Security and Communication Networks

Special Issue on
Moving Target Defenses

CALL FOR PAPERS

The static nature of computing systems has traditionally created an asymmetry between attackers and defenders. Attackers can exploit one or a small number of vulnerabilities to compromise, in some cases millions of machines that have the same internals, while defenders should protect against a myriad of attacks and vulnerabilities. This has created an imbalance in favor of attacks. Moving Target (MT) defenses seek to rebalance cybersecurity in favor of defense by incorporating dynamism, randomization, and diversification techniques in computer systems and networks. By making the target less deterministic and less static, MT defenses attempt to increase the workload for attackers and enhance the resiliency of systems to attacks. MT defenses encompass a wide-range of systems security, resiliency, and network security techniques including (but not limited to) dynamic networks, dynamic platforms, dynamic runtime environments, dynamic software applications, and dynamic data techniques.

This special issue welcomes original research papers in the broad area of MT techniques, their evaluation and assessment, and their control and management. We welcome original papers in the areas of novel MT defenses, engineering MT defenses, MT evaluation/impact assessment/analysis methodologies, and MT control and management.

Submissions must not substantially overlap with papers published or simultaneously submitted to a journal or a conference. Papers previously published in academic journals are *not* eligible for submission. Papers previously published in academic conferences are eligible for this special issue provided that the submission includes new results, analyses, or findings compared to the conference version and the conference is clearly indicated in the submission and the conference version of the paper is included in the submission as well.

Potential topics include but are not limited to the following:

- Randomization/diversification/dynamism techniques
- System randomization
- Automated software diversity
- Compiler-based randomization
- MT for communication and network security
- MT protocols
- MT in wireless networks
- Memory layout and runtime code randomization
- Dynamic networks and address randomization
- Migration-based and service rotation techniques
- Cloud-based MT techniques
- MT techniques to secure embedded and IoT devices
- Adaptive defenses
- Cyber maneuvering and agility
- MT evaluation and assessment
- MT attacks and negative results
- MT metrics and assessment methodologies
- Game-theoretic analysis of MT defenses
- Empirical studies and measurements
- MT control and management
- Usability and human interfaces of MT defenses
- Theory and models of MT

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/mtd/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Hamed Okhravi, MIT Lincoln Laboratory, Lexington, USA
hamed.okhravi@ll.mit.edu

Guest Editors
Cliff Wang, US Army Research Office, Durham, USA
xiaogang.x.wang.civ@mail.mil

Per Larsen, University of California, Irvine, USA
perl@immunant.com

Submission Deadline
Friday, 29 June 2018

Publication Date
November 2018