

# Parkian hexad vs the cia triad essay



**ASSIGN  
BUSTER**

“ Is the Parkerian Hexad superior to the CIA Triad in describing the framework necessary for information systems security? ” Yes, the Parkerian Hexad is superior to the CIA Triad because it is an updated approach that expands on the original three elements of the CIA Triad. In order to answer this question let’s look at some definitions and history of information security. The U. S.

Committee on National Security Systems (“ CNSS”) defines “ Information Systems Security” as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (CNSS, Instruction No. 4009). There are several different approaches that provide a guide on how best to accomplish information systems security. The two that I will compare are the CIA Triad and the Parkerian Hexad.

In 1994, The National Security Telecommunications and Information Systems Security Committee created the Comprehensive Model for Information Systems Security or the CIA Triad (Whitman & Mattord, 2009). The CIA Triad stands for Confidentiality, Integrity, and Availability. Confidentiality is defined by the CNSS as “ the property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information” (CNSS, Instruction No. 4009).

This is the need for only authorized people to have access to specific information and can also be the need to withhold specific information for an unauthorized person. An example of this is when a business, such as a credit card companies agrees not to share/sell your information to a third party.

When I give my information to the credit card company I expect confidentiality and they; therefore, have a responsibility to provide it. The second part is Integrity. This is not the integrity of the person/entity holding one's personal information.

This is the integrity of the data itself after it is given. The CNSS defines Integrity as " the property whereby an entity has not been modified in an unauthorized manner" (CNSS, Instruction No. 4009). Modification or corruption of data can occur during the original transmission or during storage. Availability relates to accessing the data when needed. It is defined by the CNSS as " the property of being accessible and useable upon demand by an authorized entity" (CNSS, Instruction No. 4009). It can look at a wide range of issues from the proper controls of the system, to how the request for information is communicated, and to external factors such as hardware failures. The Parkerian Hexad is a term coined by M. E. Kabay, a professor at Norwich University in Northfield, Vermont (Kabay, 2009). It refers to an information security approach put together by Donn B. Parker in 1998. It updates the CIA Triad to include three additional elements: Authenticity, Utility, and Possession (Dardick, 2010).

Possession expands on Confidentiality to ensure that the information remains with the authorized entity. For example, " valuable public documents and websites are owned and protected legally by proprietary rights addressed by trade secret, copyright, and trade mark laws and require application of security controls and practices to ensure exclusive or desired possession" (Parker, 2010). Authenticity expands on Integrity to ensure that the original information is by the submitted by the correct person.

<https://assignbuster.com/parkian-hexad-vs-the-cia-triad-essay/>

Donn Parker states “ the primary issue here is difference between condition (integrity) and validity (authenticity)” because “ it is inconsistent and incorrect to make integrity mean both integrity and authenticity when information could exclusively have one of these states of security but not the other” (Parker, 2010). For example, an unintended material deterioration in condition (e. g. , “ 1234567890” that is so faint that you can barely read it) would be a loss of integrity and different from an unintended but readable modification (e. g. , “ 2134567890”) that changes content and authenticity (Parker, 2010).

Utility expands on Availability to ensure that information is useful. For example, encrypted information for which the key is unknown may be available (usable) for cryptanalysis but might not be useful in its present form (Parker, 2010). The CIA Triad looks at information and the thought process needed to protect it. It doesn't have any elements that ensure that these are working. The Parkerian Hexad goes farther because it looks at “ forces and what people do as owners, users, custodians, and defenders of an organization's assets and the abusers, misusers, or wrongdoers that would cause harm” (Parker, 2010).

The following is an example that shows necessity of the three additional elements. Ann, a teller has an emergency and thinks that she needs a short, quick loan. She has a checking account with her employer, the bank. Using a her bank credentials, she logs on the bank database and makes a small deposit into her account by altering her bank balance. She then goes to the ATM and withdraws her money since the database still shows that the balance is available. Using the CIA Triad, there was no breach of

confidentiality because the balance wasn't disclosed nor was there a breach of Integrity because the database is still intact.

However, with the Parkerian Hexad this would not pass the additional test of authenticity because Ann did not have the authority to change her balance.

The best argument that I could find that addressed the CIA Triad being superior to the Parkerian Hexad is that the Hexad is too many steps and is too complex to explain to somebody not in the security industry. This could lead to each aspect not being addresses properly. Donn Parker alleviates this concern by, instead of having six separate steps when identifying the method, teach it as three pairs: Confidentiality and possession, integrity and authenticity, and availability and utility.