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 may ....

	Date	Topic	Reading
1.	Wed, Jan 4	Introduction; what is computer security	§1
2.	Fri, Jan 6	Introduction (con't)	§1
3.	Mon, Jan 9	Robust programming	handout
	Wed, Jan 11	*Discussion Section*: Defensive programming	
4.	Wed, Jan 11	Robust programming (con't)	handout
5.	Fri, Jan 13	Security in programming	
	Mon, Jan 16	***Martin Luther King Day; no class***	
	Wed, Jan 18	***Monday classes; no discussion section***	
6.	Wed, Jan 18	Security in programming	
7.	Fri, Jan 20	Principles of secure design, penetration analysis	§13, 23.1–23.2
8.	Mon, Jan 23	Penetration analysis, Flaw Hypothesis Model	§23.1–23.2
	Wed, Jan 25	*Discussion Section*: Structuring a penetration test	
9.	Wed, Jan 25	Vulnerability models	§23.3–23.4
10.	Fri, Jan 27	Vulnerability models (con't)	§23.3–23.4
11.	Mon, Jan 30	Access control matrix, HRU result	§2, 3.1–3.2
	Wed, Feb 1	*Discussion Section*: Lattices and partial orders	
12.	Wed, Feb 1	Security policies	§4.1–4.5
13.	Fri, Feb 3	Bell-LaPadula Model	§5.1–5.2.2, 5.3
14.	Mon, Feb 6	Biba Model	§6.1–6.2
	Wed, Feb 8	*Discussion Section*: Review for midterm	
15.	Wed, Feb 8	Clark-Wilson Model	§6.4
16.	Fri, Feb 10	***midterm***	§9.1–9.2.2
17.	Mon, Feb 13	Basics of cryptography, classical cryptography	§6.4
	Wed, Feb 15	*Discussion Section*: Fast modular exponentiation	
18.	Wed, Feb 15	DES, public key cryptography	§9.2.3–9.3
19.	Fri, Feb 17	Public key cryptography, cryptographic checksums	§9.4
	Mon, Feb 20	***Presidents' Day; no class***	§12.3–12.4, 14.1–14.4
	Wed, Feb 22	*Discussion Section*: The campus authentication system	
20.	Wed, Feb 22	Key exchange, Needham-Schroeder and Kerberos	§10.1–10.2
21.	Fri, Feb 24	Authentication	§12.1–12.3
22.	Mon, Feb 28	Biometrics and multiple methods, identity	§12.3–12.4, 14.1–14.4
	Wed, Mar 1	*Discussion Section*: Otway-Rees authentication protocol	
23.	Wed, Mar 1	Identity on the web	§14.6
24.	Fri, Mar 3	Access control lists, capabilities	§15.1–15.2
25.	Mon, Mar 6	Rings; confinement problem and approaches	§15.4, 17.1–17.2
	Wed, Mar 8	*Discussion Section*: Privilege in modern systems	
26.	Wed, Mar 8	Assurance	§18
27.	Fri, Mar 10	Malware	§22 (except 22.6)
28.	Mon, Mar 13	Network security: firewalls and SSL	§11.4.2, 26.3–26.3.2.2
	Wed, Mar 15	*Discussion Section*: PGP, review for final	
29.	Wed, Mar 15	Review	
	Sat, Mar 18	***Final exam***	