

Principles of Information Security CS 5323 Lecture 18

Prof. William Winsborough
November 6, 2007

Business

- For Thursday 11/8, read Badger et al., Practical Domain and Type Enforcement for UNIX, 1995 IEEE SS&P
- I need two volunteers to administer the IDEA survey on Thursday
 - Be sure to pick up the survey by 5:30pm
 - We'll do the survey at the end of class

6 November 2007

Winsborough CS 5323 Lecture 18

2

BLP Has Been Criticized

- Does not deal with integrity, only confidentiality
 - Not necessarily a bad thing
- Does not address the management of access control
 - Originally did not anticipate changing security levels
- Contains covert channels (unregulated information flow)
 - If high security objects can be seen by low security subjects, their presence or absence can convey one bit
 - So can their security level

6 November 2007

Winsborough CS 5323 Lecture 18

3

Multics

- MULTIpIexed Information and Computing Service
- Big complicated systems project with ambitious security goals in 1970's
 - Became unwieldy and several project members split off and designed Unix instead

6 November 2007

Winsborough CS 5323 Lecture 18

4

The Biba Model

- Integrity: reliability, trustworthiness
- Objects can be labeled with elements of an integrity lattice
 - High integrity data must not depend on low integrity data
 - Information can flow down, but not up or sideways

6 November 2007

Winsborough CS 5323 Lecture 18

5

Biba Model

- $f = (f_S, f_O)$ in which
 - $f_S : S \rightarrow L$ gives the subject's integrity level
 - $f_O : O \rightarrow L$ gives the object's integrity level
- Several reasonable integrity policies are possible

6 November 2007

Winsborough CS 5323 Lecture 18

6

Static Integrity Levels

- Simple Integrity Property
 - If subject s can modify object o , then $f_O(o) \leq f_S(s)$ (no write up)
- Integrity *-Property
 - If subject s can read o and write p , then $f_O(p) \leq f_O(o)$
- Dual to BLP policies

6 November 2007

Winsborough CS 5323 Lecture 18

7

Dynamic Integrity Levels

- Subject low watermark property
 - Subject s can read an object o at any integrity level
 - The new value of $f_S(s)$ is $\text{glb}(f_S(s), f_O(o))$
- Object low watermark property
 - Subject s can modify an object o at any integrity level
 - The new value of $f_O(o)$ is $\text{glb}(f_S(s), f_O(o))$
- Danger: all s and o eventually have lowest integrity level

6 November 2007

Winsborough CS 5323 Lecture 18

8

Chinese Wall Model

- Avoids conflict of interest in consultancy business
 - Policy: information flow must not cause a conflict of interest
- C – the set of companies
- S – the set of subjects (analysts)
- O – set of objects, each of which contains information about just one company
- $y : O \rightarrow C$ – yields the company dataset of each object
- $x : O \rightarrow \wp(C)$ – yields the *conflict of interest class* (set of companies that must not receive information from object)
- $(x(o), y(o))$ – the security label of object o
 - A sanitized object o has label $(\emptyset, y(o))$

6 November 2007

Winsborough CS 5323 Lecture 18

9

Conflicts of Interest Depend on History of Accesses

- N is a matrix in $S \times O \rightarrow \text{Boolean}$
 - $N_{s,o} = \text{true}$, if s has had access to o
 - $N_{s,o} = \text{false}$, otherwise
- Initially, N is false everywhere

6 November 2007

Winsborough CS 5323 Lecture 18

10

Security Properties

- ss-property
 - s is permitted access to o only if for all o' with $N_{s,o'} = \text{true}$, $y(o) = y(o')$ or $y(o) \notin x(o')$
- *-property
 - s is permitted write access to o only if s has no read access to any o' with $y(o) \neq y(o')$ and $x(o') \neq \emptyset$

6 November 2007

Winsborough CS 5323 Lecture 18

11