Security Models

Tom Kelliher, CS 325

Oct. 31, 2011

1 Administrivia

Announcements

Status reports due.

Assignment

Read 5.4.

From Last Time

Trust and security policies.

Outline

1. Modeling multiple levels of security.
2. Modeling theoretical limitations of security systems

Coming Up

Trusted operating system design.

2 Modeling Multiple Levels of Security

That is, the military model.

2.1 Lattice

A lattice defines a partial order on a set using a user-defined $\leq$ operator. The operator must satisfy two properties over the set:

1. Transitive: If $a \leq b$ and $b \leq c$ then $a \leq c$.

2. Antisymmetric: If $a \leq b$ and $b \leq a$ then $a = b$.

A *bounded* lattice has a top and bottom:

1. t is the top if $x \leq t$ for all x in S.

2. b is the bottom if $b \leq x$ for all x in S.

Examples:

1. The power set of $\{a, b, c\}$ under the operation "is a subset of."

   Is it bounded?

2. The natural numbers under the mathematical operation $\leq$.

   Is it bounded? Isn't it a total order?

2.2 Bell-La Padula Confidentiality Model

1. Goal is to describe secure information flows and acceptable information flows between subjects and objects.

2. Subjects may have read or write access to objects.

3. $C(O_i)$ denotes the classification of O_i.

   Similarly, $C(S_i)$ denotes the *clearance* of S_i.

Suppose:

- $C(S_1) = 3$.
- $C(S_2) = 1$.
- $C(O_1) = 2$.
- $C(O_2) = 1$.

1. What objects can S_1 be allowed to read? S_2?
2. If S_1 has read access to O_1, can it be granted write access to O_2?

Necessary properties for ensuring confidentiality:

1. Simple security property: S may read O only if $C(O) \leq C(S)$.
2. *-Property: If S has read access to O_1, it may be granted write access to O_2 only if $C(O_1) \leq C(O_2)$.

Information should only flow from less secure objects to more secure objects.

Biba's integrity model is similar — non-trusted information should not influence trusted information.

3 Modeling Theoretical Limitations of Security Systems

1. Is security configuration X attainable?

2. Given security configuration Y, can subject S gain access to object O?

3. Trivial example.

   Suppose S_1 has a transferable read right on O_1.

   Can S_2 gain access to O_1? Will it?

3.1 Graham-Denning Model

Model consists of subjects, objects, an access control matrix (all subjects are also treated as objects, to implement the "control" right), and a set of rights.

Two special rights: own (on objects) and control (on subjects)

Operations:

1. Create object; create subject. Creating subject owns or controls, respectively.

2. Delete object; delete subject. Deleting subject must own or control, respectively.

3. Read access right R of S on O. Subject must control S or own O.

4. Grant right R to S on O. Subject must own O.

5. Delete right R of S on O. Subject must own O *or* control S.

6. Transfer right R to S on O. Subject must have R* (transferable version of R) on O.

Graham-Denning is a general access control model.

Harrison-Ruzzo-Ullman generalizes Graham-Denning to ask if certain situations are obtainable.

Take-Grant Systems are yet another model.