

## Tentative Syllabus

#	date	topic	reading <sup>a</sup> and notes
1.	Fri, Sep 26	Introduction; what is computer security	§1
2.	Mon, Sep 29	Principles of secure design	§13
3.	Wed, Oct 1	Robust programming	<i>handout</i>
	Wed, Oct 1	<i>Discussion:</i> class project, robust programming	
4.	Fri, Oct 3	Access control matrix, HRU result	§2, 3.1–3.2
5.	Mon, Oct 6	Security policies	§4.1–4.4, 4.6
6.	Wed, Oct 8	Confidentiality models: Bell-LaPadula Model	§5.1,5.2.1–5.2.2
	Wed, Oct 8	<i>Discussion: to be arranged</i>	§30
7.	Fri, Oct 10	Integrity models: Biba strict integrity, Clark-Wilson	§6.1,6.2.3,6.4
8.	Mon, Oct 13	Basic cryptography: classical	§9.1–9.2
9.	Wed, Oct 15	Basic cryptography: public key	§9.3
	Wed, Oct 15	<i>Discussion:</i> modular arithmetic, Euclidean algorithm	§31
10.	Fri, Oct 17	Basic cryptography: cryptographic hashes	§9.4
11.	Mon, Oct 20	Key distribution	§10.1–10.2
12.	Wed, Oct 22	Certificates and PKI, digital signatures	§10.4,10.6
	Wed, Oct 22	<i>Discussion:</i> Entropy, uncertainty	§32
13.	Fri, Oct. 24	Cryptography and networks	§11.1,11.3–11.4
14.	Mon, Oct. 27	Authentication: passwords	§12.1–12.2
15.	Wed, Oct 29	Authentication: other methods	§12.3–12.6
	Wed, Oct 29	<i>Discussion:</i> review for midterm	
16.	Fri, Oct 31	Identity: users, groups, roles	§14.1–14.4
17.	Mon, Nov 3	<b><i>midterm</i></b>	
18.	Wed, Nov 5	Identity: names, anonymity	§14.5–14.6
	Wed, Nov 5	<i>Discussion:</i> Passwords, salts	§12.2
19.	Fri, Nov 7	Access control mechanisms: ACL, C-List	§15.1–15.2
20.	Mon, Nov 10	Access control mechanisms: others	§15.3–15.5
21.	Wed, Nov 12	Information flow: compiler-based mechanisms	§16.1,16.3
	Wed, Nov 12	<i>Discussion:</i> review of midterm	
22.	Fri, Nov 14	Information flow: execution-based mechanisms	§16.4–16.5
23.	Mon, Nov 17	Assurance: introduction and basic concepts	§18
24.	Wed, Nov 19	Formal evaluation of systems: TCSEC, CC	§21.2, 21.8
	Wed, Nov 19	<i>Discussion:</i> Review of robust programming	
25.	Fri, Nov 21	Malicious logic: taxonomy	§22.1–22.5
26.	Mon, Nov 24	Malicious logic: defenses	§22.7
27.	Wed, Nov 26	Penetration studies, Flaw Hypothesis Methodology	§23.1–23.2
	Wed, Nov 26	<i>Discussion: to be arranged</i>	
	Fri, Nov 28	<b><i>no class</i></b> (Thanksgiving Holiday)	

---

---

#	date	topic	reading <sup>a</sup> and notes
28.	Mon, Dec 1	Vulnerability taxonomies	§23.3–23.4
29.	Wed, Dec 3	Auditing systems	§24
	Wed, Dec 3	<i>Discussion: review for final</i>	
30.	Fri, Dec 5	<i>to be arranged</i>	
	Tue, Dec 9	<i>final exam</i>	4:00PM to 6:00PM

---

---

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