MATRIX ACADEMIC INTERNATIONAL ONLINE JOURNAL OF ENGINEERING AND TECHNOLOGY
ISSN: 2348-3326,
www.maioj.org © MAIOJET
Volume 3, Issue 2

Comparative Analysis of Information Security Pillars

Savita Singh[#1], Bineet Kumar Gupta[#2]

[#] *Department of Computer Science & Engineering, Shri Ramswaroop Memorial University Lucknow, India*

[1]savi0016@gmail.com

[2]bkguptacs@gmail.com

***Abstract*— We are living in the world of information, information is everywhere. Confidentiality, integrity and availability abbreviated as CIA are the security pillars which are really very important in the way of securing information. In order to achieve security, we are required to achieve these three pillars. If we are able to achieve these pillars, we can secure information very efficiently. Here, we are doing comparative analysis of these three pillars.**

***Keywords*— Confidentiality, integrity, availability, information, security pillar.**

I. INTRODUCTION

As technology advances and access to the information expand, the need to protect information to ensure its confidentiality, integrity, and availability also increases. Almost all organization whether social, governmental, educational etc., have now automated their information systems and other operational functions. They have maintained the databases that contain the crucial information. Information security is a serious concern because it is act as a brick for any kind of organization. Securing information becomes very essential because of its increased value. Information confines a very big part of any organization. It is used in almost every organization like in education, business, factories, MNCs etc. In educational institute, information about student is stored, maintained and transferred. In case of business organization, information regarding its employee, their performance, yearly profit etc has been stored and transferred.

All the information needs to be stored and transferred in secure way. Information security is an act of protecting information by means of achieving security pillars i.e. confidentiality, integrity, and availability. In other words, protecting the confidential/sensitive information is actually the information security. It deals with making transmission and storage of information secure from any form of illegal access or threat at any level. The three pillars are heart of information security. In order to secure information, it is required to fulfil these pillars. The CIA triad confines the fundamental security objectives for data and information. If CIA triad is violated, violation of information security also takes place.

Organizations that are running successfully demand the confidentiality of their information. They do not allow the unauthorized access to their data/information. And they also demand the assurance that their data is protected against any malicious or accidental modification. Data protection and confidentiality are the security concerns.

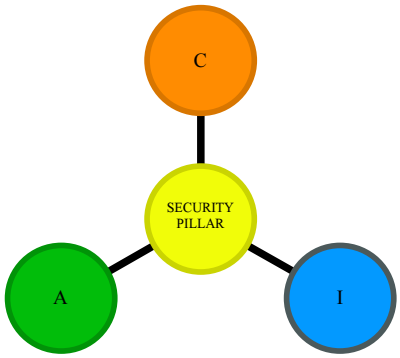

Fig. 1 Security Pillars

Information is something that is meaningful in some context for its receiver. For example, if we are considering the sentence: Neha school 9 am go to at. This sentence is data because it is raw and meaningless. If the above sentence is arranged in proper way, it becomes information because it contains some meaning: Neha go to school at 9 am. When information is transmitted from sender to receiver, it is probable that some intruder can access this information and use this information for their own profit.

Suppose there are two bunches of army persons and are fighting against traitors who are trying to harm their motherland. If a person of one group wants some come confidential information to deliver other group regarding their strategies of fighting, in such condition, it is very important to transmit the message in secure way so that unauthorized persons are unable to access this information, there shouldn't be any unauthorized modification and last but not the least information must be available only to authorized persons.

In this paper, we are going to focus on CIA security pillars and their comparative analysis with example.

II. CONFIDENTIALITY

The term confidentiality is the set of rules that restricts the access for a particular kind of information; it limits the access i.e. only intended persons are able to access the information. Confidentiality is the act that preserves authorized restrictions on information access and its disclosure. A loss of confidentiality is the unauthorized disclosure of information.

For example, there are two persons named as Maahi and Prashant who wants to communicate with each other via transferring information between them. Suppose Maahi sends secret information to Prashant and on the way the third person Ray reads this secret information, then its confidentiality is violated. If no one is able to access this information while communication and its storage, then confidentiality of information is maintained.

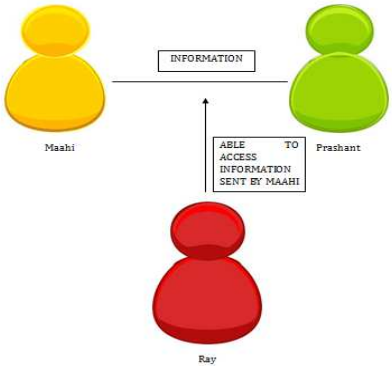

Fig. 2 Violation of Confidentiality

III. INTEGRITY

Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information. So, in order to maintain integrity of information, it is required that none other than authorized persons have permission to modify the content of information being transmitted and stored.

For example, Suppose Maahi sends prashant :hey. But before Prashant receives this information, Ray modifies this to :hey, meet me at 4 pm. Ray is not the authorized person in the communication of Maahi and Prashant, so the modification made by ray is unauthorized modification by unauthorized user. So that integrity of information is violated. But if such kind of modification does not take place, in this condition, integrity of information will be maintained.

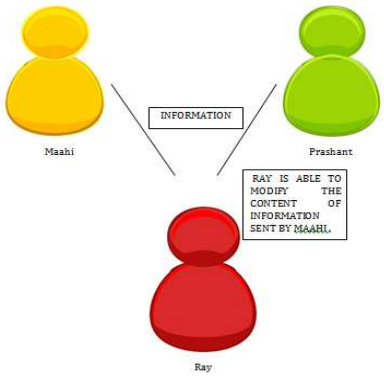

Fig. 3 Violation of Integrity

IV. AVAILABILITY

It ensures timely and reliable access and use of information. It makes us sure that information will be available to authorized user in timely manner. A loss of availability is the disruption of access to or use of information or an information system.

For example, if Maahi and Prashant are communication through transmission information, then information must be available to both of them whenever they required. Suppose Maahi sends her mobile number to Prashant. The mobile number must be available to Prashant when he needs.

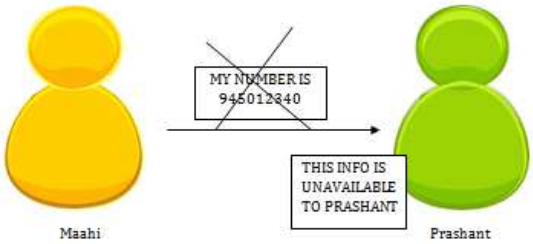

Fig. 4 Violation of Availability

V. COMPARISON & EXPLANATION

Here, we are considering a database named as student information database which describe information about student with the help of tables. This database consist nine tables mentioned below.

TABLE I
STUDENT

FIELD	TYPE	KEY
STUDENT ID	INT	PRIMARY KEY
FIRST NAME	VARCHAR(10)	
LAST NAME	VARCHAR(10)	
GENDER	VARCHAR(6)	
FATHER NAME	VARCHAR(15)	
FATHER'S OCCUPATION	VARCHAR(15)	
MOTHER NAME	VARCHAR(15)	
COURSE	VARCHAR(10)	
YEAR	INT	

TABLE III
STUDENT_DETAIL

FIELD	TYPE	KEY
STUDENT DETAIL ID	INT	PRIMARY KEY
STUDENT ID	INT	FOREIGN KEY
DOB	DATE	
ADDRESS	VARCHAR(50)	
GRADES IN 10^{TH}	INT	
BOARD OF 10^{TH}	VARCHAR(20)	
YEAR OF 10^{TH}	INT	
GRADE IN 12^{TH}	INT	
BOARD OF 12^{TH}	VARCHAR(20)	
YEAR OF 12^{TH}	INT	
EMAIL ID	VARCHAR(30)	
MOBILE NO.	INT	
ADDIONAL QUALIFICATON	VARCHAR(50)	
LANGUAGE KNOWN	VARCHAR(20)	

TABLE IIIII
COURSE

FIELD	TYPE	KEY
COURSE ID	INT	PRIMARY KEY
COURSE NAME	VARCHAR(30)	
COURSE COORDINATOR	VARCHAR(30)	

TABLE IVV
SUBJECT

FIELD	TYPE	KEY
SUBJECT ID	INT	PRIMARY KEY
SUBJECT NAME	VARCHAR(30)	
SUBJECT TEACHER	VARCHAR(30)	

TABLE V
ASSIGNMENT

FIELD	TYPE	KEY
STUDENT ID	INT	PRIMARY KEY
COURSE ID	INT	FOREIGN KEY
SUBJECT ID	INT	FOREIGN KEY
ASSIGNMENT STATUS	VARCHAR(20)	
DUE DATE	DATE	
REMARK	VARCHAR(15)	

TABLE VI
ATTANDANCE

FIELD	TYPE	KEY
STUDENT ID	INT	FOREIGN KEY
COURSE ID	INT	FOREIGN KEY
SUBJECT ID	INT	FOREIGN KEY
DATE OF ATTANDANCE	DATE	
STATUS	VARCHAR(15)	

TABLE VII
FEE

FIELD	TYPE	KEY
STUDENT ID	INT	FOREIGN KEY
COURSE ID	INT	FOREIGN KEY
DEPOSIT DATE	DATE	
FEES	INT	
BALANCE	INT	
MODE	VARCHAR(20)	
FINE	INT	

TABLE VIII
EXAM

FIELD	TYPE	KEY
COURSE ID	INT	FOREIGN KEY
EXAM ID	INT	PRIMARY KEY
DATE OF EXAM	DATE	
EXAM NAME	VARCHAR(15)	

TABLE IX
RESULT

FIELD	TYPE	KEY
STUDENT ID	INT	FOREIGN KEY
GRADES	INT	
EXAM NAME	VARCHAR(15)	

Here, communication takes place between administrator of this database and a particular student getting information and for the purpose of updating data of students.

Suppose student wants to his/grades. It is important that this information should be propagated through a secure channel so that information security should be achieved. While sending this to student, if no one accessed this information, there isn't any unauthorized modification and this information is available to student, which means information is securely transmitted to student and there isn't any kind of security violation. Vikas wants to know his grades and sends request to admin, after getting his request his grade 7.6, Vikas receives this this information and comes to know that he gets 7.6 cgpa which is only known to him. That means all the three pillars are achieved. Admin sends grade 7.6 and Vikas received the same grade 7.6, that means there isn't any unauthorized modification i.e. integrity is maintained. Only Vikas knows his grade i.e. confidentiality is maintained. Information regarding grades is available to Vikas i.e. availability is achieved.

Since all the security pillars are of equivalent importance but if we compare these three pillars confidentiality, integrity and availability to each other, then which one is the most important among them. In my opinion, availability of information is needed before integrity & confidentiality. It is possible to have availability without having confidentiality and integrity but we cannot have confidentiality or integrity without having access to the information we seek for. For example, if information about grades isn't available to Vikas, then there isn't any usefulness of confidentiality and integrity. Availability is the degree to which information is available upon user demand. Users experience frustration when their data is unavailable, and they do not understand or care about any problem due to which information is unavailable. When information is unavailable to user, this can lead to lost productivity, bad publicity. We cannot have confidentiality without integrity.

ACKNOWLEDGMENT

We are thankful to the faculty of Computer Science and Engineering, Shri Ramswaroop University for the motivation and continuous support time to time.

REFERENCES

[1] Shelly Rohilla, Pradeep Kumar Mittal, "Database Security: Threats and Challenges.," International Journal of Advanced Research in Computer Science and Software Engineering, 2013.

[2] William Stallings, *Cryptography and Network Security*. 5th Ed, 2011.

[3] Shauki Abdusalam Fatshul, Salahedin Ali Namroush, "Security issues, attack Trends related to the confidentiality, integrity, and availability of information assets on an organization's computer system," Proceedings of the Postgraduate Annual Research Seminar 2006.

[4] Sattarova Feruza Y. and Prof.Tao-hoon Kim, "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security," International Journal of Multimedia and Ubiquitous Engineering Vol. 2, No. 2, April, 2007.