MTD'20: 7th ACM Workshop on Moving Target Defense

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

Cliff Wang
Army Research Office
Durham, NC, USA
cwnewmail@gmail.com

ABSTRACT

The seventh ACM Workshop on Moving Target Defense (MTD) Workshop is held virtually on November 9, 2020, in conjunction with the 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 network, new metric and analysis frameworks to assess and quantify the effectiveness of MTD, and discuss challenges and opportunities that such defenses provide. New this year the workshop has incorporated a number of invited papers to capture systematization of knowledge (SoK) from experts in this field that investigate the past ten years of MTD and discuss the way forward. We have constructed an exciting and diverse program of three refereed papers, five invited papers, and two invited keynote talks that will provide the participant with a vibrant and thought-provoking set of ideas and insights.

CCS CONCEPTS

• 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

ACM Reference format:

Hamed Okhravi and Cliff Wang. 2020. MTD'20: 7th ACM Workshop on Moving Target Defense. In *Conference on Computer and Communications Security (CCS), November 9-13, 2020, Virtual Event.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3372297.3416244

CCS '20, November 9–13, 2020, Virtual Event, USA
© 2020 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-7089-9/20/11.
https://doi.org/10.1145/3372297.3416244

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 turn an adversary's asymmetric advantage into disadvantage by making systems random, diverse, and 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 significant uncertainty just like defenders do today. The ultimate goal of MTD is to increase the attackers' workload and cost in order to level the cybersecurity playing field for defenders and attackers – ultimately tilting it in favor of the defender.

The MTD'2020 workshop aims to provide a forum for researchers and practitioners in this area to exchange their novel ideas, findings, experiences, and lessons learned. A particular focus this year has been given to systematizing the past decade of MTD work and charting the way forward for the community.

2 SCOPE

Randomization, diversification, and dynamism can be applied to many different components of a computer system/network, and among 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/proactive defenses
- Intelligent countermeasure selection
- MTD strategies and planning
- Deep learning for MTD
- MTD quantification methods and models
- MTD evaluation and assessment frameworks
- Large-scale MTD (using multiple techniques)

- Moving target in software coding, application API virtualization
- Autonomous technologies for MTD
- Theoretic study on modeling trade-offs of using MTD approaches
- Human, social, and usability aspects of MTD
- AI, machine learning, and data analytics related MTD
- Other related areas

3 WORKSHOP OBJECTIVES

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

The seventh MTD workshop will also have a focus on the systematization of knowledge from the past decade of work in the area of moving target, and the way forward for the research community.

4 MTD PROGRAM

The seventh MTD workshop is a one-day pre-conference workshop that will happen in conjunction with ACM CCS. We have two invited keynote speakers. Prof. Ahmad-Reza Sadeghi (Technische Universität Darmstadt, Germany) will talk about contact tracing during the current pandemic and the role of randomization in privacy preservation. Prof. Trent Jaeger (Pennsylvania State University, USA) will talk about static analysis opportunities for improving agile and moving target defenses. We will also have an exciting set of three refereed full papers, and, new for this year, we will have five invited systematization of knowledge papers from experts in this field.

It is our hope that this vibrant and exciting program sparks more debate in our community and charts a vision for the next decade of research in the area of moving target defenses.

5 ORGANIZERS

Dr. 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 cybersecurity, science of security, security evaluation, and operating systems. He is the recipient of the 2019 MIT Lincoln Laboratory's Best Invention Award, 2018 R&D 100 Award, 2015 Team Award, and 2014 MIT Lincoln Laboratory Early Career Technical Achievement Award for his work on cyber moving target research. He is also the recipient of an award at the 2015 National Security Agency's 3rd Annual Best Scientific Cybersecurity Paper Competition. He is an associate editor of the IEEE Security & Privacy journal and has served as the program chair for the MTD workshop and the poster chair of the IEEE SecDev Conference. In addition, he has served as a program committee member for various academic conferences and workshops including ACM CCS, NDSS, RAID, AsiaCCS, ICCAD, MILCOM, ACNS, and the IEEE SecDev. Dr. Okhravi actively contributes to various national, Laboratory, and division-level strategic planning activities, and has led the development of multiple national-level R&D roadmaps. Dr. Okhravi earned his MS and PhD degrees 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://web.mit.edu/ha22286/www/.

Dr. Cliff Wang (PC co-chair) graduated from North Carolina State University with a PhD in computer engineering in 1996. He has been carrying out research in the area of computer vision, medical imaging, high speed networks, and most recently information security. He has authored over 50 technical papers and 3 Internet standards RFCs. Dr. Wang also authored/edited for 18 books in the area of information security and hold 4 US patents on information security system development.

Since 2003, Dr. Wang has been managing extramural research portfolio on information assurance at US Army Research Office. In 2007 he was selected as the chief of the computing sciences division at ARO while in the same time managing his program in cyber security. For the past 17 years, Dr. Wang managed over $200M research funding which led to significant technology breakthroughs. Dr. Wang also holds adjunct professor appointment at both Department of Computer Science and Department of Electrical and Computer Engineering at North Carolina State University. Dr. Wang is a Fellow of IEEE.

ACKNOWLEDGMENTS

This material is based upon work supported by the Under Secretary of Defense for Research and Engineering under Air Force Contract No. 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 Under Secretary of Defense for Research and Engineering.

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] Bryan Ward, Steven Gomez, Richard Skowyra, David Bigelow, Jason Martin, James Landry, and Hamed Okhravi, "Survey of Cyber Moving Targets - Second Edition," Massachusetts Institute of Technology Lincoln Laboratory, Technical Report 1228, 2018