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 Apr 1	Introduction to computer security	*text* §1	
dis 1.		Case study: Buffer overflow, ROP	[Ale96, Sha07]	
2.	Wed Apr 3	Robust programming, part 1	[Bis11]	
3.	Fri Apr 5	Robust programming, part 2	*text* §29	
4.	Mon Apr 8	Common vulnerabilities	[Chr11, OWA13]	
dis 2.		More on robust programming	[VBKM00, CCS06]	
5.	Wed Apr 10	Principles of secure design	*text* §13, [Bel07]	
6.	Fri Apr 12	Flaw hypothesis methodology, part 1	*text* §23.1–23.2, [Bis07a]	homework #1
7.	Mon Apr 15	FHM part 2; vulnerability models	*text* §23.1–23.4, [PTE12]	
dis 3.		Some vulnerabilities; *nmap*		
8.	Wed Apr 17	Vulnerability models, part 2	*text* §23.3–23.4	
9.	Fri Apr 19	Access control matrix, HRU result	*text* §2, 3.1–3.2	
10.	Mon Apr 22	Policies	*text* §4.1–4.4, [War70]	
dis 4.		PTES methodology		
11.	Wed Apr 24	Policy languages	*text* §4.5	
12.	Fri Apr 26	Confidentiality: Bell-LaPadula model	*text* §5	homework #2
13.	Mon Apr 29	Integrity: Biba model	*text* §6 (*not* 6.3)	
dis 5.		Review for midterm examination		
14.	Wed May 1	***Midterm*** (*in class*)		
15.	Fri May 3	*Guest Speaker*: Zane Lackey, etsy		
16.	Mon May 6	Integrity: Clark-Wilson model	*text* §6.4	
dis 6.		About the midetem examination		
17.	Wed May 8	Classical cryptography	*text* §9.1–9.2	
18.	Fri May 10	Classical, public key cryptography	*text* §9.3	
19.	Mon May 13	Public key cryptography	*text* §9.3–9.4	homework #3
dis 7.		Breaking a Vigenère Cipher		
20.	Wed May 15	Key management, digital signatures	*text* §10.1–10.4, 10.6	
21.	Fri May 17	Cryptographic protocols, authentication	*text* §11.3, 11.4.1, 12	
22.	Mon May 20	Authentication	*text* §12	
dis 8.		Using a source code analyzer		
23.	Wed May 22	Authentication	*text* §12	
24.	Fri May 24	Access control mechanisms	*text* §15	homework #4
—.	Mon May 27	*Holiday: Memorial Day*		
25.	Wed May 29	Malware	*text* §22 (*not* 22.6), [Nac97]	
26.	Fri May 31	Malware, network security	*text* §11.4, 22 (*not* 22.6), [Nac97]	
27.	Mon Jun 3	Basic assurance	*text* §18, [Mei06, VE06]	
dis 9.		Review for Final Examination		
28.	Wed Jun 5	Electronic voting	[BBG07, Bis07b, BW07, RAB04]	
—.	Thu Jun 6			homework #5 project report
—.	Tue Jun 11	***Final examination*** (at 10:30am)		

References

[Ale96] AlephOne. Smashing the stack for fun and profit. *Phrack*, 7(49), 1996.

[BBG07] Earl Barr, Matt Bishop, and Mark Gondree. Fixing federal e-voting standards. *Communications of the ACM*, 50(3):19–24, Mar. 2007.

[Bel07] Steve Bellovin. DRM, complexity, and correctness. *IEEE Security and Privacy*, 5(1):80, Jan. 2007.

[Bis07a] Matt Bishop. About penetration testing. *IEEE Security and Privacy*, 5(6):84–87, Nov. 2007.

[Bis07b] Matt Bishop. Overview of red team reports, July 2007.

[Bis11] Matt Bishop. Robust programming. handout for ECS 153, Computer Security, Mar. 2011.

[BW07] Matt Bishop and David Wagner. Risks of e-voting. *Communications of the ACM*, 50(11):120, Nov. 2007.

[CCS06] Pravir Chandra, Brian V. Chess, and John Steven. Putting the tools to work: How to succeed with source code analysis. *IEEE Security and Privacy*, 4(3):80–83, May 2006.

[Chr11] Steve Christey. 2011 CWE/SANS top 25 most dangerous software errors, Sep. 13, 2011. Available at `http://cwe.mitre.org/top25/`.

[Mei06] J. D. Meier. Web application security engineering. *IEEE Security and Privacy*, 4(4):16–24, July 2006.

[Nac97] Cary Nachenberg. Computer virus-antivirus coevolution. *Communications of the ACM*, 40(1):46–51, Jan. 1997.

[OWA13] OWASP. Owasp top 10 - 2013 rc1: The ten most critical web application security risks. Technical report, The Open Web Application Security Project, 2013.

[PTE12] Penetration testing execution standard, January 2012. Available at `http://www.pentest-standard.org/index.php/Main\_Page`.

[RAB04] RABA Innovative Solution Cell. Trusted agent report Diebold AccuVote-TS voting system. Technical report, RABA Technologies LLC, Columbia, MD, Jan. 2004.

[Sha07] Hovav Shacham. The geometry of innocent flesh on the bone: Return-into-libc without function calls (on the x86). In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, CCS '07, pages 552–561, New York, NY, USA, 2007. ACM.

[VBKM00] John Viega, J. T. Bloch, Yoshi Kohno, and Gary McGraw. ITS4: a static vulnerability scanner for C and C++ code. In *Proceedings of the 16th Annual Computer Security Applications Conference*, pages 257–267, Los Alamitos, CA, USA, Dec. 2000. IEEE Computer Society.

[VE06] John Viega and Jeremy Epstein. Why applying standards to web services is not enough. *IEEE Security and Privacy*, 4(4):25–31, July 2006.

[War70] Willis 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.