

## Principles of Information Security CS 5323 Lecture Six

Prof. William Winsborough  
September 18, 2008

## Business

- Read chapters 6 and 7
- Hand in Homework 1
- Questions from previous lectures?

18 September 2008

Winsborough CS 5323 Lecture 6

2

## Integrity

- Integrity is essentially trustworthiness
  - Requires systems and procedures that prevent corruption of information, malicious or otherwise
- Systems require data to be changed accurately and follow the rules.
  - Disclosure is not a major concern.
  - Common priority in business

18 September 2008

Winsborough CS 5323 Lecture 6

3

## Integrity Procedures

- Lipner [636] identifies five requirements for preserving data integrity:
  1. Users will not write their own programs, but will use existing production programs and databases.
  2. Programmers will develop and test programs on a nonproduction system; if they need access to actual data, they will be given production data via a special process, but will use it on their development system.
  3. A special process must be followed to install a program from the development system onto the production system.
  4. The special process in requirement 3 must be controlled and audited.
  5. The managers and auditors must have access to both the system state and the system logs that are generated.

18 September 2008

Winsborough CS 5323 Lecture 6

4

## Policies that Support Integrity

- 3 principles of operation:
  - Separation of duty
    - At least two different people participate in each critical function
  - Separation of function
    - E.g., programs are not developed on production system
  - Auditing
    - A process of analyzing systems to determine what actions took place and who performed them
    - Uses extensive logging
    - Commercial systems emphasize recovery and accountability

18 September 2008

Winsborough CS 5323 Lecture 6

5

## Integrity Models

- Integrity *levels* are associated with subjects and with objects through labels
  - i(s) and i(o)
  - Higher levels are more trustworthy than lower levels
  - These are different from confidentiality (security) labels
    - Integrity labels serve to inhibit modification of information

18 September 2008

Winsborough CS 5323 Lecture 6

6

## Biba Integrity Model

- Rules are dual to BLP:
  - s can read o if  $i(s) \leq i(o)$ 
    - Prevents implant of incorrect or false data
  - s can write o if  $i(s) \geq i(o)$ 
    - Recognizes that the subject might rely on the data for correct operation
  - $s_1$  can execute  $s_2$  if  $i(s_1) \geq i(s_2)$ 
    - Prevents a less trusted invoker to control the execution of more trusted subjects
    - This rule cannot always be enforced
      - System calls

18 September 2008

Winsborough CS 5323 Lecture 6

7

## Biba Variants

- Fixed subject labels
  - Subjects are prevented from reading lower integrity objects
- Low-water mark
  - On reading low integrity data, a subject's label is lowered accordingly
  - Subjects tend to become less and less trusted as execution proceeds

18 September 2008

Winsborough CS 5323 Lecture 6

8

## Clark-Wilson Integrity Model

- Transaction oriented
  - More accurately models commercial systems
- Terminology
  - CDI: Constrained data item
    - Data subject to integrity control
  - UDI: Unconstrained data item
  - Two procedures:
    - Integrity verification procedure (IVP): verify the CDIs conform to the integrity constraints at the time IVPs are run
    - Transformation procedure (TP): change the state of the data in the system from one valid state to another
  - Two kinds of rules: Certification rules and Enforcement rules.

18 September 2008

Winsborough CS 5323 Lecture 6

9

## Certification and Enforcement Rules

- Certification rule 1 (CR1)
  - When any IVP is run, it must ensure that all CDIs are in a valid state
- Certification rule 2 (CR2)
  - For some associated set of CDIs, a TP must transform those CDIs in a valid state into a (possibly different) valid state
- Enforcement rule 1 (ER1)
  - The system must maintain the *certified* relations, and must ensure that only TPs certified to run on a CDI manipulate that CDI

18 September 2008

Winsborough CS 5323 Lecture 6

10

## Certification and Enforcement Rules, cont.

- Enforcement rule 2 (ER2)
  - The system must associate a user with each TP and set of CDIs
    - The TP may access those CDIs on behalf of the associated user
    - If a user is not associated with a particular TP and CDI, the TP cannot access that CDI on behalf of that user
  - This defines a set of triples (*user*, *TP*, *CDI set*) to capture the association of users, TPs, and CDIs
    - This relation is called *allowed*
    - Allowed relations must be certified

18 September 2008

Winsborough CS 5323 Lecture 6

11

## Certification and Enforcement Rules, cont.

- Certification rule 3 (CR3)
  - The allowed relation must meet the requirements imposed by the principle of separation of duty
- Enforcement rule 3 (ER3)
  - The system must authenticate each user attempting to execute a TP
- Certification rule 4 (CR4)
  - All TPs must append enough information to reconstruct the transaction to an append-only CDI (the log)

18 September 2008

Winsborough CS 5323 Lecture 6

12

## Certification and Enforcement Rules, cont.

- Certification rule 5 (CR5)
  - Any TP that takes as input a UDI may perform only valid transformations, or no transformations, for all possible values of the UDI. The transformation either rejects the UDI or transforms it into a CDI.
- Enforcement rule 4 (ER4)
  - Only the certifier of a TP may change the list of entities associated with that TP
  - No certifier of a TP, or of an entity associated with that TP, may ever have execute permission with respect to that entity.

18 September 2008

Winsborough CS 5323 Lecture 6

13

## Clark-Wilson Satisfies Lipner's Requirements

- Requirement 1. If users are not allowed to perform certifications of TPs, but instead only "trusted personnel" are, then CR5 and ER4 enforce this requirement. Because ordinary users cannot create certified TPs, they cannot write programs to access production databases. They must use existing TPs and CDIs—that is, production programs and production databases.
- Requirement 2. This requirement is largely procedural, because no set of technical controls can prevent a programmer from developing and testing programs on production systems. (The standard procedural control is to omit interpreters and compilers from production systems.) However, the notion of providing production data via a special process corresponds to using a TP to sanitize, or simply provide, production data to a test system.

18 September 2008

Winsborough CS 5323 Lecture 6

14

## Clark-Wilson Satisfies Lipner's Requirements

- Requirement 3. Installing a program from a development system onto a production system requires a TP to do the installation and "trusted personnel" to do the certification.
- Requirement 4. CR4 provides the auditing (logging) of program installation. ER3 authenticates the "trusted personnel" doing the installation. CR5 and ER4 control the installation procedure (the new program being a UDI before certification and a CDI, as well as a TP in the context of other rules, after certification).
- Requirement 5. Finally, because the log is simply a CDI, management and auditors can have access to the system logs through appropriate TPs. Similarly, they also have access to the system state.

18 September 2008

Winsborough CS 5323 Lecture 6

15

## Comparison with Biba Model

- Clark-Wilson Model has two levels:
  - Objects are either constrained and unconstrained
  - Subjects have two levels: certified (the TPs) and uncertified (all other procedures)
- Clark-Wilson Model has certification rules. Biba doesn't
- Clark-Wilson has procedure to verify trusted entities and their actions
- Clark-Wilson requires a trusted entity certifies the method of upgrading integrity level.
  - Biba would require a trusted entity to manually upgrade individual objects

18 September 2008

Winsborough CS 5323 Lecture 6

16