Foundations of Computer Security

Lecture 11: Access Control Policies

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Access Control Policies

The Bell and LaPadula Model is an example of an *Access Control Policy*. This is a popular way of conceptualizing and implementing security.

The basic idea is to introduce rules that control what accesses (i.e., *actions*) *subjects* may take with respect to *objects*.

Aside: MAC vs. DAC

Specifically, BLP is a *mandatory* access control system, as distinguished from a discretionary system.

Mandatory Access Controls (MAC): rules are enforced on *every* attempted access, not at the discretion of any system user;

Discretionary Access Controls (DAC): rule enforcement may be waived or modified by some users.

What that means for BLP is that no access is ever allowed unless it satisfies the Simple Security Property and *-Property.

Contrast that with Unix file protection system; Unix implements DAC since file protections can be modified by a file's owner.

Access Control Matrix

In general, any access control policy can be represented by an *access control matrix* (ACM). Given all subjects and objects in the system, the matrix shows explicitly what accesses are allowed for each subject/object pair.

	$\mathbf{object}_1$	...	$\mathbf{object}_k$
$\mathbf{subject}_1$	A_i, A_j		$\emptyset$
...			
$\mathbf{subject}_n$	A_l		A_i, A_m

BLP Access Control Matrix

Suppose we had a BLP system with exactly three subjects and objects with the given labels. Suppose also that $H > L$.

Subjects	**Level**	**Objects**	**Level**
Subj1	$(H, \{A, B, C\})$	Obj1	$(L, \{A, B, C\})$
Subj2	$(L, \{\})$	Obj2	$(L, \{\})$
Subj3	$(L, \{A, B\})$	Obj3	$(L, \{B, C\})$

The following is the associated access control matrix.

	Obj1	**Obj2**	**Obj3**
Subj1	R	R	R
Subj2	W	R, W	W
Subj3	W	R	-

Access Control Matrix

As with any access control policy, you *could* define an ACM for a large Bell and LaPadula system. However, the matrix would be huge for most realistic systems.

The matrix is *implicit* in the rules (Simple Security and the *-Property), so access permissions can be computed on the fly.

Lessons

- BLP is an example of a class of policies called "access control policies."
- BLP is also an example of a *mandatory* policy in that the rules are enforced on every attempted access.
- Any access control policy can be modeled as an explicit matrix.

Next lecture: Lattice-based Security and the BLP Metapolicy