SoK: Integrity, Attestation, and Auditing of Program Execution

Mahmod Ammar (Independent Researcher), *Adam Caulfield (University of Waterloo)*, Ivan De Oliveira Nunes (University of Zurich)

Motivation

- Control Flow Integrity (CFI) and Control Flow Attestation (CFA) share a common threat
- Have not been systematically discussed to compare their trade-offs and synergies.

Research Questions

[Q1] How do CFA and CFI goals differ?

[Q2] What are the differences/similarities in assumptions, features, design spaces, of CFI and CFA?

[Q3] What makes CFA different from remotely attesting adherence to a CFI policy? Could CFA uncover attacks that CFI would not (and vice versa)?

[Q4] Could CFI and CFA coexist on the same platform?

Design factors and effects from current proposals

Objectives:
Local detection: detection mechanism is on executing device (CFI)
Remote Detection: detection mechanism is not on executing device (CFA)
Auditing: enabled through reliable delivery of evidence (CFA)

Mechanisms:
Enforcement: abort when violate or require only valid dest. (CFI)
Monitoring: via a tracked trace of control flow transfers (both)
Hybrid: combination of enforcement and monitoring (both)

Exec. Environments:
HW-agnostic: use SW instrumentation (both)
Extension specific – rely on ISA specific feature (both)
RoT-based – needs root of trust for key storage, measurement, signing

Objectives
Local Detection
Remote Detection
Auditing

Mechanisms
Enforcement
Monitoring
Hybrid

Exec. Env.
HW-Agnostic
Extension Specific
RoT-based

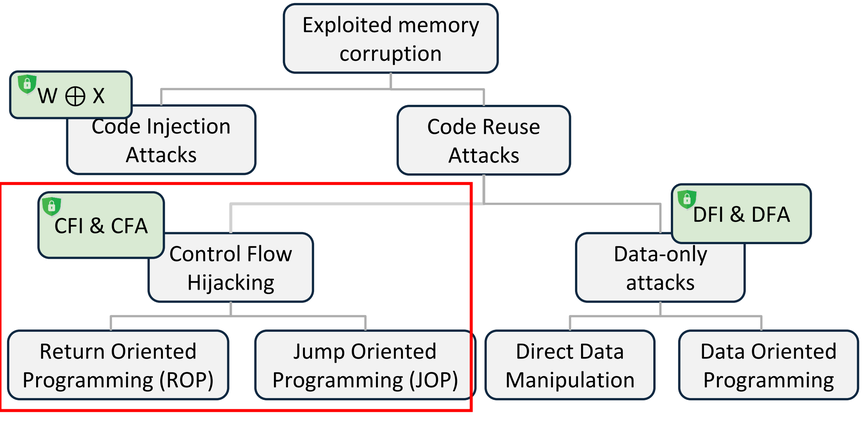
Effectiveness:
Coverage:
Granularity of scheme
Static vs. dynamic linking
Context vs. path sensitive
Observability of other attacks
Feasibility:
Effort to implement
Compatibility:
Binary vs. modular support
Hardware Dependence:
Relying on dedicated HW
Performance:
Runtime, network, hardware

Attack Vectors:
Pitfalls: exploited limitations
CFB: when using static CFG
Race conditions: TOCTOU
Side-channels: Spectre

Effectiveness
Coverage
Compatibility
Feasibility
Performance
Scalability

Attack Vectors
Pitfalls
Control Flow Bending
Race Conditions
Side-channels

Runtime Attack Landscape



Takeaways

CFI focuses on **local** detection of control-flow violations.

CFA provides **remote evidence** of execution behavior regardless of underlying policy enforcement.

CFI and CFA schemes **share many commonalities** in their strategies.

But, they have **distinct system requirements**

CFI is the best choice for **local** detection
CFA enables **remote** execution path analysis: potentially revealing logical bugs, complex path deviations, exploit root causes.

A **hybrid CFI-CFA** approach could offer **local responses** to simple attacks and **remote visibility** to complex ones.
On the other hand, **overheads** of both approaches on the same platform could challenge practical adoption.