Outline for January 29, 2008

Reading: text, §23.2, §26.4; [Th84]; [TL00]

Discussion Problem. In 2003, Senator Orin Hatch said he wanted copyright holders to be able to use special-purpose hardware to prevent piracy. The following paragraph is quoted from the PoliTech mailing list, and is dated June 19, 2003, at 10:12AM

> Sen. Orrin Hatch, R-UT, said he was drafting legislation to require devices in PCs permitting the destruction of hardware used for wide-scale copyright infringement by sending a secret command to the remote computer. A copyright holder would be required to offer two warnings before the "kill switch" was activated and the computer destroyed or permanently disabled, Hatch said.

1. What are the arguments in favor of Sen. Hatch's proposal?
2. What are the arguments against Sen. Hatch's proposal?
3. If this proposal had been adopted, what safeguards should be put into place to prevent unauthorized activation of the "kill switch"?

Lecture Outline

1. Models of Attacks
   a. Example attack: *rsh* and synflooding
   b. Capabilities and requires/provides models
   c. Attack trees
2. Penetration Studies
   d. Why? Why not direct analysis?
   e. Effectiveness
   f. Interpretation
3. Flaw Hypothesis Methodology
   a. System analysis
   b. Hypothesis generation
   c. Hypothesis testing
   d. Generalization
4. System Analysis
   a. Learn everything you can about the system
   b. Learn everything you can about operational procedures
   c. Compare to other systems
5. Hypothesis Generation
   d. Study the system, look for inconsistencies in interfaces
   e. Compare to other systems' flaws
   f. Compare to vulnerabilities models
6. Hypothesis testing
   g. Look at system code, see if it would work (live experiment may be unneeded)
   h. If live experiment needed, observe usual protocols