Designing a Provenance Analysis for SGX Enclaves

Flavio Toffalini, Mathias Payer, Jianying Zhou, Lorenzo Cavallaro

SGX Prohibits Provenance

Adversaries use memory corruption errors to mount code-reuse attacks
External observers cannot distinguish correct and hijacked executions

Design

Properties guaranteed:
1) Secure streaming of runtime information
2) Detecting code-reuse attacks

Design: Tracing

Design: Streaming

Evaluation: Overhead

Evaluation: Model

Symex explores the majority of the functions
We fallback to static analysis only for few cases

Macrobenchmark over StealthDB (PostgreSQL’s SGX plugin) has limited overhead

Partially Sponsored By