Outline for February 19, 2008

Reading: text, §10.1–10.2, 10.4.2, 10.6, 14.1–14.4, 14.6

Discussion Problem. Currently, the United States has no national identification card. The closest things to it are passports and identification issued by the state Departments of Motor Vehicles (or their equivalents), which some people do not have. Recently, there has been discussion about creating such a card by requiring all state driver licenses and non-driver identification to conform to a federal guideline—and requiring everyone to have one.

Without going into the politics of whether a national identification card is good, bad, appropriate, or inappropriate, what are some of the technical challenges that must be overcome in issuing national identification cards?

Lecture Outline

1. Key Exchange
   a. Needham-Schroeder and Kerberos
   b. Public key; man-in-the-middle attacks
2. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
3. Digital Signatures
   a. Judge can confirm, to the limits of technology, that claimed signer did sign message
   b. RSA digital signatures: sign, then encipher
4. Identity
   a. Principal and identity
   b. Users, groups, roles
   c. Identity on the web