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

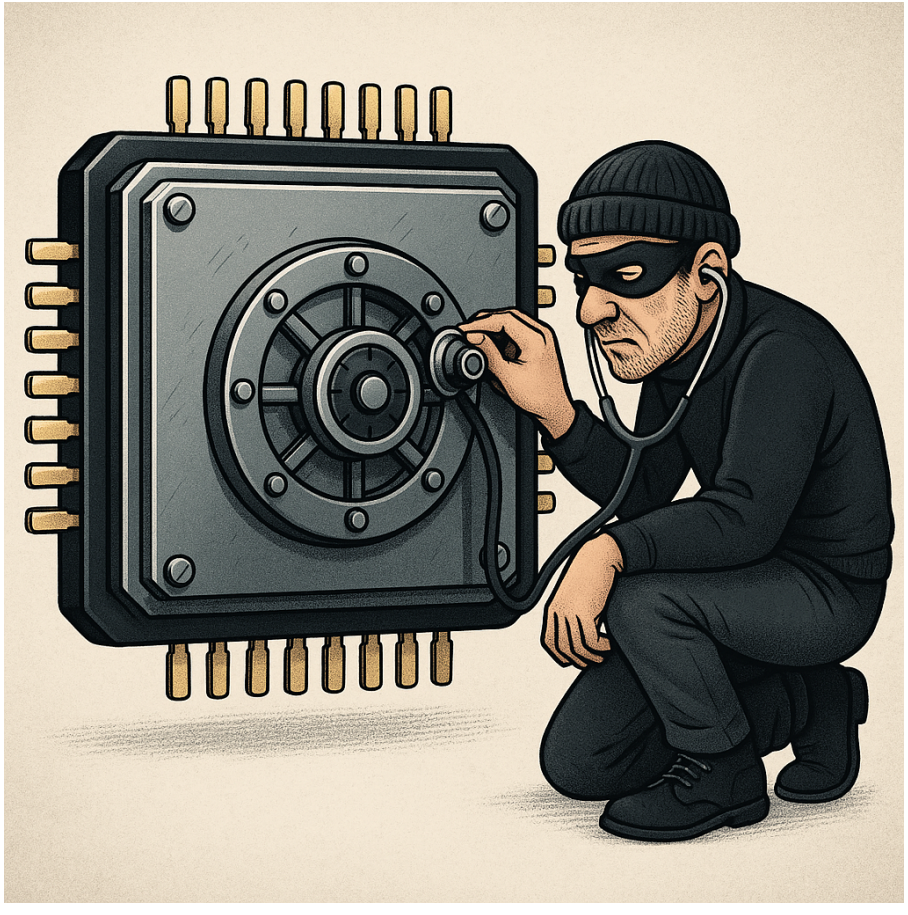
Daan Vanoverloop[1], Andrés Sánchez[2,4], Flavio Toffalini[2,3], Frank Piessens[1], Mathias Payer[2], Jo Van Bulck[1]

[1]DistriNet, KU Leuven, Belgium, [2]EPFL, Switzerland, [3]RUB, Germany, [4]Amazon

DistriNet KU LEUVEN EPFL RUHR UNIVERSITÄT BOCHUM RUB

Intel SGX: Hardware-Level Isolation

Side-Channel Attacks on Intel SGX



Side-Channel Attacks on Intel SGX

Side-Channel Attacks on Intel SGX

Spatial Resolution

Side-Channel Attacks on Intel SGX

Spatial Resolution

Temporal Resolution

SGX-Step

Side-Channel Attacks on Intel SGX

Spatial Resolution

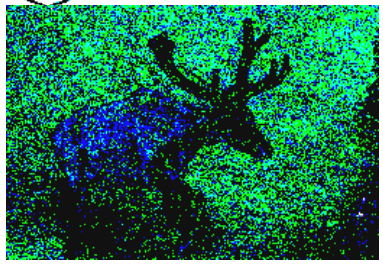
Temporal Resolution

2 years ago at USENIX: **AEX-Notify**

Limit temporal resolution

Side-Channel Attacks on Intel SGX

Spatial Resolution



Still possible with AEX-Notify mitigation!

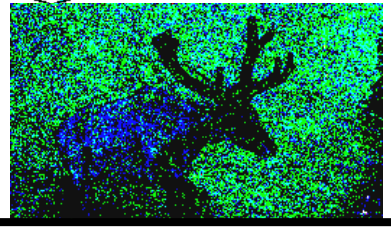
Temporal Resolution

2 years ago at USENIX: **AEX-Notify**

Limit temporal resolution

Side-Channel Attacks on Intel SGX

Spatial Resolution

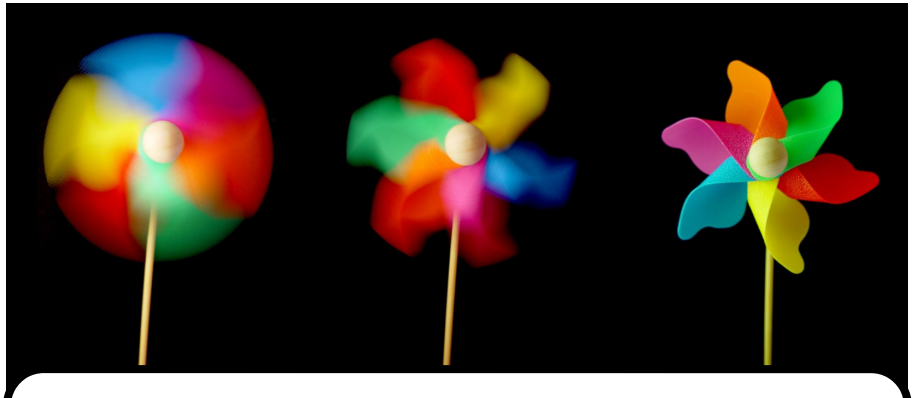


Today at USENIX:

TLBlur

Limit spatial resolution

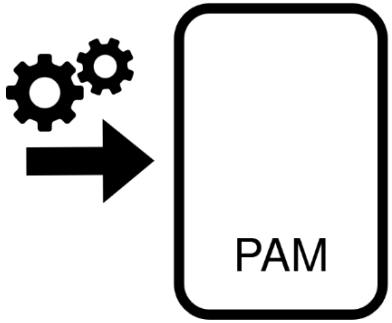
Temporal Resolution

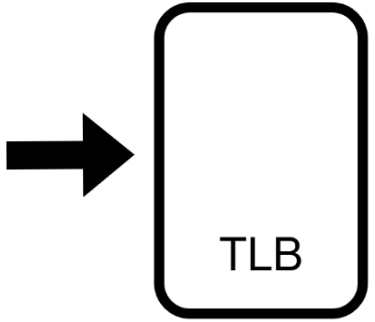


2 years ago at USENIX: **AEX-Notify**

Limit temporal resolution

TLBlur Overview





① Instrumentation ② Page-access tracing ③ Page Prefetching