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.

lec	date	topic	reading	due
1.	Jan 9	Introduction, overview of security	§1	
2.	Jan 11	Access control matrix model	§2; [Z+05]	
3.	Jan 13	Safety question and the HRU result	§3.1, 3.2	
—.	Jan 16	*no class; Martin Luther King, Jr. Day*		
4.	Jan 18	Take-Grant Protection Model	§3.3; [Bi96]	
5.	Jan 20	Schematic Protection Model	§3.4	project selection, homework #1
6.	Jan 23	Expressive power, ESPM, TAM, MTAM	§3.5	
7.	Jan 25	Comparison of models	*handout*	
8.	Jan 27	Security policies, mechanisms	§4; [LT05]	
9.	Jan 30	Bell-LaPadula Policy Model	§5, 30; [Sa93]	
10.	Feb 1	Declassification, tranquility, System Z	*handout*, §5.3, 5.4	
11.	Feb 3	Biba, Clark-Wilson Integrity Models	§6.2, 6.4	homework #2
12.	Feb 6	Trust models	*handout*	
13.	Feb 8	Availability policy models	*handout*	
14.	Feb 10	Chinese Wall, Other Hybrid Policy Models	§7.1, 7.2; [WB04]	
15.	Feb 13	ORCON, RBAC Access Control Models	§7.3, 7.4	
16.	Feb 15	Deterministic Noninterference	§8.1, 8.2; [KR02]	progress report
17.	Feb 17	Nondeducibility, restrictiveness, composition	§8.3–8.5; [Ma02]	homework #3
—.	Feb 20	*no class; Presidents' Day*		
18.	Feb 22	Identity	§14	
19.	Feb 24	Information flow policies	§16.1, 16.2; [B+07]	
20.	Feb 27	Information flow	§16.3–16.5	
21.	Feb 29	Confinement problem, isolation	§17.1, 17.2, 33	
22.	Mar 2	Analyzing covert channels	§17.3; [S+06]	homework #4
23.	Mar 5	The insider problem	[B+08, B+09]	
24.	Mar 7	Basic assurance	§18	
25.	Mar 9	Assurance in requirements and design	§19.1, 19.2.1–19.2.2	
26.	Mar 12	Assurance in design and implementation	§19.2.3–19.3	
27.	Mar 14	Application: electronic voting systems	*handout*	
28.	Mar 16	*To be arranged*		homework #5
29.	Mar 19	*To be arranged*		completed project

References

[B+07] M. Backes, M. Dümuth, and D. Unruh, "Information Flow in the Peer-Reviewing Process (Extended Abstract)," *Proceedings of the 2007 IEEE Symposium on Security and Privacy* pp. 187–191 (May 2007).

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

[B+08] M. Bishop, S. Engle, S. Peisert, S. Whalen, and C. Gates, "We Have Met the Enemy And He Is Us," *Proceedings of the 2008 Workshop on New Security Paradigms* pp. 1–12 (Sep. 2008).

[B+09] B. Bowen, M. Ben Salem, S. Hershkop, A. Keromytis, and S. Stolfo, "Designing Host and Network Sensors to Mitigate the Insider Threat," *IEEE Security & Privacy* **7**(6) pp. 22–29 (Nov. 2009).

[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).