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)
Topics: Introduction to computer security
Reading: §1

Week 2: April 4-April 8 (2 classes)
Topics: Principles of secure design; access control matrix model, HRU result
Reading: §2, 3.1–3.2,13

Week 3: April 11-April 15 (2 classes)
Topics: Take-Grant Protection Model, SPM, expressive power, TAM
Reading: §3.3–3.5

Week 4: April 18-April 22 (2 classes)
Topics: Policies in general, Bell-LaPadula confidentiality model, System Z
Reading: §4, 5

Week 5: April 25-April 29 (2 classes)
Topics: Integrity policy models, other policy models
Reading: §6, 7

Week 6: May 2-May 6 (2 classes)
Topics: Noninterference, nondeducibility
Reading: §8

Week 7: May 9-May 13 (2 classes)
Topics: Basic cryptography, key management, PKI
Reading: §9, 10, 14.5

Week 8: May 16-May 20 (2 classes)
Topics: Authentication, access control mechanisms
Reading: §12, 15

Week 9: May 23-May 27 (2 classes)
Topics: Information flow, confinement problem
Reading: §16, 17

Week 10: May 30-June 3 (2 classes)
Topics: Auditing, Intrusion detection
Reading: §24, 25
Week 11: June 6-June 8 (1 class)
Topics: Review
Reading: none