

Principles of Information Security CS 5323 Lecture Nine

Prof. William Winsborough
September 27, 2007

Business

- Recall: we will have an exam covering material we (read and) discussed in class October 11
 - This one will be worth about 20% of the final grade
 - I plan to provide a study aid next week

27 September 2007

Winsborough CS 5323 Lecture 9

2

Partial Orders

- Not all elements (labels) have to be comparable
- Def: Given a set (of security labels) L and a relation $\leq \subset L \times L$, (L, \leq) is a partial ordering if it is
 - Reflexive: for all $a \in L$, $a \leq a$
 - Transitive: for all $a, b, c \in L$, if $a \leq b$ and $b \leq c$, then $a \leq c$
 - Anti-symmetric: for all $a, b \in L$, if $a \leq b$ and $b \leq a$, then $a = b$

27 September 2007

Winsborough CS 5323 Lecture 9

3

Examples

- $(\wp(X), \subseteq)$, the powerset of a set X ordered by subset
- $(\mathbb{N}, |)$, the natural numbers ordered by “divides”
- (Σ^*, \leq) , the set of strings ordered by prefix ($\beta \leq \alpha$ if there is a string γ such that $\alpha = \beta\gamma$)
- VSTa Microkernel uses (Σ^*, \leq) in which $\Sigma = \mathbb{N}$
 - As in most systems, the policy is that a subject labeled α can read an object labeled β if $\beta \leq \alpha$

27 September 2007

Winsborough CS 5323 Lecture 9

4

Lattices

- Lattices are partial orders in which least upper bounds and greatest lower bounds are guaranteed to exist

27 September 2007

Winsborough CS 5323 Lecture 9

5

Multilevel Security

- Mandatory Access Control (MAC) policies and multilevel security policies of the “Orange Book” are based on earlier procedures based on security level and clearance
- Need-to-know policies were based on:
 - H , a set of (linearly ordered) *classifications*
 - C , a set of *categories*; a *compartment* is a set of categories
 - Security labels have the form (h,c) , in which $h \in H$ is a security level and $c \subseteq C$ is a compartment
 - The partial ordering \leq of security labels is given by $(h_1, c_1) \leq (h_2, c_2)$ iff $h_1 \leq_H h_2$ and $c_1 \subseteq c_2$

27 September 2007

Winsborough CS 5323 Lecture 9

6

Enforcement Mechanisms

- We will talk more about security policies later
 - It is a formal statement of the strategy for meeting the system's security objectives
- Reference Monitor
 - Abstract machine that mediates all accesses
- Security Kernel
 - Implementation of reference monitor
 - Must be verifiably correct and protected from modification
- Trusted Computing Base (TCB)
 - Collection of all protection mechanisms that together enforce a security policy
 - Includes any mechanism whose correct operation is necessary to guarantee policy enforcement

27 September 2007

Winsborough CS 5323 Lecture 9

7

Placement of Reference Monitor

- Can go in any architectural layer
 - Hardware
 - OS kernel: *hypervisor* is a virtual machine
 - OS
 - Services layer (middle ware, JVM,...)
 - Application
- Position with respect to application
 - Lower level
 - Interpreter (e.g., Java)
 - Rewrite application to include AC (usually automated)

27 September 2007

Winsborough CS 5323 Lecture 9

8

Enforcement Mechanism Alternatives

- *Execution monitor* (Schneider, 2000)
 - Looks only at history of actions
 - Makes no attempt to “understand” the application and its possible future actions
 - Typically what I think of as a “reference monitor”
- Static application analysis
 - Security-typed languages, dataflow analysis for security
- Modifying the target of the request to prevent policy violation

27 September 2007

Winsborough CS 5323 Lecture 9

9

OS Integrity

- Suppose the RM is placed in the OS
 - Need to have support from architecture, too
- How to prevent the user from:
 - Modifying the OS
 - Gaining direct access to hardware without OS mediation
- Modes of operation
 - Reflects status of code currently executing
 - E.g., user, IO drivers, OS, OS kernel
 - Certain instructions can be performed and memory locations, referenced only in privileged modes
- Controlled invocation
 - System calls can change the status flags
 - Control is transferred to fixed OS entry points
 - Status flags are restored upon return

27 September 2007

Winsborough CS 5323 Lecture 9

10

Low-level Security Features

- As seen in previous slide, low-level features (e.g., modes of operation and controlled invocation) are needed to prevent attacker getting direct access to layers below other enforcement mechanisms
- Low-level features may
 - (Pro) Be easier to analyze, yielding higher assurance
 - (Pro) Reduce performance overheads
 - (Con) Not match the level at which some security policy needs to be stated

27 September 2007

Winsborough CS 5323 Lecture 9

11