Outline for February 21, 2008

Reading: text, §14.6, 12.1–12.2

Discussion Problem. Your friend has asked you to retrieve a book from inside a trunk he left at your house. The trunk is a hard plastic trunk, with the lid attached to the trunk's body by a continuous hinge in the back and two releasable latches on the front securing the lid. The trunk is secured by a lock that goes through a hole at the edge of the lid and a hole at the top of the body of the trunk. The lock is a very thick keyed lock. Unfortunately, your friend has lost the key. So, you find a pair of bolt cutters at your house—but the lock is too thick to cut. What should you do in order to get into the trunk? What questions should you ask to begin?

Lecture Outline

1. Identity
    a. Identity on the web
    b. Host identity: static and dynamic identifiers
    c. State and cookies
2. Authentication
    a. Validating client (user) identity
    b. Validating server (system) identity
    c. Validating both (mutual authentication)
3. Basis: what you know/have/are, where you are
4. Passwords
    a. Problem: common passwords
    b. May be pass phrases: goal is to make search space as large as possible, distribution as uniform as possible
    c. Other ways to force good password selection: random, pronounceable, computer-aided selection
5. Password Storage
    a. In the clear; why this is bad
    b. Enciphered; key must be kept available
    c. Hashed; show UNIX versions, including salt
6. Attacks
    a. Exhaustive search: password is 1 to 8 chars, say 96 possibles; it's about 7×1016
    b. Inspired guessing: think of what people would like (see above)
    c. Random guessing: can't defend against it; bad login messages aid it
    d. Scavenging: passwords often typed where they might be recorded as login name, in other contexts, etc.
    e. Ask the user: very common with some public access services