Lecture 16, May 6

Reading: §6.4, 9.1–9.2 **Assignments due:** Homework #3, due May 13, 2013

Discussion Problem. Currently, the United States has no national identification card. The closest things to it are passports and identification issued by the state Departments of Motor Vehicles (or their equivalents), which some people do not have. Recently, there has been discussion about creating such a card by requiring all state driver licenses and non-driver identification to conform to a federal guideline—and requiring everyone to have one.

Without going into the politics of whether a national identification card is good, bad, appropriate, or inappropriate, what are some of the technical challenges that must be overcome in issuing national identification cards?

Lecture outline.

1. Greetings and felicitations!
   a. We will return the midterms in discussion section, so please come.
2. Clark-Wilson Model
   a. Theme: military model does not provide enough controls for commercial fraud, etc. because it does not cover the right aspects of integrity
   b. Components
      i. Constrained Data Items (CDI) to which the model applies
      ii. Unconstrained Data Items (UDIs) to which no integrity checks are applied
      iii. Integrity Verification Procedures (IVP) that verify conformance to the integrity spec when IVP is run
      iv. Transaction Procedures (TP) takes system from one well-formed state to another
3. Certification and enforcement rules of the Clark-Wilson Model
   a. C1. All IVPs must ensure that all CDIs are in a valid state when the IVP is run.
   b. C2. All TPs must be certified to be valid, and each TP is associated with a set of CDIs it is authorized to manipulate.
   c. E1. The system must maintain these lists and must ensure only those TPs manipulate those CDIs.
   d. 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.
   e. C3. The list of relations in E2 must be certified to meet the separation of duty requirement.
   f. E3. The system must authenticate the identity of each user attempting to execute a TP.
   g. C4. All TPs must be certified to write to an append-only CDI (the log) all information necessary to reconstruct the operation.
   h. C5. Any TP taking a UDI as an input must be certified to perform only valid transformations, else no transformations, 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).
   i. 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
4. Cryptography
   a. Codes vs. ciphers
   b. Attacks: ciphertext only, known plaintext, chosen plaintext
   c. Types: substitution, transposition
5. 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 is monoalphabetic or polyalphabetic, then Kasiski method.
   e. Problem: eliminate periodicity of key
6. Long key generation
   a. Autokey cipher:

M = `THETREASUREISBURIED`
K = `HELLOTHETREASUREISB`
C = `ALPEFXHWNIIIKVLVQWE`

b. Running-key cipher:

M = `THETREASUREISBURIED`
K = `THESECONDCIPHERISAN`
C = `MOILVGOFXTMXZFLZAEQ`

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.)

c. Perfect secrecy: when the probability of computing the plaintext message is the same whether or not you have the ciphertext

d. Only cipher with perfect secrecy: one-time pads; C = `AZPR`; is that `DOIT` or `DONT`?

7. Product ciphers: DES, AES