CSE 543 - Computer Security (Fall 2006)

Lecture 22 - Language-based security
November 16, 2006
URL: http://www.cse.psu.edu/~tjaeger/cse543-f06/

The Morris Worm

- Robert Morris, a 23 doctoral student from Cornell
  - Wrote a small (99 line) program
  - November 3rd, 1988
  - Simply disabled the Internet
- How it did it
  - Reads /etc/password, they tries the obvious choices and dictionary, /usr/dict words
- Used local /etc/hosts.equiv, .rhosts, .forward to identify hosts that are related
  - Tries cracked passwords at related hosts (if necessary)
  - Uses whatever services are available to compromise other hosts
- Scanned local interfaces for network information
- Covered its tracks (set is own process name to sh, prevented accurate cores, re-forked itself)

Engineering Disaster?

- Millions of Bots
  - Compromised applications
- Programming errors
  - Enable code insertion
- What can we do to fix them?
- Just starting to get serious...