Cybersecurity Transition-to-Practice Acceleration Workshop

April 17, 2018 | New York, NY

Quad Chart for: *Principled and Practical Software Shielding against Advanced Exploits*

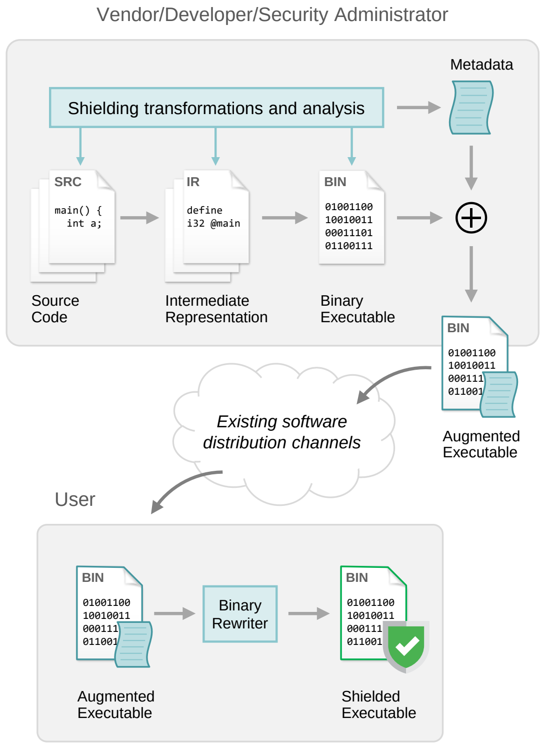
Challenge:

- Software monocultures and code bloat are facilitators for the exploitation of software vulnerabilities
- The operational benefits of software uniformity have so far prevented the deployment of techniques that introduce diversity or specialization

Main Objectives:

Design novel software shielding techniques, and enable their practical applicability to commodity systems

- Consider the strong adversarial models imposed by the latest exploitation advancements: disclosure-aided exploitation and data-only attacks
- Code specialization and data protection techniques to introduce process-level unpredictability and limit the exposure of critical data
- Hardware-assisted implementation by leveraging recent CPU features



NSF CAREER: CNS-1749895

PI: Michalis Polychronakis

Contact: mikepo@cs.stonybrook.edu

Stony Brook University   HEXLAB

Broader Impact:

- Improved security against the threat posed by vulnerability exploitation for both legacy and recent software
- Facilitate the transparent deployment of existing and novel protections that break software uniformity and currently face deployment hurdles
- The project's software prototypes will be publicly available and readily applicable on third-party applications, and will thus benefit both end users and security researchers

Metadata Tag:

- Prototype implementation for Linux applications built on top of the LLVM compiler and the `apt` package manager
- Look for upcoming IEEE S&P '18 paper and code release
- TTP will require more resources to support the engineering effort needed for seamless integration with Linux and complex applications