Definition

Examples

Advantages

Disadvantages

When to use

**Commonly Used Security Methods**

To address the key requirements of the AIC triad, one can employ a number of commonly used security methods:

* Least privilege
* Defense-in-depth
* Minimization
* Keep things simple
* Compartmentalization
* Use choke points
* Fail securely/safely
* Leverage unpredictability
* Separation of duties

**Least Privilege**

**(Definition) States that:** do not provide more privileges than are required. This applies to both users and applications.

* Example: No administrative rights to guests accounts, unidentified applications should not be able to have the power to change the system file etc.)
* This principle applies not only to privileges of users and applications on a computer system, but also to other noninformation systems privileges of an organization’s staff.
* The principle of least privilege is a preventive control, because it reduces the number of privileges that may be potentially abused and therefore limits the potential damage.
* Some examples of application of this principle include the following:
* Giving users only read access to shared files if that’s what they need, and making sure write access is disabled
* Not allowing help desk staff to create or delete user accounts if all that they may have to do is to reset a password
* Not allowing software developers to move software from development servers to production servers
* Privilege : The ability to access data to run processes and applications
* Product: keep system more stable by giving less privilege to untrustworthy users

**Advantages:**

* Minimizes the attack surface, diminishing avenues a malicious actor can use to access sensitive data or carry out an attack by protecting superuser and administrator privileges.
* Reduces malware propagation by not allowing users to install unauthorized applications. The principle of least privilege also stops lateral network movement that can launch an attack against other connected devices by limiting malware to the entry point.
* Improves operational performance with reductions in system downtime that might otherwise occur as a result of a breach, malware spread or incompatibility issues between applications.
* Safeguards against human error that can happen through mistake, malice or negligence.

**Disadvantages:**

When to use: (Why is it important)

* The principle of least privilege is an important information security construct for organizations operating in today’s hybrid workplace to help protect them from cyberattacks and the financial, data and reputational losses that follow when ransomware, malware and other malicious threats impact their operations.
* The principle of least privilege strikes a balance between usability and security to safeguard critical data and systems by minimizing the attack surface, limiting cyberattacks, enhancing operational performance and reducing the impact of human error.

**Defense in Depth** (multiple types of security controls in different layers)

* The principle of defense in depth is about having more than one layer or type of defense.
* The reasoning behind this principle is that any one layer or type of defense may be breached, no matter how strong and reliable you think it is, but two or more layers are much more difficult to breach.
* Defense in depth works best when you combine two or more different types of defense mechanisms—
* such as using a firewall between the Internet and your LAN, plus the IP Security Architecture (IPSEC) to encrypt all sensitive traffic on the LAN. In this scenario, even if your firewall is compromised, the attackers still have to break IP Security to get to your data flowing across the LAN.

Eg.

1st layer – Deterrent control (easy to implement, use it to warn hackers to not attack, breaching policies may not be legal)

2nd layer – Preventive control (Firewall installed on server that monitors all the traffic gg btw the internet and internal network and intercept any suspicious activities)

3rd layer – Detective layer (Network monitoring tools like intrusion detection systems that will alert ppl on any attacks being made on the system)

4th layer – Corrective layer (software installed like antivirus that could get rid of virus that the computer has been infected)

5th layer – Recovery layer (Data backup, another image of the system software for recovery in the event that the system breaks)

Generally, different types of controls should be used together:

* first, preventive controls should be in place to try and prevent security incidents from happening at all;
* second, detective controls are necessary so that you can know whether preventive controls are working or have failed;
* and third, corrective controls are needed to help you respond effectively to security incidents and contain damage.
* However, the defense in depth principle does not mean that you should indiscriminately apply all the controls and security measures you can get your hands on: balance has to be found between security provided by the defense in depth approach and the financial, human, and organizational resources you are willing to expend following it. This balance is addressed by the cost-benefit analysis.

**Minimisation**

*States that:*  the system should not run any applications that are not strictly required to complete its assigned task

* The minimization principle is the cousin of the least privilege principle and mostly applies to system configuration.
* For example, a computer whose only function is to serve as an e-mail server should have only e-mail server software installed and enabled. All other services and protocols should either be disabled or not installed at all to eliminate any possibility of compromise or misuse.
* Advantages: Adherence to the minimization principle not only increases security but usually also improves performance, saves storage space, and is a good system administration practice in general.

**Keep Things Simple**

a security system should be kept simple as any complexity introduced leads to insecurity in the overall system

* Complexity is the worst enemy of security. Complex systems are inherently more insecure because they are difficult to design, implement, test, and secure.
* The more complex a system, the less assurance we may have that it will function as expected.
* Although complexity of information systems and processes is bound to increase with our increasing expectations of functionality, we should be very careful to draw a line between avoidable and unavoidable complexity and not sacrifice security for bells and whistles, only to regret it later.
* When you have to choose between a complex system that does much and a simple system that does a bit less but enough, choose the simple one.