Problem Set 7 Solutions

Problem 7-1. Steganography vs Fingerprinting

Both Steganography and Fingerprinting embeds messages in larger objects, although from different purposes. The main differences are the following:

- In steganography the size of the embedded message may be large, while the size of a fingerprint does not have to be bigger than a few bytes.
- Since steganography is used to preserve secrecy, usually the design of the scheme must be kept secret as well. Fingerprinting instead can be in some cases an open scheme.
- The larger object is not important in steganography, while in fingerprinting is the reason the while the whole schemne is put in place.
- Generally sender and receiver in steganogrpahy are two different people who must agree on some secret "key" in order to transmit messages between them. In fingerprinting the person who puts the print is usually the same person who later verifies so there is no need to share secret information among parties.

Problem 7-2. Clark–Wilson Integrity Model

Constructing IVPs is difficult. In the CW integrity model the IVPs are used to check that data items (CDI's) are in fact in a valid state.

IVPs can be usually constructed for things like binaries in a system. Since these are not supposed to change, a signature can be associated with them. It's CDI's like user documents who are hard to check for integrity since they change frequently.

The CW model without IVPs reduces to a series of access control lists denoting who can perform specific operations on specific pieces of data. Attempting to limit or signal the damage done by a user is then left to the Transformation Procedure (TP).