

Preface

Distributed Systems are complex systems, and cyber attacks targeting these systems have devastating consequences. Several cybersecurity solutions have failed to protect distributed systems primarily due to asymmetric warfare with cyber adversaries. Most cybersecurity solutions have to grapple with the tradeoff between detecting one breach vs. blocking all possible breaches. Current cyber threats are sophisticated and comprised of multiple attack vectors caused by organized attackers. Most of the current cyber defenses are blackbox or set-and-forget approaches which can protect against zero-day attacks and are ineffective against dynamic threats. The asymmetric conundrum is to determine which assets (software, embedded devices, routers, back-end infrastructure, dependencies between software components) need to be protected. Recently, Moving Target Defense (MTD) has been proposed as a strategy to protect distributed systems. MTD-based approaches take a leaf out of the adversaries book by not focusing on fortifying every asset and make the systems move to the defender's advantage. MTD is a game-changing capability to protect distributed systems by enabling defenders to change system/network behaviors, policies, or configurations automatically such that potential attack surfaces are moved in an unpredictable manner. MTD is also a cost-effective approach for intrusion detection, active response, and recovery in distributed systems. To realize an effective MTD-based defense, several challenges have to be addressed.

This book presents MTD techniques to determine placement of virtual machines in cloud data centers. The techniques focus on secure risk assessment of virtual machines and physical machines in cloud data centers and placement of virtual machines while taking into security risk as a criteria and evaluating cost of MTD. This book is organized as follows:

- Chapter 1 presents an overview of MTD and the need for research on developing novel MTD schemes at several levels: program (instruction set), host (IP address, memory), cloud computing platform, network, and mobile systems.
- Chapter 2 presents an approach to perform secure-aware Virtual Machine (VM) migration in cloud data centers.

- Chapter 3 presents an approach to develop MTD-based network diversity models. to evaluate the robustness of cloud data centers against potential zero-day attacks.
- Chapter 4 presents a network-aware VM placement scheme in cloud data centers
- Chapter 5 presents a cost model to evaluate the cost of MTD in cloud data centers.

Nashville, TN, USA
Beijing, China
Houghton, MI, USA
January 2016

Sachin Shetty
Xuebiao Yuchi
Min Song

Moving Target Defense for Distributed Systems

Shetty, S.; Yuchi, X.; Song, M.

2016, XVII, 76 p. 36 illus., 28 illus. in color., Hardcover

ISBN: 978-3-319-31031-2