Full paper at ACM CCS 2021

SmashEx

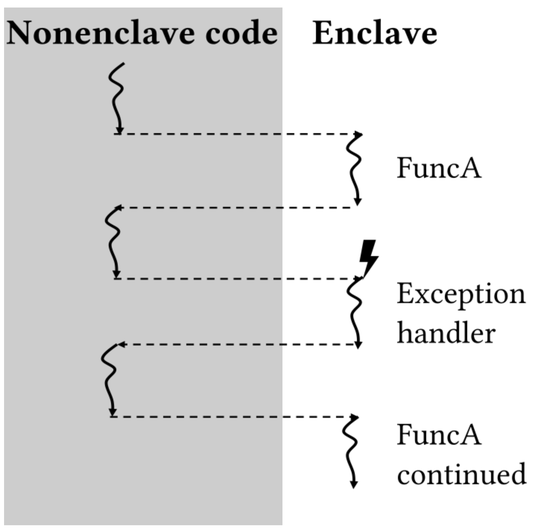
Smashing SGX Enclaves Using Exceptions

Jinhua Cui[1] Jason Zhijingcheng Yu[2] Shweta Shinde[3] Prateek Saxena[2] Zhiping Cai[1]

[1] National University of Defense Technology, Changsha [2] National University of Singapore [3] ETH Zürich

Overview

In-Enclave Exception Handling



Safety Requirements

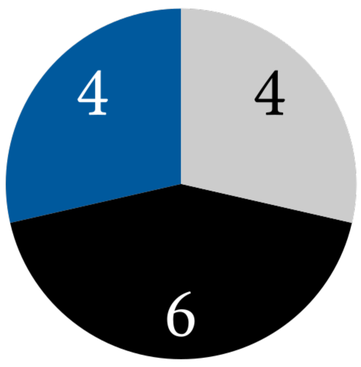
- ✓ Context save/restore
- ✓ Safe control resumption
- ✗ Atomicity

Lacking in enclaves!

SmashEx

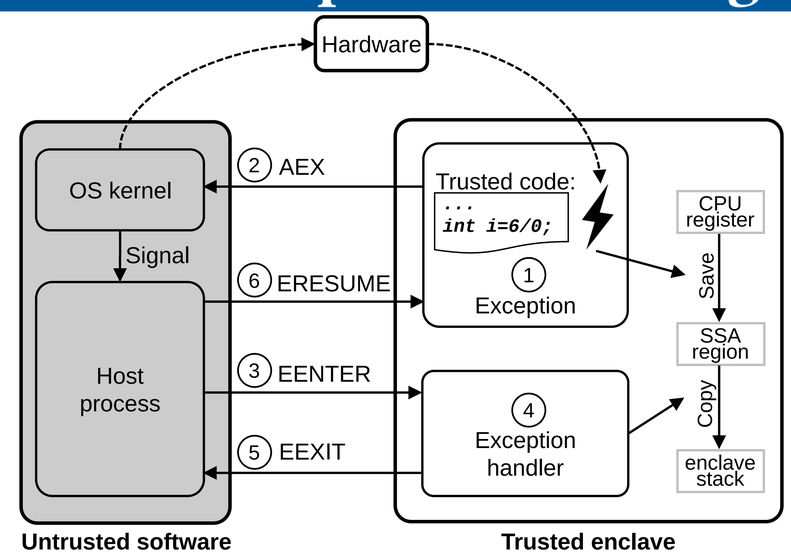
Exploits **enclave runtimes**
(e.g., Intel SGX SDK, OpenEnclave)
- Memory corruption
- Return-oriented programming

Among 14 surveyed enclave runtimes

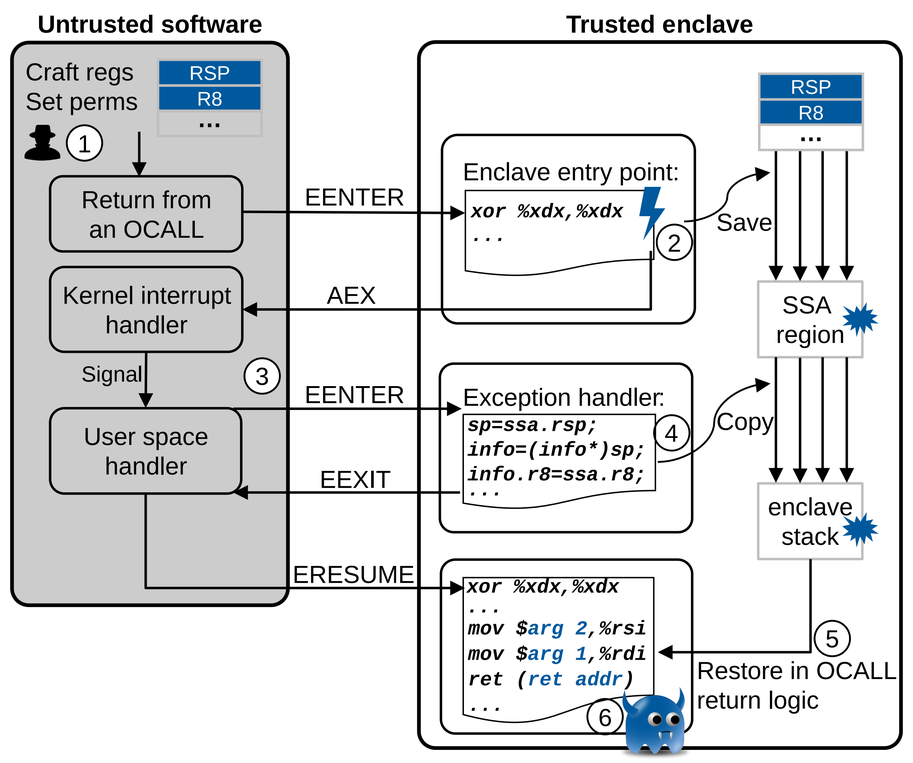


- affected on both SGX 1 and SGX 2
- affected on SGX 2 but not SGX 1
- unaffected

SGX Exception Handling

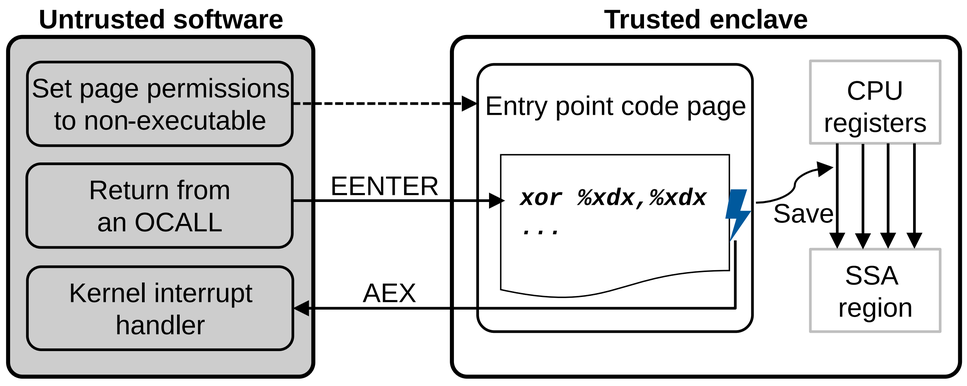


Attack Overview

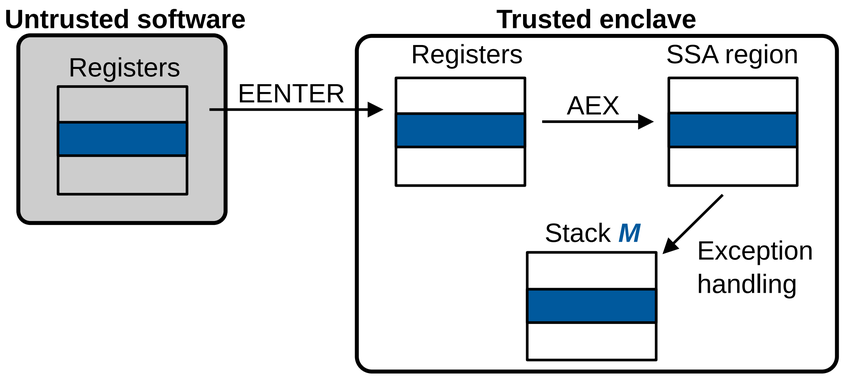


Attack Process

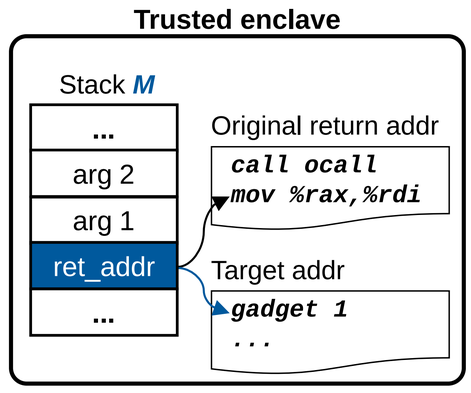
AEX injection



Stack corruption



Control-flow hijacking



Mitigations and Defences

Unaffected runtimes

Ratel
Dedicated exception handling stack

Fortanix Rust EDP, Alibaba Inclavare
Disabling exception handling

Graphene-SGX
Re-entrant exception handler

Other software defences

Stack canary
ASLR

Can be circumvented!

Hardware atomicity interfaces

Temporarily disabling exceptions
Temporarily disabling enclave re-entries

Responsible Disclosure

May 2021
Notified Intel and Microsoft.

October 2021
Intel assigned CVE and released advisory.
SmashEx released publicly.

July 2021
Intel and Microsoft released patches.
Microsoft assigned CVE and released advisory.

CCS '21 Paper	Web page	Jason's homepage

NUS National University of Singapore

ETH zürich

国防科技大学 National University of Defense Technology