MTD 2016: Third ACM Workshop on Moving Target Defense

Peng Liu
Pennsylvania State University
pliu@ist.psu.edu

Cliff Wang
U.S. Army Research Office
cliff.x.wang.civ@mail.mil

ABSTRACT

The 2016 MTD (Moving Target Defense) workshop seeks to bring together researchers from academia, government, and industry to report on the latest research efforts on moving-target defense, and to have productive discussion and constructive debate on this topic. It is a single day workshop co-located with ACM CCS (Conference on Computer and Communications Security) 2016.

CCS Concepts

• Security and Privacy → Systems security, Network security, Software and application security

Keywords

Moving Target Defense, Cybersecurity

1. BACKGROUND

The static nature of current computing systems has made them easy to attack and harder 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. With a constantly changing system and its ever adapting attack surface, attackers will have to deal with a great deal 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.

2. WORKSHOP GOALS

This workshop seeks to bring together researchers from academia, government, and industry to report on the latest research efforts on moving-target defense, and to have productive discussion and constructive debate on this topic. We solicit paper and system demo submissions on original research in the broad area of MTD, with possible topics such as those listed below. Since MTD research is still in its nascent stage, the list should only be used as a reference. We welcome all works that fall under the broad scope of moving target defense, including research that shows negative results.

- System randomization
- Artificial diversity
- Cyber maneuver
- Bio-inspired defenses
- Dynamic network configuration
- Moving target in the cloud
- System diversification techniques
- Dynamic compilation techniques
- Adaptive defenses
- MTD quantification methods and models
- Large-scale MTD (using multiple techniques)
- Moving target in software coding, application APIs virtualization
- Autonomous technologies for MTD
- Theoretic study on trade-offs of using MTD approaches
- Human, social, and psychology aspects of MTD

3. WORKSHOP PROGRAM FORMAT

The workshop is a single day event co-located with the 2016 ACM Conference on Computer and Communications Security (ACM CCS). We have invited Ehab Al-Shaer of University of North Carolina, Charlotte to give a keynote speech; we have also invited Jason Li of Intelligent Automation, Inc. to serve as the industry speaker. We have received 27 submissions from Asia, Europe, and North America. Out of these submissions, we hope to accept 9 to 12 papers.

4. PROGRAM COMMITTEE

Gail-Joon Ahn (Arizona State University), Massimiliano Albanese (George Mason University), Hasan Cam (U.S. Army Research Laboratory), Ping Chen (Penn State University), Scott A. Deloach (Kansas State University), Robert Erbacher (Army Research Laboratory), Michael Franz (University of California, Irvine), Jason Hamlet (Sandia National Laboratories), Trent Jaeger (Penn State University), Sushil Jajodia (George Mason University), Myong Kang (NRL), Dan dongseong Kim (University of Canterbury New Zealand), Srikanth Krishnamurthy (University of California, Riverside), Christopher Lamb (University of New Mexico), Karl Levitt (University of California, Davis), Jason Li (Intelligent Automation Inc.), Zhuo Lu (University of Memphis), Patrick McDaniel (Penn State University), Sanjai Narain (Applied Communication Sciences), Iulian Neamtiu (University of California, Riverside), Hamed Okhravi (MIT Lincoln Laboratory), Simon Ou (University of South Florida), Vipin Swarup (MITRE), Kun Sun (College of William and Mary), Jason Syversen (Siege Technologies), Michael Wellman (University of Michigan), Minghui Zhu (Penn State University).

5. ACKNOWLEDGMENTS

We thank all authors who submitted papers. We thank the program committee members and additional reviewers for their great effort towards a strong program. We are also very grateful to the invited speakers for their presentations. Finally, we thank the ACM CCS organizers, particularly the workshop chairs Mathias Payer and Stefan Mangard for their support and help.

CCS'16, October 24-28, 2016, Vienna, Austria
ACM 978-1-4503-4139-4/16/10.
http://dx.doi.org/10.1145/2976749.2990483