PRIWDEN: Universally Hardening SGX Programs via Load-Time Synthesis

Georgia Tech College of Computing
School of Cybersecurity and Privacy

Fan Sang[1], Ming-Wei Shih[2], Sangho Lee[3], Xiaokuan Zhang[1], Taesoo Kim[1]
[1]Georgia Institute of Technology, [2]Microsoft, [3]Microsoft Research

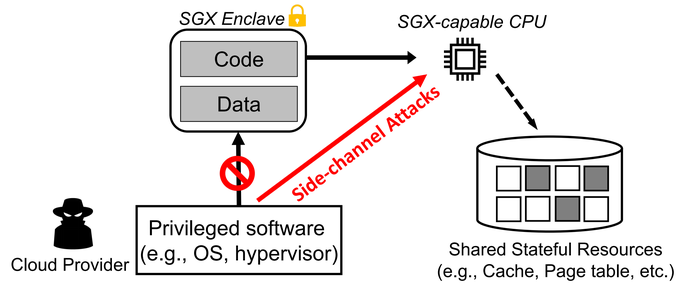
Motivation

Side-channel Attacks against SGX

- Shared resources as side channels
  - Page table [SP'15, Security'17]
  - Cache [WOOT'17, ATC'17, CHES'17]
  - Branch predictor [Security'17, ASPLOS'18]
  - TLB [CCS'17]
  - Spectre[Secuirty'18]

→ **Break the security guarantees of SGX**

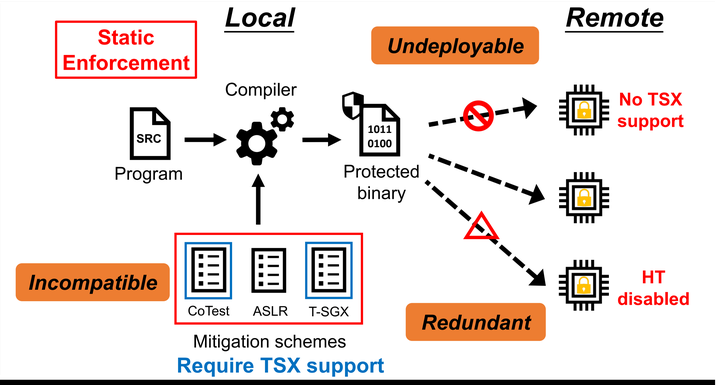
Cloud providers as attackers (with root privilege)
- **Side-channel inference with low-noise, high-resolution**



Statically Enforced Defenses

- Multiple side channels can co-exist
- Naively composite mitigations:
  - **Undeployable:** unavailable features
  - **Redundant:** over-protection
  - **Incompatible:** conflicting mitigations

→ **Problems with scheme composition**



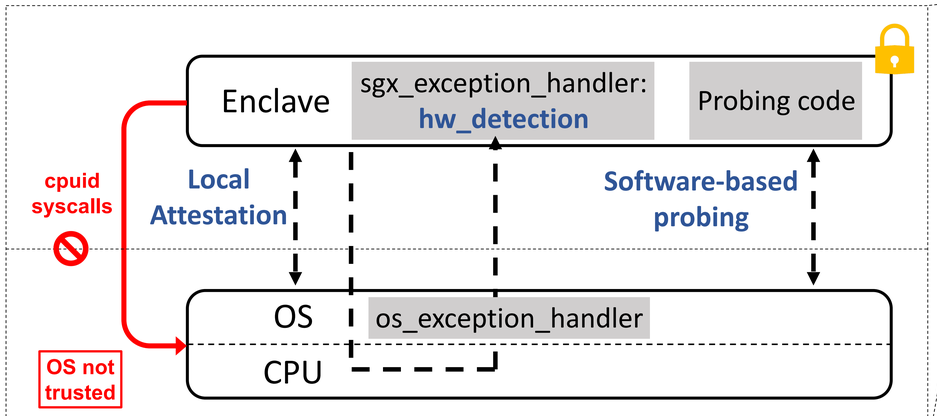
PRIDWEN Framework

A framework that uses ***load-time synthesis*** to ***dynamically*** harden SGX programs by ***selectively applying*** different mitigation techniques according to the ***configurations on the target execution platform***.

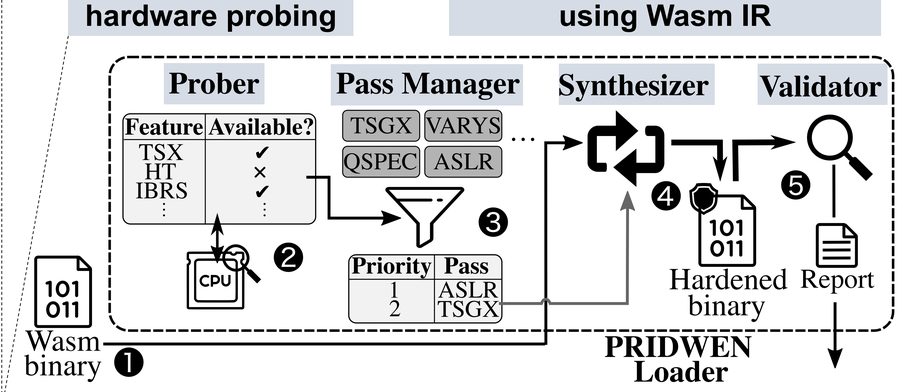
Goals of PRIDWEN:

- **Adaptivity:** select mitigation techniques that confirm to the capabilities of the target platform
- **Attestability:** support remote attestation of the dynamically generated binary
- **Extensibility:** support legacy and future mitigation techniques and platforms

→ **Universally hardening SGX programs**



User-mode hardware probing | **Load-time program synthesis using Wasm IR**



Optimal pass selection | **Post-synthesis validation & final binary attestation**

Evaluation

Prototype implementation

- Fine-grained ASLR
- T-SGX
- Varys
- QSpecture

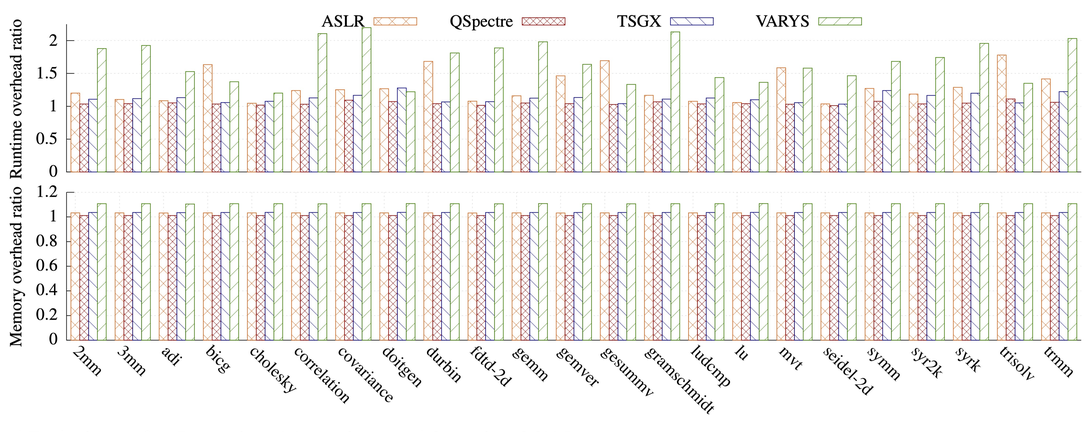
Evaluation metrics:

- Security analysis
- Correctness
- Performance of PRIDWEN
- Performance of synthesized binaries

→ **Poses moderate performance overhead**

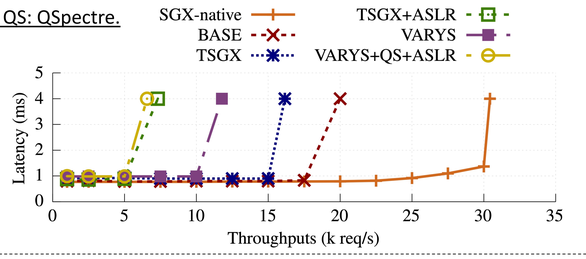
→ **Retains faithfulness of execution semantics**

Runtime performance and memory overheads of PRIDWEN-hardened, compared to BASE.



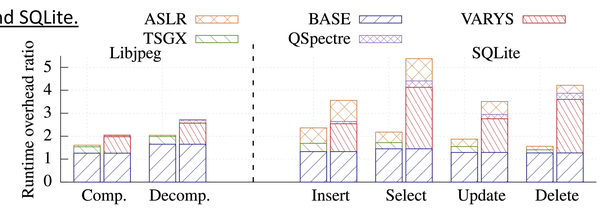
The performance of Lighttpd; QS: QSpectre.

Base: **1.5x**
T-SGX: **1.9x**
Varys: **2.6x**
Multiple: **4.6x**



The performance of libjpeg and SQLite.

Base: **1.2-1.7x**
HW-assisted: **1.9x**
SW-only: **3.4x**



NSF 1563848: TWC: Medium: Collaborative: Systems, Tools, and Techniques for Executing, Managing, and Securing SGX Programs