Slide 1

Administrivia

- Reminder: Homework 7 due today.
- No more required homeworks. I will put together a set of extra-credit problems, soon.

Slide 2

Homework 5 Essays

- (This was the second set of problems on memory management.)
- Most people (but not all!) seemed to find these problems easier than previous assignments.
- Several people said the first programming problem (timing loops) was interesting in that it confirms what the written problem predicts.
- Several people said the coding for the second programming problem wasn't very difficult, once they had figured out what to code and how to make use of the starter code.

Slide 3

Security — Overview

- Goals:
  - Data confidentiality — prevent exposure of data.
  - Data integrity — prevent tampering.
  - System availability — prevent DOS (denial of service).
- What can go wrong:
  - Deliberate intrusion — from casual snooping to "serious" intrusion.
  - Accidental data loss — "acts of God", hardware or software error, human error.

Slide 4

User Authentication

- Based on "something the user knows" — e.g., passwords. Problems include where to store them, whether they can be guessed, whether they can be intercepted.
- Based on "something the user has" — e.g., key or smart card. Problems include loss/theft, forgery.
- Based on "something the user is" — biometrics. Problems include inaccuracy/spoofing.

Slide 5

Attacks From Within

- Trojan horses (and how this relates to `$PATH`).
- Login spoofing (and how this related to the Windows control-alt-delete login prompt).
- Logic bombs and trap doors.
- Buffer overflows (and how this relates to, e.g, `gets`).
- Code injection attacks.
- And many more . . .

Slide 6

Buffer Overflows

- How many times, when you read the technical description of a security flaw, do you notice the phrase “buffer overflow”? (For me — often.)
- You already know what a buffer overflow is, from writing programs in C, and how it can lead to interesting(?) bugs.
- How can this be turned to advantage by crackers? Textbook provides a brief description. A frequently-mentioned paper is called “Smashing the Stack for Fun and Profit”. Interesting reading, but the methods apparently don’t work on systems that disallow executing code from “the stack”. Textbook mentions alternatives that do still work.

Slide 7

"Attacks From Within" — Summary?

- 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 8

Attacks From Outside

- Can categorize as viruses (programs that reproduce themselves when run), worms (self-replicating), spyware, etc. — similar ideas, though.
- Many, many ways such code can get invoked — when legit programs are run, at boot time, when file is opened by some applications ("macro viruses"), etc.
- Also many ways it can spread — once upon a time floppies were vector of choice, now networks or e-mail. Common factors:
  - Executable content from untrustworthy source.
  - Human factors.

  "Monoculture" makes it easier!
- Virus scanners can check all executables for known viruses (exact or fuzzy matches), but hard/impossible to do this perfectly.
- Better to try to avoid viruses — some nice advice in textbook.

Slide 9

"Attacks From Outside" — Summary?

- 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 10

Safe Execution of "Mobile" Code

- Is there a way to safely execute code from possibly untrustworthy source?
- Maybe — approaches include sandboxing, interpretation, code signing.

Slide 11

Safe Execution of "Mobile" Code — Java(?)

- Java designed from the beginning to make it possible to execute code from possibly-untrustworthy source safely:
  - At source level, very type-safe — no way to use `void*` pointers to access random memory. (Contrast with C and 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.
- Sadly, apparently implementations are flawed, so this nice scheme doesn't work as well as hoped for.

Slide 12

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 13

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 14

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).

Minute Essay

- The textbook claims that one reason computer systems are typically so insecure is that users are assumed to prefer features to security. Agree or disagree?

Slide 15