

Outline for May 3, 2005

Reading: §10.4.2, §10.5.2, §10.6, §12

Outline

1. Cryptographic Key Infrastructure
 - a. Certificates (X.509, PGP)
 - b. Certificate, key revocation
2. Digital Signatures
 - a. Judge can confirm, to the limits of technology, that claimed signer did sign message
 - b. RSA digital signatures: sign, then encipher
3. Authentication:
 - a. Basis: what you know/have/are, where you are
4. Passwords
 - a. How UNIX does selection
 - b. Problem: common passwords
 - c. May be pass phrases: goal is to make search space as large as possible, distribution as uniform as possible
 - d. Other ways to force good password selection: random, pronounceable, computer-aided selection
 - e. Go through problems, approaches to each, *esp.* proactive
5. Password Storage
 - a. In the clear; MULTICS story
 - b. Enciphered; key must be kept available; get to it and it's all over
 - c. Hashed; present idea of one-way functions using identity and sum; show UNIX version, including salt
6. Attack Schemes Directed to the Passwords
 - a. Exhaustive search: UNIX is 1-8 chars, say 96 possibles; it's about $7e16$
 - 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
 - f. Expected time to guess
7. Password aging
 - a. Pick age so when password is guessed, it's no longer valid
 - b. Implementation: track previous passwords vs. upper, lower time bounds
8. Ultimate in aging: One-Time Password
 - a. Password is valid for only one use
 - b. May work from list, or new password may be generated from old by a function
 - c. Example: S/Key
9. Challenge-response systems
 - a. Computer issues challenge, user presents response to verify secret information known/item possessed
 - b. Example operations: $f(x) = x+1$, random, string (for users without computers), time of day, computer sends $E(x)$, you answer $E(D(E(x))+1)$
 - c. Note: password never sent on wire or network
 - d. Attack: man-in-the-middle
 - e. Defense: mutual authentication