Researchers identify novel cybersecurity approach to protect Army systems

4 March 2020

Researchers at the Army's corporate laboratory in collaboration with the University of California, Riverside have identified an approach to network security that will enhance the effectiveness and timeliness of protection against adversarial intrusion and evasion strategies.

Networked devices and infrastructure are becoming increasingly complex, making it nearly impossible to verify an entire system, and new attacks are continuously being developed.

To rapidly protect Army systems from attack in ways that don't require massive amounts of manual intervention, the researchers have developed and approach called SymTCP.

SymTCP is a proposed approach that can be used to identify previously unknown ways to bypass deep packet inspection, or DPI, checks in networked appliances, often what internet service providers use to prevent malicious attacks from being launched or to censor certain content.

"Identifying strategies that attackers use to evade DPI in networked systems has been generally a manual process," said Dr. Kevin Chan, researcher at the U.S. Army Combat Capabilities Development Command's Army Research Laboratory. "This research provides an automated method to identify potential vulnerabilities in the Transmission Control Protocol, or TCP, state machines of DPI implementation."

Chan stated that this research has found previously undiscovered vulnerabilities in TCP, which is what the internet is built on; most of internet traffic is TCP. However, it is very difficult to find vulnerabilities in the implementation of TCP, as some of these vulnerabilities are found in obscure parts of the code and require a specific sequence of packets to be sent in order to trigger the vulnerability.

"Our approach uses symbolic execution to explore the state of TCP implementation of an endhost to identify ways to reach critical points in the code," Chan said. "If such a point is found, then packets can be inserted and be undetected by DPI. This method is evaluated against several state-of-the-art DPI systems such as Zeek and Snort and identifies previously known evasion strategies in addition to new ones that were not previously documented."

The search space is enormous, and being able to make sense of the state and explore it efficiently is a great achievement, Chan said.

"This research will improve the security of Army networks in terms of being able to protect against future intrusion and evasion strategies," Chan said. "It has developed an efficient way to find and patch vulnerabilities in future Army network infrastructure."

According to the researchers, information must be securely transmitted between domains (i.e. air and land) and within domains (i.e. cyber domains) for various Army functions, making this research crucial to each of the Army Modernization Priorities in support of enabling Multi-Domain Operations, with direct applicability to the Army's Network Modernization Priority.

"This type of research helps focus cyber defense resources," said Dr. Tracy Braun, computer scientist at CCDC ARL. "It can reveal weaknesses and suggest more efficient deployments of network defenses. This helps protect networks against advanced attacks. It can also help guide the design of future Army network infrastructure and cyber defense strategies."

This collaborative research endeavor was made possible by ARL's Cyber Security Collaborative Research Alliance, which has the objective to develop a fundamental understanding of cyber phenomena, including aspects of human attackers,

cyber defenders and end users, so that fundamental laws, theories, and theoretically grounded and empirically validated models can be applied to a broad range of Army domains, applications and environments.

CRAs are partnerships between Army laboratories and centers, private industry and academia that are focusing on the rapid transition of innovative science and technology for Army modernization.

"Collaboration by the teams of academic, industry and government researchers in the CRA, including students, builds enduring relationships and maintains a focus on cross-cutting foundational research addressing important Army challenges," said Dr. Michael Frame, Cyber Security CRA collaborative alliance manager.

The team's research was accepted to be presented at the Network and Distributed System Security Symposium 2020, which took place Feb. 23-26 in San Diego, California.

According to Dr. Zhiyun Qian, Everett and Imogene Ross associate professor in the Computer Science and Engineering Department at the University of California Riverside, future research includes the continuous analysis of future generation of DPI boxes, as well as better designs of DPIs that can be made robust against evasion attempts.

Provided by The Army Research Laboratory