CPSC 525: Clark–Wilson
An Integrity Model Tied to Trustworthy Execution

Michael E. Locasto

Department of Computer Science
UofC
CPSC 525/625

January 30, 2013
Announcements (10 minutes)
Learning Objectives for Today (1 minute)
Clark–Wilson model (35 minutes)
Readings (1 minute)
→ Fork-the-Law: possible source for HW1 optional source
→ Rewrite US CFAA in e-prime?
→ Go over the major components of the Clark–Wilson model
Model rules
Well-formed transactions
Separation of Duty
→ Contrast with Biba, but structurally and logically
→ Lab2Lecture: Research considerations on Model Kinematics and briding the semantic gap
Let’s consider the challenge of creating an environment that implements Clark–Wilson.

What do we need?
Programming language with UDI, CDI, TP, IVP

A compiler that produces a binary (or several binaries) implementing the various roles and separations of duty.

Manual certification of various entities in the resulting system.

An OS that will load these binaries and maintain their semantics. (plus certification of that OS).

Hardware that supports these interactions.
Model Kinematics tries to provide a mechanism whereby we can estimate the likely cost of trying to build a security system that corresponds to an abstract security model using real world primitives.

Questions:

- need to create a map from these abstract concepts to an actual artifact
- machine instruction? memory location?
- associate a cost with extracting each piece of state or aggregating other pieces of state
- articulate cost of each function / procedure in the model
- articulate frequency of incurring cost
Read the Clark–Wilson paper.