IEEE SecDev '18 Poster Abstract

Command, Control and Coordination of Moving Target Defenses

Marco Carvalho, Ph.D.
Florida Institute of Technology

Conventional computer network defense (CND) has traditionally been centered on the protection boundaries at multiple levels, or detection mechanisms in the network, hosts, or services designed to identify and separate malicious/unauthorized activities from legitimate and authorized activities. Moving Target Defense (MTD) proposes a conceptual shift in this paradigm. The MTD concept proposes that the target itself does not need to be static, and that a dynamic (or moving) target design can be conceived in a way that maintains functionality for legitimate users, while making it difficult for adversaries to identify and exploit system vulnerabilities.

Moving Target Defense capabilities have evolved and matured significantly in the last several years. The MTD community has designed and implemented several advanced tools and techniques that have been demonstrated in relevant operational scenarios for multiple domains. In practice, the deployment and of MTD concepts have been generally successful in settings where the capability is embedded as part of the systems and services being protected, essentially hidden or transparent to users and operations. Address space layout randomization is a common example.

The challenges with broader adoption are often associated with the deployment and integration of MTDs with systems, services, and networks that may not have been designed to operate with such defenses. Most of our operational settings rely on assumptions of persistence, control, and visibility that are not necessarily in line with the MTD paradigm. Adoption barriers in such cases are significant and have greatly affected broader adoption.

Our prior research in this space has focused in some of these key challenges. In particular, we have designed and implemented tools and frameworks to facilitate the deployment, control, and monitoring of individual MTDs, as well as collections of defenses operating over a common infrastructure. The MTD Command and Control (MTC2) infrastructure developed as part of our work has introduced a resilient middleware designed to provide the safe integration of MTDs with other running services and conventional defenses in the infrastructure. MTC2 is extensible and also includes an integrated policy enforcement framework to enable the concurrent operation of multiple MTDs and multiple coordination (or orchestration) components.

Other elements of our research in this space have also included systems designed for the automated testing and characterization of MTDs, and the semi-automated wrapping and packaging of MTDs for enterprise deployment and control. Our most recent work has focused on extending the enterprise control and coordination elements of our work to build a federated command and control capability across different enterprises (or administrate domains) running their own adaptive and moving target defense frameworks.

With significant advances and progressive conversion of multiple efforts in the community, MTDs continue to be a promising paradigm for the design of truly resilient computer network systems and services. The future of the technology will depend not necessarily on the capabilities of individual defenses, but on how well they can integrate and operate with one another and with pre-existing systems and users. The future is promising.