Defense-in-Depth Similarity and Differences

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

**Defense-in-Depth Similarity and Differences**

1. **Similarity:**

The major similarity between different frameworks is that most defense-in-depth provides different layers of protection to ensure that one attack can’t compromise a network or system. The layers that use in defense-in-depth include physical hardware, software, network architecture, technical administrative, and human elements. According to (1), The core concept of the defense-in-depth design used by security experts around the world is the C-I-A Triad which consists of confidentiality, integrity, and availability.

* Confidentiality: Information is not accessible or disclosed to unauthorized systems or individuals.
* Integrity: Ensure that information has not been modified by unauthorized users or systems and remains accurate and consistent.
* Availability: Ensure that system, data, network, or service is available and can be used or accessed.

1. **Differences:**

The NSA’s Information Assurance is based on people, technology, and operations:

* People: training and rewarding staff to ensure that they know the right thing to do based on policy and procedures. enforce those requirements with affect the system administration and physical security
* Technologies implementation is slightly different but the core concept is similar to other frameworks
* Operations: Where daily activities of defense in depth occur here.

The 20 CIS Control is based on 3 types and 20 different control:

* Organizational (security awareness and training program; application software security; incident response & management; penetration tests & red team exercise)
* Foundational (Email and Web browser protection; Malware defense; Limitation and control of network ports, protocol, and service; Data recovery capabilities; Secure configuration for network devices such as firewalls, routers, and switch; Boundary defense; data protection; Control access based on the need to know; Wireless access control; Account monitoring and control)
* Basic (inventory control of hardware assets; Inventory control of software assets; Continuous vulnerability management; Control use of administrative privileges; Secure configuration for hardware and software on mobile devices, laptops, workstations, and servers; Maintenance, monitoring, and analysis of audit logs)

The Department of Defense Cyber security discipline implementation plan focused on four distinct areas: Strong authentication; Divine hardening; Reduce attack surface; Alignment to cybersecurity/ computer network defense.

Over time, the US government grew CND into a complete discipline with dedicated cyber warfare support organizations. The list has grown with the addition of new element and additional technology such as artificial intelligence, machine learning, containerization, and cloud services have become commonplace.

References

Chapple, M., & Seidl, D. (2023). Chapter 9: Defense-in-Depth Strategies In *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 103–124). essay, Jones & Bartlett Learning. (1)

Wikipedia (n.d.) Edward Snowden. Retrieved from <https://en.wikipedia.org/wiki/Edward_Snowden> (2)