Planned Syllabus

This is what I plan to cover, and when. It will undoubtedly change as the quarter progresses. If there is a topic you're interested in but not shown, please let me know; I may well change things to cover it. All readings are from the texts unless otherwise indicated.

#	date	topic	notes
1.	Sep 25	Intro to computer security	*Reading*: §1
2.	Sep 27	Design principles; robust programming	*Reading*: §14, [2]
D–.	*Disc sec*	*No discussion section this week*	
3.	Sep 30	Robust programming	[2]
4.	Oct 2	Elections and voting	[2, 6]
5.	Oct 4	Elections and voting (*con't*)	[6]
D1.	*Disc sec*	Requirements and design of software	
6.	Oct 7	Policy models	*Reading*: §4.1–4.4
7.	Oct 9	Policy models, confidentiality models	*Reading*: §4.5–4.6, G, 5.1–5.2.1, A
8.	Oct 11	Confidentiality models, integrity models	*Reading*: §5.2–5.2.2, 6–6.1
D2.	*Disc sec*	Common implementation errors; lab 1	§31
9.	Oct 14	Tranquility, declassification, Integrity models	*Reading*: §5.3, 6.2, 6.4
10.	Oct 16	Integrity models	*Reading*: §6.4
11.	Oct 18	Miscellaneous policy models, symmetric key cryptography	*Reading*: §8.4–8.5, 10–10.2
D3.	*Disc sec*	Lab 1; common implementation errors	§31
12.	Oct 21	Symmetric, public key cryptography	*Reading*: §10.2–10.3
13.	Oct 23	Public key cryptography, digital signatures	*Reading*: §10.3–10.4
14.	Oct 25	Key management	*Reading*: §11.1–11.2, [5]
D4.	*Disc sec*	=	
15.	Oct 28	Key management (*con't*)	*Reading*: §11.3–1.4, 12.1
16.	Oct 30	Cipher techniques	*Reading*: §12.3–12.4, 12.5.3
17.	Nov 1	***Midterm exam; in class***	
D5.	*Disc sec*	Review for midterm	
18.	Nov 4	TLS/SSL, authentication	*Reading*: §12.5.3,13
19.	Nov 6	Anonymity, access control matrix	*Reading*: §15.7, 2.1–2.3
20.	Nov 8	Access control matrix, safety question, access control mechanisms	*Reading*: §2.4, 3.1–3.2, 16.1
D6.	*Disc sec*		
—.	Nov 11	***University holiday (Veterans Day); no class***	
21.	Nov 13	Access control mechanisms, information flow entropy analysis	*Reading*: §16.2–16.4, 17.1
22.	Nov 15	Information flow	*Reading*: §17.4
D–.	*Disc sec*	*No discussion section this week*	
23.	Nov 18	Firewalls, malware	*Reading*: §17.5–17.6, 23.1–23.2
24.	Nov 20	Malware	*Reading*: §23.3, [3, 4]
25.	Nov 22	Malware (*con't*)	*Reading*: §23.4–23.5
D7.	*Disc sec*		
26.	Nov 25	Malware (*con't*)	*Reading*: §23.6–23.7
27.	Nov 27	Vulnerability analysis: models	*Reading*: §23.9, 24.3–24.4.1, [1]
—.	Nov 29	***University holiday (Thanksgiving); no class***	
D–.	*Disc sec*	*No discussion section this week*	
28.	Dec 2	Vulnerability analysis, penetration testing	*Reading*: §24.4.2–24.4.5
29.	Dec 4	Standards	*Reading*: §24.5, 24.2
30.	Dec 6	Example penetration testing; intrusion detection	*Reading*: 24.2.7–24.2.8, 26.1–26.3
D8.	*Disc sec*	Review for final	
—.	Dec 11	***Final Exam, 10:30–12:30pm***	

References

[1] AlephOne. "Smashing the Stack for Fun and Profit," *Phrack* **7**(49) (Nov. 1996).
URL: http://phrack.org/issues/49/14.html

[2] M. Bishop. "Robust Programming," *unpublished* (Mar. 2011); handout for ECS 153, Computer Security, and other classes.

[3] M. W. Eichin and J. A. Rochlis. "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988," *Proceeding of the 1989 Symposium on Security and Privacy* pp. 326–343 (May 1989).
DOI: 10.1109/SECPRI.1989.36307

[4] R. Langner. "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy* **9**(3) pp. 49–51 (May 2011).
DOI: 10.1109/MSP.2011.67

[5] S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System," *unpublished* (2008)
URL: https://bitcoin.org/bitcoin.pdf.

[6] B. I. Simidchieva, S. J. Engle, M. Clifford, A. C. Jones, S. Peisert, M. Bishop, L. A. Clarke, and L. J. Osterweil. "Modeling and Analyzing Faults to Improve Election Process Robustness," *Proceedings of the 2010 Electronic Voting Technology/Workshop on Trustworthy Elections* (*EVT/WOTE '10*) (Aug. 2010).
URL: https://www.usenix.org/conference/evtwote-10/modeling-and-analyzing-faults-improve-election-process-robustness