Lecture 10: October 16, 2019

Reading: *text*, §6.4, 10.1–10.2

Assignments: Lab 1, due October 18, 2019
Homework 2, due October 21, 2019

1. Greetings and felicitations!
2. Puzzle of the Day
3. Clark-Wilson 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 to be valid, and each TP is associated 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 system 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 reconstruct 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.
4. Originator-controlled access control
5. Role-based access control
6. Break-the-glass policies
7. Cryptography
   (a) Codes vs. ciphers
   (b) Attacks: ciphertext only, known plaintext, chosen plaintext
   (c) Types: substitution, transposition
8. Symmetric Cryptography
   (a) Monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   (b) Example: Caesar (shift) cipher with $k = 3$, `RENAISSANCE` $\rightarrow$ `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