Advances in Robotics & Automation

ISSN: 2168-9695

Keung HY, Adv Robot Autom 2014, 3:2
DOI: 10.4172/2168-9695.1000e120

Editorial Open Access

Basic Principle of Information Security

YAU Hon Keung*

Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Kowloon, Hong Kong

***Corresponding author:** YAU Hon Keung , Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Kowloon, Hong Kong; E-mail: honkyau@cityu.edu.hk

Rec Date: March 31 2014; **Acc Date:** March 31 2014; **Pub Date:** April 2 2014

Introduction

According to Steichen [1], there are several principles of information security. We know to use confidentiality, integrity and availability which known as the CIA Triad for over twenty years, as the core principles of information security.

CIA Triad

Confidentiality

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a **laptop computer** containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information.

Integrity

In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus **infects** a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial -of- service attacks.

Later Parker [2] proposed “the Parkerian hexad” which adds three additional attributes to the three classic security attributes of the CIA triad. It is a set of six elements of information security model. These attributes of information are not broken down into further constituents, also all of them are non-overlapping [3].

References

1. Steichen P (2009) Principles and fundamentals of security methodologies of information systems- Introduction .
2. Parker DB (2009) Toward a New Framework for Information Security.
3. Bosworth S, Kabay ME (Ed.) Computer Security Handbook. John Wiley & Sons, New York, USA.