

Analysis of the Appropriate Security Models to Apply in a Distributed Architecture

Moisés Toapanta¹, Jean Nazareno², Raúl Tingo³, Felix Mendoza⁴, Antonio Orizaga⁵, Enrique Mafla⁶

^{1,2,3,4}Computer Science Department, Universidad Politécnica Salesiana – Sede Guayaquil, Chambers 227 and 5 of junio, Guayaquil, Ecuador – stoapanta@ups.edu.ec, jnazareno@est.ups.edu.ec, rtingo@ups.edu.ec, fmendoza@ups.edu.ec.

⁵Informations Systems Department CUCEA, Universidad de Guadalajara, Periférico Norte No 799, Nucleo Universitario, Los Belenes, C.P. 45100, Zapopan, Jalisco, México – jose.orizaga@academicos.udg.mx.

⁶Faculty in Engineering Systems, Escuela Politécnica Nacional, Ladrón de Guevara E11-253, Quito, Ecuador. Enrique.mafla@epn.edu.ec.

Abstract. The availability of information generated on a large scale has allowed sharing without considering the levels of risk that can be caused by not considering the confidentiality, integrity and authenticity of the information; any misuse, destruction, modification or unauthorized access with confidentiality, integrity and authentication information in an organization may affect the privacy or well-being of individuals and society. The objective is to perform the analysis of security models to generate a prototype of model to mitigate information security problems. The deductive method was used to review and analyse the referenced information and identify the ideal security models that allow to improve the security of information in a distributed architecture. Turned out a prototype model merging the characteristics of the BiBa model and the Bell-Lapadula model, creating a new model that offers integrity, confidentiality and access control as an alternative to improve the security of information. It was concluded that it is necessary to have an appropriate security model that conforms to the objectives, operational, tactical and strategic of the organization to mitigate the confidentiality, integrity and authenticity.

1. Introduction

The large volume of information that is currently generated in different types of organizations worldwide provides a better lifestyle for people, this information can be used for educational, commercial, research or decision making purposes.

Among the different types of information handled are those that require integrity, availability all the time and others that require protection such as: Medical, financial, commercial and even military information. Any unauthorized use, destruction, modification or unauthorized access of confidential information in an organization can affect the privacy or well-being of people.

To mitigate these security problems, it is necessary to have a security model that adapts to the mission, vision and objectives of the organization. Based on this, security rules and policies for information management are defined with confidentiality, integrity and authenticity[1][2].

Among the most prominent security models are the Bell-LaPadula and BiBa model, which were created to mitigate the problems of confidentiality and integrity, respectively, classifying data and



people at different levels of security. There are other models, such as the Clark-Wilson integrity security model, the Chinese Wall model, McCumber, among others that have been created; with the objective of improving the security of information.[3][4][5].

Why is it necessary to perform the analysis of security models for a distributed architecture?

For determine the security model suitable to work in a distributed environment in a public or private organization to mitigate the threats, vulnerability and risks of information.

The objective is to perform the analysis of security models to generate a prototype of a new model the security to mitigate information security problems.

The revised articles related to security models are:

An Analysis of Sensitive Information System Security Models[1], Data-driven Software Security: Models and Methods[2], Analysis of Security Models Based on Multilevel Security Policy[3], Assessment of the Security Architecture of Control System Using Discretionary Security Models[4], An Application Security Model Based on Business Process in Information System[5], Modeling and Validation for Embedded Software Confidentiality and Integrity[6], The revival of ancient information security models, insight in risks and selection of measures[7], On The Modeling of Bell-LaPadula Security Policies Using RBAC[8], Configuring Clark-Wilson Integrity Model to Enforce Flexible Protection[9], SCWIM An Integrity Model for SOA Networks[10], Information Confidentiality and the Chinese Wall Model in Government Tender Fraud[11].

The method used is the deductive to review and analyze the information referred to and to identify the security models, in order to improve the security of the information in a distributed architecture.

The result obtained in this research phase is a prototype of a security model based on the characteristics of the BiBa and Bell-Lapadula model; as an alternative to improve the integrity, confidentiality and authenticity of the information in a distributed environment.

It is concluded that it is necessary to have an adequate security model that adjusts to the operational, tactical and strategic objectives of the organization to improve the confidentiality, integrity and authenticity of the information; based on the Biba model, Bell-LaPadula, China Wall, Crak Wilson among others.

2. Material and Methods

2.1 Methods

In this research the deductive method is applied to determine the main security models suitable to implement in an organization with a distributed architecture.

In the Table I shows the comparison of the different security models proposed, with the purpose of analyzing each of them and being able to determine the most appropriate to apply in a distributed architecture. It is determined that this information is necessary to be able to adopt an adequate security model that allows us to mitigate the security of information.

2.2 Materials

There are several security models, with their different strengths in confidentiality, integrity and authenticity; but for the purposes of the analysis the following were considered [6][8]:

Modelo Bell-LaPadula

The Bell-LaPadula model is the first and most widely used multilevel security model, this model was designed by D.Ellott.Bell and Leanard J.LaPadula in 1973[8]. This model is mainly used to mitigate the problems of confidentiality and control of access to information. In this model the subjects and the objects are classified by security rank, this avoids that the information of a high level can be of access by a subject of low level.

By enforcing a Bell-LaPadula model policy, a subject can have access to an object, if and only if the subject is authorized to access the object by both the multi-level security policy and the control policy discretionary access.

BiBa model

The Biba model was introduced by K. J. Biba in 1977, was the first security model in the field of integrity, it is also a lattice-based access control security model that deals with sensitive information at various levels. In commercial applications, data integrity is more important than confidentiality.

The emphasis of the BiBa model is to protect the integrity of the information system. The main idea is to execute the information flow strategy using mandatory access control to strengthen discretionary access control. In the BiBa model, each subject and object have its own level of integrity. The higher level of data has greater accuracy and reliability than a lower level.

The advantages of the BiBa model are its simplicity and the possibility of combining it with the Bell-LaPadula model. Its implementation is intuitive and easy to understand. It is easily combined with the Bell-LaPadula model to produce an integration security model that can provide both confidentiality security and integrity security[7].

Clark-Wilson Model

The Clark-Wilson model is a model of integrity, which was developed by computer scientists David Clark and accountants David Wilson, published in 1987[9].

The Clark-Wilson model focuses on research and protection, the integrity of information and the system. In the Clark-Wilson model, the user cannot access and control objects directly. An agent program is applied to access the objects in order to protect the integrity of the objects[10].

The main idea of the Clark-Wilson model is to use a benign transaction processing mechanism and a separation of tasks mechanism to guarantee the consistency of the data and the integrity of the transaction. The benign transaction processing mechanism means that the processing of information must be restricted in certain privileges and ranges. Users cannot process data arbitrarily. The task separation mechanism divides a task into subsets of different tasks. Each subset must be finished by at least two people. Although the Clark-Wilson model is a bit complex and cannot provide effective confidentiality protection, it is the origin of integrity strategies and integrity mechanisms. There are three goals of integrity protection:

1. Prevent unauthorized users from modifying the data.
2. Maintain the consistency of the data.
3. Prevent authorized users from modifying data in an unauthorized manner.

The Clark-Wilson model is the only integrity model that achieves these three objectives. The Clark-Wilson model is designed for the business environment and is generally used to protect the integrity of data in the banking system. It is a good model for business applications.

Chinese Wall Model

The China Wall model is proposed as a solution to mitigate the risks associated with the loss of information security[11]; the basis of the model is that it provides an information barrier designed to mitigate the conflict of interest problem in the organization. This model has been applied to different scenarios where there may be a conflict of interest.

The model builds a conceptual wall to avoid leakage of privileged information. The idea behind this model is similar to that of a personal firewall in a computing environment. The firewall is a security system designed to allow or deny communications based on a certain security policy. The personal firewall is not holistic, but selective in the information it protects. Similarly, the China Wall model is designed to limit the dissemination of confidential information to unauthorized persons in a given circumstance. In one circumstance, an individual may have a conflict of interest, but in another, he may not execute.

TABLE I. SECURITY MODELS.

Models	Objective	Field of application	Advantage	Disadvantage
Bell-LaPadula	Confidentiality	Military	Strict security classification	Does not consider integrity
BiBa	Integrity	Versatility	Simplicity and possibility of	Does not consider confidentiality

			combination	
Clark-Wilson	Integrity	Business	Triple integrity protection	Does not consider confidentiality
Chinese Wall	Access control	Business	Access flexibility	Does not consider integrity

As shown in table I, the comparison of these models helps to evaluate the strengths and weaknesses of each of them, it also manages to identify the best performance environment for its application.

3. Results

The results obtained in this phase are the following:

1. Consider the security models analyzed previously for possible future implementation in an organization with distributed architecture, to mitigate information security problems.
2. It was obtained in this research phase is a prototype of a security model based on the characteristics of the BiBa and Bell-Lapadula model; as an alternative to improve the integrity, confidentiality and authenticity of the information in a distributed environment.

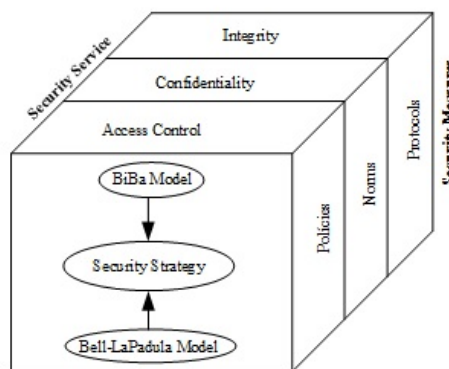


Fig. 1 Prototype security model

4. Discussion

In a distributed architecture it is necessary to adopt a security model to mitigate information security problems; It depends on the mission, vision and strategic objectives of the organization to determine the appropriate security model for its implementation.

The base models considered for adoption in a new prototype security model are based on the BiBa and Bell-Lapadula model, since their merged features offer a model with integrity, confidentiality and authenticity; which can be considered as an alternative to improve the security of information.

To mitigate threat problems, information security vulnerabilities in a distributed architecture, security policies, security models, rules, protocols, and appropriate security algorithms must be defined.

It is concluded that it is necessary to have an adequate security model that adjusts to the operational, tactical and strategic objectives of the organization to improve the confidentiality, integrity and authenticity of the information.

5. Future Work and Conclusions

Take as reference the proposed BBLP model; to help in future analyzes or possible implementations as an alternative to a security model.

It is concluded that it is necessary to have an adequate security model that adjusts to the operational, tactical and strategic objectives of the organization to improve the confidentiality, integrity and authenticity of the information; based on the Biba model, Bell-LaPadula, China Wall, Crak Wilson among others.

Acknowledgment

The authors thank CUCEA of Universidad de Guadalajara, Jalisco, México, Program IT PhD Information Technologies, Universidad Politécnica Salesiana del Ecuador, to the research group of the Guayaquil Headquarters "Computing, Security and Information Technology for a Globalized World" (CSITGW) created according to resolution 142-06-2017-07-19 and Secretaria de Educación Superior Ciencia, Tecnología e Innovación (Senescyt).

References

- [1] T. Lu, X. Guo, L. Zhao, Y. Li, and P. Lin, "An Analysis of Sensitive Information System Security Models," 2014 7th Int. Conf. Secur. Technol., pp. 22–25, 2014.
- [2] Ú. Erlingsson, "Data-driven software security: Models and methods," 2016.
- [3] J. Jin and M. Shen, "Analysis of Security Models Based on Multilevel Security Policy," Manag. e-Commerce e-Government (ICMeCG), 2012 Int. Conf., pp. 95–97, 2012.
- [4] V. G. Promyslov, "Assessment of the security architecture of control system using discretionary security models," Proc. 2017 10th Int. Conf. Manag. Large-Scale Syst. Dev. MLSD 2017, pp. 1–4, 2017.
- [5] P. Xu, M. Chen, L. Feng, G. Wu, F. Ma, and D. Wang, "An application security model based on business process in information system," 2017 12th Int. Conf. Intell. Syst. Knowl. Eng., pp. 1–4, 2017.
- [6] X. Hu, Y. Zhuang, Z. Cao, T. Ye, and M. Li, "Modeling and Validation for Embedded Software Confidentiality and Integrity," 2017.
- [7] S. Schinagl, R. Paans, and K. Schoon, "The revival of ancient information security models, insight in risks and selection of measures," Proc. Annu. Hawaii Int. Conf. Syst. Sci., vol. 2016-March, no. 1, pp. 4041–4050, 2016.
- [8] G. Zhao and D. W. Chadwick, "On the modeling of Bell-LaPadula security policies using RBAC," Proc. Work. Enabling Technol. Infrastruct. Collab. Enterp. WETICE, pp. 257–262, 2008.
- [9] Q. Xu and G. Liu, "Configuring Clark-Wilson integrity model to enforce flexible protection," CIS 2009 - 2009 Int. Conf. Comput. Intell. Secur., vol. 2, no. 1, pp. 15–20, 2009.
- [10] M. Al-kofahi, S. Chang, and T. E. Daniels, "SCWIM An Integrity Model for SOA Networks," in 2008 IEEE International Conference on Web Services, 2008, pp. 675–682.
- [11] S. Rama, S. V. Flowerday, and D. Boucher, "Information confidentiality and the Chinese wall model in government tender fraud," 2012 Inf. Secur. South Africa - Proc. ISSA 2012 Conf., 2012.