Authentication and Access Control Architecture for Software Defined Networks

Diogo Menezes Ferrazani Mattos, Otto Carlos Muniz Bandeira Duarte
Universidade Federal do Rio de Janeiro – GTA/PEE/COPPE – DEL/POLI – Rio de Janeiro, RJ – Brasil

***Abstract*—In this work, we propose a host authentication and access control architecture for software defined networks. The key idea is to authenticate at Layer 2, using IEEE 802.1X standard and Extensible Authentication Protocol (EAP). EAP exchanges authentication information between the supplicant host and a RADIUS authentication server. We developed the proposed authenticator as an OpenFlow application on top of POX controller. The authenticator blocks or accepts network traffic from supplicant depending on the authentication success.**

I. Introduction

Deploying new protocols and services in the core of the Internet is rejected by most service providers, due to the high risk that these changes represent for the proper network operation. Future Internet architecture proposals and new protocol experimentation, however, require real-scale and real-traffic testing environments. Network virtualization techniques offer the capability of sharing a physical router between different virtual routers, which are isolated virtual environments with their own operating systems and their own set of applications. Therefore, we develop the Future Internet Testbed with Security (FITS), an experimentation environment based on virtual networks that offers network isolation, secure access, and quality of service differentiation. The virtual network environment allows experimentations of Future Internet proposals by virtualizing routers with Xen and managing data flows with OpenFlow [1].

FITS hosts heterogeneous and untrusted virtual environments, whose vulnerabilities compromise the availability of the testbed resources. FITS aims at providing a secure and isolated infrastructure for experimenting new proposals for the Future Internet. Vulnerabilities may occur in experimental application or even in experimental operating system kernels. Therefore, authenticating and securing access to the virtual infrastructure is an essential challenge for FITS [2]. In this work, we develop an authentication and access control mechanism for FITS network. Each virtual machine in FITS authenticates itself with FITS global controller, a POX[1] application that controls packet forwarding all over the testbed. Authenticator uses IEEE 802.1X and Extensible Authentication Protocol (EAP).

II. Architecture

Our architecture is composed of physical servers, OpenFlow switches, a POX controller, an authenticator and an authentication server. Physical servers are the FITS nodes which host virtual machines. OpenFlow switches forward virtual machine packets. In FITS, the OpenFlow switch is an Open vSwitch[2] instantiated in every physical node. POX controller runs an application that handles all packets of IEEE 802.1X standard and forwards them to the authenticator. Authenticator is a RADIUS client that implements IEEE 802.1X. Our authenticator is an adapted version of `hostapd`, which is a wireless authentication daemon. `Hostapd` was modified to work with POX application to authenticate virtual networks. Finally, the authentication server is a RADIUS server, which authenticates virtual machines through a Lightweight Directory Access Protocol (LDAP) database. The authentication mechanism works as follows. A virtual machine sends an authentication request that is redirected by POX to the authenticator. Then, authenticator replies and the supplicant VM sends its credentials. Authenticator checks VM credentials with the RADIUS server. If credentials are correct, authenticator sends a `success` message to supplicant VM and sends an authorization message to POX through a secure channel, identifying the VM and the successful authentication. After that, POX allows the supplicant VM to access the virtual network. In case of revoking VM credentials, authenticator communicates with POX, which immediately suspends VM access to the network.

[1]POX is an open source OpenFlow controller. It enables to develop Python applications to control an OpenFlow network. POX is available at http://www.noxrepo.org/pox/about-pox/.

[2]http://www.openvswitch.org/.

III. Conclusion

Virtual machines sharing Future Internet Testbed with Security infrastructure are untrusted and may present vulnerabilities even in the operating system kernel. Therefore, providing authentication and access control to FITS is a key challenge. In this work, we propose an architecture that authenticates and controls access to FITS infrastructure based on IEEE 802.1X and RADIUS authentication. The proposed architecture implements a LDAP authentication with RADIUS. Our proposal, however, is extensible to other authentication methods, such as EAP-TLS, which authenticates nodes based on X.509 certificates. Our preliminary results suggest that the authentication architecture prevents unauthorized virtual machines to access virtual network, even when a virtual machine has already authenticated and, then, loses its privileges.

Acknowledgments

The authors would like to thank FINEP, FUNTTEL, CNPq, CAPES, FAPERJ and UOL for their financial support.

References

[1] P. H. Guimarães, L. Ferraz, J. V. Torres, D. Mattos, A. Murillo, M. A. Lopez, I. Alvarenga, C. Rodrigues, and O. C. M. B. Duarte, "Experimenting Content-Centric networks in the future internet testbed environment," in *IEEE International Conference on Communications 2013: IEEE ICC'13 - Workshop on Cloud Convergence: challenges for future infrastructures and services (WCC 2013) (ICC'13 - IEEE ICC'13 - Workshop WCC)*, Budapest, Hungary, Jun. 2013, pp. 1398–1402.

[2] A. K. Nayak, A. Reimers, N. Feamster, and R. Clark, "Resonance: dynamic access control for enterprise networks," in *Proceedings of the 1st ACM workshop on Research on enterprise networking*, ser. WREN '09. Barcelona, Spain: ACM, 2009, pp. 11–18.