INVITED TALK: A Cyber Mutation: Metrics, Techniques and Future Directions

Ehab Al-Shaer
CyberDNA Research Center
University of North Carolina Charlotte
Department of Software & Information Systems
Charlotte, USA
ealshaer@uncc.edu

ABSTRACT

After decades of cyber warfare, it is well-known that the static and predictable behavior of cyber configuration provides a great advantage to adversaries to plan and launch their attack successfully. At the same time, as cyber attacks are getting highly stealthy and more sophisticated, their detection and mitigation become much harder and expensive.

We developed a new foundation for moving target defense (MTD) based on cyber mutation, as a new concept in cybersecurity to reverse this asymmetry in cyber warfare by embedding agility into cyber systems. Cyber mutation enables cyber systems to automatically change its configuration parameters in unpredictable, safe and adaptive manner in order to proactively achieve one or more of the following MTD goals: (1) deceiving attackers from reaching their goals, (2) disrupting their plans via changing adversarial behaviors, and (3) deterring adversaries by prohibitively increasing the attack effort and cost.

In this talk, we will present the formal foundations, metrics and framework for developing effective cyber mutation techniques. The talk will also review several examples of developed techniques including Random Host Mutation, Random Rout Mutation, fingerprinting mutation, and mutable virtual networks. The talk will also address the evaluation and lessons learned for advancing the future research in this area.

CCS Concepts

•**Security and privacy** → **Formal security models;**

Keywords

Proactive cyber defense; formal security analytics; security metrics

MTD'16 October 24-24 2016, Vienna, Austria

ACM ISBN 978-1-4503-4570-5/16/10.

DOI: http://dx.doi.org/10.1145/2995272.2995285