

## Tentative Syllabus

These topics are tentative and subject to change without warning. In particular, if I don't discuss something you're interested in, ask about it! I may very well add it or modify what I'm covering to include it.

All readings are from the text and a handout that is available on Canvas.

### Lectures

| lec. | date       | topic                             | reading                  | notes                                   |
|------|------------|-----------------------------------|--------------------------|---|
| 1.   | Mon Mar 29 | Intro to computer security        | §1                       | Homework #1 out                         |
| 2.   | Wed Mar 31 | Design principles                 | §14                      |   |
| 3.   | Fri Apr 2  | Robust programming                | handout, §31.1–31.4      | Lab #1 out                              |
| 4.   | Mon Apr 5  | Robust programming                | handout                  |   |
| 5.   | Wed Apr 7  | Vulnerability analysis            | §24.1–24.2, 24.5         | Homework #1 due, #2 out                 |
| 6.   | Fri Apr 9  | Vulnerability models              | §24.3–24.4, 31.5         |   |
| 7.   | Mon Apr 12 | Attacks                           | §27.1–27.2               |   |
| 8.   | Wed Apr 14 | Introduction to assurance         | §19                      |   |
| 9.   | Fri Apr 16 | Access control matrix, HRU result | §2, 3.1–3.2              | Lab #1 due, #2 out                      |
| 10.  | Mon Apr 19 | Policy models                     | §4.1–4.5                 |   |
| 11.  | Wed Apr 21 | Example policies                  | §4.6, G                  | Homework #2 due, #3 out                 |
| 12.  | Fri Apr 23 | Confidentiality models            | §5.1–5.2.2, 5.3, A       |   |
| 13.  | Mon Apr 26 | Integrity models                  | 6.1, 6.2.3, 6.4          |   |
| 14.  | Wed Apr 28 | Trust models                      | 6.5                      | <i>midterm given out</i>                |
| 15.  | Fri Apr 30 | Other models                      | §8.1, 8.3, 8.4           | Lab #2 due, #3 out                      |
| 16.  | Mon May 3  | Introduction to cryptography      | §10.1–10.2, F            | <i>midterm due</i>                      |
| 17.  | Wed May 5  | Public key cryptography           | §10.3–10.5, B            | Homework #3 due, #4 out                 |
| 18.  | Fri May 7  | Key exchange                      | §11.1–11.2, 11.4         |   |
| 19.  | Mon May 10 | Cipher techniques                 | §12.1, 12.3–12.4, 12.5.3 |   |
| 20.  | Wed May 12 | Authentication                    | §13                      |   |
| 21.  | Fri May 14 | Anonymity, ACLs                   | §15.7, 16.1              | Lab #3 due, #4 out                      |
| 22.  | Mon May 17 | C-lists, other mechanisms         | §16.2–16.4               |   |
| 23.  | Wed May 19 | Information flow                  | §17.1, 17.3, C           | Homework #4 due, #5 out                 |
| 24.  | Fri May 21 | More information flow             | §17.4, 17.6              |   |
| 25.  | Mon May 24 | Malware                           | §23.1–23.7               |   |
| 26.  | Wed May 26 | Malware defenses                  | §23.9                    |   |
| 27.  | Fri May 28 | Intrusion detection               | §26                      | Lab #4 due                              |
| —.   | Mon May 31 | <b>Memorial Day</b> (no class)    |                          |   |
| 28.  | Wed Jun 2  | <i>to be arranged</i>             |                          | Homework #5 due: <i>final given out</i> |
| —.   | Wed Jun 9  | Final exam period; not held       |                          | <i>final due at 8:00pm</i>              |

### Discussion Sections

| dis. | dates         | topic                                 |
|------|---------------|---------------------------------------|
| —.   | Mar 29, 31    | <i>No discussion section</i>          |
| 1.   | Apr 5, 7      | Password management                   |
| 2.   | Apr 12, 14    | Cross-site scripting                  |
| 3.   | Apr 19, 21    | Phishing, hooking                     |
| 4.   | Apr 26, 28    | Review for midterm                    |
| 5.   | May 3, 5      | SQL and command injection             |
| 6.   | May 10, 12    | <i>ssh, tor</i>                       |
| 7.   | May 17, 19    | <i>wireshark</i> , net traces         |
| 8.   | May 24, 26    | Review midterm answers, and for final |
| —.   | May 31, Jun 2 | <i>No discussion section</i>          |