Cloud-assisted Security Services
Secure Systems Group, Aalto University

Aaro Lehikoinen, Thomas Nyman, Ghada Dessouky, Shaza Zeitouni, Andrew Paverd, N. Asokan, Ahmad-Reza Sadeghi

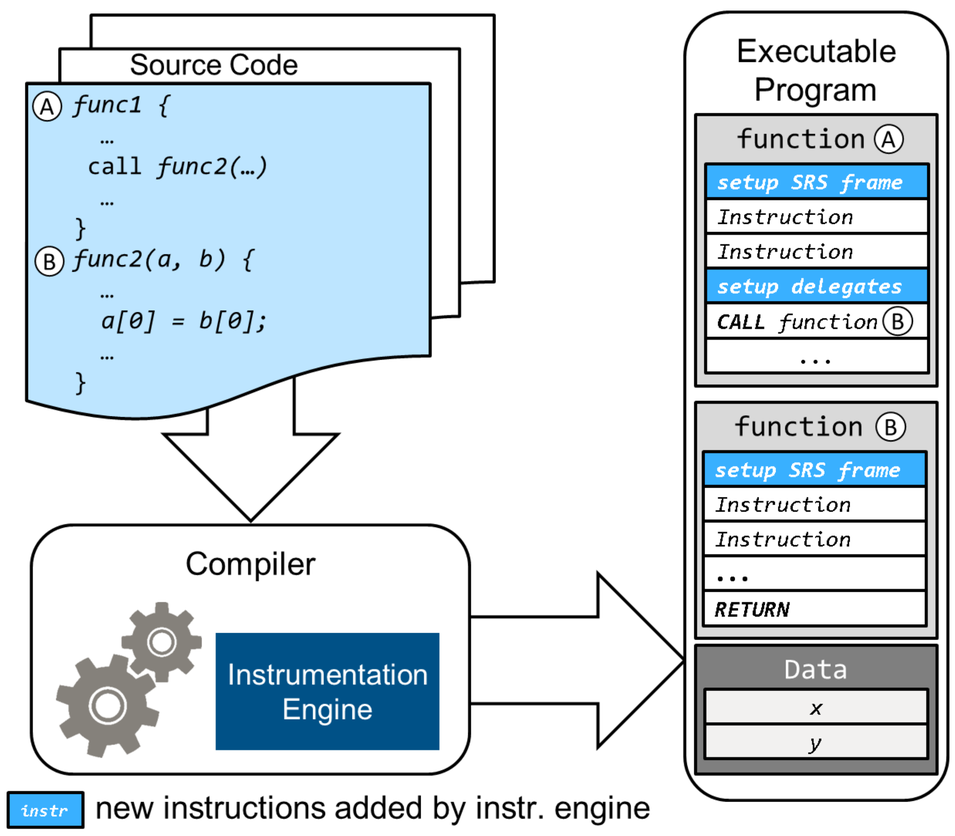
HardScope: Thwarting DOP with Hardware-assisted Run-time Scope Enforcement

Motivation: Data-Oriented Programming (DOP) Attacks

- Memory unsafe languages are prone to memory corruption vulnerabilities
- DOP attacks corrupt non-control data to e.g. escalate privilege or leak information
- Existing security features including *NX*, *ASLR*, *CFI* are ineffective against these attacks
- Current practical DOP attacks rely on accessing out-of-scope variables

High-level Idea

- Enforcing variable visibility rules at run-time
- Challenge: Preventing DOP attacks requires mediating all memory accesses, cumbersome in software only
- Solution: Hardware-assisted enforcement through extensions to instruction set, processor and compiler
- Protects program data at run-time (e.g., control-data, local and global variables)
- Prevents out-of-scope memory accesses



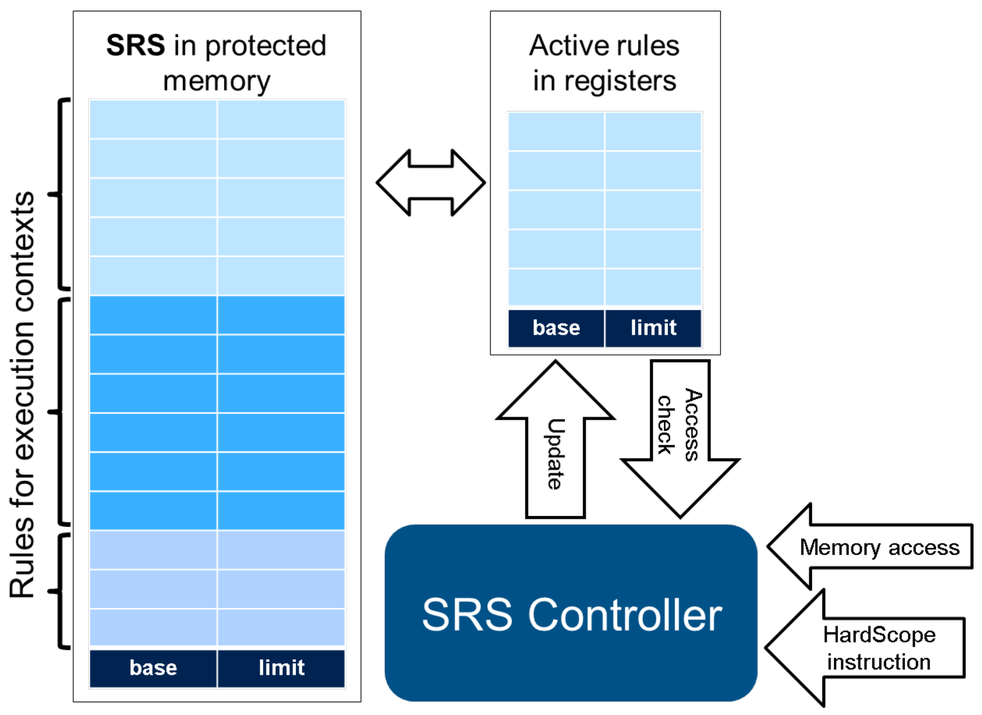
Compile-phase design of HardScope

Implementation

- Program code instrumented during compilation
  - Analyze variables used in C program functions
  - Instrument function prologues, epilogues and call-sites with HardScope instructions
- Hardware assisted run-time enforcement
  - Instrumented HardScope instructions maintain memory access rules during execution
  - Rules can be delegated on context switches
  - Rules enforced on each memory access

Storage Region Stack (SRS)

- Each *SRS frame* contains *storage regions* accessible from an *execution context*, i.e. code block
- Frames are pushed and popped to stack on context switches
- Permission to access memory from current context is checked on each load/store



HardScope SRS architecture and operations

Evaluation

- RISC-V instruction set extension, Spike simulator and Pulpino core hardware support
- Low performance overhead (~7%)
- Small area size in hardware implementation

Aalto University

TECHNISCHE UNIVERSITÄT DARMSTADT

https://github.com/runtime-scope-enforcement/hardscope-materials

https://arxiv.org/abs/1705.10295