Slide 1

Administrivia

- Short Homework 7 (about chapter 9) and Homework X ("extra credit") on Web tomorrow. Due Monday December 15 at 5pm.

Slide 2

Security — Overview

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

CSCI 4320 December 4, 2003

Slide 3

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 4

Attacks From Within

- Trojan horses (and how this relates to `$PATH`).
- Login spoofing.
- Logic bombs and trap doors.
- Buffer overflows (and how this relates to, e.g, `gets`).
- And many more . . . (see also the "famous flaws" section).

Slide 5

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 6

Attacks From Outside

- Can categorize as viruses (programs that reproduce themselves when run) and worms (self-replicating) — 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 on p. 633.

CSCI 4320 December 4, 2003

Slide 7

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.
  - 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 8

Protection Mechanisms

- Abstract discussion of "domains" — who has which rights to which objects. Two approaches — for each object who has rights, for each process what it can do.
- Unix file-permissions scheme — three groups, plus bits for "set user/group ID".

Slide 9

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 10

"Risks" Mailing List

- `comp.risks` newsgroup / mailing list / `http://catless.ncl.ac.uk/Risks`.

CSCI 4320 December 4, 2003

Slide 11

Minute Essay

- How did this exam compare to your expectations?