Cybersecurity Fundamentals

Module 3 : Access Control Concepts

WHAT IS SECURITY CONTROL?

A control is a safeguard or countermeasure designed to preserve Confidentiality, Integrity and Availability of data

Access control involves limiting what objects can be available to what subjects according to what rules

One brief example of a control is a firewall

CONTROL OVERVIEW

Access is based on three elements:

- Subject : any entity that requests access to our assets
- Object : An object is a device, process, person, user, program, server, client or other entity that responds to a request for service
- Rules : instruction developed to allow or deny access to an object by comparing the validated identity of the subject to an access control list

SUBJECT

- Is a user, a process, a procedure, a client (or a server), a program, a device such as an endpoint, workstation, smartphone or removable storage device with onboard firmware.
- Is active: It initiates a request for access to resources or services.
- Requests a service from an object.
- Should have a level of clearance (permissions) that relates to its ability to successfully access services or resources.

OBJECT

- Is a building, a computer, a file, a database, a printer or scanner, a server, a communications resource, a block of memory, an input/output port, a person, a software task, thread or process.
- Is anything that provides service to a user.
- Is passive.
- Responds to a request.
- May have a classification.

RULES

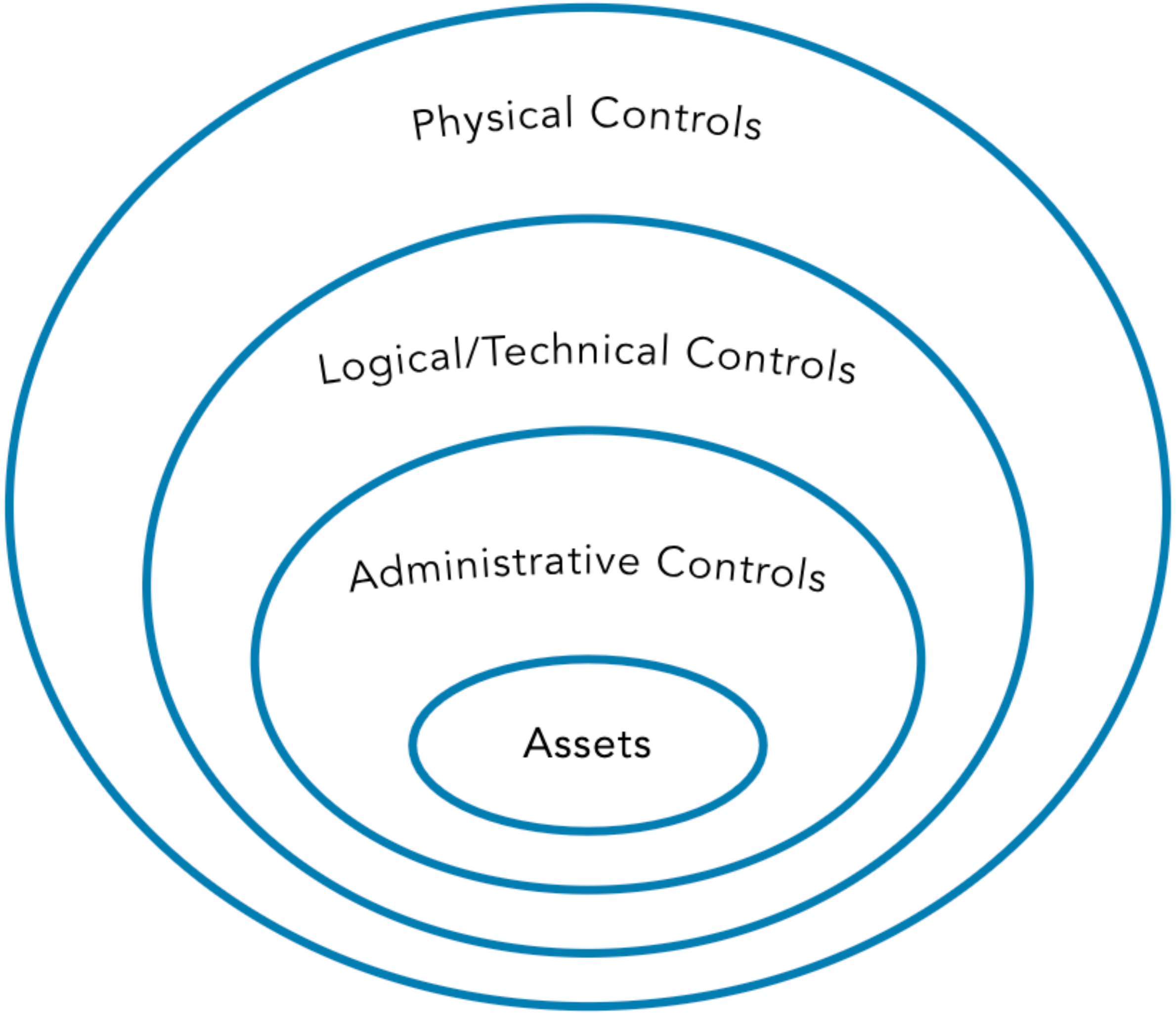
- Example of a rule is a firewall access control list
- Compare multiple attributes to determine appropriate access.
- Allow access to an object.
- Define how much access is allowed.
- Deny access to an object.
- Apply time-based access.

CONTROL ASSESSMENT

- Risk reduction depends on the effectiveness of the control. It must apply to the current situation and adapt to a changing environment.

DEFENSE IN DEPTH

- Layered defense strategy



PRINCIPLE OF LEAST PRIVILEGE

- a standard of permitting only minimum access necessary for users or programs to fulfill their function

PRIVILEGE ACCESS MANAGEMENT

- ABC, Inc., has a small IT department that is responsible for user provisioning and administering systems. To save time, the IT department employees added their IDs to the Domain Admins group, effectively giving them access to everything within the Windows server and workstation environment. While reviewing an invoice that was received via email, they opened an email that had a malicious attachment that initiated a ransomware attack. Since they are using Domain Admin privileges, the ransomware was able to encrypt all the files on all servers and workstations. A privileged access management solution could limit the damage done by this ransomware if the administrator privileges are only used when performing a function requiring that level of access. Routine operations, such as daily email tasks, are done without a higher level of access.

PRIVILEGED ACCOUNTS

Privileged accounts are those with permissions beyond those of normal users, such as managers and administrators.

Systems administrators, who have the principal responsibilities for operating systems, applications deployment and performance management.

Help desk or IT support staff, who often need to view or manipulate endpoints, servers and applications platforms by using privileged or restricted operations.

Security analysts, who may require rapid access to the entire IT infrastructure, systems, endpoints and data environment of the organization.

SEGREGATIO N OF DUTIES

- Core element of authorization
- No one person should control an entire high-risk transaction from start to finish
- Breaks the transaction into separate parts and requires a different person to execute each part of the transaction
- Two-person rule is a security strategy that requires a minimum of two people to be in an area together
- Reduce insider threats to critical area

Authorized vs Unauthorized Personnel

What are Physical Security Control

- Physical mechanisms deployed to prevent, monitor, or detect direct contact with systems or areas within a facility
- Examples of physical access controls include security guards, fences, motion detectors, locked doors/gates, sealed windows, lights, cable protection, laptop locks, badges, swipe cards, guard dogs, cameras, mantraps/turnstiles, and alarms.

Why Have Physical Security Controls?

- Prevent unauthorized individuals from entering a physical site
- Protect physical assets such as computers
- Protect the health and safety of the personnel inside

Types of Physical Access Control

BADGE SYSTEM AND GATE ENTRY

ENVIRONMENTAL DESIGN

BIOMETRICS

Monitoring

- Cameras
- Alarm Systems
- Logs
- Security Guards

What are Logical Access Controls ?

Electronic methods that limit someone from getting access to systems, and sometimes even to tangible assets or areas

Types of logical access controls include:

Passwords

Biometrics (implemented on a system, such as a smartphone or laptop)

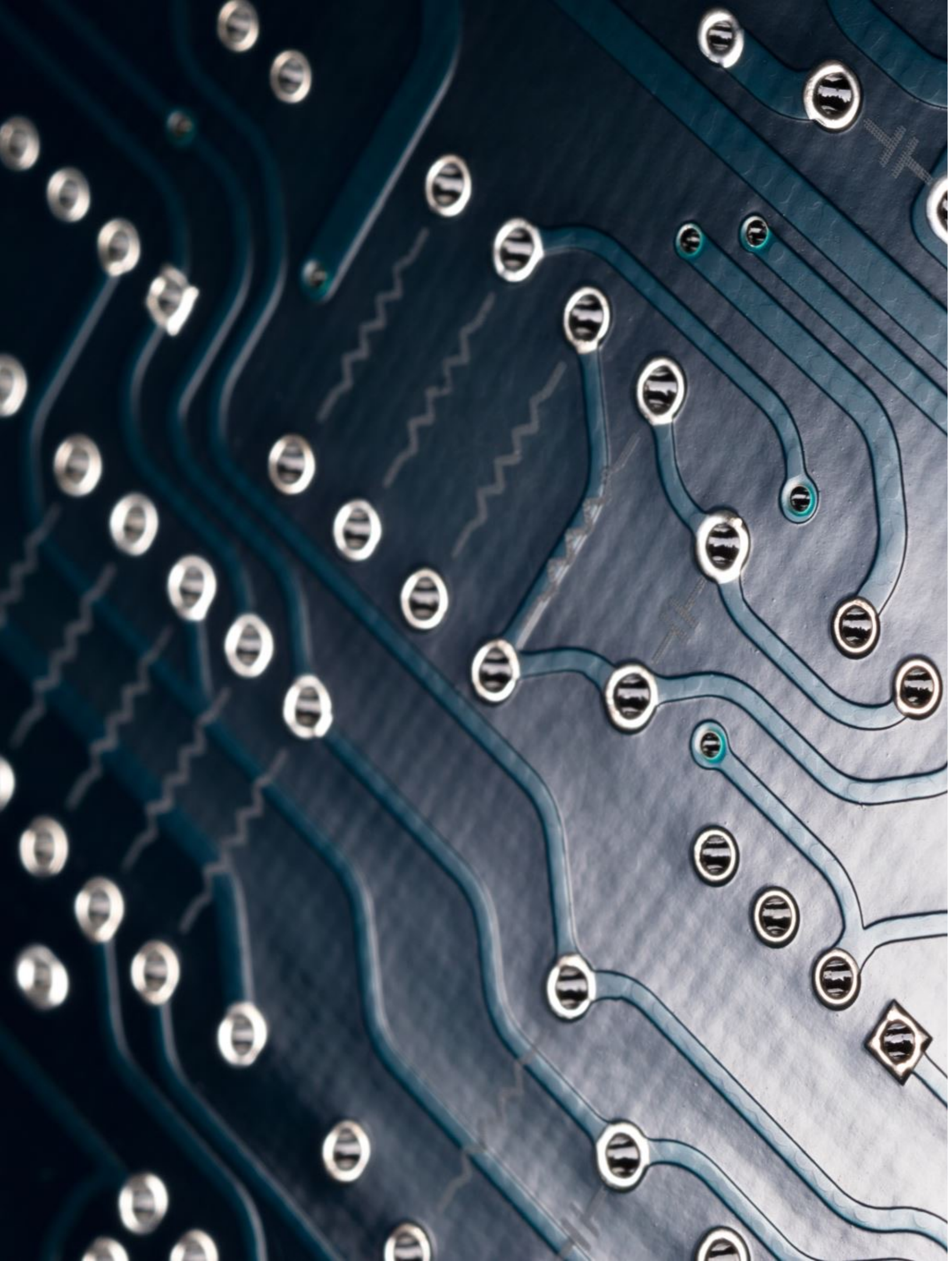
Badge/token readers connected to a system

Discretionary Access Control

Specifies that a subject who has been granted access to information can do one or more of the following:

- Pass the information to other subjects or objects
- Grant its privileges to other subjects
- Change security attributes on subjects, objects, information systems or system components
- Choose the security attributes to be associated with newly created or revised objects; and/or
- Change the rules governing access control; mandatory access controls restrict this capability

Rule-based access control systems are usually a form of DAC.



Mandatory Access Control

- A mandatory access control (MAC) policy is one that is uniformly enforced across all subjects and objects within the boundary of an information system
- Subject is constrained from doing any of the following:
  - Passing the information to unauthorized subjects or objects
  - Granting its privileges to other subjects
  - Changing one or more security attributes on subjects, objects, the information system or system components
  - Choosing the security attributes to be associated with newly created or modified objects
  - Changing the rules governing access control
- MAC vs DAC, System Administrator vs Object's Owner

Role-Based Access Controls

- Role-based access control (RBAC) sets up user permissions based on roles.
- Each role represents users with similar or identical permissions.
- A role is created and assigned the access required for personnel working in that role. When a user takes on a job, the administrator assigns them to the appropriate role. If a user leaves that role, the administrator removes that user and then access for that user associated with that role is removed.
- RBAC works well in an environment with high staff turnover and multiple personnel with similar access requirements.