Virtual Networks for Cyber Security Testing of Future Internet Proposals

Andrés Murillo, Otto Carlos Muniz Bandeira Duarte
Universidade Federal do Rio de Janeiro - GTA/COPPE - Rio de Janeiro, Brazil

***Abstract*—Testing cyber security in realistic Internet scenarios requires large scale environments. DeterLab is one of the main testbeds for cyber security research. Nevertheless, DeterLab has limited physical resources and users contend to obtain experimental nodes, limiting the scale of possible tests. This paper proposes the use of virtual networks developed in the Future Internet Testbed with Security (FITS) to enhance DeterLab current capabilities.**

I. Introduction

Internet cyber security development emphazises in a reactive approach, risks are insuficiently evaluated at design and implementation phases and security mechanisms are developed as responses to successful attacks. Integration of Internet technologies in critical infrastructures would greatly increase the impact of security attacks. Therefore, better tools to evaluate cyber security and aid the development of security mechanisms during the whole stage of design and implementation are neccesary. Simulation is an alternative to test network topologies and protocols; nonetheless, many risks in cyber security are present in the application layer. Using simulations to model behavior at application layer is a complex and expensive process. Realistic and scalable environments to test cyber security, that represent application layer behavior are necessary

II. Testbeds for Research in Internet of the Future and Cyber Security

Testbeds offer an infrastructure that represents in a realistic way the technologies and protocols under study, because testbeds implement the protocol stack until application level, allowing to test vulnerabilities in specific implementations. The Grupo de Teleinformática e Automação (GTA), in collaboration with other institutions, developed the Future Internet Testbed with Security (FITS). FITS is an open source testbed based in Openflow and Xen virtualization technologies [1]. In FITS Xen virtual machines use OpenFlow to create experimental networks, which makes the testbed compatible with any operating system. The virtualization mechanisms of Xen and OpenFlow guarantee strong isolation between networks [1]. The use of virtual machines allows testing of protocols real behavior and applications under any given kernel supported by Xen.

DeterLab [2] is a cyber security research testbed based in Emulab [3]. DeterLab users describe their experiment with a language that extends Ns-2. After description, users gain root access to a specified node set with a custom operating system. Deterlab provides a safe environment to perform cyber security experiments through the following features: Experiment network topology is built using VLAN tags and a switched network; firewalls are used to ensure that no traffic leaves the experimental network and physical nodes are formatted between experiments. Finally, DeterLab offers an attack and defense tools repository. Nevertheless, DeterLab has limited physical resources that should be shared among testbed users and limits the scale of experiments performed. Large scale scenarios are desired to effectively test cyber security mechanisms in Internet applications against attacks like Denial of Service (DoS) or worm propagation. Also, the only routing algorithm currently supported by DeterLab is OSPF, which limits the type of experiments that can be performed.

III. Virtual Networks Testbed for Cyber Security Research

This paper proposes the integration of virtual networks technologies developed in FITS with DeterLab to enhance its current capabilities. We argue that the integration of Xen virtual routers and software defined networks capabilities of OpenFlow provides the following benefits: i) improve the use of physical resources inside DeterLab, which would enable the creation of large scale experiments that better represent DoS and worm propagation attacks in Internet scenarios, ii) the use of OpenFlow allows to perform cyber security experiments in novel routing protocols, which is not yet possible in DeterLab, iii) the integration of DeterLab repository and environment provides a testbed to test OpenFlow, Xen and in general Future Internet vulnerabilities and risks.

IV. Conclusion and Future Work

We presented the proposal to extend DeterLab current capabilities with the use of FITS technologies to create a cyber security testbed for Future Internet. As future work, we propose an evaluation of OpenFlow performance under DoS experiments and network routing performance of virtual machines sharing the same Deterlab physical nodes.

Acknowledgments

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

References

[1] P. H. V. Guimarães, L. H. G. Ferraz, J. V. Torres, D. M. F. Mattos, A. F. Murillo P., M. Andreoni, I. D. Alvarenga, C. S. C. Rodrigues, and O. C. M. B. Duarte, "Experimenting content-centric networks in the future internet testbed environment," *IEEE International Conference on Communications (ICC)-Workshop on Cloud Convergence*, june 2013.

[2] J. Mirkovic, T. Benzel, T. Faber, R. Braden, J. Wroclawski, and S. Schwab, "The DETER Project: Advancing the Science of Cyber Security Experimentation and Test," in *IEEE International Conference on Technologies for Homeland Security (HST)*, 2010.

[3] C. Siaterlis, A. Garcia, and B. Genge, "On the Use of Emulab Testbeds for Scientifically Rigorous Experiments," *IEEE Communications Surveys Tutorials*, vol. 15, no. 2, pp. 929–942, 2013.