Tentative Syllabus

These topics are tentative and subject to change without warning. In particular, if I don't discuss something you're interested in, ask about it! I may very well add it or modify what I'm covering to include it.

lecture	date	topic	reading	due
1.	Jan 4	Introduction, overview of security	§1	
2.	Jan 6	Access control matrix model	§2	
3.	Jan 11	Safety question and the HRU result	§3.1, 3.2	
4.	Jan 13	Take-Grant Protection Model	§3.3; [Bi96]	project selection
5.	Jan 18	Schematic Protection Model	§3.4	homework 1
6.	Jan 20	Expressive power, ESPM, TAM, MTAM	§3.5; [Z+05]	
7.	Jan 25	Security policies, mechanisms	§4; [LT05]	
8.	Jan 27	Bell-LaPadula Policy Model, System Z	§5, 30; [Sa93]	
9.	Feb 1	Biba, Clark-Wilson Integrity Policy Models	§6.2, 6.4	homework 2
10.	Feb 3	Availability Policy Models		progress report
11.	Feb 8	Chinese Wall, Other Hybrid Policy Models	§7.1, 7.2; [WB04]	
12.	Feb 10	ORCON, RBAC Access Control Models	§7.3, 7.4	
13.	Feb 15	Deterministic Noninterference	§8.1, 8.2; [KR02]	homework 3
14.	Feb 17	Nondeducibility, restrictiveness, composition	§8.3–8.5; [Ma02]	
15.	Feb 22	Information flow, policies	§16.1, 16.2, 32; [HS97]	
16.	Feb 24	Covert channels and isolation	§17.1, 17.2; [S+06]	
17.	Mar 1	Analyzing covert channels	§17.3	homework 4
18.	Mar 3	Basic assurance	§18	
19.	Mar 8	Assurance in requirements and design	§19.1, 19.2.1–19.2.2	
20.	Mar 10	Assurance in design and implementation	§19.2.3–19.3	completed project, homework 5

References

[Bi96] M. Bishop, "Conspiracy and Information Flow in the Take-Grant Protection Model," *Journal of Computer Security* **4**(4) pp. 331–359 (1996).

[HS97] T. Himdi and R. Sandhu, "Lattice-Based Models for Controlled Sharing of Confidential Information in the Saudi Hajj System," *Proceedings of the 13th Annual Computer Security Applications Conference* pp. 164–174 (Dec. 1997).

[KR02] C. Ko and T. Redmond, "Noninterference and Intrusion Detection," *Proceedings of the 2002 IEEE Symposium on Security and Privacy* pp. 177–187 (May 2002).

[LT05] N. Li and M. Tripunitara, "On Safety in Discretionary Access Control," *Proceedings of the 2005 IEEE Symposium on Security and Privacy* pp. 96–109 (May 2005).

[Ma02] H. Mantel, "On the Composition of Secure Systems," *Proceedings of the 2002 IEEE Symposium on Security and Privacy* pp. 88–101 (May 2002).

[Sa93] R. Sandhu, "Lattice-Based Access Control Models," *IEEE Computer* **26**(11) pp. 9–19 (Nov. 1993).

[S+06] G. Shah, A. Molna, and M. Blaze, "Keyboards and Covert Channels," *Proceedings of the 15th USENIX Security Symposium* pp. 59–78 (Aug. 2006)

[WB04] T. Walcott and M. Bishop, "Traducement: A Model for Record Security," *ACM Transactions on Information and System Security* **7**(4) pp. 576–590 (Nov. 2004).

[Z+05] X. Zhang, Y. Li, and D. Nalla, "An Attribute-Based Access Matrix Model," *Proceedings of the 2005 ACM Symposium on Applied Computing* pp. 359–363 (Mar. 2005).