 1</b> (for Week 1, 2, 3) (Quiz is after this week's modules)</li> </ul>
Week 4  (Lecture 4)	Confidentiality, Integrity: (BLP, Biba models)	<ul style="list-style-type: none"> <li>• <i>Understand/Explain</i> the confidentiality, integrity and <i>relate</i> them to application needs</li> <li>• <i>Employ</i> them to new applications and synthesize solution</li> </ul>	<ul style="list-style-type: none"> <li>• Chap 4 –7 : Security Policies, Confidentiality and Integrity Models</li> <li>• <b>Lab 2 Out (Due after: 2 Weeks)</b></li> </ul>
Week 5  (Lecture 5)	Hybrid Policy Models (Clark-Wilson, Chinese Wall, RBAC)	<ul style="list-style-type: none"> <li>• <i>Understand/Explain</i> the hybrid policy models and <i>relate</i> them to application needs</li> <li>• <i>Employ</i> them to new applications and synthesize solution</li> </ul>	<ul style="list-style-type: none"> <li>• RBAC (refer to NIST Standard paper in Reading List)</li> <li>• <b>Homework 3 (Due after 2 Weeks)</b></li> </ul>
Week 6  (Lecture 6)	Privacy Issues/Models	<ul style="list-style-type: none"> <li>• <i>Understand/Explain</i> general privacy issues, models and solution approaches</li> </ul>	<ul style="list-style-type: none"> <li>• Reading (PrivacyPaper1.pdf, PrivacyPaper2.pdf, PrivacyPaper3.pdf )</li> <li>• <b>Quiz 2</b> (for Week 4, 5, and 6; after module 6)</li> </ul>
Week 7  (Lecture 7)	Authentication and Identity, Basics of Cryptography	<ul style="list-style-type: none"> <li>• <i>Recognize/explain</i> and use the authentication techniques, identity issues, and basic cryptographic techniques</li> </ul>	<ul style="list-style-type: none"> <li>• Chap 9: Basic Cryptography and Network Security</li> <li>• <b>Homework 4 Out (Crypto/NetSec) 3 (Due after 2 Weeks)</b></li> </ul>

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

Week 8 (Lecture 8)	Network Security	<ul style="list-style-type: none"> <li>• <i>Explain and employ</i> the basic network security techniques (Secure protocols, certificates, signatures, etc.)</li> </ul>	<ul style="list-style-type: none"> <li>• Chap 9, 11, 20</li> <li>• <b>Quiz 3 (for Week 7 and 8)</b></li> </ul>
Week 9	<b>Midterm</b>	<b>Programming Project/Assignment</b> <b>Java programming Project Out (Due: Last Week of the Semester)</b>	
Week 10	<b>Spring Break</b>		
Week 11 (Lecture 11)	Security Evaluation, Legal and Ethical Issues	<ol style="list-style-type: none"> <li>1. <i>Explain</i> the main idea behind common criteria</li> <li>2. <i>Recognize, define/explain</i> legal and ethical concerns related to security</li> </ol>	<ol style="list-style-type: none"> <li>3. Legal Issues (Stallings book: Chapter 18)</li> <li>4. Chap 18: Evaluation standards</li> <li>5. <b>HW 5 (Due after 1 Week)</b></li> </ol>
Week 12 (Lectures 12.1, 12.2, 12.3)	Malicious Code, Vulnerability Analysis; Risk Management,	<ol style="list-style-type: none"> <li>6. <i>Recognize, compare/contrast, explain</i> different types of malicious code</li> <li>7. <i>Recognize</i> the importance of risk management process and <i>employ</i> it to <i>assess</i> and <i>solve</i> organizational security</li> <li>8. <i>Recognize, classify</i> and <i>compare</i> vulnerability (taxonomy/classification)</li> </ol>	<ol style="list-style-type: none"> <li>9. Chapters: 19, 20</li> <li>10. NIST Risk Management document (<a href="http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf">http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf</a>)</li> </ol>
Week 13 (Lecture 13)	Software Security	<ol style="list-style-type: none"> <li>11. <i>Recognize, compare/contrast, explain</i> different types of coding related software issues (e.g., program exploits, buffer overflow, SQL Injections, etc.)</li> </ol>	<ol style="list-style-type: none"> <li>12. Chapter on String from Seacord's "Secure Programming in C/C++" (and reading list</li> <li>13. <b>Quiz 4</b> (for Week 11, 12 and 13)</li> </ol>
Week 14 (Lecture 14)	IDS; Auditing; Firewalls	<ol style="list-style-type: none"> <li>14. <i>Recognize, explain</i> and <i>analyze</i> auditing/IDS/Auditing systems</li> </ol>	<ol style="list-style-type: none"> <li>15. Chap 20, 21, 22</li> <li>16. <b>HW6 (Reading assignment): DDoSSurvey.pdf paper – write a 1 page summary</b></li> </ol>
Week 15 (Lecture 15)	Overview of security of emerging systems/issues (Cloud, SN, BigData, ATP)	<ol style="list-style-type: none"> <li>17. <i>Recognize, explain</i> the basic security and privacy issues in new systems</li> <li>18. <i>Understand, explain</i> privacy models and approaches</li> </ol>	<ol style="list-style-type: none"> <li>19. Readings: <ol style="list-style-type: none"> <li>1. NIST 800-144, "<a href="#">Guidelines on Security and Privacy in Public Cloud Computing</a>"</li> <li>2. H. Takabi, J. Joshi, G-J Ahn, "<a href="#">Security and Privacy Challenges in Cloud Computing Environments</a>" IEEE Security and Privacy, 2010</li> <li>3. <a href="http://www.isaca.org/Groups/Professional-English/big-data/GroupDocuments/Big_Data_Top_Ten_v1.pdf">http://www.isaca.org/Groups/Professional-English/big-data/GroupDocuments/Big_Data_Top_Ten_v1.pdf</a></li> </ol> </li> <li><del>20.</del> <b>Quiz 5</b> (for Week 14, 15)</li> </ol>
Week 16	21. Final Exams		