CSCI 240 Systems Security Fundamentals

Spring 2019

Day 7

1. Access Control Related to Access Control Matrix structures
2. Access Control List (Column of ACM) – explain, then show in Kali; and btw, show how to get home directories working
   1. Technical details
      1. Each object has a list: <subject, rights>
      2. That’s a lot of users… so categories instead
      3. Owner, group, the rest of the world (in Unix, user-group-world)
   2. Questions
      1. What does ls -l do?

It will list out files and directories in long list format within a directory.

* + 1. Changing access rights… Suppose we have a file hw1.txt… what does chmod 600 do?

“chmod” can be used with alphanumeric or numeric option.

“chmod 600” : a private file only changeable by the user who entered this command.

1. Privilege List
   1. What it is: basically a row of the access control matrix
      1. Each user has a list of <object, rights>
   2. Questions
      1. What is something a privilege list makes easy?

When there are a few users, it is easy to manage the privileges or access rights by using the matrix.

* + 1. What is something harder to do with a privilege list?

When the users are increasing, it will get harder to manage the privileges and access rights for a given subject.

1. Capability
   1. Technical details
      1. Instead of the system keeping track, the subject (user) does
      2. Unforgeable token for an object indicating rights
      3. Creator can give capabilities – to anything – and specify the operations, down to granularity
      4. Leads to the notion of a domain: collection of objects to which a subject (process) has access
   2. Questions
      1. What are two ways to create “unforgeable” tokens?
         1. Do not give the tickets directly to the user
         2. Unforgeable token cen be encrypted under a key available only to the access control mechanism/ if the encrypted capability contains the identity of its rightful owner, user A cannot copy the capability and give it ro user B.
      2. Can capabilities transfer? (or why not?)

It can transfer or propagate. A subject having this right can pass copies of capabilities to other subjects. The capabilities have a list of permitted types of accesses, one of which might also be transferred. For example, process A can pass a copy of a capability to B, who can then pass a copy to C.

* + 1. What happens upon revocation?

Privilege list is ease of revocation: If a user is removed from the system, the privilege list shows all object to which the user has access so that those right can be removed from the object.

1. Questions

Access control on a single machine can be (somewhat) handled by the directory list, or the variants of access control matrices (including ACLs, Privilege lists), or Capabilities. What happens if assets are across a network?

* 1. How does remote access change how the subject interacts with the access control system?

Remote access is allowed people to access a computer from a remote location. For example, employee can work offsite. A subject requests access to a resource that contains the information

* 1. Does the change introduce vulnerabilities in any of the access control methods?

I guess it does not introduce vulnerabilities, because the access control policies should be capable of dynamically changing to decreases the security risk.

1. Context-based models
   1. Procedure Oriented
      1. Technical points
         1. Procedure attached to each object
         2. Allows finer-grained access, e.g., the object could do its own access control, can make smaller granularity
      2. Questions
      3. Let’s think about implementation. How does procedure-oriented access control relate to object-oriented models of programming – i.e., how might one use classes to implement this type of access control?

The procedure-oriented access control is existence of procedures that access to object. A procedure forms a capsule round the objects, permitting only certain specific accesses.

* + 1. Why is this method of access control less efficient than the access matrix-related techniques?

For the procedure-oriented access control, you have to go through the procedure to execute the file. If there is something wrong in the middle of the procedure, you have to start at the beginning. But for the matrix, you can easily to tell which one you should follow.

* 1. Role-based
     1. Technical points
        1. Access based on job role
        2. System tracks job role
     2. Questions
        1. Provide pros/cons of this method versus the access control lists we typically use.

Pros: easy to manage/ flexible, for example, a user’s access right can be varied via different means.

Cons: the role explosion, due to the increasing roles, we need to increasing roles to properly encapsulate the permissions./ it is not really good at manage individual rights.