

Preface

One of the most vexing problems in defending against computer intrusions is the seemingly endless supply of exploitable software bugs that exist despite significant progress in secure software development practices. At least once a month (e.g., on Patch Tuesday), major software vendors publish patches that fix the vulnerabilities in their deployed software code base that have been discovered. These patches are often published after the vulnerabilities are known and have been exploited, in some cases for months and years. In currently deployed systems, the attacker has a static target to study and find vulnerabilities, and then a window of exposure to exploit the vulnerability to gain privileged access on other people's machines and networks, until the exploit is noticed, vulnerability found, patch released, and then applied widely. The dynamics of this process significantly favors the attacker over the defender because the attacker needs to find only a single exploitable bug while the defender must ensure none exist. The attacker has plenty of time to analyze the software code, while the defender does not know when the attacker will strike. And finally, the defender typically can only block the exploit once the exploit or vulnerability is known, giving the attacker an automatic advantage in gaining access with zero-day vulnerabilities.

Against this backdrop, the topic of moving target defenses (MTDs) was developed to level the playing field for defenders versus attackers. The basic concept of MTD is to dynamically vary the attack surface of the system being defended, thus taking away the adversary's advantage of being able to study the target system offline and find vulnerabilities that can be exploited at attack time. MTD systems offer probabilistic protections despite exposed vulnerabilities, as long as the vulnerabilities are not predictable by the adversary at the time of attack. MTD has been identified as one of the four key areas of thrust in the White Houses strategic plan for cyber security research and development.

In the first volume of MTD, we presented papers on MTD foundations, MTD approaches based on software transformations and network and software stack configurations. In this follow-on second volume of MTD, a group of leading researchers describe game-theoretic, cyber maneuver, and software transformation approaches for constructing and analyzing MTD systems.

Moving Target Defense II

Application of Game Theory and Adversarial Modeling

Jajodia, S.; Ghosh, A.K.; Subrahmanian, V.S.; Cohan, V.;

Wang, C.; Wang, X.S. (Eds.)

2013, XII, 204 p., Hardcover

ISBN: 978-1-4614-5415-1