Outline for February 14, 2003

Reading: text, §6.2, 9.1–9.3

Discussion Problem

All computer security experts seem to like puns. So, if you want to talk like a computer security expert, here are 14 puns from what the Book of Lists 2 has called the world's worst puns. Consider yourselves armed (or forewarned)!

1. The Eskimo stabbed himself with an icicle. He died of cold cuts.
2. In his dessert list, a San Antonio restaurateur suggests, "Remember the alamode!"
3. There was an advice-to-the-lovelorn editor who insisted, "If at first you don't succeed, try a little ardor."
4. The commuter's Volkswagen down once too often. So he consigned it to the Old Volks Home.
5. The wise old crow perched himself on a telephone wire. He wanted to make a long-distance caw.
6. A talkative musician couldn't hold a job. Every time he opened his mouth, he put his flute in it.
7. A farmer with relatives in East Germany heard that a food package he had sent had never arrived. Optimistically, he assured them, "Cheer up! The wurst is yet to come."
8. When the promoter of a big flower show was told that a postponement was necessary because the exhibits coud-not be installed on time, he explained to his backers, "We were simply caught with our plants down."
9. A critic declared that he always praised the first show of a new theatrical season. "Who am I," he asked, "to stone the first cast?"
10. Egotist: a person who's always me-deep in converstion.
11. "It's raining cats and dogs," one man remarked. "I know," said another. "I just stepped into a poodle."
12. An eccentric bachelor passed away and left a nephew nothing but 392 clocks. The nephew is now busy winding up the estate.
13. The baseball pitcher with a sore arm was in the throws of agony.

Outline for the Day

1. Clark-Wilson
   a. Theme: military model does not provide enough controls for commercial fraud, *etc*. because it does not cover the right aspects of integrity
   b. "Constrained Data Items" (CDI) to which model applies, "Unconstrained Data Items (UDIs) to which no integrity checks applied, "Integrity Verification Procedures" (IVP) verify conformance to the integrity spec when IVP is run, "Transaction Procedures" (TP) take system from one well-formed state to another
   c. Certification and enforcement rules:
      C1. All IVPs must ensure that all CDIs are in a valid state when the IVP is run
      C2. All TPs must be certified as valid; each TP is assocated with a set of CDIs it is authorized to manipulate
      E1. The system must maintain these lists and must ensure only those TPs manipulate those CDIs
      E2: The system must maintain a list of User IDs, TP, and CDIs that that TP can manipulate on behalf of that user, and must ensure only those executions are performed.
      C3. The list of relations in E2 must be certified to meet the separation of duty requirement.
      E3. The sysem must authenticate the identity of each user attempting to execute a TP.
      C4. All TPs must be certified to write to an append-only CDI (the log) all information necessary to reson-struct the operation.
      C5. Any TP taking a UDI as an input must be certified to perform only valid transformations, else no trans-formations, for any possible value of the UDI. The transformation should take the input from a UDI to a CDI, or the UDI is rejected (typically, for edits as the keyboard is a UDI).
      E4. Only the agent permitted to certify entities may change the list of such entities associated with a TP. An agent that can certify an entity may not have any execute rights with respect to that entity
2. Cryptography
   a. codes vs. ciphers
   b. attacks: ciphertext only, known plaintext, chosen plaintext
3. Classical Cryptography
   a. monoalphabetic (simple substitution): $f(a) = a + k \bmod n$

   b. example: Caesar with $k = 3$, RENAISSANCE → UHQDLVVDQFH
   c. polyalphabetic: Vigenère, $f_i(a) = (a + k_i) \bmod n$
   d. cryptanalysis: first do index of coincidence to see if it's monoalphabetic or polyalphabetic, then Kasiski method.
   e. problem: eliminate periodicity of key
4. Long key generation
   a. Running-key cipher: M=THETREASUREISBURIED; K=THESECONDCIPHERISAN; C=MOIL-VGOFXTMXZFLZAEQ; wedge is that (plaintext,key) letter pairs are not random (T/T, H/H, E/E, T/S, R/E, A/O, S/N, *etc*.)
   b. Perfect secrecy: when the probability of computing the plaintext message is the same whether or not you have the ciphertext
   c. Only cipher with perfect secrecy: one-time pads; C=AZPR; is that DOIT or DONT?
5. DES
6. Public-Key Cryptography
   a. Basic idea: 2 keys, one private, one public
   b. Cryptosystem must satisfy:
      i. given public key, CI to get private key;
      ii. cipher withstands chosen plaintext attack;
      iii. encryption, decryption computationally feasible [note: commutativity ***not*** required]
   c. Benefits: can give confidentiality or authentication or both
7. RSA
   a. Provides both authenticity and confidentiality
   b. Go through algorithm:

      Idea: $C = M^e \bmod n$, $M = C^d \bmod n$, with $ed \bmod \phi(n) = 1$.

      Proof: $M^{\phi(n)} \bmod n = 1$ [by Fermat's theorem as generalized by Euler]; follows immediately from $ed \bmod \phi(n) = 1$.

      Public key is (e, n); private key is d. Choose $n = pq$; then $\phi(n) = (p–1)(q–1)$.
   c. Example:

      $p = 5$, $q = 7$; $n = 35$, $\phi(n) = (5–1)(7–1) = 24$. Pick $d = 11$. Then $de \bmod \phi(n) = 1$, so choose $e = 11$. 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: $p = 53$, $q = 61$, $n = 3233$, $\phi(n) = (53–1)(61–1) = 3120$. Take $d = 791$; then $e = 71$. Encipher M = RENAISSANCE: A = 00, B = 01, …, Z = 25, blank = 26. Then:

      M = RE NA IS SA NC Eblank = 1704 1300 0818 1800 1302 0426

      $C = (1704)^{71} \bmod 3233 = 3106$; *etc.* = 3106 0100 0931 2691 1984 2927