CYBERSECURITY FIRST PRINCIPLES

OVERVIEW

- Abstraction
- Domain Separation
- Information Hiding
- Layering
- Least Privilege
- Minimization
- Modularization
- Process Isolation
- Resource Isolation

Poll

Which First Principles does the graphic represent?

- Simplicity
- Abstraction
- Least Privilege
- Modularity

ABSTRACTION

- A representation of an object or concept
- Speedometer
- Map

Poll

Your school maintains records on each student and their academic performance. The records with this type of information is placed on another more secure network segment. Which First Principle would BEST apply?

- Domain Separation
- Abstraction
- Information Hiding
- Simplicity

DOMAIN SEPARATION

- Managing resources by keeping them separate
- Personal banking
- Business banking
- Wealth management

Poll

When you take selfies with your smart phone, it may contain something called a geotag. A geotag reveals your exact location on a map. Removing this tag from a picture before posting it on social media is a practice that belongs to which principle?

- Information Hiding
- Least Privilege
- Modularity
- Simplicity

INFORMATION HIDING

- Preventing information from being see by people
- Encryption
- Processes of how information is delivered

Poll

You started a new job at a local store. When you log into the system the store provides for you to do you job. Each application you open you must re enter your username and password. Which principle BEST does this address?

- Abstraction
- Layering
- Domain Separation
- Information Hiding

LAYERING

- Uses the concept of defense-in-depth or layered security to provide better protection
- Combined, these are layering (defense-in-depth)
  - A credential to enter the building
  - A code to enter a room
  - A username and password to log on
  - A separate username and password to access an application

Poll

While at work, you only have access to applications and data you need to complete your job. Which principle addresses this concept?

- Abstraction
- Least Privilege
- Information Hiding
- Domain Separation

LEAST PRIVILEGE

- Limiting access to only those who need the information to do their job
- Need-to-know
- Using rights and permissions on systems to restrict who can access and use information

Poll

While at work, you are completing a project from a remote location. You are not allowed to save the file to the computer you are on, but only to the remote computer you have accessed. Which principle applies?

- Least Privilege
- Minimization
- Process Isolation
- Abstraction

MINIMIZATION

- Keeping the processes simple to minimize the ways something can be compromised
  - Turning off unneeded features
  - Close Ports

Poll

The ability to connect different devices such as keyboards, monitors, USB devices and network cables to the Raspberry Pi is an example of which principle?

- Least Privilege
- Abstraction
- Modularity
- Domain Separation

MODULARIZATION

- Using modules to create a larger project.
- Can be added or removed
- Has separate functions

Poll

Ensuring only authorized users, processes and devices can access information or data. Which principle applies?

- Least Privilege
- Domain Separation
- Layering
- Process Isolation

PROCESS ISOLATION

- Isolating a process so in the event of failure, it doesn't impact other processes
- One program interfering from other programs

Poll

Information is stored when it is at rest. Usually on a device such as a hard drive, memory, CD/DVD or thumbdrive. Which principle applies?

- Domain Separation
- Resource Encapsulation
- Least Privilege
- Abstraction

RESOURCE ENCAPSULATION

- Separating resources and used in the way they were intended
- Disks
- Memory
- Linked Lists

Poll

Jain's company works with sensitive data. In order to assure the secrecy of that data **hey have a rule to use only their private servers to compute/modify that data. Whic principle would apply?**

- Abstraction
- Domain Separation
- Least Privilege
- Simplicity

SIMPLICITY OF DESIGN

- Keeping designs simple.
- The more complex processes are the more likelihood of a compromise
- Easier to troubleshoot and fix