Southern New Hampshire University

CIA Triad and Fundamental Security Design Principles

The terms listed below are essential in the field of cybersecurity and will be a topic of conversation and application throughout the program. It is therefore important for you to familiarize yourself with these terms and their definitions.

Note that the CIA triad is sometimes referred to as the tenets of cybersecurity. The Fundamental Security Design Principles are sometimes called fundamental design principles, cybersecurity first principles, the cornerstone of cybersecurity, and so on.

CIA Triad

Information that is secure satisfies three main tenets, or properties, of information. If you can ensure these three tenets, you satisfy the requirements of secure information (Kim & Solomon, 2013).

- **Confidentiality**
  Only authorized users can view information (Kim & Solomon, 2013).

- **Integrity**
  Only authorized users can change information (Kim & Solomon, 2013).

- **Availability**
  Information is accessible by authorized users whenever they request the information (Kim & Solomon, 2013).

Fundamental Security Design Principles

These principles offer a balance between aspirational (and therefore unobtainable) “perfect security,” and the pragmatic need to get things done. Although each of the principles can powerfully affect security, the principles have their full effect only when used in concert and throughout an organization. These principles are a powerful mental tool for approaching security: one that doesn’t age out of usefulness or apply only to a few specific technologies and contexts; one that can be used for architecture, postmortem analysis, operations, and communication. The principles are ultimately only one piece in the security practitioner’s toolkit, but they are a flexible piece that will serve different roles for different people (Sons, Russell, & Jackson, 2017).

- **Abstraction**
  Removal of clutter. Only the needed information is provided for an object-oriented mentality. This is a way to allow adversaries to see only a minimal amount of information while securing other aspects of the model (Tjaden, 2015).

- **Complete Mediation**
  All accesses to objects should be checked to ensure that they are allowed (Bishop, 2003).

- **Encapsulation**
  The ability to only use a resource as it was designed to be used. This may mean that a piece of equipment is not being used maliciously or in a way that could be detrimental to the overall system (Tjaden, 2015).

- **Fail-Safe Defaults / Fail Secure**
  The theory that unless a subject is given explicit access to an object, it should be denied access to that object (Bishop, 2003).

- **Information Hiding**
  Users having an interface to interact with the system behind the scenes. The user should not be worried about the nuts and bolts behind the scenes, only the modes of access presented to them. This topic is also integrated with object-oriented programming (Tjaden, 2015).

- **Isolation**
  Individual processes or tasks running in their own space. This ensures that the processes will have enough resources to run and will not interfere with other processes running (Tjaden, 2015).

- **Layering**
  Having multiple forms of security. This can be from hardware or software, but it involves a series of checks and balances to make sure the entire system is secured from multiple perspectives (Tjaden, 2015).

- **Least Astonishment (Psychological Acceptability)**
  Security mechanisms should not make the resource more difficult to access than when security mechanisms were not present (Bishop, 2003).

- **Least Privilege**
  The assurance that an entity only has the minimal amount of privileges to perform their duties. There is no extension of privileges to senior people just because they are senior; if they don't need the permissions to perform their normal everyday tasks, then they don't receive higher privileges (Tjaden, 2015).

- **Minimization of Implementation (Least Common Mechanism)**
  Mechanisms used to access resources should not be shared (Bishop, 2003).

- **Minimize Trust Surface (Reluctance to Trust)**
  The ability to reduce the degree to which the user or a component depends on the reliability of another component (Bishop, 2003).

- **Modularity**
  The breaking down of larger tasks into smaller, more manageable tasks. This smaller task may be reused, and therefore the process can be repurposed time and time again (Tjaden, 2015).

- **Open Design**
  The security of a mechanism should not depend on the secrecy of its design or implementation (Bishop, 2003).

- **Separation (of Domains)**
  The division of power within a system. No one part of a system should have complete control over another part. There should always be a system of checks and balances that leverage the ability for parts of the system to work together (Tjaden, 2015).

- **Simplicity (of Design)**
  The straightforward layout of the product. The ability to reduce the learning curve when analyzing and understanding the hardware or software involved in the information system (Tjaden, 2015).

- **Trust Relationships**
  A logical connection that is established between directory domains so that the rights and privileges of users and devices in one domain are shared with the other (PC Magazine, 2018).

- **Usability**
  How easy hardware or software is to operate, especially for the first-time user. Considering how difficult applications and websites can be to navigate through, one would wish that all designers took usability into greater consideration than they do (PC Magazine, 2018).

References

Bishop, M. (2003). *Computer security: Art and science*. Boston, MA: Addison-Wesley Professional.

Kim, D., & Solomon, M. G. (2013). *Fundamentals of information systems security* (2nd ed.). Burlington, MA: Jones & Bartlett Publishers.

PC Magazine. (2018). *Encyclopedia*. Retrieved from https://www.pcmag.com/encyclopedia

Sons, S., Russell, S., & Jackson, C. (2017). *Security from first principles*. Sebastopol, CA: O'Reilly Media, Inc.

Tjaden, B. C. (2015). *Appendix 1: Cybersecurity first principles*. Retrieved from https://users.cs.jmu.edu/tjadenbc/Bootcamp/0-GenCyber-First-Principles.pdf