Fix the leak: Side-Channel Protection for SGX using Data Location Randomization

Alexandra Dmitrienko
Julius-Maximilians-Universität Würzburg
alexandra.dmitrienko@uni-wuerzburg.de
Who am I?

- High-tech woman
- Was born and grown up in Russia
- BSc and MSc in Information Security
  - from St. Petersburg State Polytechnic University
- 10+ years in security research in large research hubs in Europe
  - Ruhr-University Bochum
  - Center for Advanced Security Research in Darmstadt (CASED)
  - ETH Zurich
- Now, Professor at Uni Würzburg
  - Secure Software Systems research group
Did you know?

- It is generally hard to get professorship in Germany.
- It is double as hard for a female in technical disciplines.
- It is triple as hard for a foreigner.
Key Success Factors

- Passion
- Luck
- Support
- Ambitions
- Hard Work
- Never giving up
Last but not least: Keeping yourself motivated
What are high-tech women capable of?

• Anything what women typically do… anything that men typically do

and beyond!
Leaky Intel SGX
Intel Software Guard eXtensions

Application         Sensitive code         Application

OS

RAM
Intel Software Guard eXtensions

EPC: Enclave Page Cache

Application

Enclave

Application

OS

RAM

EPC

March 4, 2020

High-Tech Women: From Cybersecurity to Artificial Intelligence
Intel Software Guard eXtensions

EPC: Enclave Page Cache
Intel Software Guard eXtensions

EPC: Enclave Page Cache
Intel Software Guard eXtensions

EPC: Enclave Page Cache
Intel Software Guard Extensions

- Application
- Enclave
- Application
- OS
- Paging
- Caches
- RAM
- EPC

March 4, 2020
Background: Intel Software Guard Extensions

Application

Enclave

Application

OS

Paging

Caches

RAM

EPC
Leaking Information through Side-Channels

System

Entity 1

Entity 2

Victim

Attacker

Observe

Utilize

High-Tech Women: From Cybersecurity to Artificial Intelligence
Leakage through Paging Side Channel

Single-trace RSA key recovery from RSA key generation procedure of Intel SGX SSL via controlled-channel attack on the binary Euclidean algorithm (BEA)

[Weiser et al., AsiaCCS’18]

[Xu et al., IEEE S&P’15]
Information Leakage through shared hashes

Core 0
- Logical Processor 0 (App)
- Logical Processor 1 (Enclave)
- Cache L1
- Branch Pred.
- Cache L2
- Cache L3

Core 1
- Logical Processor 2 (Enclave)
- Logical Processor 3 (App)
- Cache L1
- Branch Pred.
- Cache L2
- Cache L3
Information Leakage through shared hashes

- Extract AES from key
  - Attack requires enclave interruption (incurs detectable delays) [Brasser et al., WOOT’17]

- Extract RSA key and genome data from synchronized victim
  - Use CPU branch prediction caches to infer control flow of a victim [Lee et al., Usenix Sec’17] & [arXiv:1611.06952]

- Extract AES key from synchronized victim enclave (no enclave interruption required) [Götzfried et al., EuroSec’17]

- An attacker resides in another enclave, thus evading detection [Schwarz et al., DIMVA’17 & arXiv:1702.08719]
Side-Channel Mitigations: State-of-the-art

- **Side-channel resilient code**
  - Requires:
    - High expertise
    - Vast effort

- **Annotation-based protections**
  - Requires:
    - High expertise
    - Significant effort

- **Oblivious Execution**
  - Extremely high overhead (83x, up to 220x)
  - [Obfuscuro, Ahmad et al., NDSS 2019]
Our Recent Work:
DR.SGX: Automated and Adjustable Side-Channel Protection for SGX using Data Location Randomization

Joint work with
Ferdinand Brasser\textsuperscript{1}, Tommaso Frassetto\textsuperscript{1}, Kari Kostiainen\textsuperscript{2}, Srdjan Capkun\textsuperscript{2}, Ahmad-Reza Sadeghi\textsuperscript{1}

\textsuperscript{1}TU Darmstadt, \textsuperscript{2}ETH Zurich

[ACSAC 2019]
The Big Picture

SGX

Side channel leakage

RAM

DR.SGX
Features

- Compiler-based solution does not require any code annotations.
- Continuously (re-)randomizes memory locations at runtime.
- Balances between side-channel protection and performance overhead through a configurable parameter.
DR.SGX Re-randomization

FFX Format-Preserving Encryption scheme with AES as a block cipher

Initial layout

A
B
C
D
E
F
G
H

Layout 1

Permutation $\pi_1$

F
C
G
E
D
H
A
B

Layout 2

Permutation $\pi_2$

G
D
B
E
C
H
A
F

Re-randomization window

Time

March 4, 2020
High-Tech Women: From Cybersecurity to Artificial Intelligence
Performance Evaluation using Nbench

- Without runtime re-randomization (geometric mean about 4x)
Performance Evaluation using Nbench

- With different re-randomization windows (geometric mean up to 12x)
Conclusion

• Leaky SGX
  • Side-channel attacks are a major threat to Intel SGX
  • Were deemed as ‘too difficult’ and were left out of the attacker model
  • Research has shown it otherwise

• Dr.SGX
  • provides a generic protection for Intel SGX enclaves
  • configurable and developer-friendly
  • much more efficient than ORAM