Tentative Syllabus

Here are the topics and readings for each week. This is tentative, because we may go slower (or faster) than this schedule shows, and I may add some topics and remove others. If there is something you want to hear about and it is not listed here, please ask me about it; I'm very willing to change topics based on class interest!

Week 1: March 31-April 1 (1 class, discussion section)

Topics: Introduction to computer security
Reading: §1

Week 2: April 4-April 8 (2 classes, discussion section)

Topics: Robust programming, principles of secure design
Reading: §13

Week 3: April 11-April 15 (2 classes, discussion section)

Topics: Security and integrity policies
Reading: §4.1–4.5, 5.1, 5.2–5.2.2, 5.3, 6.1–6.2, 6.4

Week 4: April 18-April 22 (2 classes, discussion section)

Topics: Cryptography and key management
Reading: §9, 10.1–10.2, 10.4 (except 10.4.1), 10.6

Week 5: April 25-April 29 (2 classes, discussion section)

Topics: Authentication
Reading: §12
Note: midterm scheduled for April 28

Week 6: May 2-May 6 (2 classes, discussion section)

Topics: Identity, access control matrix, access control mechanisms
Reading: §2, 14.1–14.4, 14.6, 15

Week 7: May 9-May 13 (2 classes, discussion section)

Topics: Assurance
Reading: §18, 19.1.2, 21.1, 21.2, 21.8

Week 8: May 16-May 20 (2 classes, discussion section)

Topics: Malicious logic
Reading: §22.1–22.5, 22.7

Week 9: May 23-May 27 (2 classes, discussion section)

Topics: Vulnerabilities analysis, including Flaw Hypothesis Methodology and models
Reading: §23

Week 10: May 30-June 3 (2 classes, discussion section)

Topics: Security in programming
Reading: §29

Week 11: June 6-June 8 (1 class)

Topics: Miscellaneous
Reading: §1