19 DEC 2024
DAVIDE MOLETTA

UNIVERSITY OF TRENTO

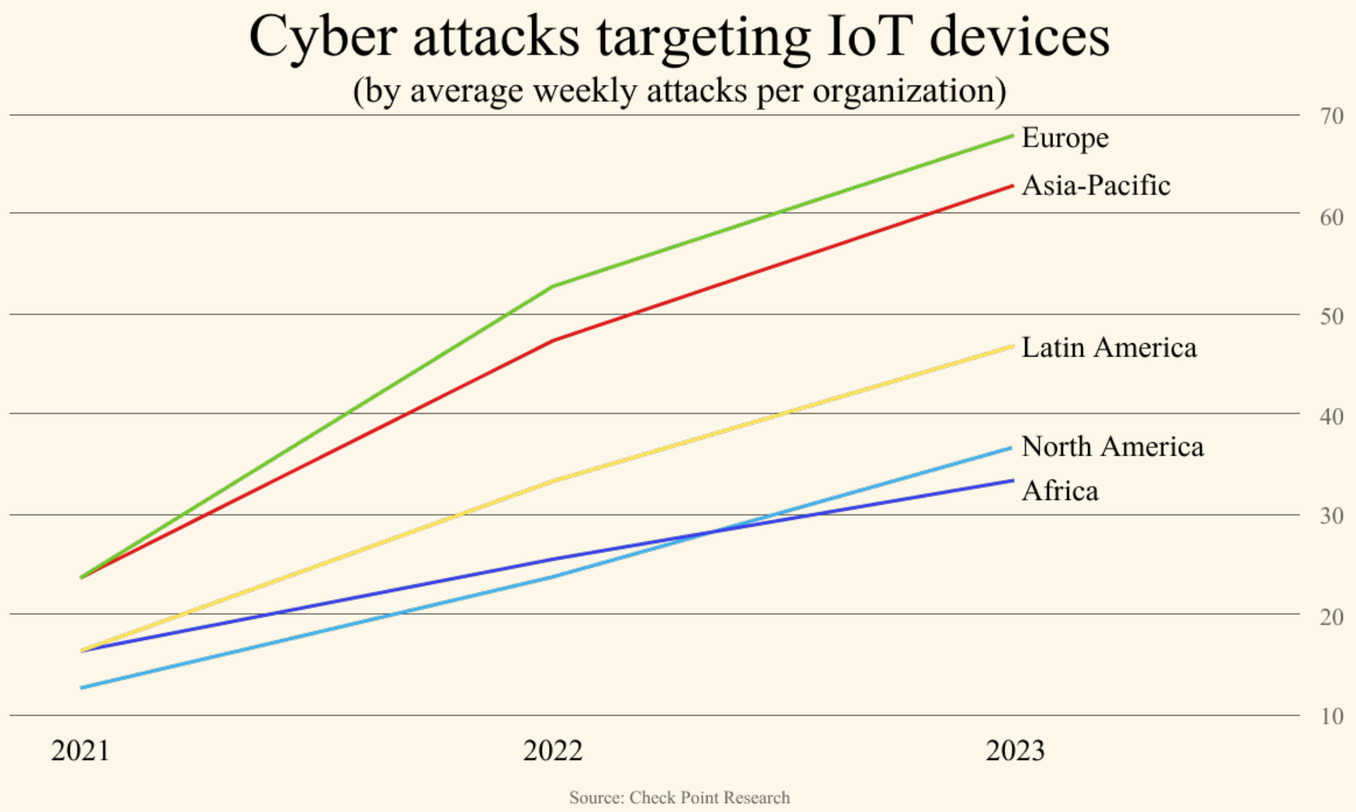
Design and Implementation of Trusted Services on RISC-V: the case of Control Flow Integrity

RISC-V

- Open-Standard Architecture
- Hardware-free Design
- No Licensing Fees

Problem

- 18B devices (2024)[1]
- 112M attacks (2022)[2]



[1]State of IoT Summer 2024
[2]IoT Cybersecurity Landscape in 2024

Control Flow Hijacking Attacks

- Code Reuse Attacks
  - Return-Oriented Programming
  - Jump-Oriented Programming
- Stack Smashing Attacks
- Function Pointer Overwrite Attacks
- Virtual Table Hijacking Attacks
- Dynamic Linking Attacks

Control Flow Hijacking Mitigations

- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)
- Stack Canary
- Control Flow Integrity (CFI)

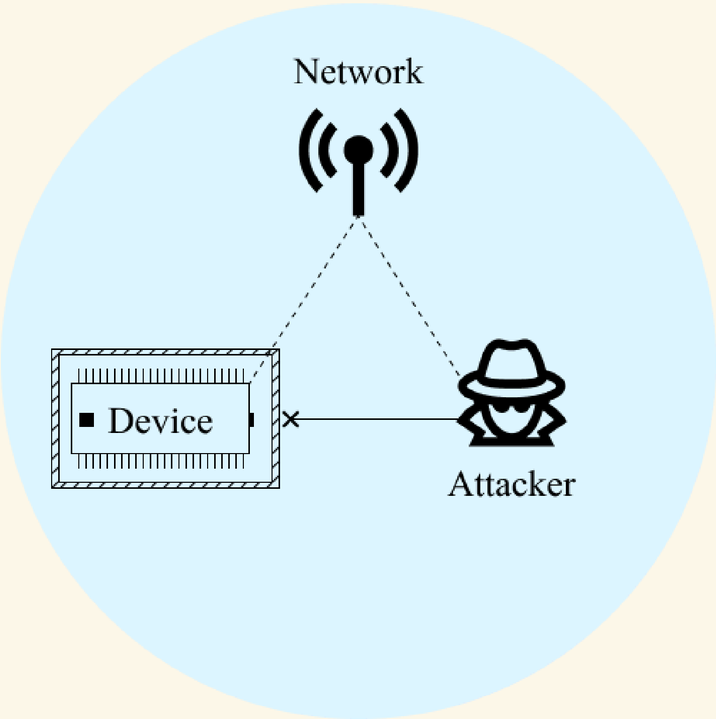
Control Flow Integrity

Ensuring that the flow of execution is not disrupted with the enforcement of:

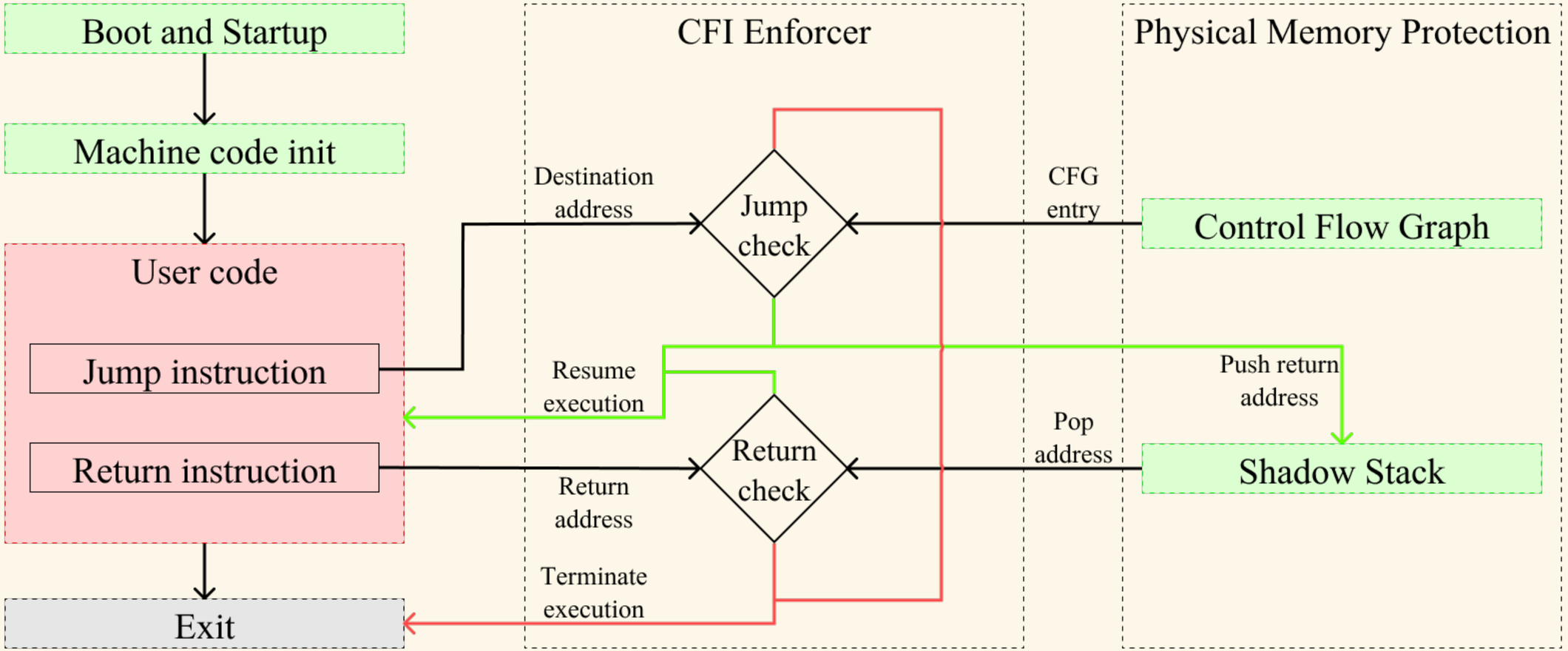
- Forward Edge Protection
- Backward Edge Protection

Threat Model

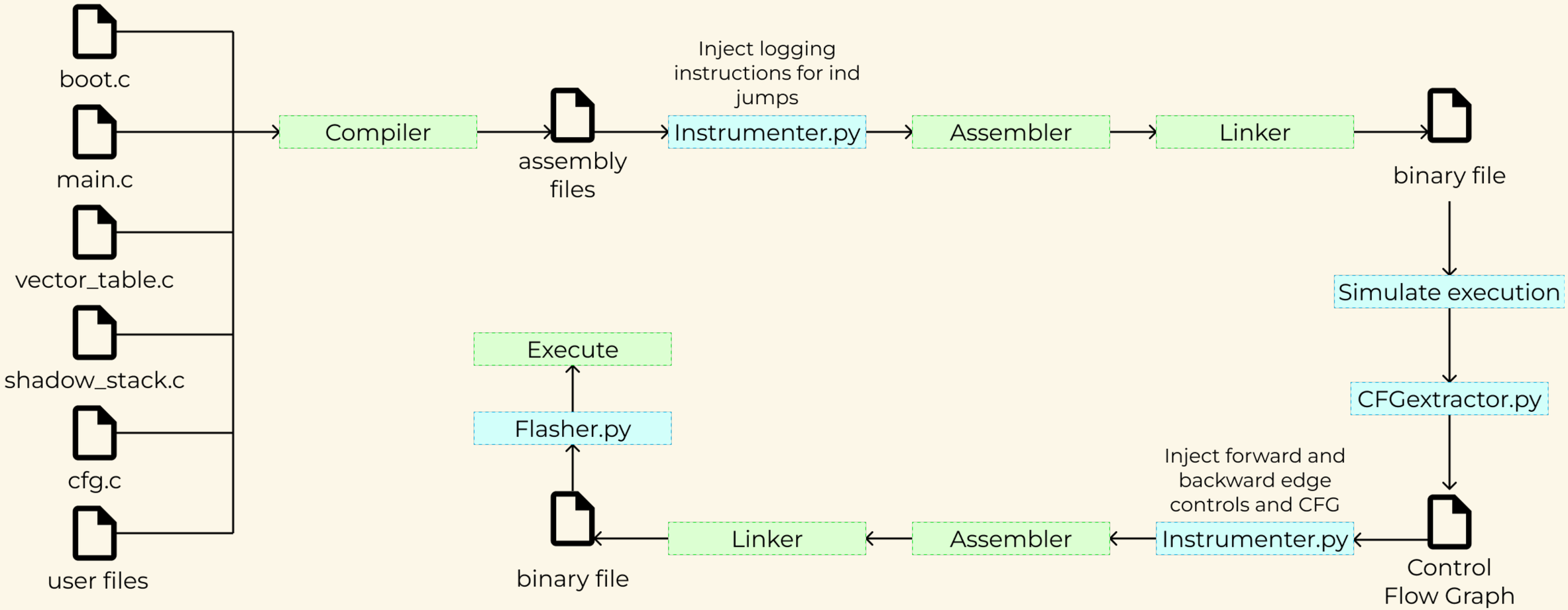
- Device running vulnerable code inside an unsafe network
- Attacker can launch Control Flow Hijacking Attacks
- Physical device inaccessible



Control Flow Integrity Enforcer



Code Instrumentation



Backward Edge Protection

Validate return instructions with a shadow stack

```
addi a7, return_register, 1
ecall
addi return_register, a7, -1
ret
```

Forward Edge Protection

Validate jump instructions with a Control Flow Graph

```
mv a7, target_register
ecall
jalr target_register
```

```
la a7, target_function
ecall
jal target_function
```

Physical Memory Protection

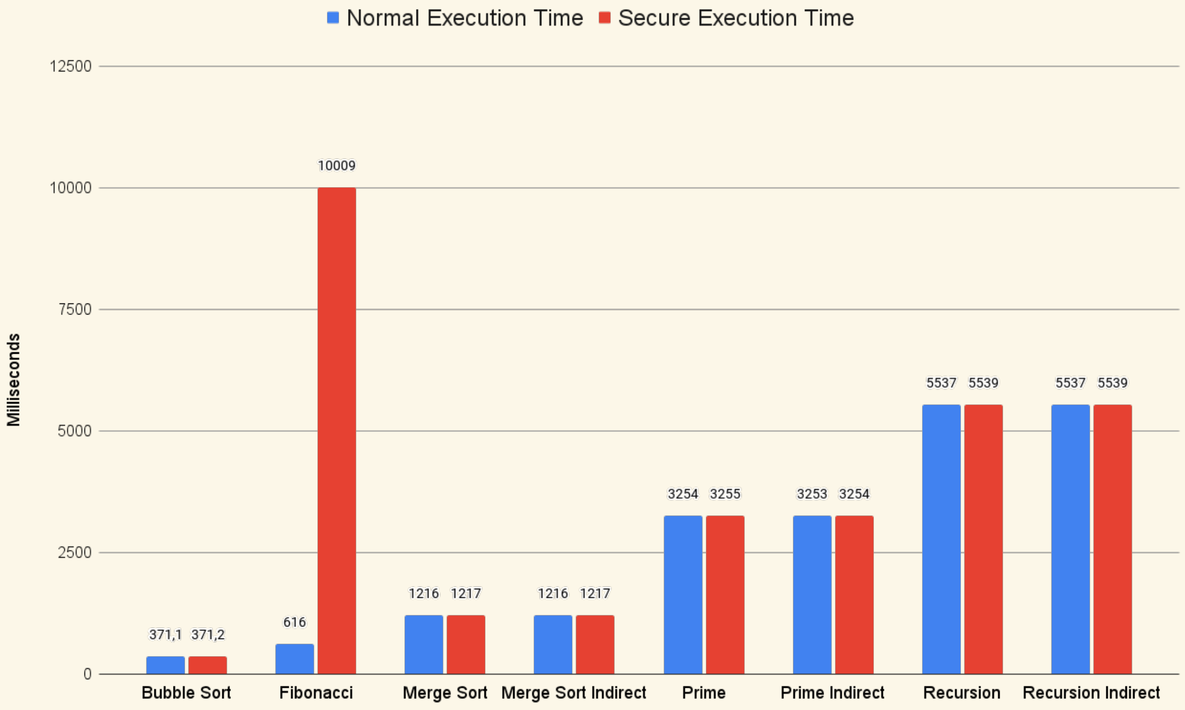
- Mechanism to prevent unauthorized access to physical memory
- Ensures memory regions are properly isolated
- Enforces access controls on read, write, and execution privileges

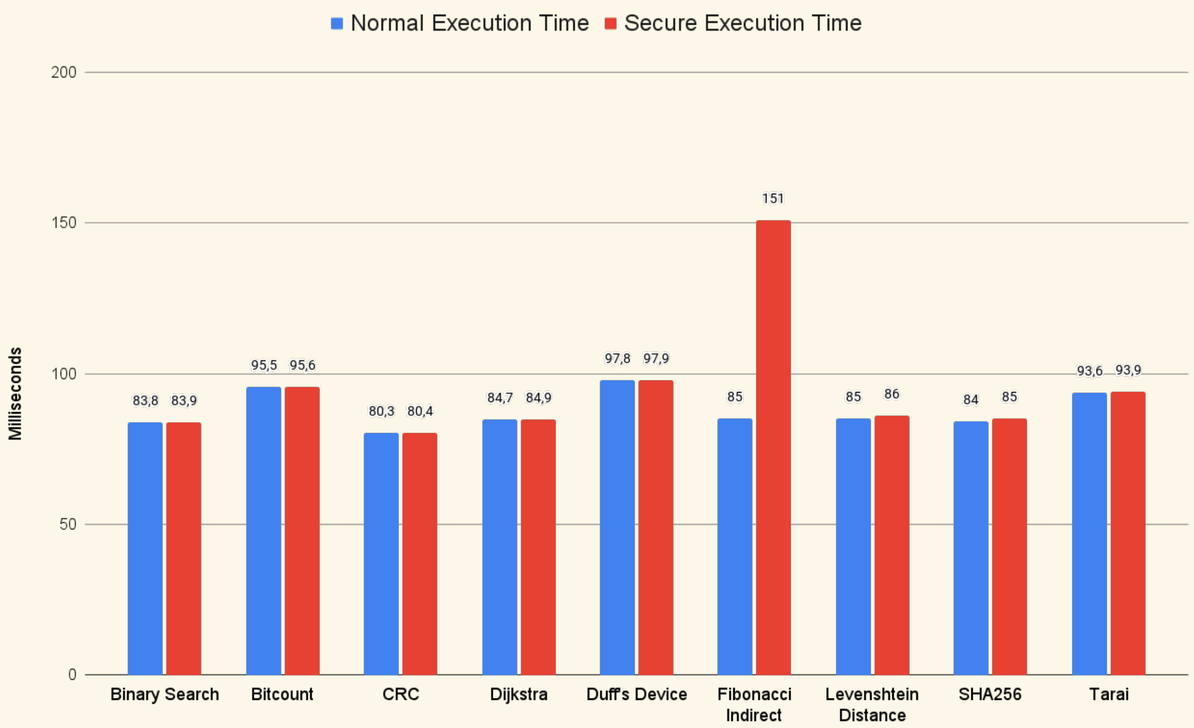
Security Analysis

- Crafted payloads to mimic ROP/JOP attacks
- Physical Memory Protection validation
- Shadow Stack validation
- Control Flow Graph validation
- Edge cases validation

Time Overhead

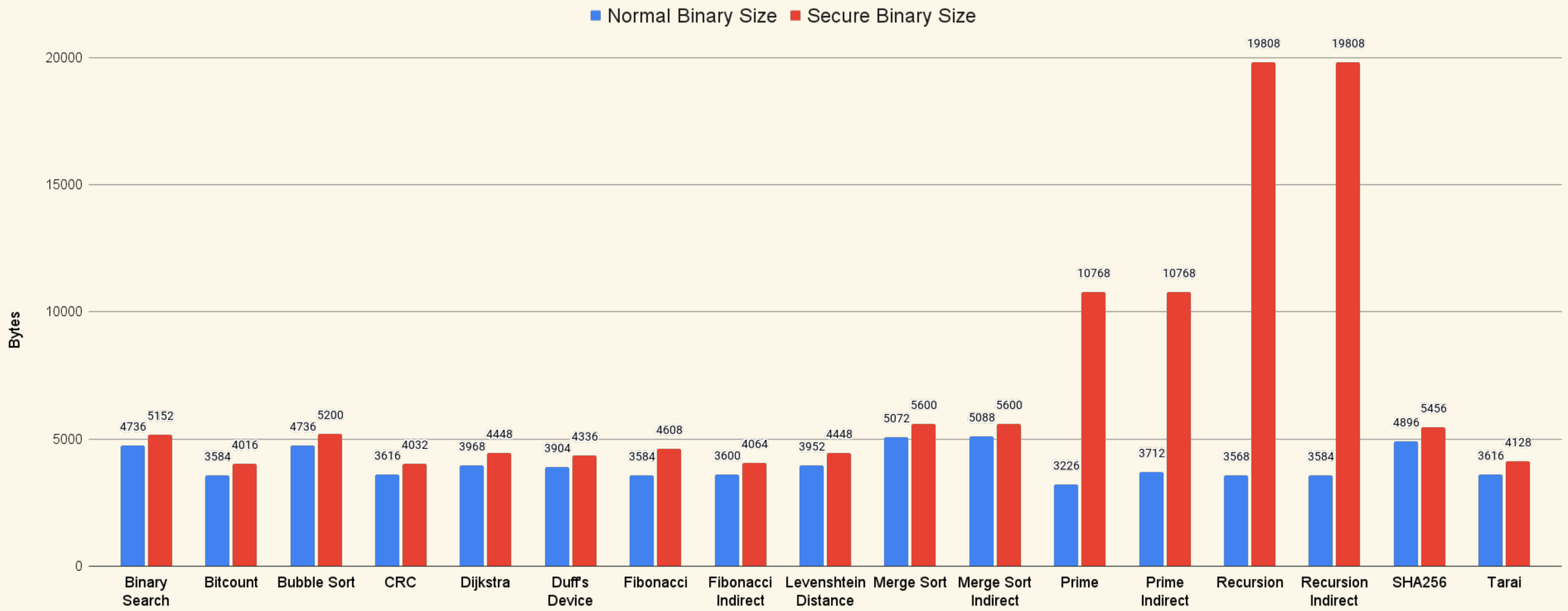
- Acceptable time overhead in most cases (med. 0,036%)
- Weak on recursive algorithms





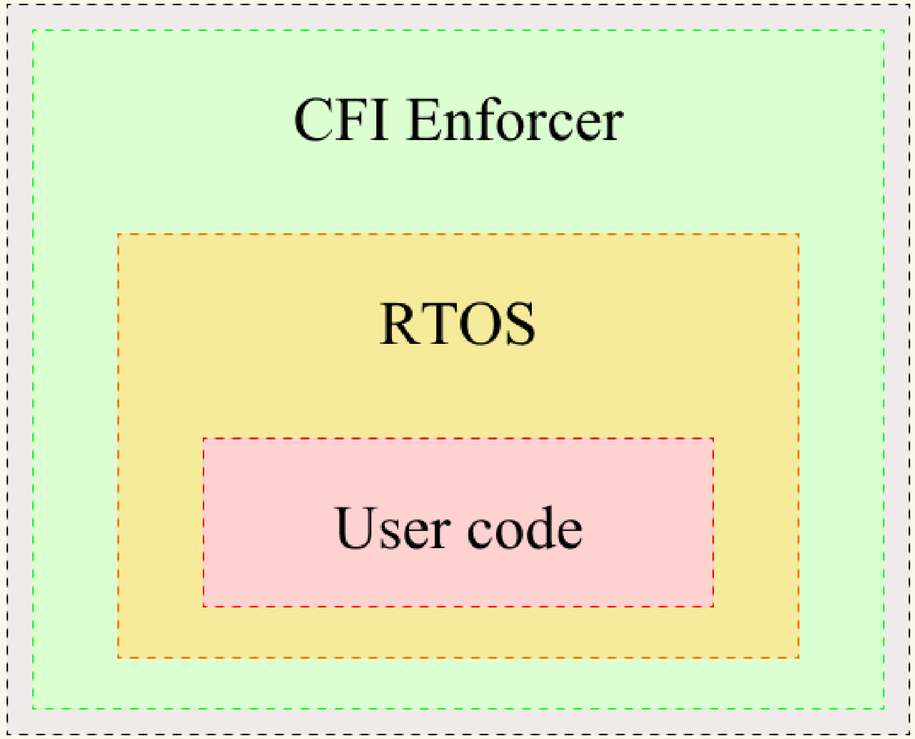
Memory Overhead

- Acceptable memory overhead in most cases (med. 12,09%)
- Weak on recursive algorithms



RTOS Integration

- Control Flow Integrity enforcer as M-mode operator
- RTOS as S-mode operator



19 DEC 2024
DAVIDE MOLETTA

UNIVERSITY OF TRENTO

Thank you for your kind attention