Lecture 14: April 28, 2021

Reading: *text*, §6.4–6.5

Assignments: Lab 2, due May 5, 2021
Homework 3, due May 7, 2021

1. Buffer overflow review
2. 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.
3. Trust models