Outline for April 19, 2005

Reading: §6.4, §9

Discussion

Some programs use passwords for access control, but do not protect the passwords in a very sophisticated manner (for example, by saving them in a file) or make determining the correct password very easy (for example, the Microsoft Word 5.0 encipherment scheme). The argument for using simple passwords and weak encipherment is that the data or programs being protected are of little value and the passwords give a small measure of privacy.

Given that what they are protecting is truly of little value, why is the use of such simple passwords and easily-broken encipherment bad?

Outline

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 resonstruct the operation.
   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).
   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
   c. Types: substitution, transposition
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=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.)

    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