Choose the Safety Element of SecFuNet

Davi Teles*; André dos Santos; Luiz G. M. Barbosa; Davi S Boger
davi.teles@insert.uece.br
Ceara State University – Information Security Research Team (INSERT) – Fortaleza, CE - Brazil

***Abstract — With increasing accessibility to media and the emergence of new technologies that support these media, is going one increases the supply and demand for online services.* Thus, these services need to ensure the safety and privacy of its customers and to give such guarantees them the services they need to identify and authenticate clients. With this, the project SecFuNet - Security fo Future Networks aims to provide an architecture for managing secure communications between machines connected to a cloud environment using virtual networks. The proposed architecture will provide solutions for the management of secure communication among all the machines connected to the cloud using virtual networks. This work contributes to the SecFuNet, choosing the security element for secure authentication and secure identification of users and customers. We used a methodology divided into two parts: a literature search and applied research of authentication technologies.**

***Keywords*—**Security. Authentication.Identification. SecFuNet.

I. INTRODUCTION

The accessibility to means of communication came with the emergence of new technologies that support the same: 3G, wifi, smartphones, notebooks, tablets, easy internet access. With this, the supply and demand for online services is growing considerably. Many of these services implement and control the access of their clients, who usufrem service, and users, those who manage the service.

There are three main techniques for performing authentication of an identity: What you know: using information that only the customer possesses; What you are: using a unique physical characteristic of the client; What you have: through something only the customer possesses.

Keeping this in view, the project SecFuNet (Security for Future Networks) proposes the development of a framework able to provide secure authentication, secure ID, secure transfer of data, secure infrastructure for virtualized networks and privacy in virtual networks and cloud environments . This development will explore techniques based on security tokens, resource management, intrusion-tolerant algorithms and cryptographic protocols. This framework will be achieved through the design and development of a coherent architecture for virtual networks and access the clouds.

To choose the security element of SecFuNet, a comparison was made between theoretical authentication technologies, leading three authentication techniques introduced and these technologies meet the security requirements of the project.

II. THEORETICAL FOUNDATION AND APPLIED RESEARCH

In literature a study was made of the best and most used solutions for identification, authentication and authorization. To achieve the goal of the research we used the following scientific basis: IEEE, ACM and SBC, as well as site specialist companies. After that, a comparison was made between the theoretical technologies, which enabled us to identify issues related to compatibility of technologies to the needs required by SecFuNet:.

The technologies which were compared: Static Password(What you know?), Biometrics(What you are?), One Time Password (What you have?) and Smart Cards(What you have). This comparison was generated the following table, where the column Encryption Algorithm indicates that the technology is compatible with advanced encryption algorithms, the column Hardwareindicates whether the technology requires specific hardware to run, the column Inviolability indicates whether technology has mechanisms inviolability and expense column indicates: 0 - do not need extra hardware; $ - extra hardware affordable; $ $ - expensive extra hardware cost.

	Encryption Algorithm	Hardware	Inviolability	Costs
Static Password	X			0
Biometrics	X	X		$$
One Time Password	X	X		$
Smart Cars	X	X	X	$

Based on the comparison table and bibliographical research, tests were performed with Smart Cards, as this proved best in this first work stage. The tests were performed with Smart Card: HTTP authentication and HTTPS, HTTP and HTTPS authentication and OpenID + time measurement card access

III. CONCLUSION

The Smart Card technology has proven to be better able to meet the security requirements of the project SecFuNet. Therefore, this work helped the project in choosing your safety element. Thanks to CNPq for the support to the research through the ICT – EU Brazil Coordinated Call (FP7-ICT-2011-EU-Brazil).

REFERENCES

[1] CHAN, Cheng L.M. Chi-Kwong. Cryptanalysis Of A Remote User Authentication Scheme Using Smart Cards. IEE Transactions on Consumer Electronics, IEEE, v. 46, n. 4, p. 992–993, nov. 2000.

[2] KIM HONG-WOO LEE, Lee & Jun. A Design of One Time Password Mechanism using Public Key Infrastructure. Fourth International Conference on Networked Computing and Advanced Information Management, IEE, n. 1, p. 18–24, ago. 2008.