Assignment 7: March 31 through April 6

For Lecture, Wednesday, March 31 (Security)

Today we start a new topic in 6.033: security. As an introduction to security, we will first discuss privacy and security in society. To get prepared, read "Teaching students about responsible use of computers" by Lerman et al. (#20). (The journal incorrectly showed Saltzer as the sole author.)

Also read Spafford's "Crisis and aftermath" (#19). It is a very interesting and entertaining security reading; it reports the events around the Internet worm constructed by Robert Morris, Jr. in 1988. This worm brought large parts of the Internet down and led to a flurry of articles in the national newspapers discussing its ethical and social implications. You might even find several of the players around MIT. Morris was fined over $10,000, sentenced to 400 hours of community service, and placed on probation for 3 years. Some people think this punishment was too light, others think it was too heavy. What do you think?

Optionally you can read the very enlightening Social Security FAQ. If you are interested in current events related to worms, follow these links to articles (completely optional):

- CERT Advisory for Melissa Macro Virus
- CERT Advisory related to a Linux worm

If you're really into security and want to discuss issues with other students, post to the 6.033 discuss meeting.

For Recitation, Thursday, April 1 (Case studies in security)

To prepare for recitation read Appendix 6.A (#23) from "The protection of information in computer systems" by Saltzer and Schroeder (pp. 6-34 to 6-55). Appendix 6.A follows after 30 pages of reading #23. You only need to read appendix 6.A today.

For Lecture, Monday, April 5 (Authentication)

In preparation for this lecture, read the first section (pp. 6-3 to 6-15) of "The protection of information in computer systems" by Saltzer and Schroeder (#23).

For Recitation, Tuesday, April 6 (Kerberos)

Read Miller et al., "Kerberos authentication and authorization system" (#21). This is an important paper, so read it with care. Try to understand the protocols and the line of reasoning behind them. Your one-page reading report should address the following issue:

Discuss one detail where you can simplify or improve the Kerberos protocol by using public-key cryptography instead of symmetric-key cryptography. The modificaton should not reduce the security of the overall system. Briefly outline the necessary modifications to the protocol. Don't hesitate to dive into the details of Kerberos in order to get the insight for this question. Use the same terminology from last week's lectures and the draft of chapter 6 handed out on April 5.

For this assignment, do not focus on the subtleties of a particular public-key cryptosystem (e.g., prime numbers, RSA, Diffie-Hellman). Rather you should focus on the general properties of public-key cryptography.

For Lecture, Wednesday, April 7 (Authorization)

In preparation for this lecture, read the second section (pp 6-16 to 6-29) of "The protection of information in computer systems" by Saltzer and Schroeder (#23).

System aphorism of the week

The unavoidable price of reliability is simplicity. (C.A.R. Hoare)
