Actual Syllabus

#	date	topic	reading[a] and notes
1.	Mon, Jan 6	Introduction; what is computer security	§1
2.	Wed, Jan 8	Introduction (*con't*)	§1
3.	Fri, Jan 10	Principles of secure design, penetration analysis	§13, 23.1–23.2
	Fri, Jan 10	*Discussion*: class project	
4.	Mon, Jan 13	Penetration analysis, Flaw Hypothesis Model	§23.1–23.2
5.	Wed, Jan 15	Vulnerability models	§23.3–23.4 ***homework 1 due***
6.	Fri, Jan 17	Vulnerability models (*con't*)	§23.3–23.4
	Fri, Jan 17	*Discussion*: security in programming	
	Mon, Jan 20	***no class*** (Martin Luther King Day)	
7.	Wed, Jan 22	Robust programming	*handout*
8.	Fri, Jan 24	Robust programming (*con't)*, access control matrix	*handout,* §2 ***project selection due***
	Fri, Jan 24	*Discussion*: ***none*** (virtual Monday)	
9.	Mon, Jan 27	Access control matrix, HRU result	§2, 3.1–3.2
10.	Wed, Jan 29	HRU result (*con't*), security policies	§3.1–3.2, 4.1–4.3 ***homework 2 due***
11.	Fri, Jan 31	Security policies, Bell-LaPadula Model	§4.4–4.5, 5.1–5.2.2
	Fri, Jan 31	*Discussion*: Lattices	§31
12.	Mon, Feb. 3	Bell-LaPadula Model (*con't*)	§5.2.1–5.2.2
13.	Wed, Feb. 5	Bell-LaPadula Model (*con't*),integrity models	§5.2.2–5.3, 6.1–6.2
14.	Fri, Feb 7	***Guest lecturer***	
	Fri, Feb 7	*Discussion*: review for midterm	
15.	Mon, Feb 10	Integrity models (*con't*), Biba	§6.1–6.2 ***homework 3 due***
16.	Wed, Feb 12	***midterm***	
17.	Fri, Feb 14	Clark-Wilson Model	§6.4
	Fri, Feb 14	*Discussion*: modular arithmetic, Euclidean algorithm	
	Mon, Feb 17	***no class*** (Presidents' Day)	
18.	Wed, Feb 19	Basics of cryptography, classical cryptography	§9.1–9.2
19.	Fri, Feb 21	DES, public key cryptography	§9.2.3–9.3
	Fri, Feb 21	*Discussion*: review of midterm	
20.	Mon, Feb 24	Public key cryptography (*con't*), cryptographic checksums	§9.3–9.4 ***project design due***
21.	Wed, Feb 26	Key exchange, Needham-Schroeder	§10.1–10.2
22.	Fri, Feb 28	Certificates and PKI	§10.4 (not 10.4.1), 10.5.2, 10.6
	Fri, Feb 28	*Discussion*: Passwords and salts	

#	date	topic	reading[a] and notes
23.	Mon, Mar 3	Authentication	§12.1–12.3 ***homework 4 due***
24.	Wed, Mar 5	Authentication (*con't*), identity	§12.4–12.6, 14.1–14.4, 14.6
25.	Fri, Mar 7	Access control mechanisms	§15.1–15.2
	Fri, Mar 7	*Discussion*: link and end-to-end encryption	
26.	Mon, Mar 10	Access control mechanisms (*con't*); malicious logic	§15.3–15.4, 22.1–22.2
27.	Wed, Mar 12	Malicious logic (*con't*), assurance	§22.3-22.5, 22.7, §18
28.	Fri, Mar 14	Assurance, review	***homework 5, project due***
	Wed, Mar 19	***final exam, both sections***	1:30PM to 3:30PM

[a] Unless otherwise noted, all readings are from the text.