Return-oriented programming payload detection using speculative code execution

Return-oriented programming (ROP) is a computer exploitation technique in which an attacker executes arbitrary code on a victim system by injecting a sequence of addresses to code fragments (referred to as gadgets) that already exist in the address space of the targeted process on the victim system. Current methods for detecting and/or preventing the execution of malicious code such as Data Execution Protection (DEP) are ineffective against ROP attacks because the injected payload in such attacks contains no identifiable malicious code. The current lack of effective ROP exploit detection methods has encouraged attackers to increasingly employ it to compromise computer systems. The technology is a software method for the detection of ROP payloads in arbitrary inputs that allows for accurate attack detection of and security from ROP based attacks.

Speculative code execution successfully detects ROP exploits without false positive signals

This technology is unique in that it is one of the few methods to detect ROP based attacks. The detection method scans the input byte by byte to determine whether it contains a sequence of valid memory addresses that point to consecutively executed unique gadgets in the executable memory segments of a target process. If the address falls into the gadget space of a process, this may be indicative of the beginning of a ROP payload, and the code emulator will speculatively start executing the code that exists at that address. These sequences can be heuristically identified because of the low probability that a benign input would contain a sequence of addresses to code fragments that read valid destination addresses from the input and transfer execution control to them. The detection threshold of the method – specifically, the number of consecutive unique gadgets executed due to a potential payload – can be tuned to increase the robustness of the method to false positives.

This technology has already been demonstrated with various ROP exploits against Windows applications with no false positives.

Lead Inventor:

Angelos D. Keromytis, Ph.D.
Applications:

- Effective identification of network-level attacks or documents that contain exploits based upon ROP.
- Integration into existing network-level intrusion detection systems and host-level malicious code/virus scanners.
- Software testing cycles to predict and identify possible security vulnerabilities that can be exploited by ROP.

Advantages:

- In contrast to existing exploit detection and prevention methods that can only identify exploits that contain malicious code, the technology can identify exploits that only contain ROP payloads.
- The technology can be combined with existing exploit detection methods to identify attacks that comprise both ROP and non-ROP components.

Patent Information:

Patent Pending (US20140344932)

Tech Ventures Reference: IR CU12079

Related Publications:


Inventors

Angelos D. Keromytis