Lecture 16 Outline

May 19, 2016

Reading: *text*, §11, 12, 13 **Assignments due:** Homework 4, on May 23

1. Greetings and felicitations!
   a. Discussion question
2. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
   b. Certificate, key revocation
3. Networks and ciphers
   a. Where to put the encryption
   b. Link vs. end-to-end
4. 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
5. Authentication
   a. Validating client (user) identity
   b. Validating server (system) identity
   c. Validating both (mutual authentication)
   d. Basis: what you know/have/are, where you are
6. 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

---

Discussion question. How does weapon development, as described in the following paragraph, compare to developing computer security mechanisms?

> Weapons developers, when given a choice, always go for the complex, elaborate solution at the expense of the simple one. Complexity leads to higher costs: purchase costs, operations costs, and maintenance costs. Higher costs result in fewer weapons, which, in turn, lead to contrived tests and analyses to prove that the relatively few complex systems can overcome the larger numbers of the simpler, less expensive weapons of the enemy. The fewer the weapons, the tighter is the control of these precious assets by a centralized command structure. The elaborate paraphernalia that comes with the centralized command structure only adds to the complexity of the overall system.[1]

[1] J. Burton, *The Pentagon Wars*, Naval Institute Press, Annapolis, MD (1993), p. 41.