Tentative Syllabus

#	date	topic	reading[a] and notes
1.	Thu, Apr 1	What is computer security?	§1
	Discussion	***No discussion section***	
2.	Tue, Apr 6	Principles of secure design, penetration analysis	§13, 23.1–23.2
3.	Thu, Apr 8	Flaw Hypothesis Model	§23.1–23.2
	Discussion	Example penetration studies	
4.	Tue, Apr 13	Vulnerability models	§23.3–23.4
5.	Thu, Apr 15	Robust programming	*handout*
	Discussion	How to test, and crash, programs	
6.	Tue, Apr 20	Security in programming	§29.1–29.4
7.	Thu, Apr 22	Security in programming (*con't*)	§29.5–29.6
	Discussion	Examples of common security programming errors	
8.	Tue, Apr. 27	Access control matrix, HRU result	§2, 3.1
9.	Thu, Apr 29	Security policies	§4.1-4.5
	Discussion	How to attack programs	
10.	Tue, May 4	Bell-LaPadula Model	§5.1,5.2.1–5.2.2,5.3
11.	Thu, May 6	Integrity models	§6.1–6.2,6.4
	Discussion	Review for midterm	
12.	Tue, May 11	***midterm***	
13.	Thu, May 13	Classical cryptography, public key cryptography	§9.1–9.3
	Discussion	Biba with categories	
14.	Tue, May 18	Public key cryptography (*con't*), cryptographic checksums	§9.3–9.4
15.	Thu, May 20	Key exchange, Needham-Schroeder, PKI	§10.1–10.2,10.4
	Discussion	Basic number theory	
16.	Tue, May 25	Authentication	§12
17.	Thu, May 27	Identity, access control mechanisms	§14.1–14.4,14.6,15.1–15.3
	Discussion	Networks and security	
18.	Tue, Jun 1	Access control mechanisms, assurance	§15.5, 18
19.	Thu, Jun 3	Assurance	§18,21.1–21.2,21.8
	Discussion	Review for final	
20.	Tue, Jun 8	Malicious logic	§22.1–22.5,22.7
	Sat, Jun 12	***final exam***	8:00AM to 10:00AM

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