A Secure Architecture for the Future Internet

André dos Santos; Luiz G. M. Barbosa*; Davi Teles;
Ceara State University – Information Security Research Team (INSERT) – Fortaleza, CE - Brazil

***Abstract*—Designed in a primarily reliable environment, the Internet today has weaknessess in parts of its arcihtecture so that the entire network suffers the consequences resulting from attacks ranging from the exploit of software failures to denial of service attacks. The future Internet will strongly rely on virtualization and cloud computing. Thus, one of the main challenges of this new scenario will be to provide a high level of security to accesses to virtual networks and to the cloud. This work introduces a general architecture for a framework that will meet the requirements of the future Internet through the exploration of techniques such as the use of secure microcontrollers (smart cards), resource management, tamper-resistant algorithms and cryptographic protocols.**

***Keywords*—**Security. Future Networks. Smart cards. SecFuNet.

I. INTRODUCTION

The Internet today doesn't satisfy the expectations of what could be called a reliable communication infrastructure [1]. Despite of its success with the end-to-end data transfer, the current Intenet was designed in a primarily reliable environment without much consideration about security, thus weaknessess in parts of its architecture makes the entire network suffers the consequences resulting from attacks ranging from the exploit of software failures to denial of service attacks. As a result, network security has been in the basis of several research activities, both in industry and academy [1][2]. Researchers are divided in those who advocate changes in the existing infrastructure and those who aim to develop a new infrastructure from the ground up.

The future Internet will strongly rely on virtualization and cloud computing. Thus, one of the main challenges of this new scenario will be to provide a high level of security to accesses to virtual networks and to the cloud. This work introduces a general architecture for a framework that will meet the requirements of the future Internet through the exploration of techniques such as the use of secure microcontrollers (smart cards), resource management, tamper-resistant algorithms and cryptographic protocols. The proposed architecture will ensure security in virtualized environments through the isolation of virtual networks and access control for users and managers. This architecture can be used by the SecFuNet project in order to provide: secure identification and authorization, secure data transfer, a secure virtualized infrastructure and privacy on virtual networks and cloud computing.

II. ARCHITECTURE

The proposed architecture uses a mechanism based on Xen to virtualize network elements and another based on OpenFlow to virtualize network flows in order to provide the isolation between the virtual machines and to create a logical partitioning of the physical network. Smart cards will be used to authenticate users and managers. Each user owns his/hers device and, at the server side, there is a grid of smart cards completing the proccess and a load balance to distribute the incoming load. Those smart cards will hold users' atributes and implement the EAP-TLS protocol in order to generate security tokens. The identity management is based on OpenId and the users have the possibility to keep more than one identity inside the smart card. Thus all the authentication-related operations will occur inside a secure element and no user's information will travel through the network in an unsafe way.

Through the combination of replication with diversification the architecture reaches a level of intrusion tolerance. The resilience mechanisms will be improved by self-healing mechanisms based on reactive and proactive approaches.

III. CONCLUSION

Through the exploration of techniques such as the use of smart cards, resource management, tamper-resistant algorithms and cryptographic protocols it's possible to ensure secure identification and authorization, secure data transfer, a secure virtualized infrastructure and privacy on virtual networks and cloud computing.

ACKNOWLEDGMENTS

Thanks to CNPq for the support to the research through the ICT – EU Brazil Coordinated Call (FP7-ICT-2011-EU-Brazil).

REFERENCES

[1] BELLOVIN, S.M. et al. A Clean-Slate Design for the Next-Generation Secure Internet. 2005. Report for NSF Global Environment for Network Innovations Workshop.

[2] BADRA, M.; URIEN, P. Adding identity protection to eap-tls smart cards. In: Proceedings of Wireless Communications and Networking Conference. Hong Kong, China: IEEE, 2007. p.
2951–2956.