MTD 2017: Fourth ACM Workshop on Moving Target Defense (MTD)

Hamed Okhravi
MIT Lincoln Laboratory
Lexington, MA, USA
hamed.okhravi@ll.mit.edu

Xinming Ou
University of South Florida
Tampa, FL, USA
xou@usf.edu

ABSTRACT

The fourth ACM Workshop on Moving Target Defense (MTD) is held in Dallas, Texas, USA on October 30, 2017, co-located with the 24th ACM Conference on Computer and Communications Security (CCS). The main objective of the workshop is to discuss novel randomization, diversification, and dynamism techniques for computer systems and networks, new metric and analysis frameworks to assess and quantify the effectiveness of MTD, and discuss challenges and opportunities that such defenses provide. We have constructed an exciting and diverse program of nine refereed papers and two invited keynote talks that will provide the participant with a vibrant and thought-provoking set of ideas and insights.

CCS Concepts/ACM Classifiers

• Security and privacy~Systems security
• Security and privacy~Network security
• Security and privacy~Software and application security
• Security and privacy~Formal security models

Keywords

Moving Target Defenses (MTD), Randomization, Diversification, Dynamism, Cyber Agility, Adaptive Defenses

1 INTRODUCTION

The static nature of current computing systems has made them easy to attack and hard to defend. Adversaries have an asymmetric advantage in that they have the time to study a system, identify its vulnerabilities, and choose the time and place of attack to gain the maximum benefit. The idea of moving-target defense (MTD) is to impose the same asymmetric disadvantage on attackers by making systems dynamic and therefore harder to explore and predict [1, 2]. With a constantly changing system and its ever adapting attack surface, attackers will have to deal with a great amount of uncertainty just like defenders do today. The ultimate goal of MTD is to increase the attackers' workload so as to level the cybersecurity playing field for both defenders and attackers - hopefully even tilting it in favor of the defender.

The MTD'2017 workshop aims to provide a forum for researchers and practitioners in this area to exchange their novel ideas, findings, experiences, and lessons learned.

2 SCOPE

Randomization, diversification, and dynamism can be applied to many different components of a computer system/network and to different layers of its software stack [3]. As a result, MTD covers a broad spectrum of techniques and their associated metrics and analysis frameworks.

Topics of interest include, but not limited to:

- System randomization
- Artificial diversity
- Cyber maneuver and agility
- Software diversity
- Dynamic network configuration
- Moving target in the cloud
- System diversification techniques
- Dynamic compilation techniques
- Adaptive defenses
- MTD quantification methods and models
- MTD evaluation and assessment frameworks
- MTD analytics
- Large-scale MTD (using multiple techniques)
- Moving target in software coding and application API
- Autonomous technologies for MTD
- Theoretical studies on trade-offs of MTD approaches
- Human, social, and usability aspects of MTD
- Other related areas

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.
CCS'17, October 30-November 3, 2017, Dallas, TX, USA.
© 2017 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-4946-8/17/10.
DOI: https://doi.org/10.1145/3133956.3137041

3 WORKSHOP OBJECTIVES

This workshop will bring together researchers from academia, government, and industry to report on the latest research efforts on MTD, and to have productive discussions and constructive debates on this topic.

The fourth MTD workshop will also have a focus on the lessons learned from the past years of research in the area of moving target, and the challenges and opportunities faced by the community moving forward.

4 MTD PROGRAM

The fourth MTD workshop is a one-day pre-conference workshop that will happen in conjunction with the ACM CCS conference. We have two invited keynote speakers. Prof. Paul Van Oorschot (Carleton University, Canada) will talk about science of security and what can be learned from the history of academic literature. Prof. Ahmad-Reza Sadeghi (Technische Universität Darmstadt, Germany) will talk about the effectiveness of system randomization. We will also have an exciting set of nine refereed full papers and two short papers, covering a broad range of topics from code/network/policy/web randomization techniques, to metrics and analysis frameworks, to botnet detection. The presentations will be grouped based on topics.

5 ORGANIZERS

Hamed Okhravi (PC co-chair) is a Senior Staff member at the Cyber Security and Information Sciences Division of MIT Lincoln Laboratory, where he leads programs and conducts research in the area of systems security. His research interests include cyber security, science of security, security evaluation, and operating systems. He is the recipient of 2014 MIT Lincoln Laboratory Early Career Technical Achievement Award and 2015 Team Award for his work on cyber moving target research. He is also the recipient of an honorable mention (runner-up) at the 2015 NSA's 3rd Annual Best Scientific Cybersecurity Paper Competition. He has served as a program committee member for many academic conferences and workshops including ACM Computer and Communications Security (CCS), Network and Distributed Systems Security (NDSS), IEEE Secure Development Conference (SecDev), ACM Asia Conference on Computer and Communications Security (AsiaCCS), Symposium on Research in Attacks, Intrusions, and Defenses (RAID), and International Conference on Applied Cryptography and Network Security (ACNS), among others. Dr. Okhravi earned his MS and PhD in electrical and computer engineering from University of Illinois at Urbana-Champaign in 2006 and 2010, respectively. More information about him can be found at http://okhravi.mit.edu/index.

Xinming (Simon) Ou (PC co-chair) is currently associate professor of Computer Science and Engineering at University of South Florida. He received his PhD from Princeton University in 2005. Before joining USF in fall 2015, he had been a faculty member at Kansas State University since 2006. Dr. Ou's research is primarily in cyber defense technologies, with focuses on human-centered approach to addressing this challenge problem. He also has broad interest and on-going work in cyber-physical system security, intrusion/forensics analysis, moving-target defense, and mobile system security. He is the author of the MulVAL attack graph tool which has been used by Idaho National Laboratory, Defence Research and Development Canada -- Ottawa, NATO, NIST, Thales Groups, General Dynamics, Johns Hopkins University Applied Physics Lab, Swedish Defence Research Agency, Army Research Laboratory, and researchers from numerous academic institutions. Dr. Ou's research has been funded by U.S. National Science Foundation, Department of Defense, Department of Homeland Security, Department of Energy, National Institute of Standards and Technology (NIST), HP Labs, and Rockwell Collins. He is a recipient of 2010 NSF Faculty Early Career Development (CAREER) Award, a three-time winner of HP Labs Innovation Research Program (IRP) award, and 2013 Kansas State University Frankenhoff Outstanding Research Award.

ACKNOWLEDGMENTS

This material is based upon work supported by the Department of Defense under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

REFERENCES

[1] Hamed Okhravi, Thomas Hobson, David Bigelow, and William Streilein. "Finding focus in the blur of moving-target techniques." IEEE Security & Privacy 12, no. 2, pp: 16-26, 2014.

[2] Sushil Jajodia, Anup K. Ghosh, Vipin Swarup, Cliff Wang, and X. Sean Wang, eds. Moving target defense: creating asymmetric uncertainty for cyber threats. Vol. 54. Springer Science & Business Media, 2011.

[3] Hamed Okhravi, Mark Rabe, Travis Mayberry, William Leonard, Thomas Hobson, David Bigelow, and William Streilein. "Survey of cyber moving target techniques." MIT Lincoln Lanoratory, Technical Report No. MIT/LL-TR-1166, 2013.