Vulnerabilities in Security Architecture and Technology Components

Evan Morgan, CISSP, CISM

@1evanski www.evanski.com

Overview

Identify the two common vulnerability type groupings

Discuss how the CIA Triad can help your organization systematically assess your environment for those concerns

Discuss more specifics on how an overall security architecture and its technology components can be vulnerable to exploitation

This is the 5th, 6th, 7th, and 8th objectives of the Security Engineering domain of the CISSP® Exam

“The only way to completely secure a system is to unplug it and bury it within a few feet of concrete”

Numerous Anonymous Security Practitioners

Two Common Vulnerability Type Groupings

Code Defect

Vulnerability in the code itself

Allows malformed requests to exploit the vulnerability and deliver a payload

Example: Buffer overflows

Is resolved to patches or upgrades to the code that is running

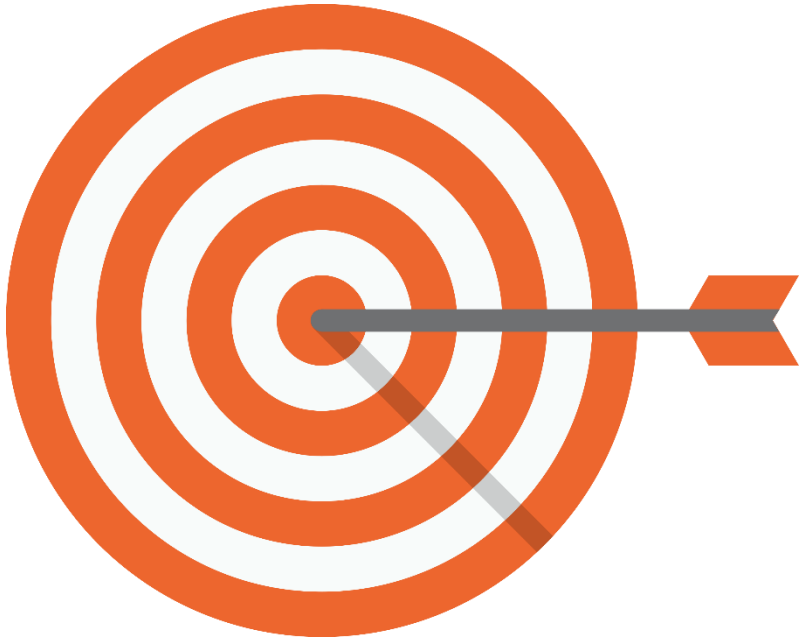
Configuration Defect

Vulnerability in the way a component (or the overall architecture) is configured

Allows for users to bypass the security level intended for a process, system, network, etc.

Example: Misconfigured access rights

Is resolved by changing the configuration of the component (or architecture)



Exploitation of vulnerabilities is the preferred method of attackers to bypass any (and potentially all) security mechanisms you have in place

Attackers only have to get it right once to compromise your security, while you have to be right all the time

Defending an organization can feel like a daunting task to accomplish, but is possible with the right people, processes, and technologies

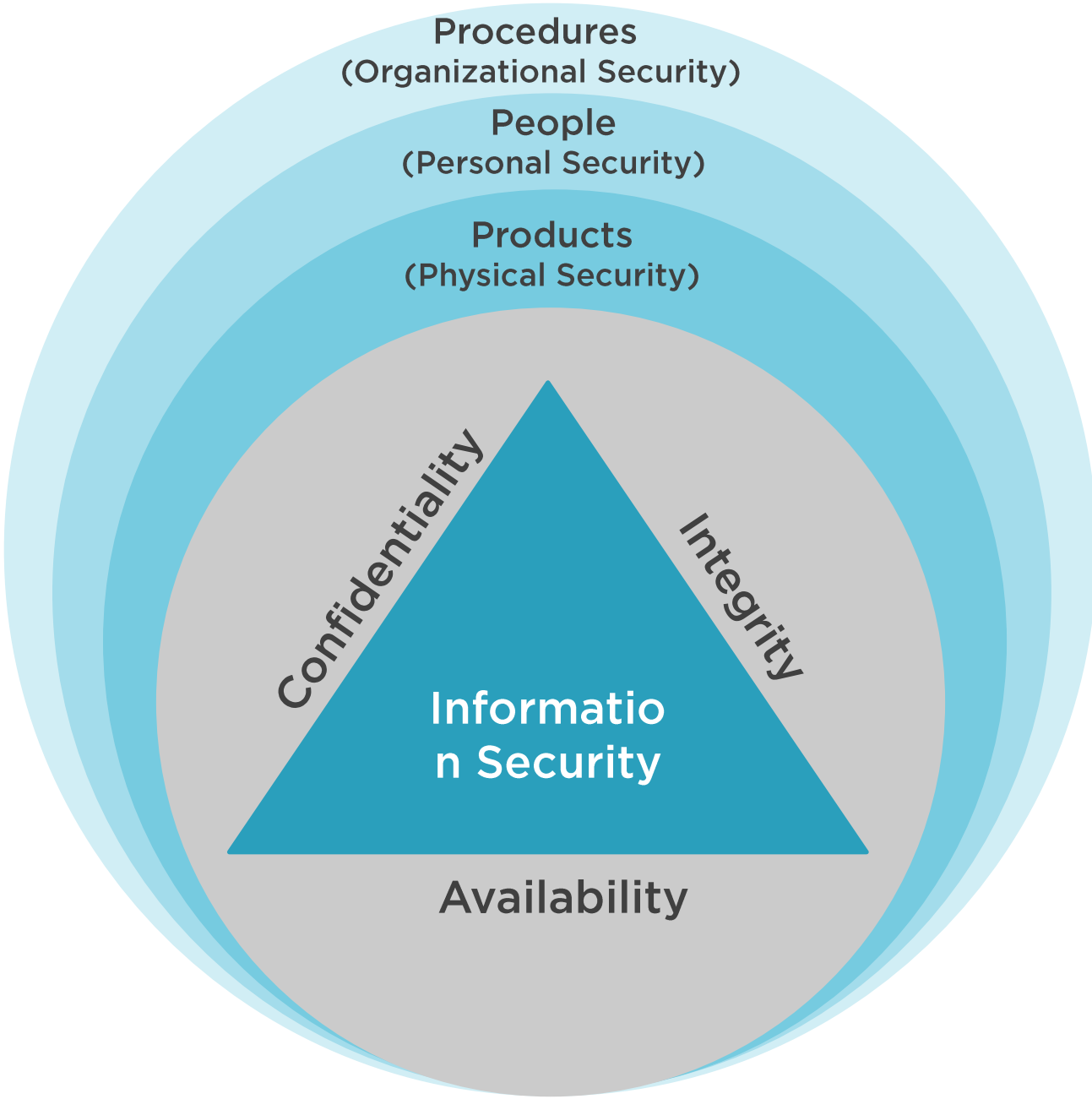
The CIA Triad

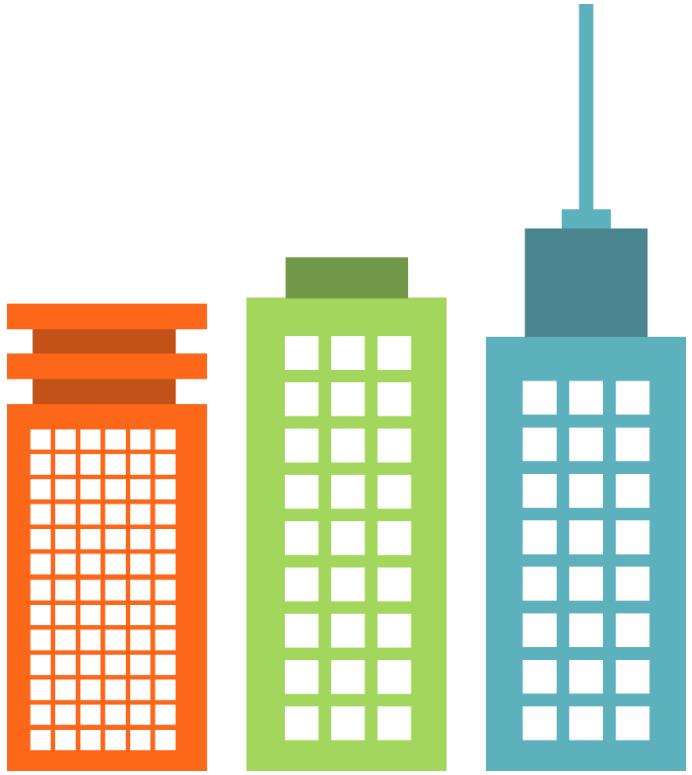
Confidentiality = C

Integrity = I

Availability = A

Security professionals would do well to strive for high levels of CIA for their organization's data





Security Architecture of an organization is very similar to traditional architecture for a building

This is because all components have to be factored in to the design to ensure that they will provide the proper result together

If security is not architected correctly, the whole environment could be at risk of exploitation by adversaries

Simply put, “a chain is only as strong as its weakest link” and the same is true for the architecture of an organization’s security

Besides vulnerabilities in technology components, an organization should also consider vulnerabilities to their overall security architecture, such as:

- What technology components are involved
- How all of the technology components work together
- Sensitivity of the data involved
- Ability to infer data without access to it
- Aggregation of non-sensitive data that creates sensitive data
- Emanations from systems in use
- Possibility of covert channel usage
- Single points of failure

Vulnerabilities in Technology Components

Server Infrastructure	End User Workstations and Mobile Devices	Cloud Computing
Applications	Databases	Networks

Summary

Identified the two common vulnerability type groupings

Discussed how the CIA Triad can help your organization systematically assess your environment for those concerns

Discussed more specifics on how an overall security architecture and its technology components can be vulnerable to exploitation

This is the 5th, 6th, 7th, and 8th objectives of the Security Engineering domain of the CISSP® Exam

What's Next?

Cryptography

What is it?

How does it relate to this module and the other modules?

Why is it important to this course and the CISSP® exam?