Lecture 22, May 20

Reading: §11.3, 11.4.1, 12

Assignments due: Project Teams, due May 20, 2013 at 11:55pm
Homework #4, due May 24, 2013 at 11:55pm

Discussion Problem. What does the following paragraph say to a system administrator or security officer seeking insight to defend her systems?

> It can be put like this: the prince who is more afraid of his own people than of foreign interference should build fortresses; but the prince who fears foreign interference more than his own people should forget about them. The castle of Milan, built by Francesco Sforza, has caused and will cause more uprisings against the House of Sforza than any other source of disturbance. So the best fortress that exists is to avoid being hated by the people. If you have fortresses and yet the people hate you they will not save you; once the people have taken up arms they will not lack for outside help. In our own time, there is no instance of a fortress proving its worth to any ruler, except in the case of the countess of Forli, after her consort, Count Girolamo, had been killed. In her case the fortress gave her a refuge against the assault of the populace, where she could wait for succor from Milan and then recover the state. Circumstances were such that the people could not obtain support from outside. But subsequently fortresses proved of little worth even to her, when Cesare Borgia attacked her and then her hostile subjects joined forces with the invader. So then as before it would have been safer for her to have avoided the enmity of the people than to have had fortresses. So all things considered, I commend those who erect fortresses and those who do not; and I censure anyone who, putting his trust in fortresses, does not mind if he is hated by the people.[1]

Lecture outline.

1. Networks and ciphers
   a. Where to put the encryption
   b. Link vs. end-to-end
2. PEM, PGP
   a. Goals: confidentiality, authentication, integrity, non-repudiation (maybe)
   b. Design goals: drop in (not change), works with any RFC 821-conformant MTA and any UA, and exchange messages without prior interaction
   c. Use of Data Exchange Key, Interchange Key
   d. Review of how to do confidentiality, authentication, integrity with public key IKs
3. Authentication
   a. validating client (user) identity
   b. validating server (system) identity
   c. validating both (mutual authentication)
4. Basis: what you know/have/are, where you are
5. 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
6. Password Storage
   a. In the clear; Multics story
   b. Enciphered; key must be kept available
   c. Hashed; show UNIX versions, including salt

[1] Niccolò Machiavelli, *The Prince*, translated by George Bull, Penguin Books, New York, NY (1972), p. 69.