Outline for October 22, 2003

Reading: Chapters 9.4, 10.1–10.2

Discussion Problem

One of the concerns in electronic voting is the integrity of the vote count. Most electronic voting schemes work by having a computerized voting machine take a user's votes through an input device like a touch screen and record it in storage. All votes are stored on three different sets of media, for redundancy. At the end of the day, one of the pieces of media is removed from the machine, and the votes on it are uploaded to a server using a modem and telephone line. The server is not on the Internet, and can only be accessed through the phone line when the operators are told to turn the modem at the server's end on.

1. One contentious issue is the need for a voter-verifiable audit trail, which is a record of how the voter voted in a form that the voter can read or hear. Is this really necessary?
2. If you were an analyst and asked to check the integrity of the electronic voting system, where would you look for potential flaws?

Outline for the Day

1. Cryptographic Checksums
   a. Function $y = h(x)$: easy to compute y given x; computationally infeasible to compute x given y
   b. Variant: given x and y, computationally infeasible to find a second x' such that $y = h(x')$.
   c. Keyed vs. keyless
2. Key Exchange
   a. Needham-Schroeder and Kerberos
   b. Public key; man-in-the-middle attacks