**Review of Computer Engineering Research**
*2016 Vol.3, No.4, pp.65-68*
*ISSN(e): 2410-9142*
*ISSN(p): 2412-4281*
*DOI: 10.18488/journal.76/2016.3.4/76.4.65.68*


# ANALYSIS OF SUITABLE SECURITY PROTOCOLS FOR APPLY A MODEL OF IDENTITY IN THE CIVIL REGISTRY OF ECUADOR

**Moisés Toapanta[1] --- Enrique Mafla[2] --- José Orizaga[3]**
*[1]Computer Science Department, Universidad Politécnica Salesiana del Ecuador Chambers 227 and 5 of Junio, Guayaquil, Ecuador*
*[2]Bachelor in Engineering Systems, Escuela Politécnica Nacional Ladrón de Guevara E11-253, Quito, Ecuador*
*[3]Information Systems Department CUCEA, Universidad de Guadalajara Periférico Norte N° 799, Núcleo Universitario Los Belenes, C.P. 45100, Zapopan, Jalisco, México*

## ABSTRACT

*Different security protocols were analyzed are used for a centralized database with distributed architecture. The goal is identify adequate security protocols to mitigate the security of information through identity of a model without relying on technological infrastructures. In this phase the suitable security protocols for a model of identity authentication, authorization and auditing (AAA) was analyzed. Deductive method is used in exploratory research to analyze security protocols more used among the main mentioned: Feret, Kerberos, Radius, Dnssec, Ipsec, Pgp, Secure Rpc, Set, Ssl, Tls, Maille, Eap, Pap, Map, Diameter, Peap, among others. It turned out that security protocols should be adopted on a model of identity for a centralized data base. It was concluded that protocols and security algorithms must have a direct relation to the identity model; allowing mitigate the vulnerabilities and risks considering To mitigate the threats and risks of information with confidentiality, integrity and availability. The technological infrastructure should not influence the implementation of different security protocols.*

**Keywords:** Security protocols, Algorithms, Models of identity, Authentication, Authorization.

**Received:** 3 October 2016/ **Revised:** 3 November 2016/ **Accepted:** 23 November 2016/ **Published:** 7 December 2016

## Contribution/ Originality

This paper provides the first analysis to adopt appropriate security protocols for an identity model with authentication, authorization and auditing without relying on specific technological infrastructure for Ecuador's civil registry; in a distributed architecture database. Different civil registries of the world with similar characteristics can refer this research project.

## 1. INTRODUCTION

The civil registry of Ecuador is part of the Public Data Center authorized to deliver information to people at different public and private organizations as: Internal Revenue Service, the National Electoral Council, Secretary of Education, organizations linked to the Ecuadorian state at national and international level. The information available is incompatible with serious problems of confidentiality, integrity and availability for this reason requires a management system trustworthy compliance with international standards [1]. It is considered information paper "Analysis to define management of identities access control of security processes for the registration civil from Ecuador" [2]. For this reason and because the information is strategic; The National Assembly of the Republic of Ecuador in the official gazette supplement 684 of 4 February 2016 It promotes a new Law for the administration of data of the civil registry according article six literal two says: Promote, in coordination with the governing body of



† Corresponding author

Science, Technology and Innovation and other public and private institutions, scientific and technological research to strengthen the management of identity and civil registration data [3]. Prior to the creation of the conceptual model is reviewed. For this reason, as a doctoral student in Information Technology at the University of Guadalajara; at this stage performed the analysis of appropriate security protocols to implement the model of identity in the Civil Registry of Ecuador that it was created [4].

Because it is necessary to apply appropriate security protocols to model civil registration identity Ecuador? For security protocols considered are not dependent on a specific technology infrastructure and mitigate the security of the database.

The aim is to perform the analysis and consider appropriate security protocols to mitigate the security of information using a conceptual model in a distributed architecture environment.

### 1.1. The Revised paper in this Phase are as Follows

Security analysis of civil registry database of Ecuador [1]. Analysis to define management of identities access control of security processes for the registration civil from Ecuador [2]. We analyze the Conceptual model for identity management to mitigate the database security of the registry civil of Ecuador [4]. Communication protocols used in Cloud Computing [5]. Image reduction operators based on non-monotonic averaging functions [6]. Biometric-Kerberos authentication scheme for secure mobile computing services [7]. Analysis, Implementation and Extensions of RADIUS Protocol [8]. Research of Mobile IPv6 Application Based On Diameter Protocol [9]. Formal verification of PAP and EAP-MD5 protocols in wireless networks: FDR model checking [10]. Implementation of network access control by using authentication, authorization and accounting protocols [11]. Redalyc. La consumer protection in electronic payment transactions [12]. Parameterization of IPsec framework for security in the smart grid interoperability [13]. The Maille authorization - a distributed, redundant authorization protocol [14].

Deductive method is used in exploratory research to analyze the security protocols used between the main mentioned: Feret, Kerberos, Radius, Dnssec, Ipsec, Pgp, Secure Rpc, Set, Ssl, Tls, Maille, Eap, Pap, Map, Diameter, Peap, among others.

It turned out that security protocols should be adopted on a model of identity for a centralized data. It was concluded that protocols and security algorithms must have a direct relation to the identity model; allowing mitigate the vulnerabilities and risks considering information confidentiality, integrity and availability (CIA); without relying on specific technological infrastructures.

### 1.2. Relate Works

SSL (Secure socket layer) is a "protocol that provides authentication and data privacy between extremes over the Internet using cryptography" SSL involves a number of basic steps such as negotiated between the parties, exchange of public keys and authentication and encryption of traffic and TLS (Security of the transport layer) are much improved "cryptographic protocols that provide secure communications over a network" with the only difference that TLS is a version [5]. Reret Image reduction is a crucial task in image processing, underpinning many practical applications. Reret Image reduction is a crucial task in image processing, underpinning many practical applications. The text emphasizes operators to improve the images. The technique of penalty function minimization is used to derive a novel mode-like estimator capable of identifying the most appropriate pixel value for representing; considering the original image defined. The aggregation function and several robust location estimators are objectively evaluated by considering a facial image to determine the task for recognition. The FERET evaluation protocol is applied to confirm that these non-monotonic functions are able to sustain task

performance compared to recognition using non-reduced images, as well as significantly improve performance on query images corrupted by noise. The technique of image reduction with aggregation functions improves the efficiency and accuracy of the information according to the practical results in the vision by computers [6]. One of the security protocols for authentication is Keberos under the client server philosophy using secure connections. After the identity authentication, client and server can encrypt all of subsequent communications to ensure privacy and data integrity [7]. RADIUS is a security protocol that provides authentication, authorization and accounting and is used to configure corporate networks; To guarantee the identity, confidentiality, integrity and availability of information. However, it has a set of vulnerabilities that are either caused by the protocol, or caused by poor implementation and exacerbated by the protocol [8]. The Diameter security protocol has authentication, authorization and accounting. This protocol is oriented to apply in IPv6 to mitigate the security of the information [9]. The MAP (Membership Authentication Protocol) and MAP (Membership Authentication Protocol) protocols are safe, the two protocols are efficient to provide mutual authentication [10]. In the system achieved: three authentication methods using EAP-TLS, PEAP and EAP TTLS; secure management of information concerning the users who can access the network and the permissions that each possesses; the use of digital certificates to prove the identity of a user or a computer running any of the most popular operating systems [11]. SET (Secure Electronic Transactions) One of the first protocols specifically designed to protect online payments was SET (Secure Electronic Transactions). This protocol was implemented by large companies owning the card brands (Visa and Masterd Card), with the purpose of providing security for payment by credit card. To guarantee the inviolability of messages transmitted, the transaction provides security, preventing access to the data associated with the card, fraudulent [12]. IPsec (Internet Protocol security) The objective of security of data interoperability in smart grid, according to the levels of demand for security services: integrity, confidentiality and availability [13]. The Maille security protocol provides efficient authorization security for organizations at the corporate level where technology infrastructures are available under a distributed environment. Service owners distribute their access control lists across the network using threshold cryptography [14].

## 3. RESULTS

1. It turned out that security protocols should be adopted on a model of identity for a centralized data.
2. The revised security protocols considered can be applied in any conceptual identity model to mitigate information security [4].
3. The analysis of security protocols to mitigate information security is determined that each protocol must adopt the independent model to the technological infrastructure.

### 3.1. Future Work and Conclusion

Adopt adequate security protocols; for an architecture distributed in the civil registry database of Ecuador to mitigate the security of the information; Without losing the principles of identity, authentication, authorization, auditing (IAAA) with confidentiality, integrity and availability (CIA).

It was concluded that protocols and security algorithms must have a direct relation to the identity model; allowing mitigate the vulnerabilities and risks considering information confidentiality, integrity and availability (CIA); without relying on specific technological infrastructures.

Funding : Universidad Politécnica Salesiana del Ecuador Sede Guayaquil
Competing Interests: The authors declare that they have no competing interests.
Contributors/Acknowledgement: The authors thank the CUCEA of Universidad de Guadalajara, Jalisco, México, Program IT PhD Information Technologies, Universidad Politécnica Salesiana del Ecuador and Secretaria de Educación Superior Ciencia, Tecnología e Innovación (Senescyt).

## REFERENCES


[1] P. D. Student, S. Moisés, T. Toapanta, P. D. Luis, and E. Mafla, "Security analysis of civil registry database of ecuador," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). "Special Section Computer Science/Networking". IEEE Catalog*, Chennai – India, 2016, pp. 1024–1029.

[2] T. J. O. Moisés and E. Mafla., "Analysis to define management of identities access control of security processes for the registration civil from Ecuador," in *2016 IEEE International Smart Cities Conference (ISC2) - IEEE ISC2 2016- Privacy and Security Track. IEEE Catalog*, Trento – Italy, 2016, pp. 122-125.

[3] R. O. S. De, H. Del, P. Barrezueta, D. E. L. E. Y. Organica, D. E. G. D. E. La, and I. Y. Datos, "Ley orgánica de gestión de la identidad y datos civiles," Quito- Ecuador, 2016.

[4] M. Toapanta, E. Mafla, and J. Orizaga, "Conceptual model for identity management to mitigate the database security of the registry civil of Ecuador," in *Materials Today: Proceedings Tracks "Computer Science/Networking". ISSN 2214-7853. Indexed in Scopus (Elsevier) and the CPCI (Thomson Reuters, Web of Science). Impact SJR*, United Kingdom, 2016.

[5] C. M. Quispe and P. D. E. Red, "Protocolos de comunicación utilizados en cloud computing," Revista de Información, Tecnología y Sociedad2012.

[6] W. Tim, "Image reduction operators based on non-monotonic averaging functions," *IEEE Xplore*, 2013.

[7] A. Han, "Biometric-Kerberos authentication scheme for secure mobile computing services," presented at the Image and Signal Processing (CISP), 2013 6th International Congress on, 2013.

[8] J. Feng and X. Coll, "Analysis, implementation and extensions of RADIUS protocol," presented at the Networking and Digital Society, 2009. ICNDS '09. International Conference on, 2009.

[9] D. Wei, Y. Liu, X. Yu, and X. Li, "Research of mobile IPv6 application based on diameter protocol," presented at the Computer and Computational Sciences, 2006. IMSCCS '06. First International Multi-Symposiums, 2008.

[10] G. K. Lee and J. Y. Choi, "Formal verification of PAP and EAP-MD5 protocols in wireless networks," presented at the Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference, 2004.

[11] J. R. Arana, A. V. Leandro, and P. Oscar, "Implementation of network access control by using authentication, authorization and accounting protocols," *Ingeniería y Competitividad*, vol. 15, pp. 127-137, 2013.

[12] R. Carrillo, "Redalyc. La consumer protection in electronic payment transactions," *Electron. Stud. Teleprocessing*, vol. 6, pp. 33-49, 2007.

[13] V. Neumann, C. L. Gomes, C. Unsihuay-Vila, K. V. Fonseca, and P. R. Torres, "Parameterization of IPsec framework for security in the smart grid interoperability," presented at the Innovative Smart Grid Technologies Latin America (ISGT LATAM), 2015 IEEE PES, 2015.

[14] A. Fritz and J. F. Paris, "Maille authorization - A distributed, redundant authorization protocol," in *Performance, Computing, and Communications Conference, 2006. IPCCC 2006. 25th IEEE International Date of Conference*, 2006.