Notes for November 14, 2000

1. Greetings and Felicitations!
2. Puzzle of the day
1. Authentication:
   a. validating client (user) identity
   b. validating server (system) identity
   c. validating both (mutual authentication)
2. Basis
   a. What you know
   b. What you have
   c. What you are
3. Passwords
   a. How UNIX does selection
   b. Problem: common passwords; Go through Morris and Thompson ; Klein and mine, *etc*.
   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
4. Password Storage
   a. In the clear; MULTICS story
   b. Enciphers; 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
   d. Show UNIX version
5. 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 (b\as login name, in other contexts, *etc*.
   e. Ask the user: very common with some public access services
   f. Expected time to guess
6. 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   a. Pick age so when password is guessed, it's no longer valid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
7. Ultimate in aging: One-Time Pads
   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™
8. 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: monkey-in-the-middle

   e. Defense: mutual authentication
9. Biometrics
   a. Depend on physical characteristics
   b. Examples: pattern of typing (remarkably effective), retinal scans, *etc*.
10. Location
   a. Bind user to some location detection device (human, GPS)
   b. Authenticate by location of the device

Puzzle of the Day

"Our ancestors, and those who were considered to be wise, were accustomed to say that it was necessary to control Pistoia by means of factions and Pisa by means of fortresses; so they fostered strife in various of their subject towns, so as to control them more easily. In those days, when there was stability of a sort in Italy, this was doubtless sensible; but I do not think it makes a good rule today. I do not believe any good at all ever comes from dissension. On the contrary, on the approach of the enemy, cities which are so divided inevitably succumb at once; the weaker faction will always go over to the invader, and the other will not be able to hold out."[1]

What does this paragraph say to a system administrator or security officer seeking insight to defend her systems?

1. Niccolò Machiavelli, *The Prince*, George Bull *trans.*, Penguin Books, New York, NY ©1995, p. 67