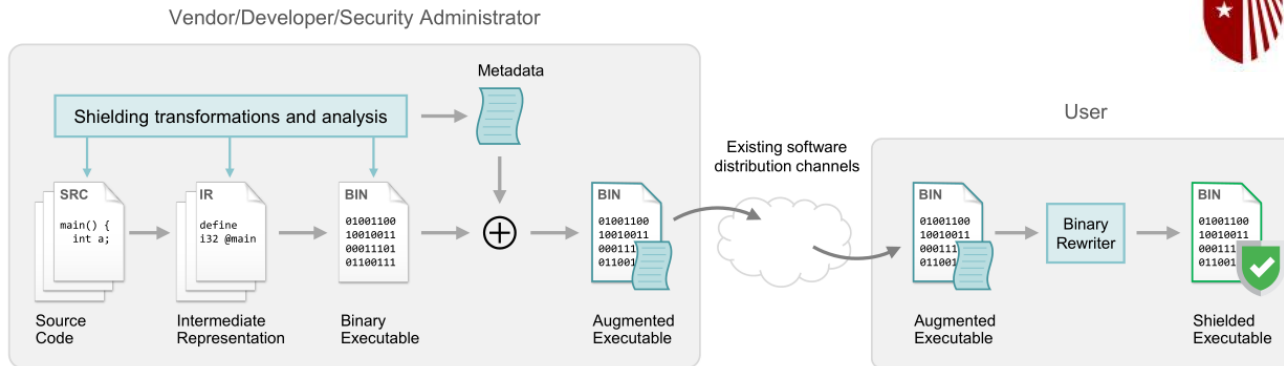


CAREER: Principled and Practical Software Shielding against Advanced Exploits



Award Number: 1749895
(2018–2023)
Stony Brook University
Michalis Polychronakis
(mikepo@cs.stonybrook.edu)

Challenge

- The continuous discovery of zero-day vulnerabilities, and the lack of effective defenses against recent exploitation techniques that leverage memory disclosure vulnerabilities, necessitate the development of additional defense mechanisms

Solution

- Design principled software shielding techniques that are readily applicable to commodity software and systems
- Three synergistic thrusts: code specialization, sensitive data protection, and binary executable augmentation

Scientific Impact

- Consideration of the latest exploitation advancements: disclosure-aided exploitation and data-only attacks
- Novel software debloating, diversification, isolation, and data protection techniques
- Hardware-assisted implementation by leveraging recent and upcoming processor features
- Focus on practical considerations, such as operational compatibility and non-disruptive deployment

Broader Impact

- Improve the state of the art in defenses against advanced exploits
- Software prototypes readily applicable on third-party applications for both end users and researchers