

Access Control -- Controls

❖ *DigitalSherlock.com | SafeHack.com*

❖ *Date: 2005/05/27*

❖ *Document Name: access_control_controls.pdf*

❖ *GNU Free Documentation License*

❖ *Version 1.00, 2005-05-27*

❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*

❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

❖ Control type

➤ What are Access Control

- **Access controls are security features that control how users and systems communicate and interact with other system and resources.**
- **Access is the flow of information between a subject and an object**
- **A subject is an active entity that requests access to an object or the data within an object**
- **A subject can be a user, a program, or process that access information**
- **An object is a passive entity that contains information**
- **An object can be a computer, database file, program, or field in a table**
- **When you lookup information in a database, you are the subject and the database is the object**

➤ Access control give the ability to:

- **Integrity**
 - Prevention of the modification of information by unauthroized users
 - Prevention of unauthorized or unintentional modification of information by authorized users
 - Preservation of internal and external consistency
 - ◆ Internal consistency ensures that internal data is consistent
 - ◆ External consistency ensures that the data stored in the database is consistent with the real world
 - Information must be accurate, complete and protected from unauthorized modification
- **Confidentiality**
 - Assures that the information is not disclosed to unauthorized persons or processes
 - Control mechanisms need to be in place to dictate who can access data and what the person can do with the accessed data
 - The first step in protecting data's confidentiality is identifying which information is sensitive
- **Availability**
 - Assures that authorized users have timely uninterrupted access to the information in the system
 - Information systems and resources need to be available to users in a timely manner so productivity will not be affected
 - Fault tolerance and recovery mechanisms are out into place to ensure the continuity of the availability of resources

➤ § Deterrent/Preventative

- **Use to discourage occurrences**

➤ § Detective

- **Detective Technical Controls warn of technical Access Control violations**
- **Used to detect or identify occurrence)**

- **§ Corrective**
 - Are used to restore systems that are victims of harmful attacks
- **§ Recovery**
 - Used to restore resources, capabilities, or losses
- **Which control is what ?**
 - **Control by action include:**
 - Preventive
 - Detective
 - Corrective
 - **Control by function include:**
 - Management controls
 - Technical controls
 - Operational controls

❖ Access Control Methods

- **Administrative**
 - **Preventive**
 - Security Policies and procedures
 - Personal Controls
 - Increased supervision
 - Security awareness and training
 - Testing
 - Separation of duties
 - Hiring procedures
 - Background Investigation
 - Termination of employee policy
 - Work habit checks
 - Disaster recovery and contingency plan
 - User Registration for computer access
 - **Detective**
 - Warn of technical Access Control violations
 - Security reviews and audits
 - Performance Evaluation
 - Required vacations
 - Rotation of duties
- **Physical**
 - **Preventive**
 - Network Segregation
 - Perimeter Security
 - ◆ Fences
 - ◆ Restrict physical access
 - ◆ Security guards
 - ◆ Man trap
 - ◆ Gates
 - ◆ Biometric access controls
 - ◆ Locks and keys
 - ◆ Badge systems
 - ◆ Securing a server room or laptops
 - ◆ Site selection

- Computer Controls
- Backup files and documentation
- Backup Power
- Fire extinguishers
- Cabling, the protection of cables
- Separation of duties
- Work Area Separation
- Motion detectors
- Smoke and fire detectors
- Closed circuit TV monitoring
- Sensors and alarms
- **Detective**
 - Motion detectors
 - Smoke and fire detectors
 - Closed circuit TV monitoring
 - Sensors and alarms
- **Logical or Technical**
 - **Role ?**
 - Restricted access
 - Technical ways of restricting who or what can access system resources
 - It is usually built into an operating system, or it can be a part of an application or program, or an add-on security package
 - Protect confidential information from being disclosed
 - **Preventive**
 - Access control Software (System access)
 - Network Architecture
 - Network Access, Dial up access, callback systems
 - Encryption
 - Antivirus software
 - Library control systems
 - Passwords
 - Smart cards
 - **Detective**
 - Auditing
 - Intrusion detection expert systems
 - IDS, logging, monitoring, clipping levels
- **Combination**
 - **Preventive/Administrative**
 - **Preventive/Technical**
 - **Preventive/Physical**
 - **Detective/Administrative**
 - **Detective/Technical**
 - **Detective/Physical**
- **Things to consider when planning access control**
 - **Threat**
 - An event or activity that has the potential to cause harm to the information systems or networks
 - Is the means through which a threat agent affect a computer system

- **Vulnerability**
 - A weakness or lack of safeguard which may be exploited by threat causing harm to the information systems or networks
 - A flaw or weakness that may allow harm to occur to an information systems
- **Risk**
 - The potential for harm or loss to an information systems or networks
 - The probability that a threat will materialize
 - Is a combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact
- **Exposure**
 - Is a specific instance of the condition of being exposed to losses resulting from the occurrence of one or more threat
- **Accountability**
 - The means of linking individuals to their interactions with an IT product
 - Auditing ensure that users are accountable for their actions
 - Whenever a discretionary security policy is invoked accountability must be assured
 - Work as deterrent to improper actions, and used for investigation
 - Derived requirements are
 - ◆ Identification
 - ◆ Authentication
 - ◆ Audit
- **Assurance**
 - Systems must guarantee correct and accurate interpretation of the security policy
 - Derived requirements are
 - ◆ System architecture
 - ◆ System integrity
 - ◆ Security testing
 - ◆ Configuration
 - ◆ Management
 - ◆ Design documentation & user guide

❖ **Controlling access (Security Policy)**

➤ **Intro**

- **Security policy must reflect the laws, regulations**
- **Security policy is a statement of intent**
- **Derived requirement**
 - System security Policy

➤ **Mandatory (MAC)**

- **Cannot be made restrictive by the subject**
- **Dependent on Labels and data classification**
- **Military Labels**
 - Unclassified
 - Confidential
 - Secret
 - Top secret
- **Policy used for system that process Classified information**
- **Rule based access is a type of mandatory access control**
- **Defines an imposed access control level**
- **Subjects access to an object**

- **Must have Need to know**
- **Subjects Clearance must match Classification of Object**
- **Mandatory controls are prohibitive**
- **Derived requirement is classification labels**
- **Mandatory Access Control models (MAC) are based on lattice rule**
- **The system makes the access decisions by comparing security labels**
- **Discretionary (DAC)**
 - **Access controls that are not policy based**
 - **Policy used for system that process Classified information**
 - **Subject has authority, within certain limitations**
 - **Access is controled often using use of ACL's**
 - **Administrators can limit access to certain times of day or days of the week**
 - **Uses Access Control Lists on files. If a user create a file he own it.**
 - **Derived object reuse**
 - **The owner determines who has access and what privilege they have**
 - **Discretionary access controls have levels of granularity.**
 - **This system assigns subjects (users) to one or more groups.**
- **Non-Discretionary (Role Based) RBAC**
 - **Is a centrally administered set of controls to met security policies**
 - **The administrative task is to grant and revoke user membership**
 - **A central authority determines what subjects can have access to certain objects**
 - **The determination is based on the organizational security policy**
 - **Often useful in organizations where there are frequent personnel changes**
 - **These controls may be based on**
 - **Role-Based**
 - ◆ **Role based access control (RBAC)**
 - ◆ **Based on the roles that individual users have as part of an organization**
 - ◆ **Access rights are grouped by role name**
 - ◆ **Reducing the complexity and cost of security administration in large networks**
 - ◆ **Role based access control (RBAC) is an alternative to traditional discretionary (DAC) and mandatory access control (MAC) policies**
 - ◆ **Access is determined by the role the user has within the company**
 - **Rule-Based**
 - ◆ **A security policy based on global rules imposed for all users.**
 - ◆ **A good example could be a firewall**
 - ◆ **Rule based access control is based on a specific profile for each user**
 - ◆ **Access is determined by the task assigned to this user**
 - ◆ **Policy Based Access Control is also known as Rule Set Based Access Control (RSBAC).**
 - **Lattice is non-discretionary control**
 - ◆ **Was developed to deal mainly with information flow in computer systems.**
 - ◆ **The basic work in this area was done around 1970**
 - ◆ **Information flow in computer systems is concerned with flow from one security class (also called security label)**
 - ◆ **A lattice is a mathematical object that characterises a relationships between things**
 - ◆ **A set and a relationship(\leq) between members**
 - ◆ **There are pairs of elements**
 - **Subject**
 - **Object**
 - ◆ **There are pairs of elements that have**

- LEAST upper bound of values
 - Greatest lower bound of values
 - ◆ Access is determined by the sensitivity level assigned to the role
- **Lattice based**
 - Provides least access privileges of the access pair
 - Greatest lower bound
 - Lowest upper bound
- **Access Control Lists [ACL]**
 - **List of subjects authorized access to some objects**
 - **Refer to**
 - Users
 - ◆ Permitted (or Denied) users
 - Groups
 - ◆ Permitted (or Denied) groups
 - Computers
 - ◆ Permitted (or Denied) network addresses
 - Processes
 - ◆ Permitted (or Denied) one or more processes
 - **2 types of ACL**
 - Elementary
 - ◆ Permission bits R W E D
 - Advanced
 - ◆ Permission bits R W E D + User Name for more information
- **Other Access Control**
 - **LOMAC**
 - LOMAC is a security enhancement for Linux
 - Uses Low Water-Mark Mandatory Access Control to protect the integrity of processes and data
 - LOMAC is implemented as a loadable kernel module
 - No kernel recompilations or changes to existing applications are required
 - **FLASK**
 - Is an operating system security architecture
 - Provides flexible support for security policies
- **Constrained User Interface**
 - **Menus & Shells**
 - **Databases views**
 - **Physically constrained user interface**
 - Provide limited number of buttons
 - Example: Automated teller machine
 - No alphabetic keyboard usually

❖ Access Control Administration

- **Implementing I & A Systems**
 - **Account Administration**
 - Accounts should be monitored regularly
 - It is good to have procedures in place to verify password strength
 - Should address lost or stolen passwords or tokens
 - **Maintain Authentication**

- Single log-in
- Host-to-host Authentication
- Authentications Servers
- User-to-host Authentication

➤ **Centralized/Remote Authentication Access Controls**

- **Intro**
 - One office or one individual configure the access controls
 - Allow very strick control over information
 - When we need fast change, central administration can be frustrating
- **RADIUS**
 - Remote Access Dial-In User Service
 - It provides a centralized server for single point of authentication
 - A protocol for carrying authentication, authorization, and configuration information
 - Uses the Client/Server model
 - Transactions between client and server are authenticated using a shared secret
 - Is a handshaking protocol
- **TACACS**
 - Terminal Access Controller Access Control System
 - A client/server protocol for handling
 - ◆ Authentication
 - ◆ Authorization
 - ◆ Accounting Messages
 - TACACS Combien its authentication and authorization processes
- **XTACACS**
 - XTACACS separates authentication and authorization and accounting processes
- **TACACS+**
 - It provides attribute control (authorization) and accounting
 - Authorization can be done on a per-user/per-group basis, and is dynamic.
 - TACACS+ is XTACACS with two authentication factor

➤ **Decentralized Access Control**

- **Intro**
 - Access is controlled by the owners or creators of the files
 - It may lead to lack of consistency among owners/creators as to procedures
- **Domains**
 - A single domain of trust that shares a single security policy and a single management source
 - Usually, domains are defined as a sphere of influence.
 - The wider the domain, the more difficult it is to maintain its integrity
- **Trust**
 - Trusted Subject is a subject that is part of the TCB
 - It has the ability to violate the security policy, but is trusted not to actually do so
 - BellLaPadulla model a trusted subject
- **Relational Database**
 - Definition
 - ◆ Relation (table) is the basis of a relational database
 - ◆ Relation is represented by a table
 - ◆ Rows = Records (tuples)
 - ◆ Column = Attributes

- ♦ The number of rows in the relation is Cardinality
 - ♦ The number of columns in the relation is the Degree
 - ♦ Cardinality - # of rows in a relationship (table)
 - ♦ Degree - # of columns in a relationship (table)
 - ♦ Foreign Key - any value that matches the primary key of another relation (table)
 - ♦ Relational Database - best suited for text
- Primary Key
 - ♦ Points to a record (tuple)
 - ♦ In each table a primary Key is required
- Relational Database Operators
- **Relational Database Security**
 - Definition
 - ♦ A database can be defined as a persistent collection of interrelated data items
 - ♦ Relational Databases support queries
 - ♦ Object oriented databases do not support queries
 - Schema
 - ♦ The Description of the database is called Schema
 - ♦ Schema is Defined by Data Description Layer (DDL)
 - Has 3 parts
 - ♦ Data structures called tables (relations)
 - ♦ Integrity Rules on allowable values
 - ♦ Operators on the data in tables
 - Database Management System (DBMS)
 - ♦ A software that Provides access to the database
 - ♦ Allows restriction of access
 - Relational Database Operators
 - ♦ Select - based on criteria i.e. all items with value > \$300.00
 - ♦ Join - join tables based on a common value
 - ♦ Union - forms a new relation (table) from two other relations
 - ♦ View - (virtual table) uses join, project, select
 - ♦ Views can be used to restrict access (least privileges)
 - ♦ Query plan
 - Comprised of implementation procedures, lowest cost plan based on "cost"
 - Costs are CPU time, Disk Access
 - Bind - used to create plan
 - Data Normalization
 - ♦ Ensures that attributes in a table rely only on the primary key
 - ♦ Eliminates repeating groups
 - ♦ Eliminates redundant data
 - ♦ Eliminates attributes not dependent on the primary key
 - SQL - Structured Query Language
 - ♦ Select
 - ♦ Update
 - ♦ Delete
 - ♦ Insert
 - ♦ Grant - Access Privileges
 - ♦ Revoke - Access Privileges
- **Object Oriented Databases - OODB**
 - Best suited for multi-media, graphics
 - Steep learning curve
 - High overhead

➤ Ø Access Rights and Permissions

- **What is Identification ?**
 - Is the means by which a user provides a claimed identity to the system
 - The act of a user professing an identity to a system
 - Identification is a means to verify who you are
 - User identification enables accountability
 - Identification usually takes the form of Logon ID or User ID
 - Logon ID characteristics
 - ♦ They must be unique
 - ♦ Not shared
 - ♦ Non descriptive of job function
- **What is Authentication ?**
 - Verification that the users claimed identity is valid
 - Authentication is what you are authorized to perform, access, or do
 - The entity could be individual user, machine, or software component
 - 3 means of authenticating a user's
 - ♦ Something a user knows (TYPE I)
 - User ID
 - Passwords
 - PINs
 - Cryptographic keys
 - ♦ Something a user has (TYPE II)
 - Memory tokens
 - Smart tokens
 - ♦ Something a user is (TYPE III)
 - Biometric
 - Fingerprint
- **Authorization**
 - Determines whether a particular is trusted for that operation
 - The system check if the subject has been given the necessary rights and privileges to carry out the requested actions
- **Access Criteria**
 - Identity (Individual of program)
 - Roles (Individual or group)
 - Location (physical or logical)
 - Time (time of day / week)
 - Transaction (based on sensitivity)
 - Service constraints (based on parameters)
 - Common access modes
 - ♦ Read
 - ♦ Write
 - ♦ Execute
 - ♦ Delete
 - ♦ Create
 - ♦ Search
- **File and data owner ship**
 - Data Owners
 - ♦ The owner must determine the appropriate classification and access controls
 - ♦ All information generated, or used must have a designated owner
 - ♦ Executive or manger of an organization

- ◆ Has the final corporate responsibility of data protection
 - ◆ Responsibilities include
 - Responsible for determining the sensitivity and criticality of the information.
 - Periodically reviews that classification to ensure that it still meets the business needs.
 - Ensures that security controls are in place commensurate with the classification.
 - Delegating the responsibility of the data protection to custodian
 - Custodians
 - ◆ Charged by the owners for the everyday care
 - ◆ This role is commonly executed by IT system personnel
 - ◆ Responsibilities include
 - Running regular backups and testing the validity of the backup
 - Performing data restoration from the backups when necessary
 - Maintain Records In Accordance with (IAW) the established policy
 - Users
 - ◆ Users are the subject that require their data to perform their jobs
 - ◆ Any employees
 - ◆ Contractors
 - ◆ External party
 - ◆ Responsibilities include
 - Users must follow the operating procedures defined by organization
 - Users must take "DUE CARE" to preserve the information's security during their work
 - They must prevent OPEN VIEW
 - They must use company computing resources only for company purposes.
- **Principle of Least Privilege**
 - Requires that a user be given no more privilege than necessary to perform a job
- **Segregation of Duties and Responsibilities**
 - Ensure that no single employee has control of a transaction from beginning to end
 - Two or more people should be responsible for the task
 - Can either be static or dynamic
 - Administrative
- **Rotation of Duties**
 - Job assignments should be changed periodically
 - This principle is effective when used in conjunction with a separation of duties
 - Rotation of duties will protect you against fraud
- **Accountability / Audit trails**
 - **Audit trail**
 - Audit trail support accountability
 - Audit trail record both system activities and user activities
 - Audit trail can assist in detecting security violations
 - Audit trail can assist in detecting performance problems
 - Audit trail can assist in detecting flaws in applications
 - Audit trail is a technical control
 - **Accountability**
 - Accountability allows system activities to be traced to the responsible
 - It means holding individual users responsible for their actions
 - It is a detection & deterrent mechanism
 - Can be accomplished through
 - ◆ Policy
 - ◆ Authorization scheme
 - ◆ Identification & authentication

- ♦ Access controls
 - ♦ Audit trails / Auditing
- **Use of audit trails & logs**
 - Logging should be done 24/7 on all necessary systems
 - Typically there are 2 kinds of audit trails
 - ♦ Record every keystroke
 - ♦ Event oriented
 - Event record should contain
 - ♦ When the event occurred date time
 - ♦ The user ID, associated with the event
 - ♦ The command used, and the results
 - System level audit trails
 - ♦ Should contain
 - Any attempt to log on
 - The log-on ID
 - Date & time
 - The device used
 - The function(s) performed once logged on
 - ♦ Should be able to identify failed log-on attempts (detect intrusion)
 - Application level audit trails
 - ♦ Monitor and log user activities
 - ♦ Including data files opened closed, reading editing deleting record
 - User audit trails Usually log
 - ♦ All commands directly initiated by the user
 - ♦ All identification and authentication
 - ♦ Files & resources accessed
 - Make sure
 - ♦ Logs are stored on a protected machine
 - ♦ Logs are encrypted when traveling on the network if possible
 - ♦ All computers have their clocks synchronized
 - ♦ Logs should not be modified without record of the modification
 - ♦ Should be kept on archive for a period of time determined by company policy