Lecture 15 Outline

May 17, 2016

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

1. Greetings and felicitations!
   a. Discussion question
2. RSA
   a. Provides both authenticity and confidentiality
   b. Go through algorithm:
   Idea: $C = M^e \bmod n$, $M = C^d \bmod n$, with $ed \bmod \phi(n) = 1$
   Public key is (e, n); private key is d. Choose $n = pq$; then $\phi(n) = (p-1)(q-1)$.
   c. Example: $p = 5$, $q = 7$; then $n = 35$, $\phi(n) = (5-1)(7-1) = 24$. Pick $d = 11$. Then $ed \bmod \phi(n) = 1$, so $e = 11$
   To encipher 2, $C = M^e \bmod n = 2^{11} \bmod 35 = 2048 \bmod 35 = 18$, and $M = C^d \bmod n = 18^{11} \bmod 35 = 2$.
   d. Example: $p = 53$, $q = 61$; then $n = 3233$, $\phi(n) = (53-1)(61-1) = 3120$. Pick $d = 791$. Then $e = 71$
   To encipher $M =$ `RENAISSANCE`, use the mapping `A = 00`, `B = 01`, ..., `Z = 25`, ␢ = 26.
   Then: $M =$ `RE NA IS SA NC E`␢ = 1704 1300 0818 1800 1302 0426
   So: $C = (1704)^{71} \bmod 3233 = 3106; \ldots = 3106\ 0100\ 0931\ 2691\ 1984\ 2927$
3. Cryptographic Checksums
   a. Function $y = h(x)$: easy to compute y given x; computationally infeasible to compute x given y
   b. Variant: given x and y, computationally infeasible to find a second x' such that $y = h(x')$
   c. Keyed vs. keyless
4. Digital Signatures
   a. Judge can confirm, to the limits of technology, that claimed signer did sign message
   b. RSA digital signatures: encipher, then signs (risks)
5. Key Exchange
   a. Needham-Schroeder and Kerberos
   b. Public key; man-in-the-middle attacks
6. Key Generation
   a. Cryptographically random numbers
   b. Cryptographically pseudorandom numbers
   c. Strong mixing function

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.