TLBlur: Compiler-Assisted Automated Hardening against Controlled Channels on Off-the-Shelf Intel SGX Platforms

Daan Vanoverloop[1], Andrés Sánchez[2,4], Flavio Toffalini[2,3], Frank Piessens[1], Mathias Payer[2], Jo Van Bulck[1]
[1]DistriNet, KU Leuven, Belgium, [2]EPFL, Switzerland, [3]RUB, Germany, [4]Amazon

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE | ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL | ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED

Controlled-Channel Attacks on Intel SGX

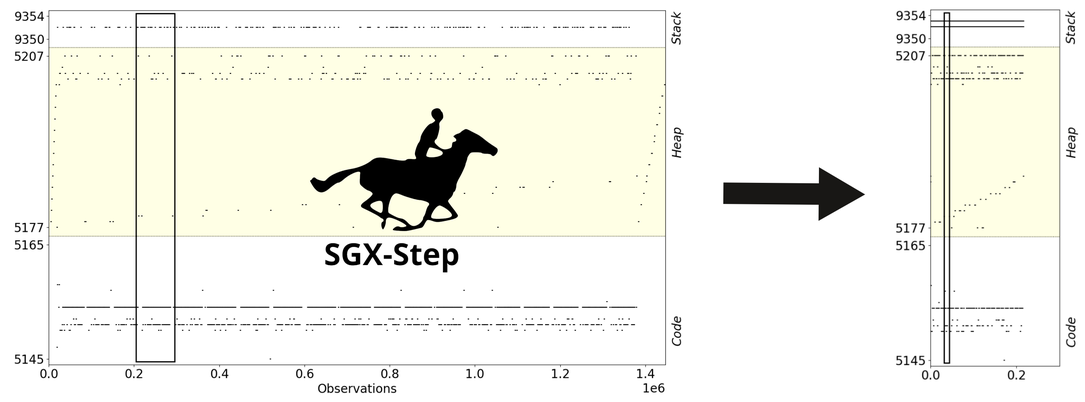
usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Original image | Xu et al. (Oakland 2015) | Our attack with AEX-Notify single-stepping mitigation

Single-stepping mitigation is not enough!

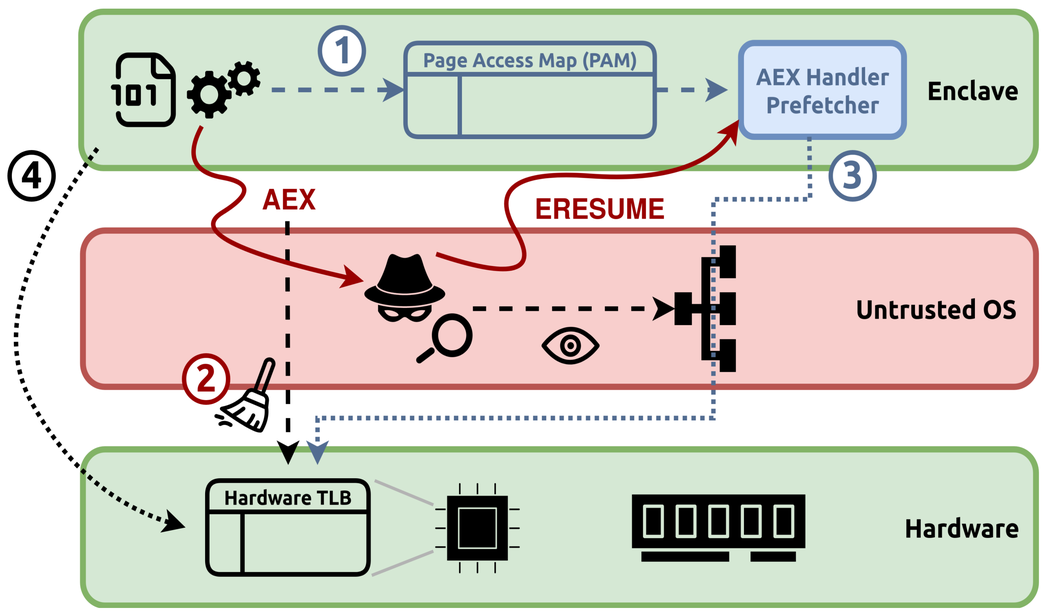
AEX-Notify: Thwarting Single-Stepping Attacks

Hardware extension: Interrupt awareness for Intel SGX enclaves
Software mitigation: Prefetch next code page + stack pages

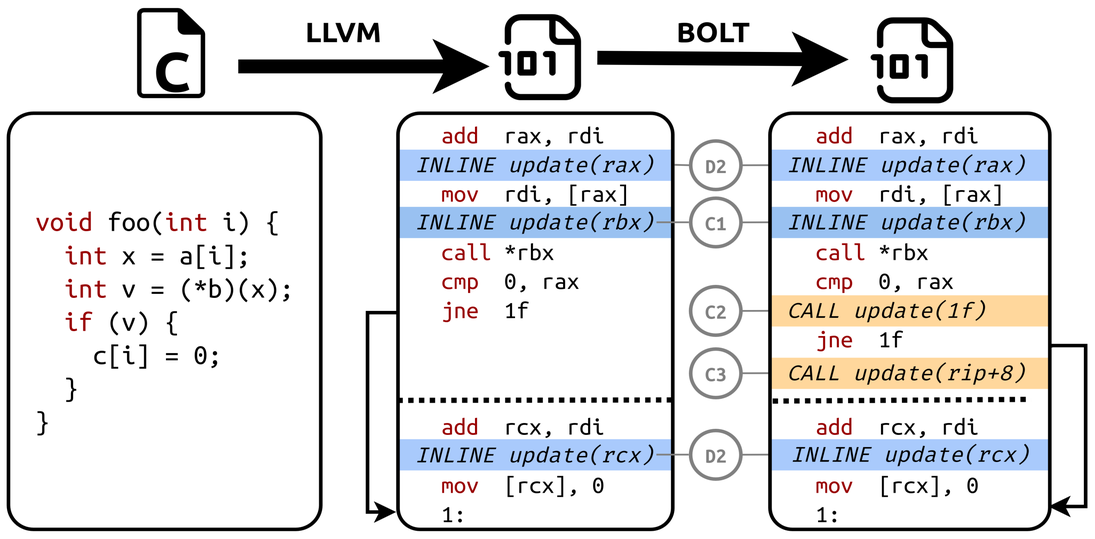


Idea: Limit temporal resolution

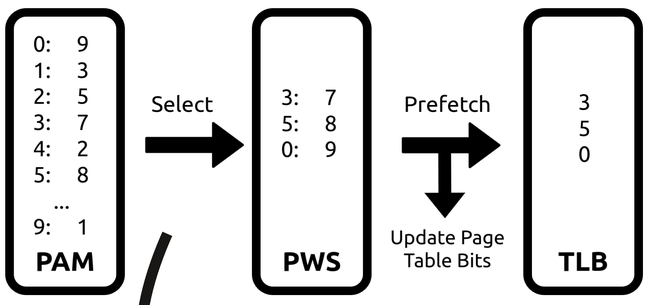
TLBlur Overview



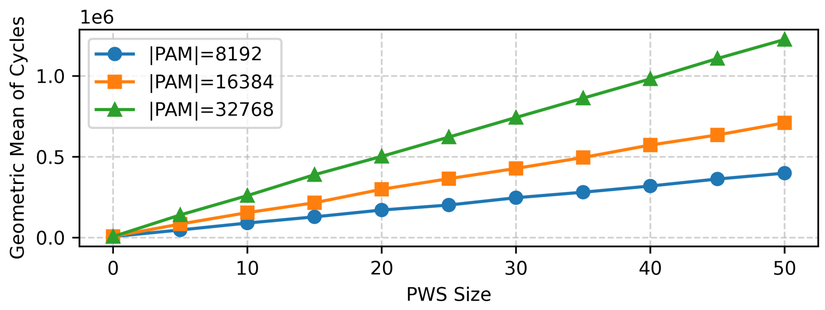
Practical Compiler and Binary Instrumentation



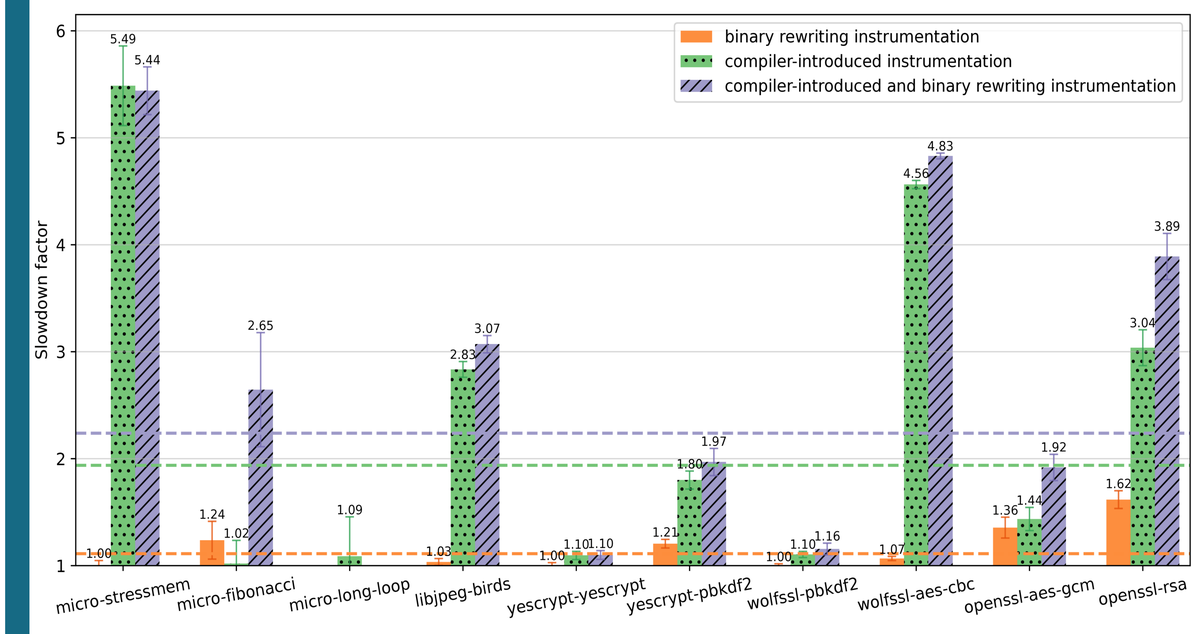
Constant-Time Working Set Estimation



After each interrupt:
- Select from Page Access Map (PAM)
- Sort Prefetch Working Set (PWS)
- Prefetch PWS into TLB

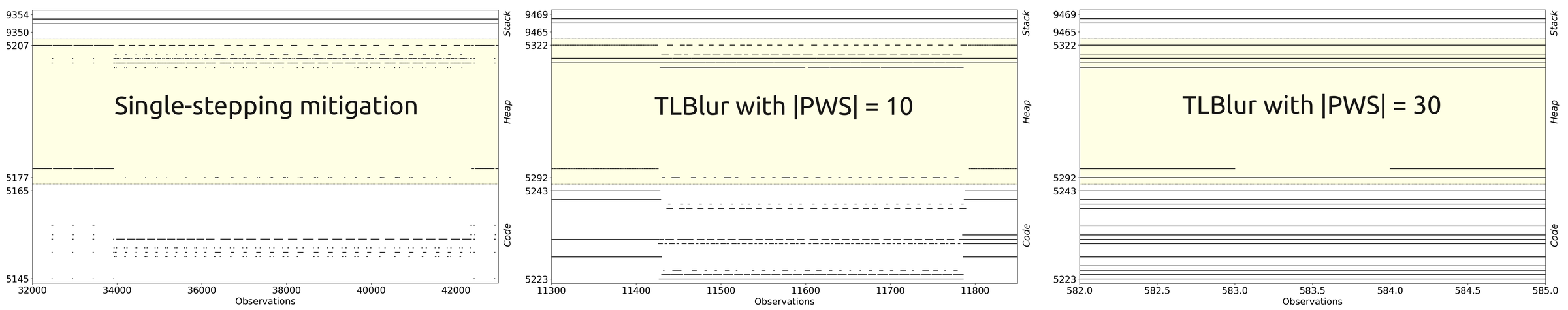


Performance Evaluation



Average: x2.24 instrumentation + 25% perfetching overhead = x2.80

Leakage Reduction in Practice: Libjpeg Compiler Hardening



34th USENIX Security Symposium, 2025

RUHR UNIVERSITÄT BOCHUM RUB EPFL KU LEUVEN DistriNet