Outline for February 28, 2003

Reading: text, §10.4 (except 10.4.1), 10.5.2, 10.6, 11.1, 11.3, 11.4.1, 12.1–12.2.2

Discussion Problem

> "To fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting. In the practical art of war, the best thing of all is to take the enemy's country whole and intact; to shatter and destroy it is not so good. So, too, it is better to capture an army entire than to destroy it, to capture a regiment, a detachment, or a company entire than to destroy it."[1]

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

Outline for the Day

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. Types of attacks
    a. Forward searches
    b. Misordered blocks
    c. Statistical regularities (repetitions)
4. Networks and ciphers
    a. Where to put the encryption
    b. Link *vs*. end-to-end
5. Example protocol: PEM
    a. Design goals
    b. How it was done
    c. Differences between it and PGP
6. Authentication:
    a. Basis: what you know/have/are, where you are
7. 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
8. 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
9. 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

[1] Sun Tzu, *The Art of War*, James Clavell, *ed*., Dell Publishing, New York, NY ©1983, p. 15