Slide 1

Administrivia

- Reminder: Homework 5 due Monday.
- Homework 6 (two problems) on Web. Due next Friday.

Slide 2

Security Risks Revisited — “Attacks From Within”

- Textbook discusses several ways programs can be made to do things their authors would not want and probably did not intend — buffer overflows, code injection attacks, etc.
- Common factor (my opinion!) is what one might call insufficient paranoia on the part of the programmers.

Slide 3

Security Risks Revisited — “Attacks From Outside”

- Textbook discusses several ways “malware” (viruses, worms, etc.) can infect a system.
- Common factor (my opinion!) is allowing execution of code that does something unwanted. (Either users don’t realize this is happening, or they don’t realize the implications?) Social engineering is often involved. Monoculture makes the malware writer’s job easier.

Slide 4

Safe Execution of “Mobile” Code

- Is there a way to safely execute code from possibly untrustworthy source? Maybe — approaches include sandboxing, interpretation, code signing.
- Example — Java’s designed-in security:
  - At source level, very type-safe — no way to use `void*` pointers to access random memory. (Contrast with C!)
  - When classes are loaded, “verifier” checks for potential security problems (not generated by normal compilers, but could be done by hand).
  - At runtime, security manager controls what library routines are called — e.g., applets by default can’t do file operations, many kinds of network access.

Slide 5

Trusted Systems

- Is it possible to write a secure O/S? Yes (says Tanenbaum).
- Why isn't that done?
  - People want to run existing code.
  - People prefer (or are presumed to prefer) more features to more security.

Slide 6

Designing a Secure System

- "Security through obscurity" isn't very.
- Better to give too little access than too much — give programs/people as little as will work.
- Security can't be an add-on.
- "Keep it simple, stupid."

Slide 7

Security — Summary

- Huge topic. Important and (I think!) interesting, though somewhat beyond the scope of this course.
- Shameless not-self-promotion: Strongly consider taking Dr. Myers's course "Information Assurance and Security" (CSCI 3311).

Slide 8

Minute Essay

- Over the course of the semester I've told several "war stories" — tales of woe that taught me (or someone) something. Do you have a favorite war story to tell?