SAND2018-7375D

The Center for Cyber Defenders

Expanding computer security knowledge

Scaling SDN-Based MTD

Mitchell Traylor, The University of Texas at Austin
Jean-Luc Watson, Stanford University

Project Mentor: William M.S. Stout, Org. 09315

Problem Statement

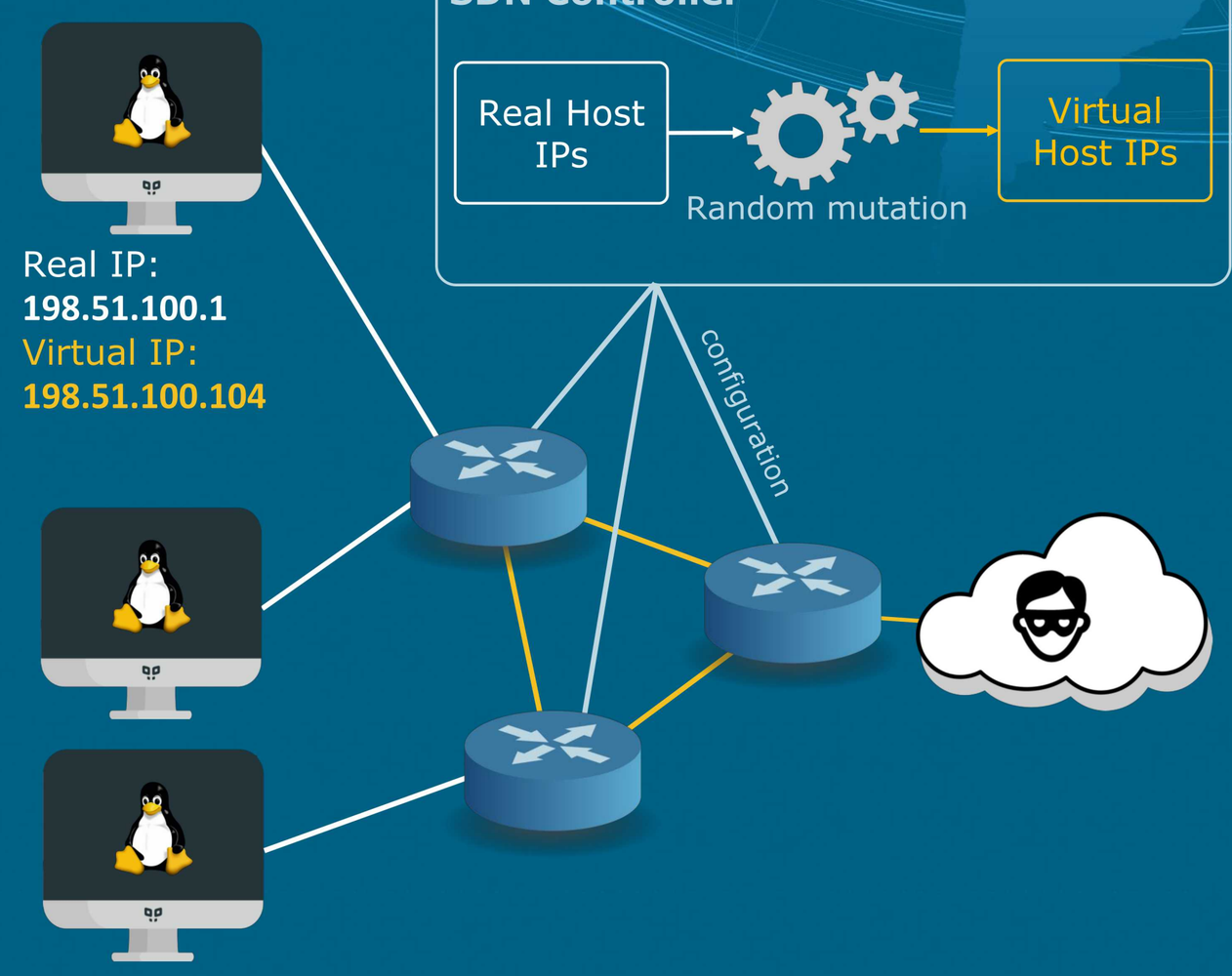
The core concept of MTD was first introduced in 2009; however a majority of research performed since then has not addressed the viability of scaling these techniques to large systems in environments where maximized performance is critical. Our goal is to create sample scenarios which mirror the size and functionality of a military network, controlled by an SDN controller, to run experiments gauging the costs and benefits of incorporating MTD.

Moving Target Defense (MTD)

MTD is a broad category of techniques where some static aspects of a system or network (IP addresses, OSs, etc.) are randomly adjusted. MTD makes it significantly more difficult for adversaries to launch successful attacks by hampering their ability to do meaningful system reconnaissance. For example, an adversary may discover an IP address via scanning, but the network invalidates it within seconds all while allowing normal operations.

Software-Defined Networks (SDN)

SDNs expose a centralized control plane separate from the network's data flow. A single SDN controller can effectively manage an entire network by using standardized interfaces on each component, installing rules for routing traffic. Using an SDN controller makes it much easier to incorporate MTD since the system does not need a complicated distributed algorithm to manage forwarding state and can make decisions with a global view of the network.



Approach

- We set up, configure, and run our experiments using JCSS, a modeling software designed for military applications and networks.
- We are using OpenDaylight Lithium as our network's SDN controller.
- The factors we measure in our experiments include how much time it takes an adversary to successfully mount an attack, the operational cost on the defending system and its users, and the effectiveness of scaling these techniques to large systems.

Benefits

Previous work has shown that MTD works in small test networks. Our experiments will evaluate its ability to be scaled to large-scale deployments and allow us to gain more insight into the potential performance bottlenecks. Future implementations that solve these issues will find widespread use in critical networks.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.