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.	Mon Mar 28	Introduction to computer security	*text*, §1	
2.	Wed Mar 30	Robust programming, part 1	[6]	
3.	Fri Apr 1	Robust programming, part 2	*text*, §29	
4.	Mon Apr 4	Common vulnerabilities (*Prof. Sean Peisert*)	[1, 8, 11]	
5.	Wed Apr 6	Case study: grading system (*Prof. Hao Chen*)		
6.	Fri Apr 8	Principles of secure design	*text*, §13, [3]	
7.	Mon Apr 11	Flaw hypothesis methodology, part 1	*text*, §23.1–2, [4]	
8.	Wed Apr 13	FHM part 2, Vulnerability models	*text*, §23.3–4	Project selection
9.	Fri Apr 15	Vulnerability models, part 2	*text*, §23.3–4	homework #1
10.	Mon Apr 18	Access control matrix	*text*, §2	
11.	Wed Apr 20	ACM and the HRU result	*text*, §3.1–2	
12.	Fri Apr 22	Policies	*text*, §4,1–4.4, [14]	
13.	Mon Apr 25	Policy languages	*text*, §4.5	
14.	Wed Apr 27	Confidentiality: Bell-LaPadula model	*text*, §5	homework #2
15.	Fri Apr 29	Integrity: Biba, Clark-Wilson model	*text*, §6 (*not* 6.3)	
16.	Mon May 2	*In class* ***midterm***		
17.	Wed May 4	Electronic voting	[2, 5, 7, 12]	
18.	Fri May 6	Classical cryptography	*text*, §9.1–2	
19.	Mon May 9	Public key cryptography	*text*, §9.3–4	
20.	Wed May 11	Key management, digital signatures	*text*, §10	
21.	Fri May 13	Cryptographic protocols	*text*, §11.1–2	
22.	Mon May 16	Authentication	*text*, §12	
23.	Wed May 18	Access control mechanisms	*text*, §15	
24.	Fri May 20	Confinement problem	*text*, §17.1–2	
25.	Mon May 23	Malware	*text*, §22 (*not* 22.6), [10]	
26.	Wed May 25	Network security	*text*, §11.3–4	
27.	Fri May 27	Basic assurance	*text*, §18, [9, 13]	
	Mon May 30	*Holiday: Memorial Day*		
28.	Wed Jun 1	*In class* ***final examination***		Completed project

References

[1] AlephOne, "Smashing the Stack for Fun and Profit," *Phrack* **7**(49) (1996).

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

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

[4] M. Bishop, "About Penetration Testing," *IEEE Security & Privacy* **5**(6) pp. 84–87 (Nov. 2007).

[5] M. Bishop, *Overview of Red Team Reports*, Office of the California Secretary of State, Sacramento, CA, USA (July 2007).

[6] M. Bishop, "Robust Programming," *unpublished* (Mar. 2011).

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

[8] S. Christey, "2010 CWE/SANS Top 25 Most Dangerous Software Errors," (Dec. 13 2010).

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

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

[11] OWASP, *Top 10 - 2010: The Ten Most Critical Web Application Security Risks*, The Open Web Application Security Project (2010).

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

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

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