

CSE 509 : COMPUTER SYSTEMS SECURITY

SPRING' 09 : LECTURE NOTES

Date 2/9/2009

Last Class: Studied different access control schemes, Harrison-Ruzzo-Ullman ACM, Belle - La Lapadula

Biba: Integrity Enforcing Model

- Has different levels to check the integrity of data
- Example of a hierarchy: Double Checked → Reliable Witness → Anonymous Tip → Stuff read on the internet
- When data that has been 'Double Checked' is merged with data which had only a 'Reliable Witness', the resultant data will only be at 'Reliable Witness' integrity level.
- Can be thought of as "Compartments".
- Opposite of Belle - La Lapadula. There we went "UP" the hierarchy.
- Good example suggested by a student: Word of God → Pope → Bishop → Followers
- (Lo, Co) and (Ls, Cs) → L = Label, C = Compartment
- To read: $Lo \geq Ls$ and Co is a superset of Cs
- To write: $Lo \leq Ls$ and Cs is a superset of Co

Role Based Access Control: RBAC

- Way to simplify mgmnt of ACM of a large system.
- Example: National Bank → Has branches → Lot of people in the same role in many branches.
- Define a role: Ex. Teller, Branch Manager, CEO...etc.
- Reduces the ACM to one row per role.
- Can have qualified roles. Ex: Branch Manger of Branch X. Not any branch.
- Can have hierarchical roles. Ex: Branch manager can act as a teller.
- Extensions: Static Separation of Roles. Ex: CEO cannot be an auditor.
- Dynamic separation of roles: User can be assigned 2 roles or more, but he has to give up one to shift to the other.

Chinese Wall Model

- Ex: People working at a law firm. Firm has clients. Clients may have conflicting interests. So lawyers of the firm cannot work for both simultaneously.
- Objects partitioned into domains
- Initially user can access any domain. As soon as he enters one, he loses access to all others. A graph of conflicting domains can be maintained.
- Discussed example of 2 applications, one of which has access to the disk and another to the network. (One Laptop Per Child)
- They should be isolated so that disk info isn't relayed on the ntwrk. No shared memory, IPC, pipes...
- Discussed covert channels. Examples: CPU usage, Memory usage, Temperature.

Implementation

- Access control policies are stored on the metadata of files.
- Access Control Lists stored with the objects. Indicates who can access and how.
- Windows uses ACLs on its NTFS.
- Positive rules: Simple to understand.
- Negative rules: Express policy more succinctly.
- Discussion of UNIX file permissions (UID, GID, R-W-X...)