Dynamic Defense against Adaptive and Persistent Adversaries

Radha Poovendran
University of Washington
Seattle, WA 98195
rp3@uw.edu

ABSTRACT

This talk will cover two topics, namely, modeling and design of Moving Target Defense (MTD), and DIFT games for modeling Advanced Persistent Threats (APTs). We will first present a game-theoretic approach to characterizing the trade-off between resource efficiency and defense effectiveness in decoy- and randomization-based MTD. We will then address the game formulation for APTs. APTs are mounted by intelligent and resourceful adversaries who gain access to a targeted system and gather information over an extended period of time. APTs consist of multiple stages, including initial system compromise, privilege escalation, and data exfiltration, each of which involves strategic interaction between the APT and the targeted system. While this interaction can be viewed as a game, the stealthiness, adaptiveness, and unpredictability of APTs imply that the information structure of the game and the strategies of the APT are not readily available.

Our approach to modeling APTs is based on the insight that the persistent nature of APTs creates information flows in the system that can be monitored. One monitoring mechanism is Dynamic Information Flow Tracking (DIFT), which taints and tracks malicious information flows through a system and inspects the flows at designated traps. Since tainting all flows in the system will incur significant memory and storage overhead, efficient tagging policies are needed to maximize the probability of detecting the APT while minimizing resource costs. In this work, we develop a multi-stage stochastic game framework for modeling the interaction between an APT and a DIFT, as well as designing an efficient DIFT-based defense. Our model is grounded on APT data gathered using the Refinable Attack Investigation (RAIN) flow-tracking framework. We present the current state of our formulation, insights that it provides on designing effective defenses against APTs, and directions for future work.

CCS Concepts/ACM Classifiers

• Security and privacy~Formal methods and theory of security
• Security and privacy~Network security

Author Keywords

Moving target defense; advanced persistent threats; game theory; dynamic information flow tracking

MTD '18, October 15, 2018, Toronto, ON, Canada

ACM ISBN 978-1-4503-6003-6/18/10.
https://doi.org/10.1145/3268966.3268977

BIOGRAPHY

Radha Poovendran is professor and chair of the Department of Electrical Engineering at the University of Washington. He is the founding director of the Network Security Lab and is a founding member and associate director of research for the UW's Center for Excellence in Information Assurance Research and Education. He has also been a member of the advisory boards for Information Security Education and Networking Education Outreach at UW. In collaboration with NSF, he served as the chair and principal investigator for a Visioning Workshop on Smart and Connected Communities Research and Education in 2016.

Poovendran's research focuses on wireless and sensor network security, adversarial modeling, privacy and anonymity in public wireless networks and cyber-physical systems security. He co-authored a book titled Submodularity in Dynamics and Control of Networked Systems and co-edited a book titled Secure Localization and Time Synchronization in Wireless Ad Hoc and Sensor Networks. He is also an associate editor for ACM Transactions on Sensor Networks.

Poovendran is a Fellow of IEEE and has received various awards including Distinguished Alumni Award, ECE Department, University of Maryland, College Park, 2016; NSA LUCITE Rising Star 1999; NSF CAREER 2001; ARO YIP 2002; ONR YIP 2004; PECASE 2005; and Kavli Fellow of the National Academy of Sciences 2007.

ACKNOWLEDGMENTS

This work is in collaboration with Dinuka Sahabandu, Shana Moothedath, and Linda Bushnell at University of Washington,

Sangho Lee and Wenke Lee at Georgia Institute of Technology, and Andrew Clark at Worcester Polytechnic Institute. We also thank J. Sukarno Mertoguno at ONR for technical discussions and feedback. This work is supported by ONR grant N00014-16-1-2710 and DARPA grant FA8650-15-C-7556.

REFERENCES

1. D. Sahabandu, B. Xiao, A. Clark, S. Lee, W. Lee, and R. Poovendran, "DIFT Games: Dynamic Information Flow Tracking Games for Advanced Persistent Threats," IEEE Conference on Decision and Control (CDC), Miami, FL, December 2018.
2. S. Moothedath, D. Sahabandu, A. Clark, S. Lee, W. Lee, and R. Poovendran, "Multi-Stage Dynamic Information Flow Tracking Game," IEEE Conference on Game and Decision Theory for Security (GameSec), Seattle, WA, October. 2018