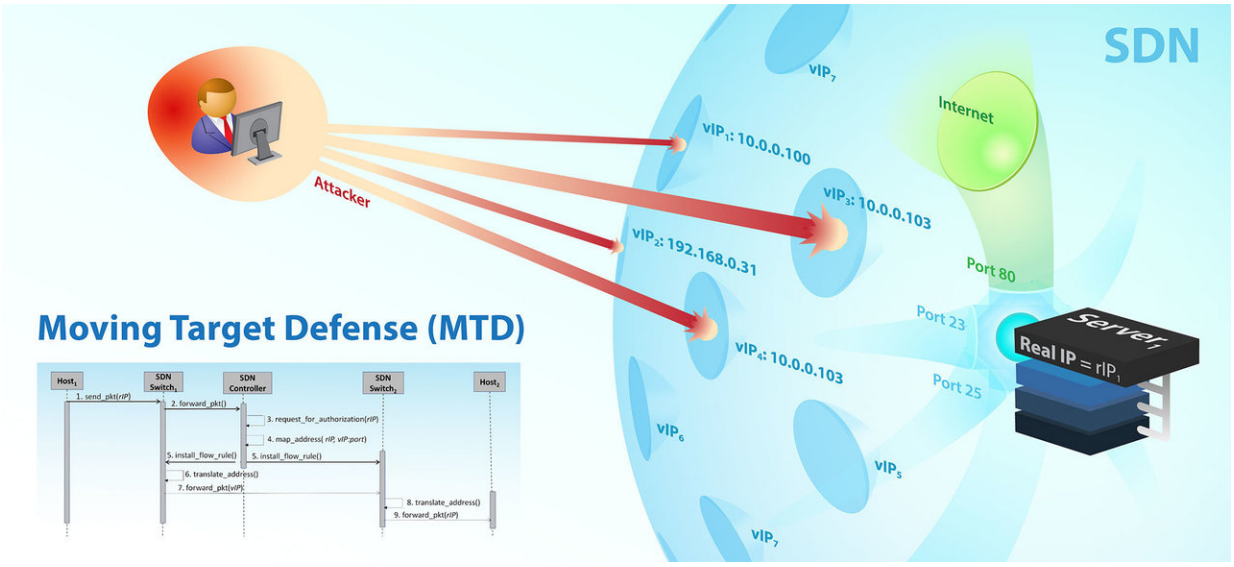
Research takes proactive approach to defending computer systems

September 7 2018



With moving target defense, uncertainty is increased and confuses the adversary, who has to expend more resources, such as time and/or computational power, to discover vulnerabilities of a target system. Credit: U.S. Army

A team of researchers from the U.S. Army Research Laboratory, the University of Canterbury in New Zealand and the Gwangju Institute of Science and Technology in the Republic of Korea have taken a step toward the development of moving target defense techniques in software-defined networks. This is a demanding cybersecurity research topic, scientists said.

This collaboration grew out of efforts of ARL researchers Dr. Jin-Hee Cho (now at Virginia Tech in the Department of Computer Science), Dr. Terrence J. Moore and Dr. Frederica Nelson reaching out to researchers in Asia Pacific regions through the international collaborative program administrated by the U.S. Army International Technology Center-Pacific.

Cyberattacks on computer systems are becoming more common. Any company with information on a computer system connected to the internet might become a victim from someone or some group who wants to steal or destroy the company's data for their own use, or for ransom.

This is possible because of the way the Internet is set up, researchers said. In order to access content on a website, a computer needs to know where to ask for the information. Websites have an address, what is known as an internet protocol, or IP, address; however, these are not just used for websites. Every computer connected to the internet has an IP address.

Cyber attackers have time to discover the IP addresses of the computers they think might have valuable information and attack them using code that is more commonly known as computer viruses or worms.

If the computer or system being attacked has a security system, such as a firewall or anti-virus software, it might be able to recognize some code as being bad and prevent itself from being infected.

What cyber attackers do is slightly modify their bad code so it is not recognized until the computer's security system is updated or patched.

Essentially, the typical defensive response to these attacks is passive, the researchers said. The attackers have time to prepare, plan and execute their attacks, whereas the potential victims are left reacting only after an

intruder breaks into a computer system.

Recently, a new proactive type of defense is being considered to protect important information in computer systems. This approach is known as moving target defense, or MTD.

"The concept of MTD has been introduced with the aim of increasing the adversary's confusion or uncertainty by dynamically changing the attack surface, which consists of the reachable and exploitable vulnerabilities," Cho said. "MTD can lead to making the adversary's intelligence gained from previous monitoring no longer useful and accordingly results in poor attack decisions."

The basic idea as it applies to IP addresses on computer networks is this: Change the IP address of the computer frequently enough so the attacker loses sight of where his victim is; however, this can be expensive, so the approach taken by the researchers in the collaboration here uses something known as software-defined networking.

This lets computers keep their real IP addresses fixed, but masks them from the rest of the internet with virtual IP addresses that are frequently changing.

Moore added that as the adage suggests, it is harder to hit a moving target.

"MTD increases uncertainty and confuses the adversary, as time is no longer an advantage," Moore said. "The adversary has to expend more resources, such as time and/or computational power, to discover vulnerabilities of a target system, but will experience more difficulty in exploiting any vulnerabilities found in the past since their location or accessibility is constantly changing."

According to Professor Hyuk Lim at GIST in the Republic of Korea, this proactive defense approach provides defense services before attackers get into a target system.

"Taking actions proactively requires extra overhead to add another layer of defense strength," Kim said. "Hence, deploying the proactive defense and security mechanisms is not for free, but brings a cost because the system needs to constantly change the attack surface such as IP addresses. This cost can be mitigated to some extent by leveraging the technology called 'Software-Defined Networking'. The SDN technology provides highly efficient programmatic and dynamic management of the network policy by removing the network control from individual devices in a network to a centralized controller. The network configuration can be defined by the SDN controller, enabling more reliable and responsive network operations under variable conditions."

Nelson explained the reason why these SDN-based MTD techniques are critical to supporting the vision of the Army and warfighters.

"The key technology of SDN-based MTD techniques, under development by the research team, is highly relevant to support the warfighters' mission execution by proactively thwarting potential attacks, which can protect the defense system so that the warfighters can properly execute the mission in the presence of highly dynamic, hostile and innovative adversaries within contested tactical environments," Nelson said.

The UC team in New Zealand led the effort of developing the MTD technology called the Flexible Random Virtual IP Multiplexing, namely FRVM.

"In FRVM, while the real IP address of a server-host remains unchanged but stays hidden, a virtual IP address of the server-host keeps being

randomly and periodically changed where the IP mapping/remapping (i.e., called multiplexing/demultiplexing) is performed by an SDN controller," said Dilli P. Sharma, a doctoral student in Prof. DongSeong Kim's cybersecurity research group at UC, New Zealand. "This effectively forces the adversary to play the equivalent of an honest shell game. However, instead of guessing among three shells (IP addresses) to find a pea (a running network service), the adversary must guess among 65,536 shells, given address space2^16. This MTD protocol is novel because it provides high flexibility to have multiple, random, time-variant IP addresses in a host, which implies the adversary will require more time to discover an IP address of the target host."

In this research, the team formulated the architecture and communication protocols for the proposed IP (de)multiplexing-based MTD to be applied in SDN environments.

The team also validated the effectiveness of the FRVM under various degrees of scanning attacks in terms of the attack success probability.

The preliminary results evaluating the FRVM were presented at the 17th Institute of Electrical and Electronics Engineers International Conference on Trust, Security and Privacy in Computing and Communications, or TrustCom'18, held in New York in August.

"Our next step is to study the trade-off in the FRVM between the dual conflicting goals of system security and performance, as proactive defense may introduce adverse effects when running MTD techniques while achieving enhanced security," Kim said.

Provided by The Army Research Laboratory