ROP Protector

A radical defense solution that protects legacy systems from Return Oriented Programming (ROP) cyberattacks

The challenge

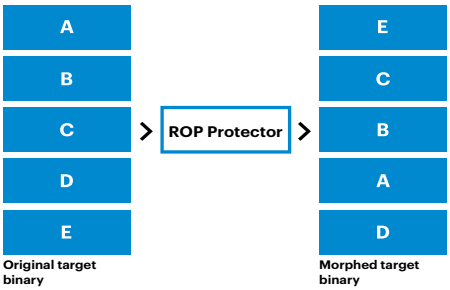
Today's cybersecurity playing field is fundamentally asymmetric. Attackers are easily able to identify weaknesses in a target system as soon as they have access to its code and configuration. As a result, defenders are continuously playing a game of catch-up after an attack has occurred to secure their network infrastructure.

Initially, the successful defense against a buffer overflow attack that injected malware into a running system was achieved by incorporating Data Execution Prevention (DEP) technology into modern software systems. DEP could prevent injected malware from being executed by the target system. However, attackers have since sidestepped DEP by developing the Return Oriented Programming (ROP) technique, which effectively uses code already present within the target system to carry out the attack. ROP attackers are able to harness software components within the legacy system. The software components that make up the attack, commonly referred to as gadgets, are part of the target. ROP attacks, once devised, are easy to carry out since they rely on the target system being static.

The ROP Protector solution

Perspecta Labs' ROP Protector is a radical defense solution that protects legacy systems from ROP cyberattacks. Considered a moving target defense cyber solution, ROP Protector ensures that the target system itself is dynamic, preventing attacks that aim to leverage gadgets within the system. ROP Protector creates a morphed version of the target system that has exactly the same set of capabilities as the original, yet does not have the gadgets that the ROP attack depends on.

ROP Protector is particularly valuable for legacy systems. The sources from which such systems were built are either not readily available, or the system build processes are not easy to tweak to introduce defenses. A pure binary-to-binary code scrambling solution, ROP Protector does not require access to the source code for the protected system. It ensures that gadgets needed to facilitate a typical ROP attack are not available for use by an attacker. Importantly, studies have shown that well-known applications (e.g., the Apache webserver) transformed by ROP Protector have comparable performance to their original versions. ROP Protector is an efficient and practical solution to the ROP defense needs of legacy systems.



About Perspecta Labs

At Perspecta Labs, we refuse to think inside the box. As the innovation hub of Perspecta, we are molding the future of emerging technologies. Our experts conduct leading research into cybersecurity, machine learning, artificial intelligence, mobile communications and Internet of Things technologies that provides customers with transformative insights and real-time situational intelligence. With our finger on the pulse of next-gen technology, you'll gain an essential edge. Drawing on our Bell Labs and Applied Communication Sciences heritage, Perspecta Labs creates innovative technologies and services to solve the most difficult and complex information and communications challenges.

perspecta LABS

perspectalabs.com | info@perspectalabs.com
150 Mount Airy Road
Basking Ridge, NJ 07920