Outline for February 26, 2003

Reading: text, §10.1–10.2, 10.4 (except 10.4.1), 10.5.2, 10.6, 11.1, 11.3, 11.4.1

Discussion Problem

> "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 peoving 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 od 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 emnity 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]

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

Outline for the Day

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)
   b. Certificate, key revocation
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. Types of attacks
   a. Forward searches
   b. Misordered blocks
   c. Statistical regularities (repetitions)
5. Networks and ciphers
   a. Where to put the encryption
   b. Link *vs*. end-to-end
6. Example protocol: PEM
   a. Design goals
   b. How it was done
   c. Differences between it and PGP

[1] Niccolò Machiavelli, *The Prince*, George Bull *trans*., Penguin Books, New York, NY ©1995, p. 69