Implementation of a Customizable Security-Aware Virtual Network

Bernardo de C. V. Camilo and Luís Henrique M. K. Costa
Universidade Federal do Rio de Janeiro - GTA/COPPE - Rio de Janeiro, Brazil

***Abstract*—In this paper, we briefly describe the implementation of a feature that allows the FITS testbed to create secure virtual networks using different ciphers and cipher modes with it. The aim of this work is to provide an easy way to manage a virtual network cryptography, allowing the testbed users to perform several tests related to network security inside the FITS testbed.**

I. Introduction

Nowadays, future internet research is still a very debated topic. Along with it, several experiments on new architectures are being conducted. However, most of these proposals are restricted to controlled environments, such as simulations or local area networks. FITS[1][1] (Future Internet Testbed with Security) provides a testbed infrastructure for network experimentation based on two different virtualization approaches, Xen[2] and OpenFlow[3]. Users can run their experiments in different network environments in order to compare the results or to choose the more suitable one for their new protocols and mechanisms [5] in a more realistic large-scale environment.

This paper describes the implementation of a new feature of FITS that allows the user to choose between all the ciphers and cipher modes available within OpenVPN[4] (used to create the testbed infrastructure's Virtual Private Network) in his own virtual network. This is an important addition for those users who need to conduct security-related tests, since it allows the user to easily deploy a virtual network with different ciphers in its virtual links. Furthermore, it will help users to compare the performance between the different security levels and let them choose the most suitable combination for their applications. The management of this feature is handled by a simple and intuitive web interface using HTML5 and Javascript.

II. Implementation

To implement this feature, different technologies and protocols were put together. The first step of this implementation was to create a Xen disk image with OpenVPN pre-installed. FITS interconnects islands (a local set of nodes) from all institutions participating in it via Virtual Private Network (VPN) connections and Generic Routing Encapsulation (GRE) tunnels to emulate layer-2 links over the Internet, as depicted in Figure 1 (more information about the operation of FITS can be found in [1]). If we want to create a virtual network with encrypted links, we should use the modified Xen disk image and each virtual node will be either an OpenVPN server or client. With this setup, we'll have a VPN in the virtual network created by the user, allowing us to choose the cipher, independently of the one that is being used in the FITS infrastructure's VPN connections, used to securely interconnect FITS islands across the Internet.

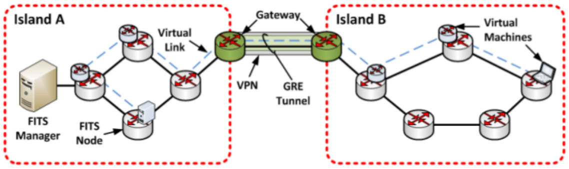

Fig. 1. FITS autonomous island interconnection architecture [5]

All the network configuration is automatically set through scripts written in Python and the user can easily interact through the user interface (UI), developed in HTML5 and Javascript. The UI provides a graphical representation of the FITS nodes and links (similar to the current one). To create a new virtual network with the possibility to manipulate the cryptography in its links, the user will need to select a custom image for the virtual routers (Xen disk image with OpenVPN) and then click on a FITS node to deploy a virtual node. After deploying the virtual nodes, the user will create virtual network links and then, finally, choose the desired cipher and cipher mode by just clicking on the links. Both scripts and the UI are currently under development and will be incorporated in FITS in the near future.

III. Conclusion

The addition of the type of security a virtual link will use is an important addition in terms of flexibility to the FITS testbed. When fully implemented, we will evaluate its usability and we intend also to analyze the performance impact of the different security choices in terms of processing, memory and bandwidth usage. We will also be looking for new additions and features to improve the security of the testbed.

Acknowledgment

This work was supported by CAPES, CNPq, FINEP and FAPERJ.

References

[1] Mattos, D. M. F., Mauricio, L. H., Cardoso, L. P., Alvarenga, I. D, Ferraz, L. H. G., and Duarte, O. C. M. B. - "Uma Rede de Testes Interuniversitária a com Técnicas de Virtualizacao Híbridas", in *Salão de Ferramentas do XXX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos - SBRC'2012*, Ouro Preto, MG, Brazil, May 2012.

[2] Takemura, C., Crawford, L. S. - "The Book of Xen", 312 pp. ISBN-13 978-1-59327-186-2, No Starch Press, October 2009.

[3] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., Turner, J. - "Openflow: Enabling Innovation in Campus Networks", *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69-74, 2008.

[4] Huyghe, S. - "OpenVPN 101: introduction to OpenVPN", Telindus High-Tech Institute, 2004.

[5] Grupo de Teleinformática e Automação (COPPE/UFRJ) - "Future Internet Testbed with Security", http://www.gta.ufrj.br/fits, 2011, [Online; accessed 01-October-2013].

[1] This work was developed under the SecFuNet project.