

# Poster: Quantifying the Security Effectiveness of Network Diversity

Huashan Chen  
UT San Antonio

Jin-Hee Cho  
US Army Research Lab

Shouhuai Xu  
UT San Antonio

## ABSTRACT

We propose a systematic, fine-grained metric framework that quantifies the security effectiveness of network diversity in computer networks.

## CCS CONCEPTS

• Security and privacy → Distributed systems security;

## KEYWORDS

Network diversity, security metrics, security quantification

### ACM Reference Format:

Huashan Chen, Jin-Hee Cho, and Shouhuai Xu. 2018. Poster: Quantifying the Security Effectiveness of Network Diversity. In *HoTSoS '18: Hot Topics in the Science of Security: Symposium and Bootcamp, April 10–11, 2018, Raleigh, NC, USA*. ACM, New York, NY, USA, 1 page. <https://doi.org/10.1145/3190619.3191680>

## 1 INTRODUCTION

The risk of employing monoculture software prompts the need of *artificial diversity* via N-version programming [1], which uses multiple, independent versions of software providing a same functionality. On the other hand, market competition leads to the so-called *natural diversity* that multiple software programs offer a same functionality, for instance, Windows and Linux for operating systems, or Chrome, Firefox, and Internet Explorer for browsers. Artificial diversity and natural diversity manifest the broader notion of *network diversity*, such that the software stack (including the application, library, and operating system layers) is diversified in a computer network.

Although the potential value of enforcing diversity in networks is well recognized [4], security effectiveness of enforcing network diversity has yet been quantified. In this work, we propose the first systematic, fine-grained framework for modeling the diversification of software stacks in networks and quantifying the security effectiveness of the network diversity via a suite of security metrics [2]. From our simulation study, we obtain useful insights on the effectiveness of network diversity in dynamic interactions between attackers and defenders [3].

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).  
*HoTSoS '18, April 10–11, 2018, Raleigh, NC, USA*  
© 2018 Copyright held by the owner/author(s).  
ACM ISBN 978-1-4503-6455-3/18/04.  
<https://doi.org/10.1145/3190619.3191680>

## 2 FRAMEWORK

Fig. 1 depicts the framework in terms of: (i) how to abstract an enterprise network, (ii) how to represent vulnerabilities in the software stacks and vulnerabilities of human users; (iii) how to represent defense mechanisms (i.e., software diversity and other defenses); (iv) how to represent attacks against the network; (v) how to define security metrics to measure the outcome of attack-defense interactions; and (vi) how to compute the security effectiveness of software diversity.

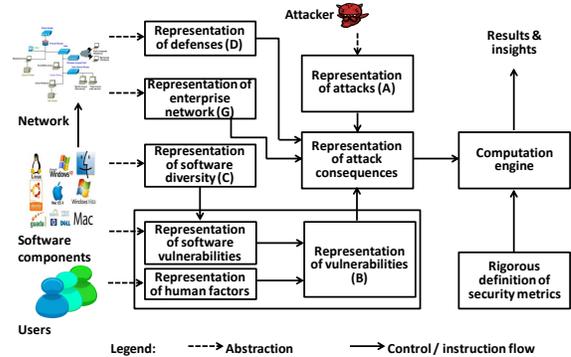


Figure 1: The framework.

Let  $G$  denote an enterprise network,  $A$  denote the attacks against the network,  $B$  denote the vulnerabilities of the network's software systems and human factors,  $C$  denote the software stack configuration of the network,  $D$  denote the defenses to protect the network, and  $M = \{m_i\}$  denote a set of security metrics of interest. The research is to characterize a family of mathematical functions  $f_i$  such that

$$m_i = f_i(G, A, B, C, D).$$

We quantify the security effectiveness of network diversity by comparing the security incurred by software stack configurations, say  $C_1$  and  $C_2$ , respectively. They are given by

$$f_i(G, A, B, C_1, D) \quad \text{and} \quad f_i(G, A, B, C_2, D)$$

for an appropriate  $f_i$  and therefore metric  $m_i \in M$  of interest. We will present some preliminary results on the security effectiveness of network diversity.

## REFERENCES

- [1] A. Avizienis. 1985. The N-version approach to fault-tolerant software. *IEEE TSE* 12 (1985), 1491–1501.
- [2] R. Pendleton, M. Garcia-Lebron, J.H. Cho, and S. Xu. 2016. A Survey on Systems Security Metrics. *ACM Computing Surveys* 49, 4 (Dec. 2016), 62:1–62:35.
- [3] S. Xu. 2014. Cybersecurity Dynamics. In *Proc. HoTSoS'14*. 14:1–14:2.
- [4] Y. Zhang, H. Vin, L. Alvisi, W. Lee, and S. K. Dao. 2001. Heterogeneous networking: a new survivability paradigm. In *Proc. WNSP'01*. ACM, 33–39.