Notes Oct 18 2018

Access Control Definitions ½

* NISTIR 7298 defines access control as: “the process of granting or denying specific requests to: (1)

Access Control Definitions 2/2

* RFC 4949 defines access control as “a process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy”

Table 4.1 Access Control Security Requirements (SP 800-171)

* Basic Security Requirements
  + Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
* Derived Security Requirements
  + Control the flow of CUI in accordance with approved authorizations.
  + Separate the duties of individuals to reduce the risk of activity without collision.

Access Control Principles

* In a broad sense, all of computer security is concerned with access control.
* RFC 4949 defines computer security as: “measures that implement and

Figure 4.1 Relationship Among Access Control and Other Security Functions.

* Security Administrator 🡨🡪 Authorization database 🡨🡪 Access control function 🡨 Authentication Function 🡨 User. System Resources

Access Control Policies

* Discretionary access control (DAC)
  + Controls access based on the identity of the requestor and on access rules (authentications) stating what requestors are (or are not) allowed to do
* Mandatory access control (MAC)
  + Controls access based on comparing security levels with security clearances.
* Role-based access control (RBAC)
  + Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.
* Attribute-based access control (ABAC)
  + Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions.

Subjects, Objects, and Access Rights

* Subject
  + An entity capable of accessing object
  + Three classes
    - Owner
    - Group
    - World
* Object
  + A resource to which access is controlled
  + Entity used to contain and / or receive information
* Access right
  + Describes the way in which a subject may access an object
  + Could Include:

Discretionary Access Control (DAC)

* Scheme in which an entity may be granted access rights that permit the entity, by its own violation, to enable another entity to access some resource
* Often provided using an access matrix
  + One dimension consists of identified subjects that may attempt data access to the resources
  + The other dimension lists the objects that may be accessed.
* Each entry in the matrix indicates the access rights of a particular subject for a particular object.

Figure 4.2 Example of Access Control Structures

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | File 1 | File 2 | File 3 | File 4 |
| User |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 4.2 Authorization Table for Files in Figure 4.2

Figure 4.3 Extended

Figure 4.4 An Organization of the Access Control Function

Protection Domains

* Set of objects together with access rights to those objects
* More flexibility when associating capabilities with protection domains
* In terms of the access matrix, a row defines a protection domain
* User can spawn processes with a subset of the access rights of the user
* Association between a process and a domain can be static or dynamic
* In user mode certain areas of memory are protected from use and certain instructions may not be executed
* In kernel mode privileged instructions may be executed and protected areas of memory may be accessed.

UNIX File Access Control

* UNIX files are administered using inodes (index nodes)
  + Control structures with key information needed for a particular file
  + Several file names may be associated with a single inode
  + An active inode is associated with exactly one file
  + File attributes, permissions and control information are sorted in the inode
  + On the disk
* Unique user identification number (user ID)
* Member of a primary group identified by a group ID
* Belongs to a specific group
* 12 protection bits
  + Specify read, write, and execute permission for the owner of the file, members of the group and all other users.
* The owner ID, group ID, and protection bits are part of the file’s inode.

Traditional UNIX File Access Control

Figure 4.6 Users, Roles, and Resources

Figure 4.8 A Family of Role-Based Access Control Models.

Constraints – RBAC

* Provide a means of adapting RBAC to the specifics of administrative and security policies of an organization.
* A defined relationship among roles or a condition related to roles.
* Types
  + Mutually exclusive toles
    - A user can only be assigned to one role in the set (either during a session or statically)
    - Any permission (access right) can be granted to only one role in the set.

Attribute0Based Access Control (ABAC)

* Can define authorizations that express conditions on properties of both the resource and the subject.
* Strength is its flexibility and expressive power
* Main obstacle is its adoption in real systems has been concern about the performance impact of evaluating predicates on both resource and user properties for each access.
* Web services have been pioneering technologies through the introduction of the eXtensible Access Control Markup Language (XAMCL)
* There is considerable interest in applying the model to cloud services.

ABAC Model: Attributes

* Subject attributes
  + A subject is an active entity that causes information to flow among objects or changes the system state.
  + Attributes define the identity and characteristics of the subject.
* Object Attributes
  + An object (for resource) is a passive information system-related entity containing or receiving information.
  + Objects have attributes that can be leverages to make access control decisions.
* Environment Attributes
  + Describe the operational technical, and even situational environment or context in which the information access occurs
  + These attributes have so far been largely ignored in most access control policies.

ABAC

* Distinguishable because it controls access to objects by evaluating rules against the attributes of entities, operations, and the environment relevant to a request.
* Relies upon the evaluation of attributes of the subject, attributes of the object, and a formal relationship or access control rule defining the allowable operations for subject-object attribute combinations in a given environment.

Figure 4.10 ABAC Scenario

* Subject Attributes
  + Name, Clearance, Affiliation, Etc.
* Object Attributes
  + Type, Owner, Classification, Etc.
* Environmental Attributes

Figure 4.11 ACL and ABAC trust Relationships

ABAC Policies

* A policy is a set of rules and relationships that govern allowable behavior within an organization, based on the privileges of subjects and how resources or objects are to be protected under which environment conditions.
  + Typically written from the perspective of the object

Identity, Credential, and Access Management (ICAM)

* A comprehensive approach to managing and implementing digital identities, credentials, and access control.
* Developed by the U.S. government.
* Designed to:
  + Create trusted digital identity representations of individuals and nonperson entities (NPEs)

Figues 4.12 Identity, Credential, and Access Management (ICAM)

Identity Management

* Concerned with assigning attributes to a digital identity and connecting that digital identity to an individual or NPE
* Goal is to establish a trustworthy digital identity that is independent of a specific application or context.
* Most common approach to access control for applications and programs is toe create a digital representation of an identity for the specific use of the application or program.
* Maintenance and protection of the identity itself is treated as secondary to the mission associated with the application.

Credential Management

* The management of the life cycle of the credential
  + Examples of credentials are smart cards, private/public cryptographic keys, and digital certificates.
* Encompasses five logical components
  + An authorized individual sponsors an individual or entity for a credential to establish the need for the credential.
* The sponsored

Access Management

* Deals with the management

Three support elements

Identity Federation

* Terms used to describe the technology

Access Control

* DAC: Discretionary Access Control
  + Definition: An individual user can set an access control mechanism to allow or deny access to an object.

Limitation of DAC:

* Global policy: DAC let users to decide the access control policies on their data, regardless of whether those policies are consistent with the global policies. Therefore, if there is a global policy, DAC has trouble to ensure consistency.
* Information flow: information can be copied from one object to another, so access to a copy is possible even if the owner of the original does not provide access to the original copy. This has been a major concern for military.
* Malicious software: DAC policies can be easily changed by owner,

MAC: Mandatory Access Control

* Definition: A system-wide policy decrees who is allowed to have access; individual user cannot alter that access.
* Relies on the system to control access.

Security Policy Model

* A Security Policy model is a concise

Multilevel Security

* People and information are classified into different levels of trust and sensitivity

Clearance level

* Indicates the level of trust given to a person with a security clearance

Classification level

* Indicates the level

Security Level

Bell-LaPadula Security Policy Model

* Proposed by David Bell and Len Lapadula in 1973, in response to U.S. Air Force concerns over the security of time-sharing mainframe systems.
* This model is the most widely recognized MLS model.
* The model deal with confidentiality only.
* Two properties: No read up and No write down.
* Simple security

The Biba Model

* Due to Ken Biba
* Deal with integrity alone and ignores confidentiality entirely.
* Biba Model covers integrity levels
* Simple Integrity Property: A low integrity subject will not write or modify high integrity data
* Property: The high integrity subject will not read low integrity data.
* Read-Up, Write Down – Subject cannot read objects of lesser integrity, subjects cannot write to objects of higher integrity.

Multilateral Security

* Instead of the information flow-control boundaries being horizontal, as in the MLS model, we instead need the boundaries to be the mostly vertical.
* Also known as compartmentation
* Multilateral security models:
  + The Chinese Wall Model
  + The BMA Model (British Medical Association)

The Chinese Wall Model

* Proposed by Brewer and Nash to model access
* Analysts have to adhere to the following security policy:
* Rule: There must be no information flow that causes a conflict of interest
* Conflict of Interest (Col) classes: indicate which companies are in competition.
* Read Rule: A subject S can read an object O if:
  + O is in the same Dataset as an object already accessed by S, or
  + O belongs to a Col class from which S has not yet