NTNU | Norwegian University of Science and Technology

Operating Systems

Lecture 22: Security (2)

Michael Engel

Overview

- **Idea:** get to know different styles of lectur(er)s
  - Here, introducing a special topic on OS security from MIT’s OpenCourseware course 6.858 Computer Systems Security
  - Based on topics we introduced in lecture 21
- **Instead of watching a lecture by me:**
  - Read the (short) paper:
    Norm Hardy: *"The Confused Deputy*
    (or why capabilities might have been invented)"
    http://www.scs.stanford.edu/13wi-cs240/sched/readings/confused-deputy.pdf
  - Watch the related MIT lecture video:
    https://www.youtube.com/watch?v=TQhmua7Z2cY

Think about the following questions

We will discuss these questions on Thursday:

1. What's the problem the authors of the "confused deputy" paper encountered?
2. What goes wrong?
3. Why isn't the /sysx/fort thing just a bug in the compiler?
4. So what's the "confused deputy"?
5. Can we solve this confused deputy problem in Unix?
6. What are examples of ambient authority?
7. How does naming an object through a capability help?
8. Could we use file descriptors to solve our problem with a setuid gcc?
9. What sorts of applications might use sandboxing?