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

Bare-metal?

A system without an OS

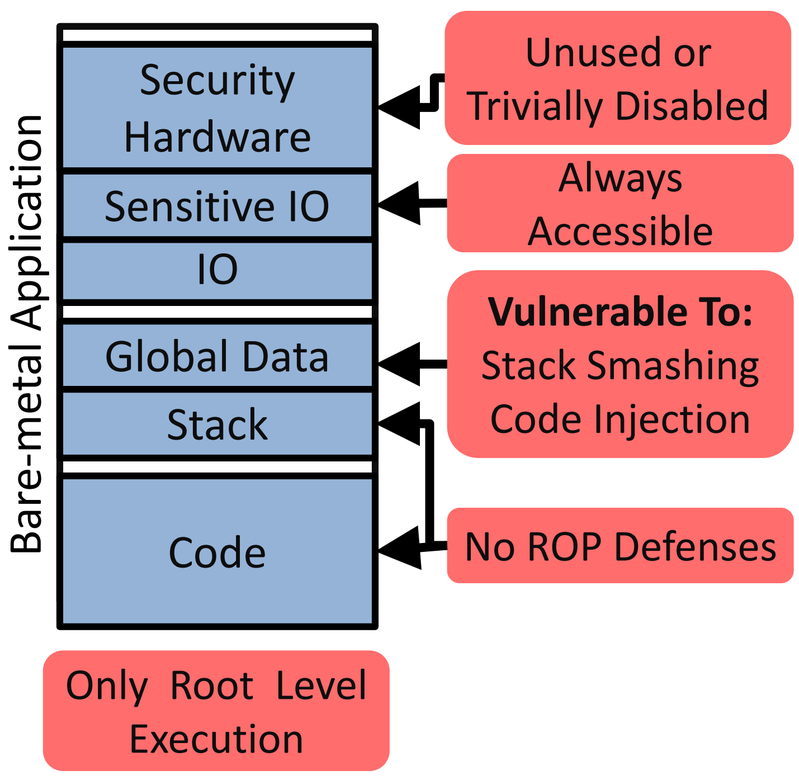
Examples:

- Amazon Dash Button
- Controller in SD Cards
- Smart Locks
- WiFi SoC's

Increasingly connected

Security is critical

Default: No Defenses



Defense Challenges

No separate privileges

- Single application
- No higher privileged software

Small memories

- 1KB - 2MB of Flash
- 1KB - 512KB RAM

No virtual memory

Run-time constraints

Low power constraints

Our Solution – EPOXY[1]

Techniques

Privilege Overlay

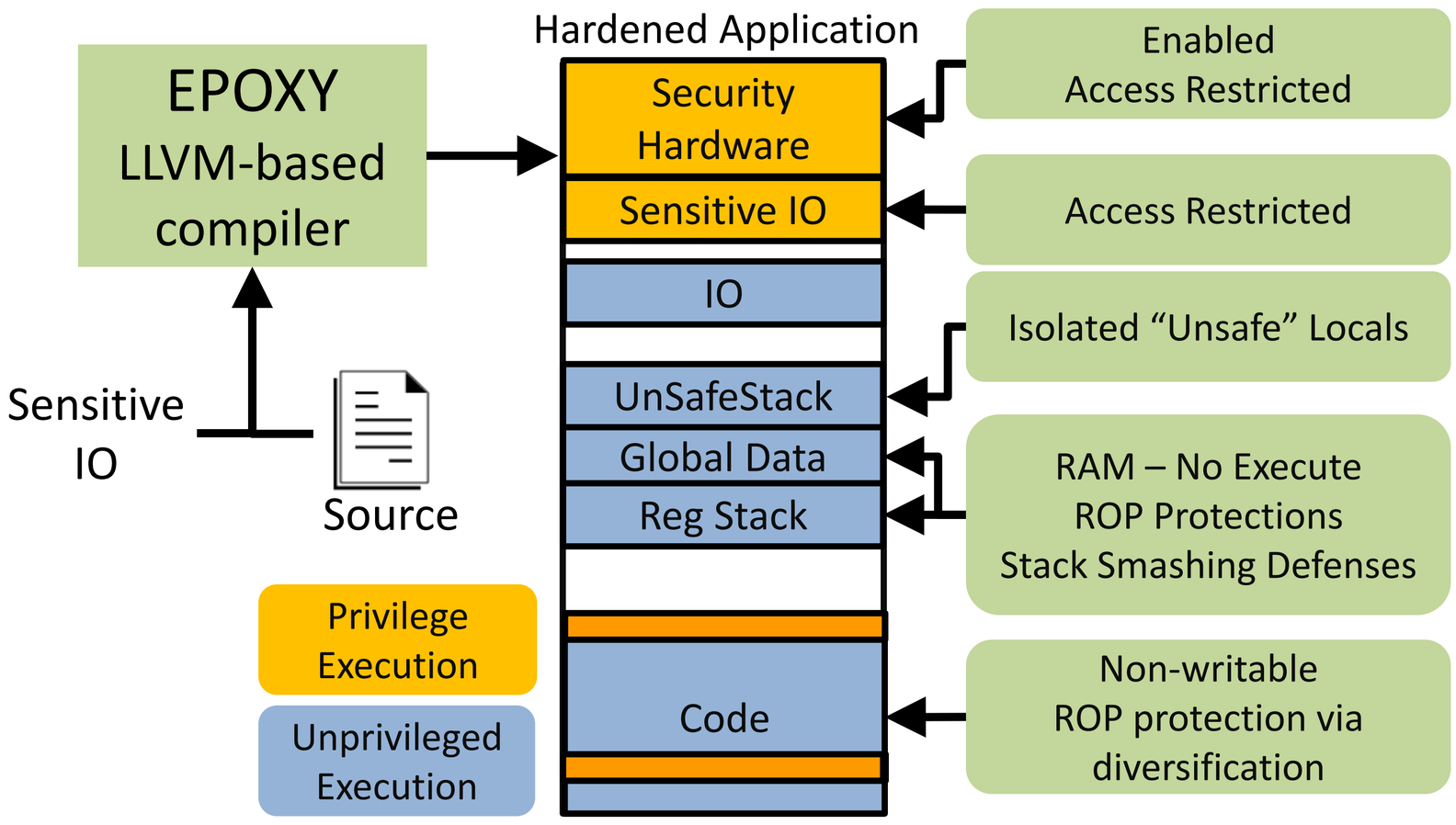
- Uses static analysis to create privileged and unprivileged execution
- Foundation for other defenses

Enable Memory Protection

- Provides DEP
- Code Integrity

SafeStack[2] and Diversity

- Protects against ROP attacks
- Protects global data



Security Analysis

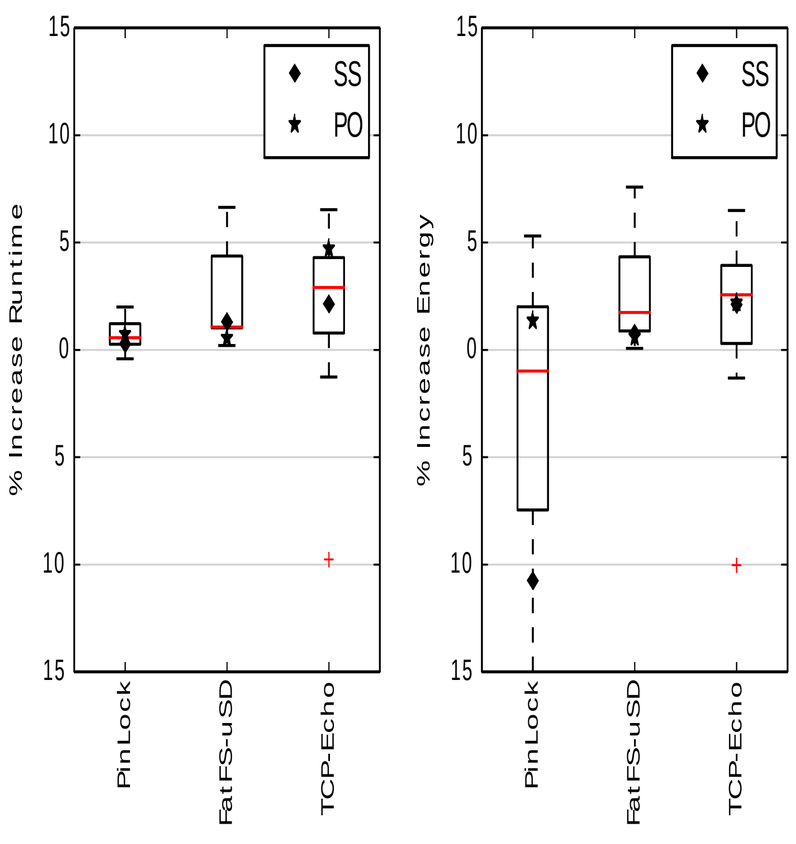
ROP gadgets survival

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

Comparison to FreeRTOS-MPU

App	Tool	Code (KB)	RAM (KB)	Instr. Exe	Priv Instr.
PinLock	EPOXY	16	2	823K	1.4K
	RTOS	44	30	823K	813K
FatFs	EPOXY	27	12	33.3M	3.9K
	RTOS	58	14	34.1M	33.0M
TCPEcho	EPOXY	43	35	310M	1.5K
	RTOS	74	51	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	2,839	18.2	164
TCPEcho	3,249	7.2	128

References

[1] Clements, A.A., et. al, "Protecting Bare-metal Systems With Privlege Overlays", *IEEE S & P 2017*.
[2] Kuznetsov, V., et al. "Code-Pointer Integrity." *OSDI*. 2014.

Acknowledgments

Partially funded under National Science Foundation Grant Numbers CNS-1464155 and CNS-1548114. Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. Also funded by Sandia National Laboratories, 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.

hexhive DCSL Sandia National Laboratories PURDUE UNIVERSITY