A Comparative Review of Business Models in Information Security

Richard Omollo
Department of Computer Science and Software Engineering
Jaramogi Oginga Odinga University of Science and Technology
Email: comolor@hotmail.com

ABSTRACT

This paper appreciates the basic tenets of information as defined by the CIA and discusses the various Information security business models. Information security has been defined as the preservation of confidentiality, integrity, and availability, also known as the CIA triad, of information by guarding against unauthorized access, use, disclosure, disruption, alteration, and destruction of information and information systems or assets. It further simplified information security by ensuring information confidentiality, integrity, and availability. It is the aspect of ensuring information is only accessible to the right persons, protecting information from unauthorized modifications, and ensuring information is available to authorized users whenever they need it. Existing Information security business models serve as a guide in comprehending the challenges to confidentiality, integrity, and availability of known systems. This research study appreciated various business models and offered their comparative review.

KEYWORDS: Information security, Information models, confidentiality, integrity.

I. INTRODUCTION

Technology has become the driving force in the business sector. Anyone ignoring it does so at their peril. It is a tremendous and effective ingredient in business. This has necessitated its acceptance. Due to this very factor, its popularity, it has momentously attracted threats in cyberspace. This has consequently obliged the development of information security practices.

This paper is arranged as follows: The related studies or works on the Information security business models are discussed in the next section, which is a literature review. The methodological approach used in the study is discussed in the proceeding section followed by discussions and conclusions sections.

II. LITERATURE REVIEW

This section discusses the various publications that have been made regarding information security business models.

1.1 Clark-Wilson Security Model

According to (Mike Chapple, and James Michael, 2020)**,** The Clark Wilson model employs a comprehensive strategy to protect data integrity. This implies that the Clark-Wilson model's purpose is to

guide data integrity. It continues to note that The Clark-Wilson approach utilizes a subject, program, object (or subject, transaction, object) three-part relationship known as a triple or an access control triplet rather than requiring the employment of a matrix structure. Objects are not accessible to subjects directly. Only programs have access to objects. Only a program, interface, or access portal can be used by a subject to access objects. This creates the separation of duty and it is an effective means to ensure data integrity.

(Avorgbedor & Liu, 2020) argues Clark Wilson Security Model consists of two main rules, enforcement and clarification. Continues to note that the model has two data items and two procedures; Constrained Data Items (CDIs), Unconstrained Data Items (UDIs), Integrity Verification Procedures (IVPs), and Transformation Procedures (TPs). Under CDIs, the user information such as username is subjected to integrity. In UDIs, information by users such as videos, is not subjected to data integrity by the model. Data is scanned using the IVPs procedure to ensure the integrity of the data items. They consist of procedures like authentication, initiation, validation, transformation, and validity enforcement.

1.2 Chinese Wall Security / Brewer and Nash Model

David Brewer and Michael Nash proposed the Chinese Wall Model, often known as the Brewer-Nash model, in 1989 (Badve et al., 2016)**.** According to (Mike Chapple, and James Michael, 2020)**,** this model was developed to allow access controls based on a user's prior activities. It addresses conflict of interest problems. (Lin, 2015)**,** describes the Chinese Wall Policy model, users can only obtain information that does not conflict with any of the information they already have.

According to (Mike Chapple, and James Michael, 2020)**,** by defining a class of data that indicates which security domains may potentially conflict, this approach precludes any subject who has access to one domain that is a member of a particular conflict class from also having access to any other domains that are members of the same conflict class. By doing this, it figuratively creates a wall around all other data in any kind of dispute.

1.3 Bell–LaPadula Model

This model was developed by the U.S. Department of Defense (DoD) in the 1970s based on the multilevel security standards of the DoD. This model guides that a user with any degree of clearance can only access resources at or below that level. Access to segregated objects is only permitted within certain levels of clearance and only to those who have a legitimate need to know (Mike Chapple, James Michael, 2020)**.** (Zhao & Chadwick, 2008)**,** also guides that, the Bell-LaPadula model implements both the Discretionary Access Control (DAC) policies and the Mandatory Access Control (MAC) policies to ensure the flexibility of access control policies and confidentiality needs are met respectively. This model guides confidentiality management based on. Its purpose is to ensure that confidential and top-secret information is only accessible to persons with appropriate levels of clearance or with apt permissions on a need-to-know basis.

(Mike Chapple, James Michael, 2020) notes that to do this, lower-class subjects are prevented from accessing higher-class objects.

There are three fundamental BLP criteria, and any operation done on objects by subjects that comply with all three of these rules is considered trustworthy. (Badve et al., 2016)**.** These criteria are: - Simple-Security Rule: The Subject can only read the object if and only if the subject's security level is higher than or equal to the object's security level. Star-Property: The subject may only write to an object if and only to the extent that the subject's security level is lower than or equal to that of the object. Discretionary-Security Property: All accesses and operations must only be permitted if they adhere to the restrictions outlined in the access control matrix.

1.4 Graham Denning Model

This model was proposed by Graham in 1972. It is an information security model that is used to give subjects and objects access rights and guarantee that the system access is properly authorized. Additionally, it guarantees that subjects and objects are added and removed safely. (Badve et al., 2016)**.** The model is a set of eight fundamental protection laws or deeds that set the limits of specific secure deeds. (Mike Chapple, James Michael, 2020)**.** These protection rules are: Securely create an object. Securely create a subject, delete an object, securely delete a subject, securely provide the read access right, provide the grant access right, securely provide the delete access right and securely provide the transfer access right. The access control matrix defines the specific rights or privileges that a subject has about a group of objects.

1.5 Harrison-Ruzzo-Ullman Model

This model named after its authors, Michael A. Harrison, Walter L. Ruzzo, and Jeffrey D. Ullman, was developed in 1976. Essentially, it is concerned with the accuracy and integrity of the information system's access privileges. (Badve et al., 2016)**.** (Mike Chapple, James Michael, 2020) notes that this model is a development of the Graham-Denning model.

Three parameters—the subjects, the objects, and the access matrix—define this model. (Mike Chapple, James Michael, 2020)

In a matrix, where the rows represent subjects and the columns represent objects, the model's current state of access rights can be described. The specific actions that each subject is permitted to take against each object are listed at the intersection of each row and column. A finite collection of primitives or instructions is also defined that governs the modification of the matrix by permitted individuals. (Mike Chapple, James Michael, 2020) **.** These primitives allow you to change the matrix's access privileges, subjects, and/or objects. A subject or object cannot be created or added to the matrix if it already exists. Likewise, for a subject or object to be removed from the matrix, it must already exist. If any commands are issued simultaneously, they must all be successful for the entire batch to be applied.

III. METHODOLOGICAL APPROACH

This part covers the approach and procedure that was used to carry out this study. The methodological approach for this study was archival study. It is purely done by review of various published and peer-reviewed literature. Its conclusion and discussion are purely based on the evaluation and assessment of what recent researchers in the field of information security have discussed on the various Information security business models. The constraint in carrying out this study was getting the most recent peer-reviewed materials.

IV. DISCUSSIONS

Businesses' information security has emerged as a major concern in recent years. This has consequently led to enormous budgetary allocation and spending. (Vitenburg & Nikishova, 2019) When designing an information security program, it is critical to understand the structure of the protected object, its functional features, and key processes that influence all of its work. As noted by (Gill et al., 2021), threat actors are constantly searching for security flaws, and failure or utter lack of protective and detective controls in businesses provides an entry point to valuable data.

With a poor understanding of the business models of a company, the management may end up making information security decisions that are of little value to the objectives. The management must take time to comprehend its business model to implement the most apt information security model.

From the review of the various traditional security models, it is clear that each focus on a particular information security aspect such as confidentiality as opposed to integrity. For example, we have Bell-LaPadula used by the military since it is based on ensuring information confidentiality. Consequently, institutes such as school institutions whose number one aim in information security is integrity can implement models that favor these needs such Graham-Denning Model. The military or DOD can employ models such as Bell-LaPadula for data confidentiality.

Table 1 Comparative Summary of Business Models in Information Security

Model	Concentrations/Focus	Applications
Clark-Wilson Security	Separation of duties through Integrity Verification Procedures.	Data integrity
Chinese Wall Security/Brewer and Nash	Information security access controls to mitigate conflict of interest	Authenticity, Authorization
Bell–LaPadula	Protection of information from unauthorized disclosures.	Data Confidentiality
Graham Denning	Assignment of specific access rights	Authentication
Harrison-Ruzzo-Ullman	Discretionary Access Control	Authentication

IV. CONCLUSIONS

As earlier noted, these models are not solutions in themselves, but guides. (Hermann, 2011) Notes that proven security policy models, when executed properly, safeguard data items from security breaches and prevent illegal sharing of information. They help a business understand the challenges encountered in ensuring confidentiality, integrity, and availability of information. The comprehension consequently guides a business in knowing its needs and consequently employing the right information security model that meets its needs. This study has dealt with the traditional information security models. These models guide on which is most appropriate when the number one need is ensuring confidentiality or integrity or even availability.

REFERENCES

Avorgbedor, F., & Liu, J. (2020). Enhancing User Privacy Protection by Enforcing Clark-Wilson Security Model on Facebook. *IEEE International Conference on Electro Information Technology*, *2020-July*, 155–161. https://doi.org/10.1109/EIT48999.2020.9208279

Badve, O., Gupta, B. B., & Gupta, S. (2016). *Reviewing the Security Features in Contemporary Security Policies and Models for Multiple Platforms* (pp. 479–504). https://doi.org/10.4018/978-1-5225-0105-3.ch020

Gill, A. K., Zavarsky, P., & Swar, B. (2021). Automation of Security and Privacy Controls for Efficient Information Security Management. *ICSCCC 2021 - International Conference on Secure Cyber Computing and Communications*, 371–375. https://doi.org/10.1109/ICSCCC51823.2021.9478126

Hermann, E. (2011). The limes Security model for information flow control. *Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011*, 573–580. https://doi.org/10.1109/ARES.2011.88

Lin, T. Y. T. Y. (2015). Chinese wall security policies information flows in business cloud. *Proceedings - 2015 IEEE International Conference on Big Data, IEEE Big Data 2015*, 1603–1607. https://doi.org/10.1109/BigData.2015.7363927

Mike Chapple , James Michael, S. D. G. (2020). CISSP Certified Information Systems Security Professional Official Study Guide 9 Edition. *Paper Knowledge . Toward a Media History of Documents*, 12–26.

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *An introduction to information security*. https://doi.org/10.6028/NIST.SP.800-12r1

Thill, F. (2022). Information Security Risk Management. *IFIP Advances in Information and Communication Technology*, *644 IFIP*, 17–22. https://doi.org/10.1007/978-3-030-99100-5_2

Vitenburg, E., & Nikishova, A. (2019). Project of automated system's information security system selection. *2019 International Science and Technology Conference "EastConf", EastConf 2019*, 0–4. https://doi.org/10.1109/Eastonf.2019.8725345

Zhao, G., & Chadwick, D. W. (2008). On the modeling of Bell-LaPadula security policies using RBAC. *Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE*, 257–262. https://doi.org/10.1109/WETICE.2008.34