Tentative Syllabus

This syllabus is tentative and subject to change as needed. If there is a topic you want to hear about and it is in the syllabus, please let me know. I won't promise to cover it, but I will try.

#	*date*	*what*	*reading*
1	Tue, Jan 8	Introduction to computer security	text, §1
2	Thu, Jan 10	Robust programming	Bi07a
3	Tue, Jan 15	Design principles	text, §13; Be07
4	Thu, Jan 17	Incident handling	text, §25.6; Ro03; St88
5	Tue, Jan 22	Policies	text, §4.1–4.6; Wa70, pp. 1–25
6	Thu, Jan 24	Assurance	text, §18, §29; Me06
7	Tue, Jan 29	Attacks, penetration testing	text, §23.2, §26.4; Th84; TL00
8	Thu, Jan 31	Access control matrix, undecidability of security	text, §2.1–2.3, 3.1–3.2
9	Tue, Feb 5	Electronic voting	BB07; Bi07b; BW07; Ra04
10	Thu, Feb 7	Models of confidentiality and integrity	text, §5.1–5.3 (*not* 5.2.2–5.2.3), 6.2, 6.4
11	Tue, Feb 12	Classical cryptography	text, §9.1–9.2
12	Thu, Feb 14	Public key cryptography	text, §9.3–9.4, 11.1–11.2
	Fri, Feb 15	***Midterm Examination*** in discussion section	
13	Tue, Feb 19	Cryptographic infrastructure	text, §10.1–10.2, 10.4.2, 10.6
14	Thu, Feb 21	Identity and authentication	text, §14.1–14.5, 12
15	Tue, Feb 26	ACLs, C-lists, rings	text, §15.1–15.4
16	Thu, Feb 28	Confinement problem	text, §17.1–17.2
17	Tue, Mar 4	Computer worms, viruses, spyware, adware	text, §22 (*not* 22.6); Na97
18	Thu, Mar 6	Vulnerabilities	text, §23.3–23.4; Al96
19	Tue, Mar 11	Securing the web: email, firewalls, SSL (TLS), IPsec	text, §11.3–11.4, 26.3; Op07, VE06
20	Thu, Mar 13	Intrusion detection	text, §25.1–25.5
	Sat, Mar 22	***Final Examination***	

Discussion sections are held every Friday. The topic of each session will be determined as the term progresses.

Readings

[text] M. Bishop, *Computer Security: Art and Science*, Addison-Wesley Professional, Boston MA (2002).

[Al96] Aleph One, "Smashing the Stack for Fun and Profit," *Phrack* **49**, 14 (Aug. 1996).

[BB07] E. Barr, M. Bishop, and M. Gondree, "Fixing Federal E-Voting Standards," *Communications of the ACM* **50**(3) pp. 19–24 (Mar. 2007).

[Be07] S. Bellovin, "DRM, Complexity, and Correctness," *IEEE Security and Privacy* **5**(1) p. 80 (Jan.-Feb. 2007).

[Bi07a] M. Bishop, "Robust Programming" (Dec. 2007).

[Bi07b] M. Bishop, "Overview of Red Team Reports", Office of the Secretary of State of California, 1500 11th St, Sacramento, CA 95814 (July 2007).

[BW07] M. Bishop and D. Wagner, "Risks of E-Voting," *Communications of the ACM* **50**(11) p. 120 (Nov. 2007).

[Me06] J. Meier, "Web Application Security Engineering," *IEEE Security and Privacy* **4**(4) pp. 16–24 (July-Aug. 2006).

[Na97] C. Nachenberg, "Computer Virus-Antivirus Coevolution," *Communications of the ACM* **40**(1) pp. 46–51 (Jan. 1997)

[Op07] R. Oppliger, "Providing Certified Mail Services on the Internet," *IEEE Security and Privacy* **5**(1) pp. 16–22 (Jan.-Feb. 2007).

[Ra04] RABA Innovative Solution Cell, "Trusted Agent Report Diebold AccuVote-TS Voting System", RABA Technologies LLC, Columbia, MD 21045 (Jan. 2004).

[Ro03] R. Rollason-Reese, "Incident Handling: An Orderly Response to Unexpected Events," *Proceedings of the 31st Annual ACM SIGUCCS Conference on User Services* pp. 97–102 (2003).

[St88] C. Stoll, "Stalking the Wily Hacker," *Communications of the ACM* **31**(5) pp. 484–497 (May 1988).

[Th84] K. Thompson, "Reflections on Trusting Trust," *Communications of the ACM* **27**(8) pp. 761–763 (Aug. 1984).

[TL00] S. Templeton and K. Levitt, "A Requires/Provides Model for Computer Attacks," *Proceedings of the 2000 New Security Paradigms Workshop* pp. 31–38 (Sep. 2000).

[VE06] J. Viega and J. Epstein, "Why Applying Standards to Web Services is Not Enough," *IEEE Security and Privacy* **4**(4) pp. 25–31 (July-Aug. 2006).

[Wa70] W. Ware, "Security Controls for Computer Systems: Report of the Defense Science Board Task Force on Computer Security," Rand Report R609-1, The Rand Corporation, Santa Monica, CA (Feb. 1970).