CERIAS

The Center for Education and Research in Information Assurance and Security

EPOXY – Enabling Robust Protections for Bare-Metal Systems

Abraham A. Clements, Naif Saleh Almakhdhub, Khaled S. Saab, Prashast Srivastava, Jinkyu Koo, Saurabh Bagchi, and Mathias Payer

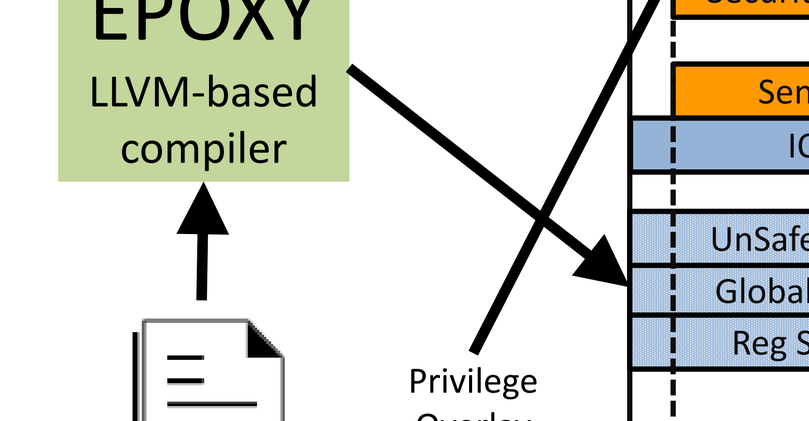
IEEE Security and Privacy 2017 [1]

Bare-metal?

A system without an OS

- Common on micro-controllers
- Examples:
  - Amazon Dash Button
  - Controller in SD Cards
  - Smart Locks
  - Network Cards
- Increasingly connected
  - Security is critical

Default: No Defenses



Defense Challenges

- Single application on system
  - Needs to access all hardware
  - Security requires restricting some accesses
- Small memory sizes
- Tight run-time constraints
- Low power requirements

Our Solution

EPOXY

Fast forwards bare-metal system security two decades

- Significantly reduces privileged instructions
- Applies DEP to stop code injection
- Protects against Stack Smashing and ROP by adapting SafeStack[2]
- Protects against ROP and data attacks using fine-grained diversity

Meets bare-metal constraints

Security Analysis

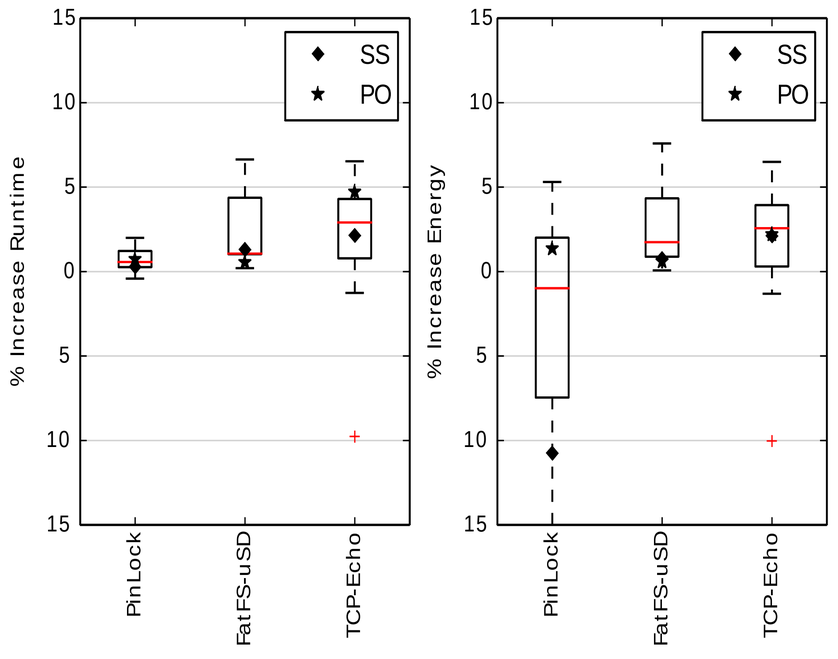
ROP gadgets survival across 1000 variants

		# Surviving Across				
App	Total	2	5	25	50	Last
PinLock	294K	14K	8K	313	0	48
FatFs-uSD	1,009K	39K	9K	39	0	32
TCP-Echo	676K	22K	9K	985	700	107

Comparison to FreeRTOS-MPU

App	Tool	Code	RAM	Instr. Exe	Priv Instr.
PinLock	EPOXY	16KB	2KB	823K	1.4K
	FreeRTOS	44KB	30KB	823K	813K
FatFs-uSD	EPOXY	27KB	12KB	33.3M	3.9K
	FreeRTOS	58KB	14KB	34.1M	33.0M
TCP-Echo	EPOXY	43KB	35KB	310M	1.5K
	FreeRTOS	74KB	51KB	322M	307.0M

Performance



SS - SafeStack Only, PO - Privilege Overlay Only

Memory Overhead (Bytes)

App	Code	Global Data	Stack
PinLock	3,390	14.6	104
FatFs-uSD	2,839	18.2	164
TCP-Echo	3,249	7.2	128

Our Team

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000

References

[1] Clements, Abraham, et. al, "Protecting Bare-metal Systems With Privlege Overlays", *IEEE Security & Privacy, 2017*.

[2] Kuznetsov, Volodymyr, et al. "Code-Pointer Integrity." *OSDI*. 2014.

PURDUE UNIVERSITY