

Principles of Information Security CS 5323 Lecture Five

Prof. William Winsborough
September 11, 2008

Business

- Read chapters 6 and 7
- Homework 1 due Tuesday 9/16
 - Section 4.8 Exercises 4 and 5; Section 5.5 Exercises 1, 2
 - Hand in on paper at the start of class
- Questions from previous lectures?

11 September 2008

Winsborough CS 5323 Lecture 5

2

The Bell-LaPadula (BLP) Model

- Corresponds to military-style classifications
 - Combines mandatory and discretionary access controls
 - Both must be satisfied for access to be granted
 - Mandatory part uses security levels that combine two components: classifications and categories
- Classifications: unclassified (U), confidential (C), secret (S), and top secret (TS)
- Subjects and objects are each associated with one of these

11 September 2008

Winsborough CS 5323 Lecture 5

3

Satisfying Classification Requirements

- Based on
 - *Security clearance* l_s of subject s
 - *Security classification* l_o of object o
- *Simple Security Condition* (without categories):
 - S can read O if and only if $l_o \leq l_s$ and S has discretionary read access to O
 - No read up
- *Star Property* (without categories):
 - S can write O if and only if $l_s \leq l_o$ and S has discretionary write access to O
 - No write down

11 September 2008

Winsborough CS 5323 Lecture 5

4

Basic Security Theorem (without categories)

- If a system starts in a secure state and the set of system state transformers obey the condition and property above, the system will remain in a secure state
 - A secure state is one in which all objects are correctly classified according to the sensitivity of the information they contain
 - The focus is on information flow

11 September 2008

Winsborough CS 5323 Lecture 5

5

Categories

- Categories tell what the information is about
 - They are used to support the “need to know” principle
 - Example: {NUC, EUR, US}
- The category part of a security level is a subset of the set of all categories
 - Sometimes called a *compartment*
 - For an object, it indicated the categories of information contained in the object
 - For a subject, it indicates the categories of information that the subject is permitted to read

11 September 2008

Winsborough CS 5323 Lecture 5

6

Combining Classification and Categories

- A security level is now given by a pair (L, C)
- Security levels are ordered
 - (L₁, C₁) *dominates* (L₂, C₂) if and only if L₂ ≤ L₁ and C₂ ⊆ C₁
 - Security levels form a lattice
 - Some levels are *incomparable*
 - “Dominates” is abbreviated *dom*

11 September 2008

Winsborough CS 5323 Lecture 5

7

The Full Theorem

- *Simple Security Condition*
 - S can read O if and only if S *dom* O and S has discretionary read access to O
- *Star Property*
 - S can write O if and only if S *dom* O and S has discretionary write access to O
- *Basic Security Theorem*
 - If a system starts in a secure state and the set of system state transformers obey the condition and property above, the system will remain in a secure state

11 September 2008

Winsborough CS 5323 Lecture 5

8

Allowing Writes Below Ones Security Level

- How to communicate with people having lower or incomparable security levels?
- A subject (process) has a *maximum security level* and a *current security level*
 - The max level is defined by the person on behalf of whom the subject is operating
 - The current level is defined by the objects that have been read so far
 - The current level is a *join* (i.e., a least upper bound) on the level of the objects read so far
- To communicate: start a new process to write at the lower level
 - Make sure it does not read any object unless it is dominated by the level at which the write is to occur

11 September 2008

Winsborough CS 5323 Lecture 5

9

DG/UX

- The Data General B2 Unix (DB/UX) system implements a modified BLP model
- Write up is prohibited
- Instead, objects and subjects have a *MAC tuple* as well as a MAC label
 - E.g., [(S, {NUC}), (TS, {NUC, EUR})]
 - The second must dominate the first
 - A subject can vary its label within the range defined by its tuple
 - To read an object, a subject's label must dominate the top of the object's range
 - To write, the subject's label must lie within the object's range

11 September 2008

Winsborough CS 5323 Lecture 5

10

Enforcing Information Flow in Programming Languages

- At the process level, the current security level presumes that it is possible that any write depends on any prior read
- Techniques have been developed to ensure that some outputs are independent of some inputs
 - They enforce *non-interference*
 - If your program has high and low confidentiality inputs and outputs, the low outputs depend only on the low inputs
 - Any two runs with the same low input, but different high input, produce the same low output

11 September 2008

Winsborough CS 5323 Lecture 5

11