Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

Secure Software Systems

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

Alexandra Dmitrienko
Julius-Maximilians-Universität Würzburg

alexandra.dmitrienko@uni-wuerzburg.de

MARCH 4, 2020

High-Tech Women: From Cybersecurity to Artificial Intelligence

Whoaml?

- 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

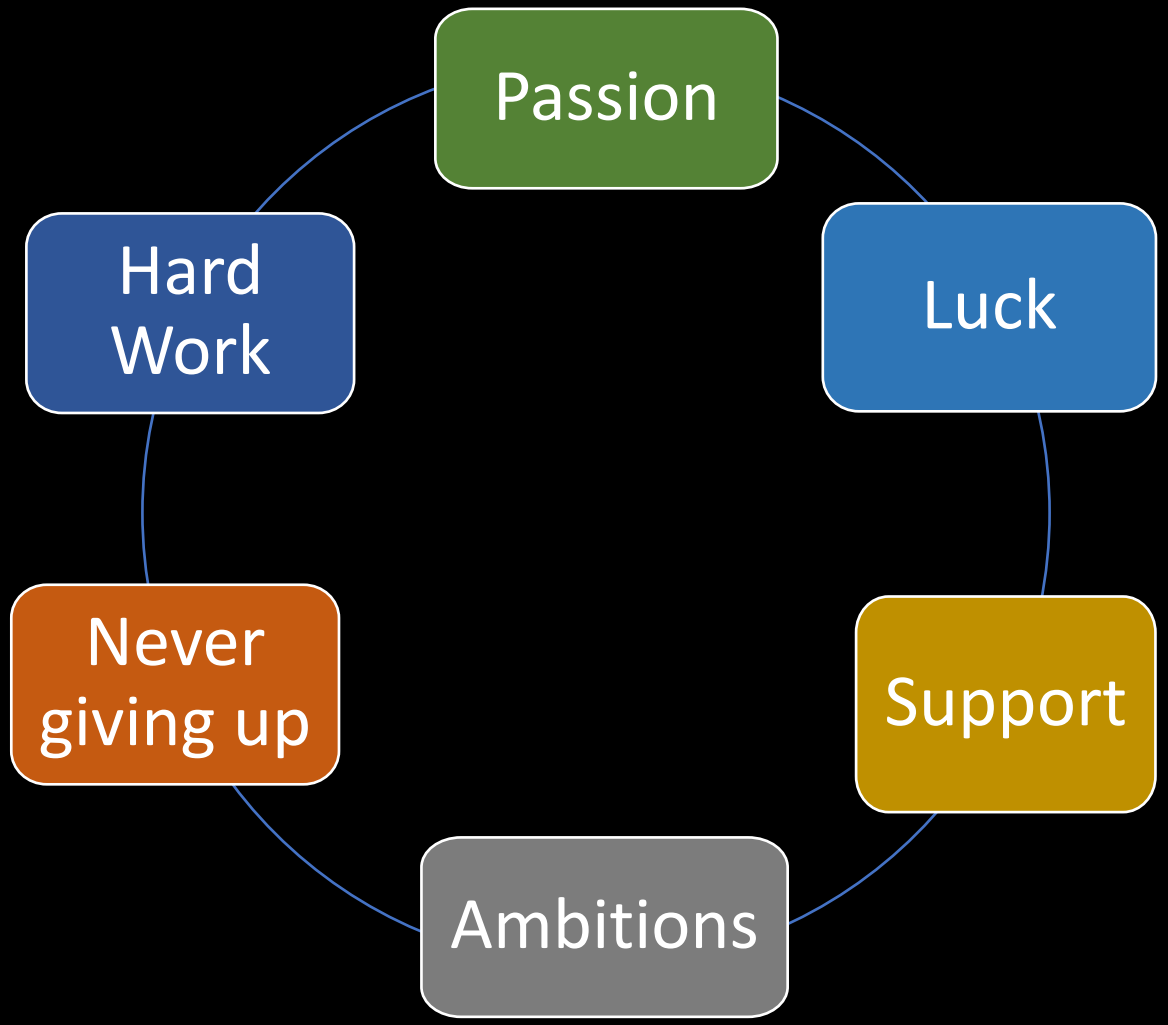
Did you know?

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



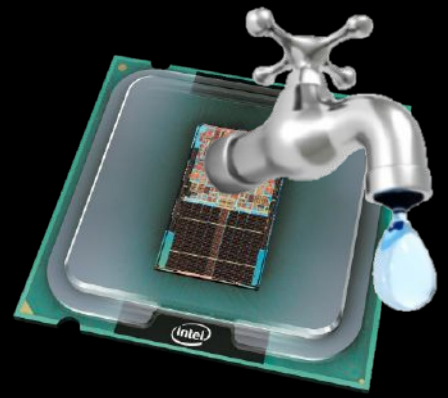
Last but not least: Keeping yourself motivated

What are high-tech women capable of?

- Anything what women typically do…

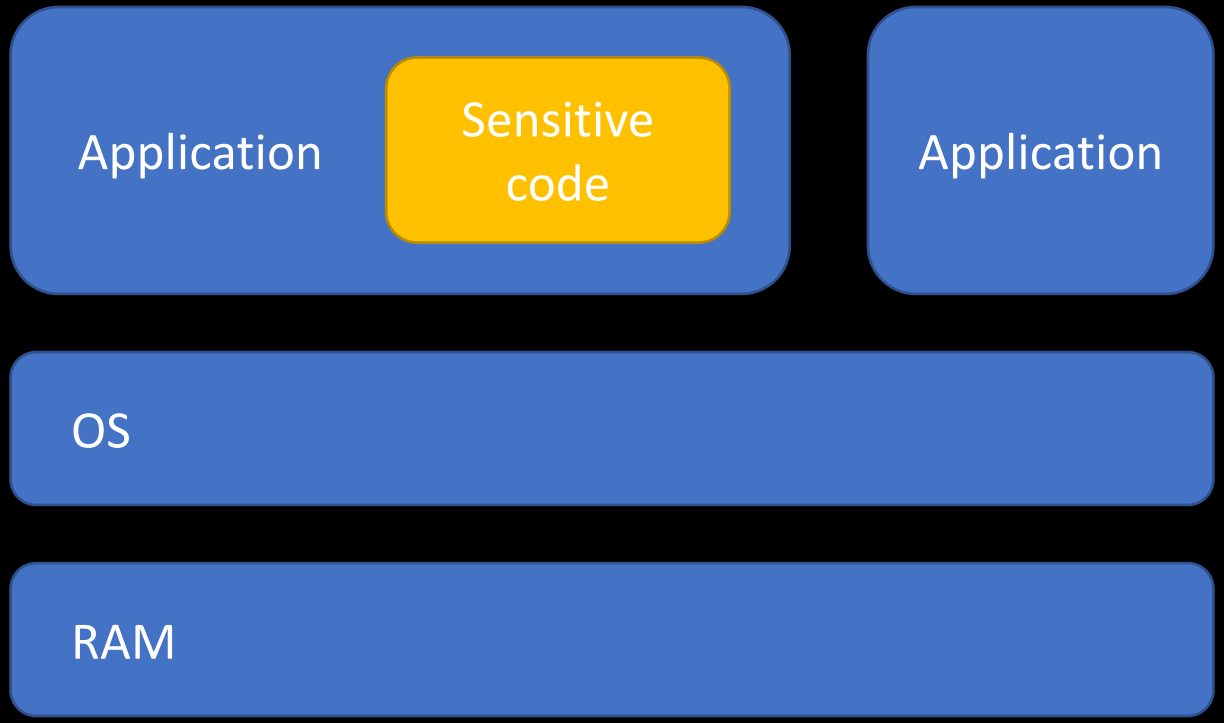
anything that men typically do

and beyond!

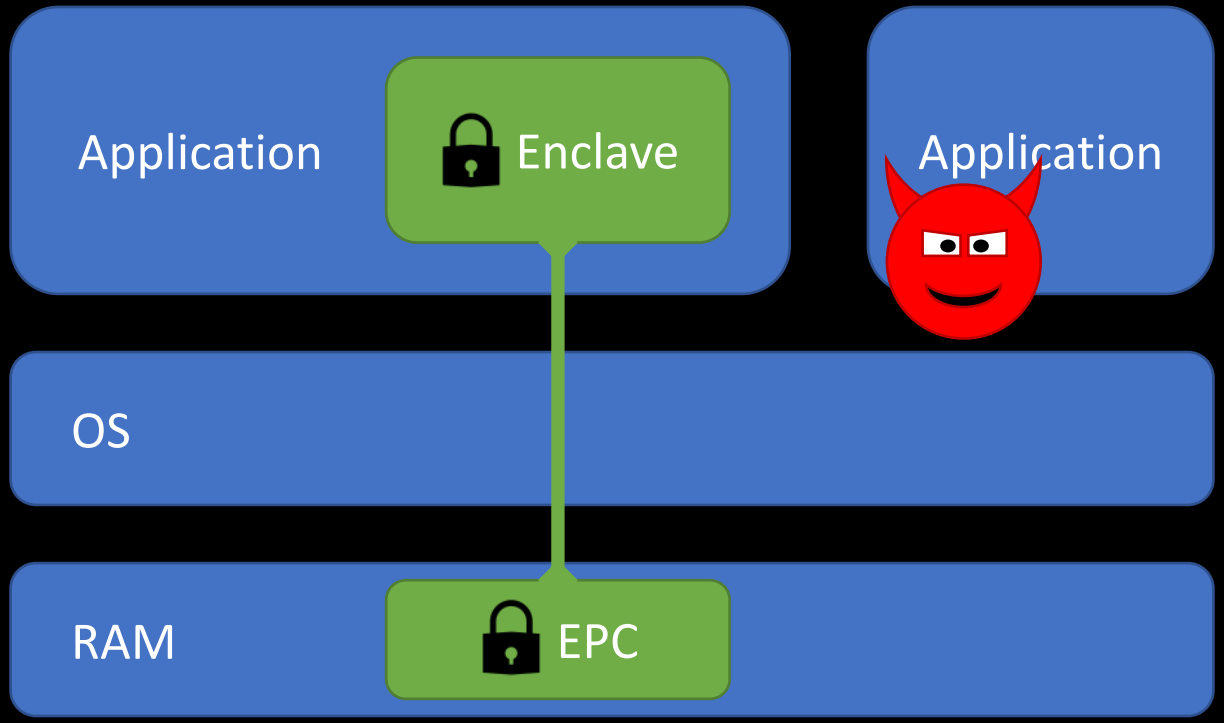


Leaky Intel SGX

Intel Software Guard eXtensions

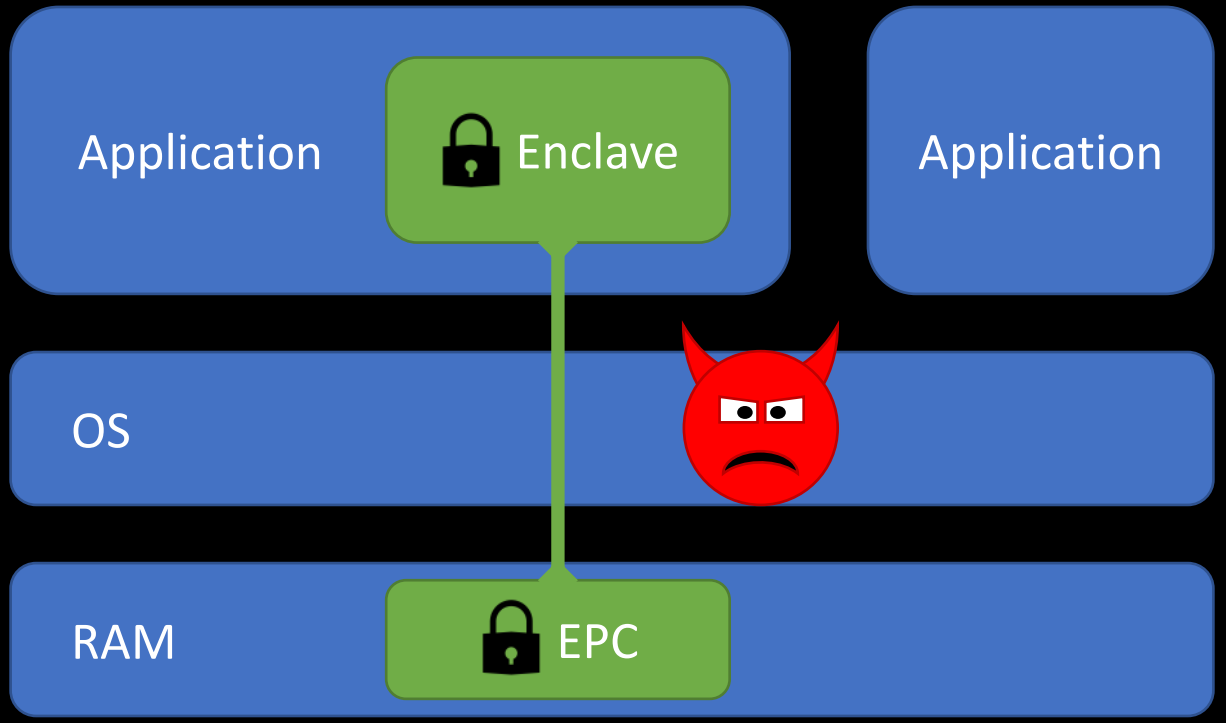


Intel Software Guard eXtensions



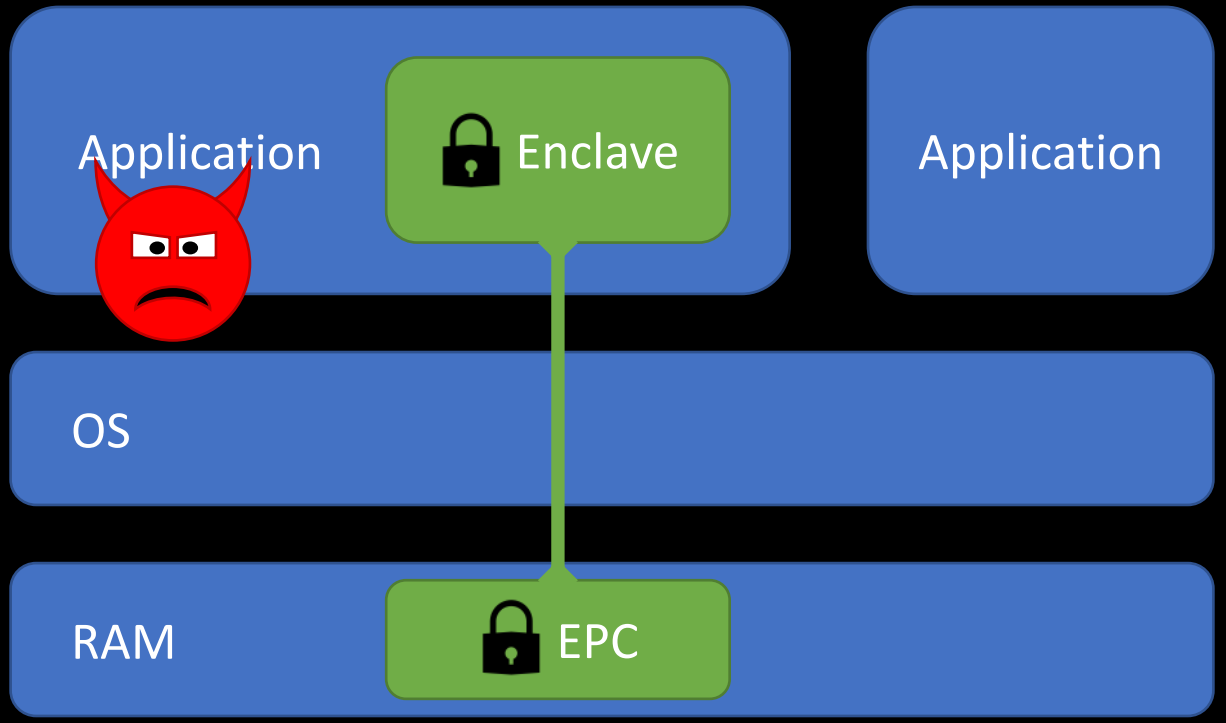
EPC: Enclave Page Cache

Intel Software Guard eXtensions



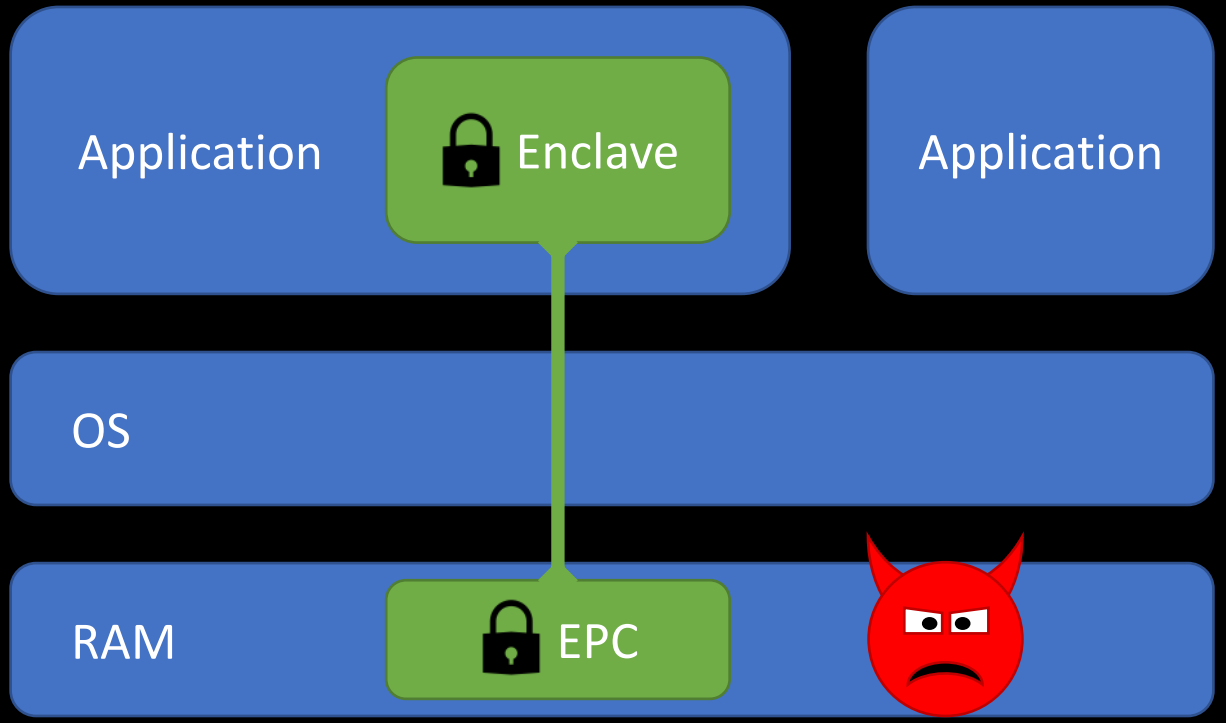
EPC: Enclave Page Cache

Intel Software Guard eXtensions



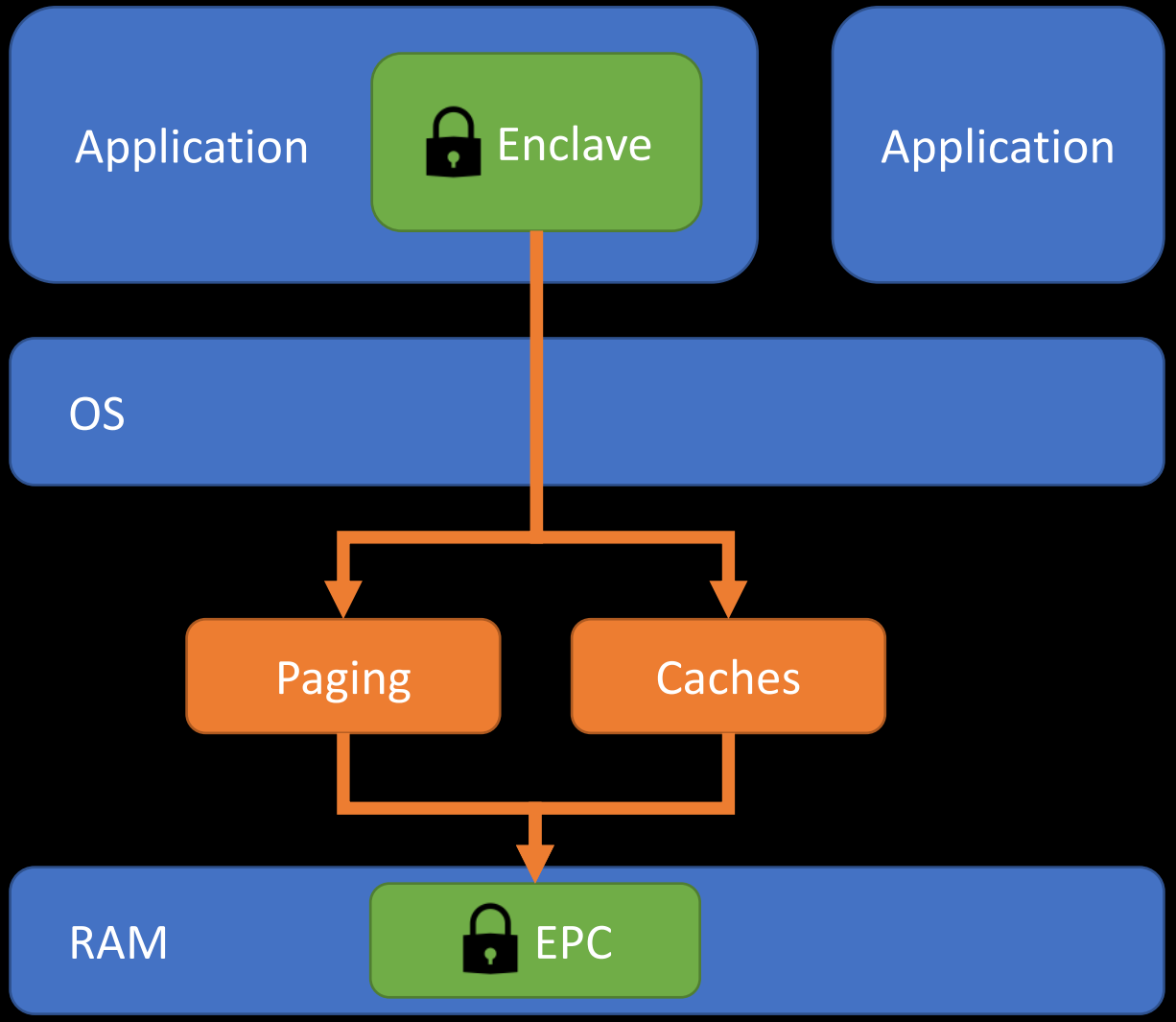
EPC: Enclave Page Cache

Intel Software Guard eXtensions

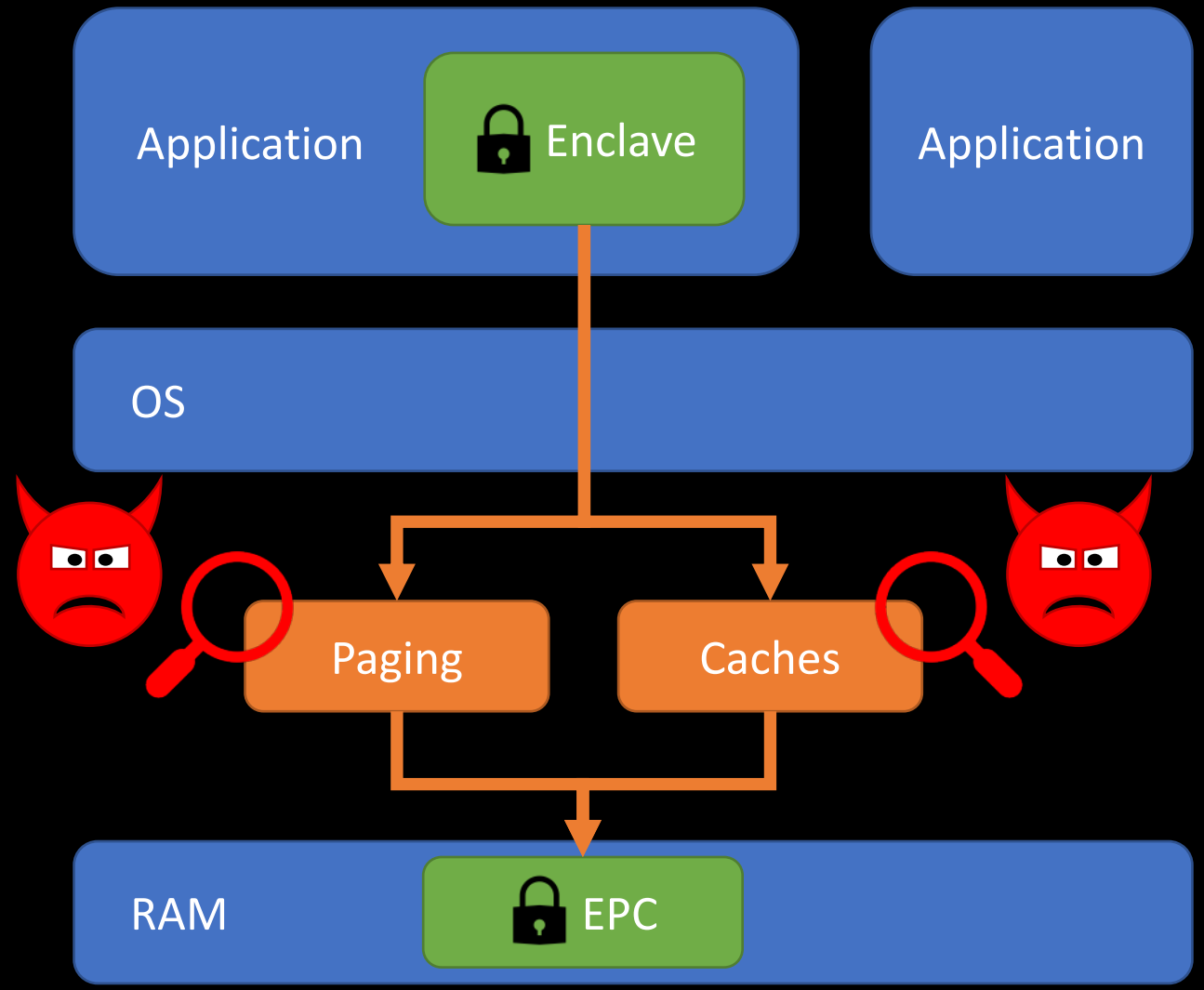


EPC: Enclave Page Cache

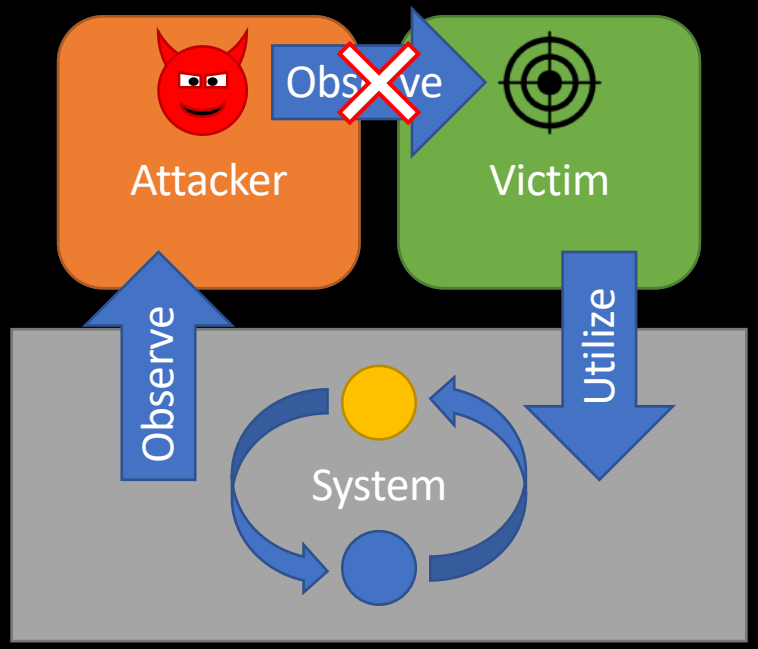
Intel Software Guard Extensions



Background: Intel Software Guard Extensions



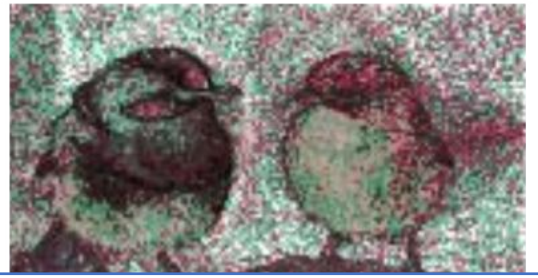
Leaking Information through Side-Channels



Leakage through Paging Side Channel

Original

Recovered

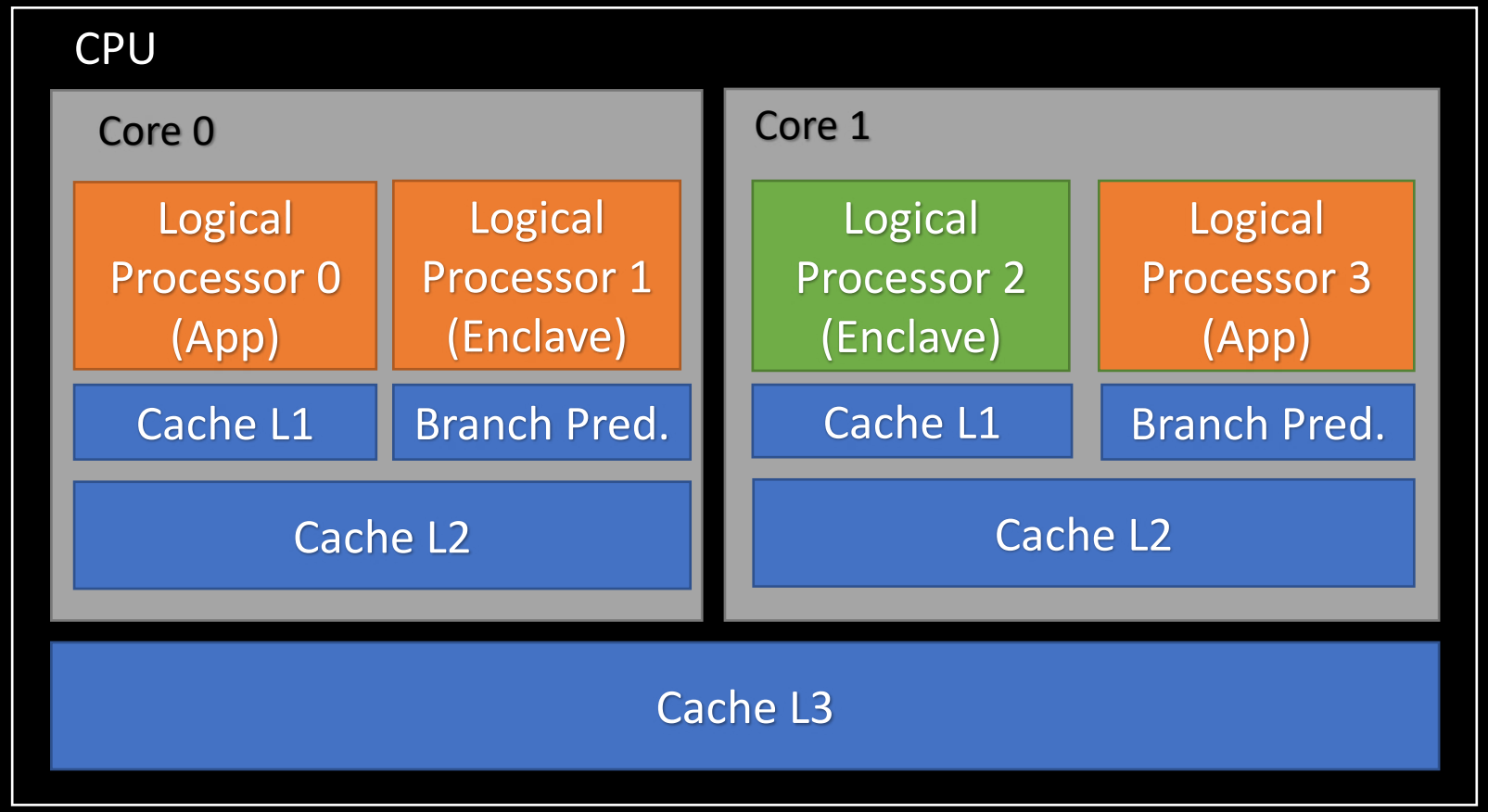


Single-trace RSA key recovery from RSA key generation procedure of Intel SGX SSL via controlled-channel attack on the binary Euclidean algorithm (BEA)

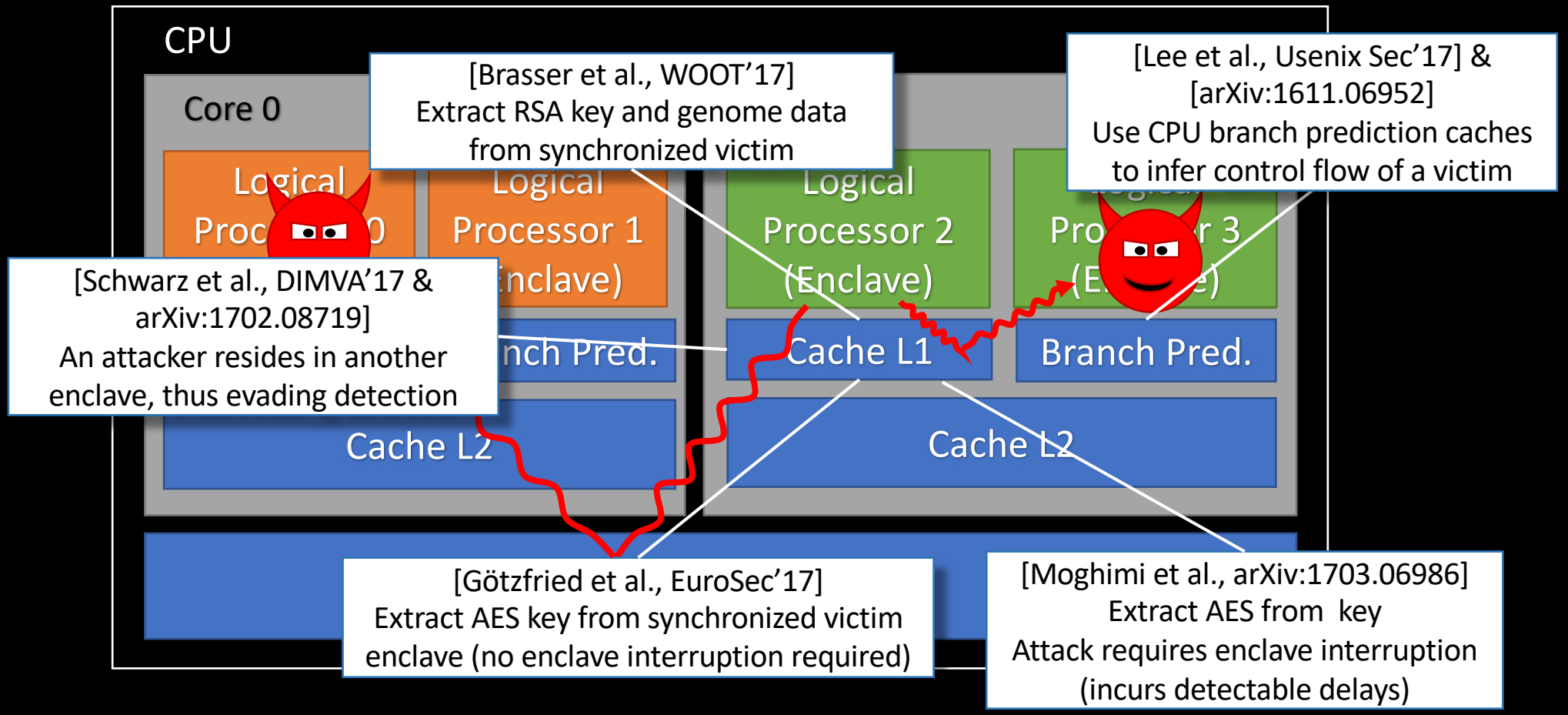
[Weiser et al., AsiaCCS'18]

[Xu et al., IEEE S&P'15]

Information Leakage through shared hashes



Information Leakage through shared hashes



Side-Channel Mitigations: State-of-the-art

Side-channel resilient code	Annotation-based protections	Oblivious Execution
Requires: • High expertise • Vast effort	Requires: • High expertise • Significant effort	Extremely high overhead (83x, up to 220×) [Obfuscuro, Ahmad et al., NDSS 2019]

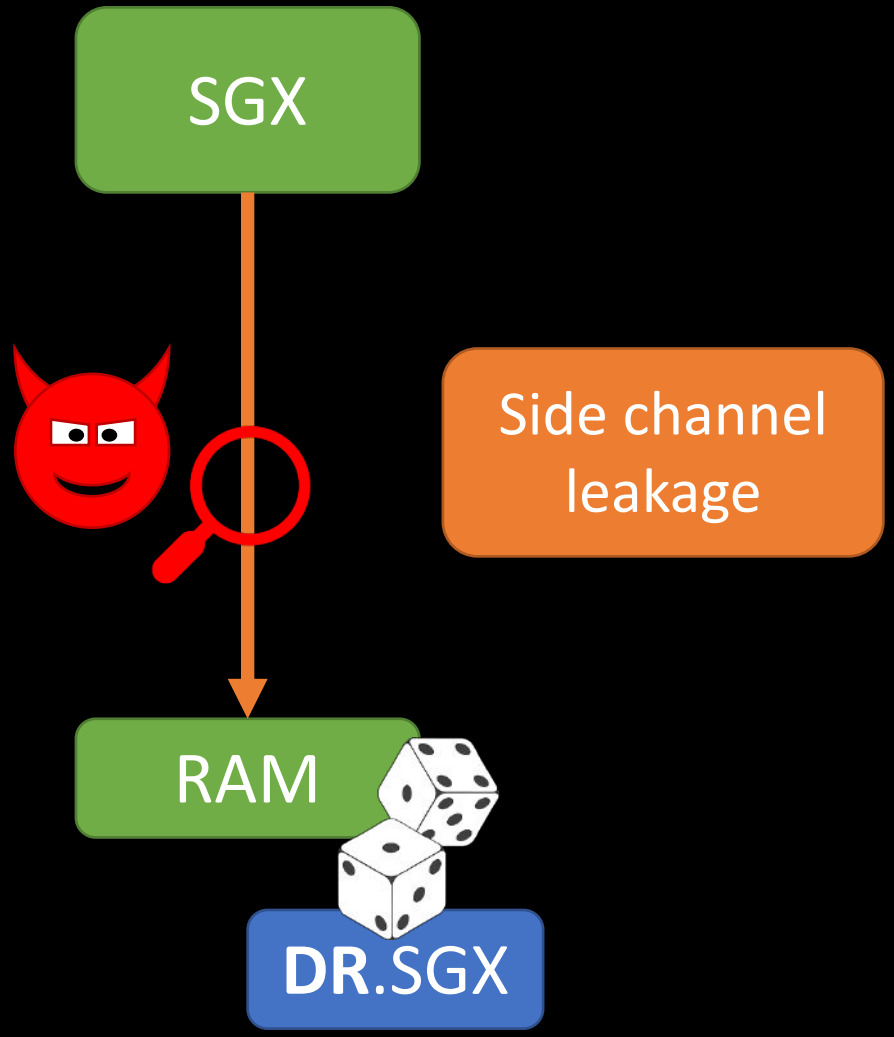
[ACSAC 2019]

Our Recent Work: DR.SGX: Automated and Adjustable Side-Channel Protection for SGX using Data Location Randomization

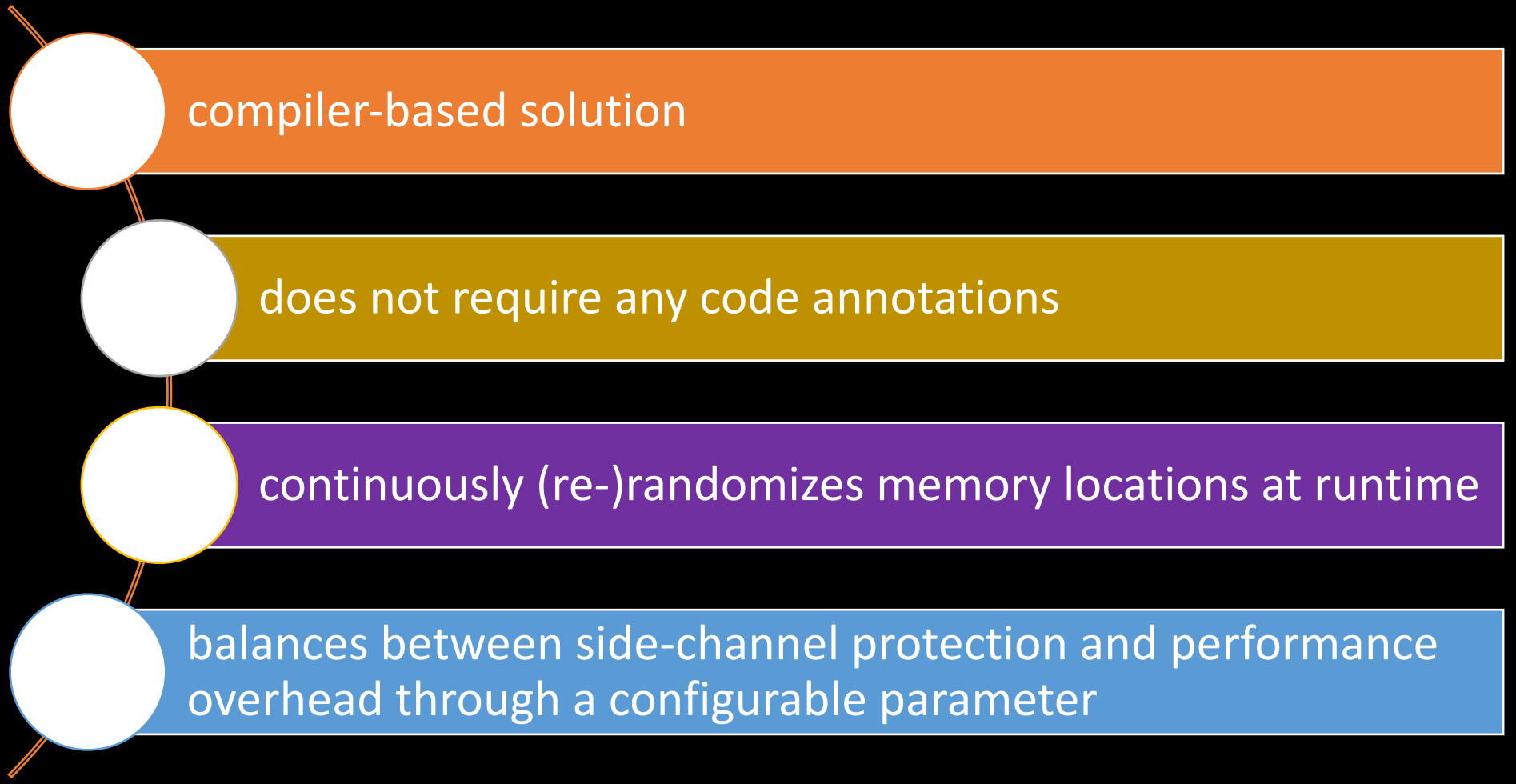
Joint work with
Ferdinand Brasser[1], Tommaso Frassetto[1], Kari Kostiainen[2], Srdjan Capkun[2], Ahmad-Reza Sadeghi[1]

[1]TU Darmstadt, [2]ETH Zurich

The Big Picture

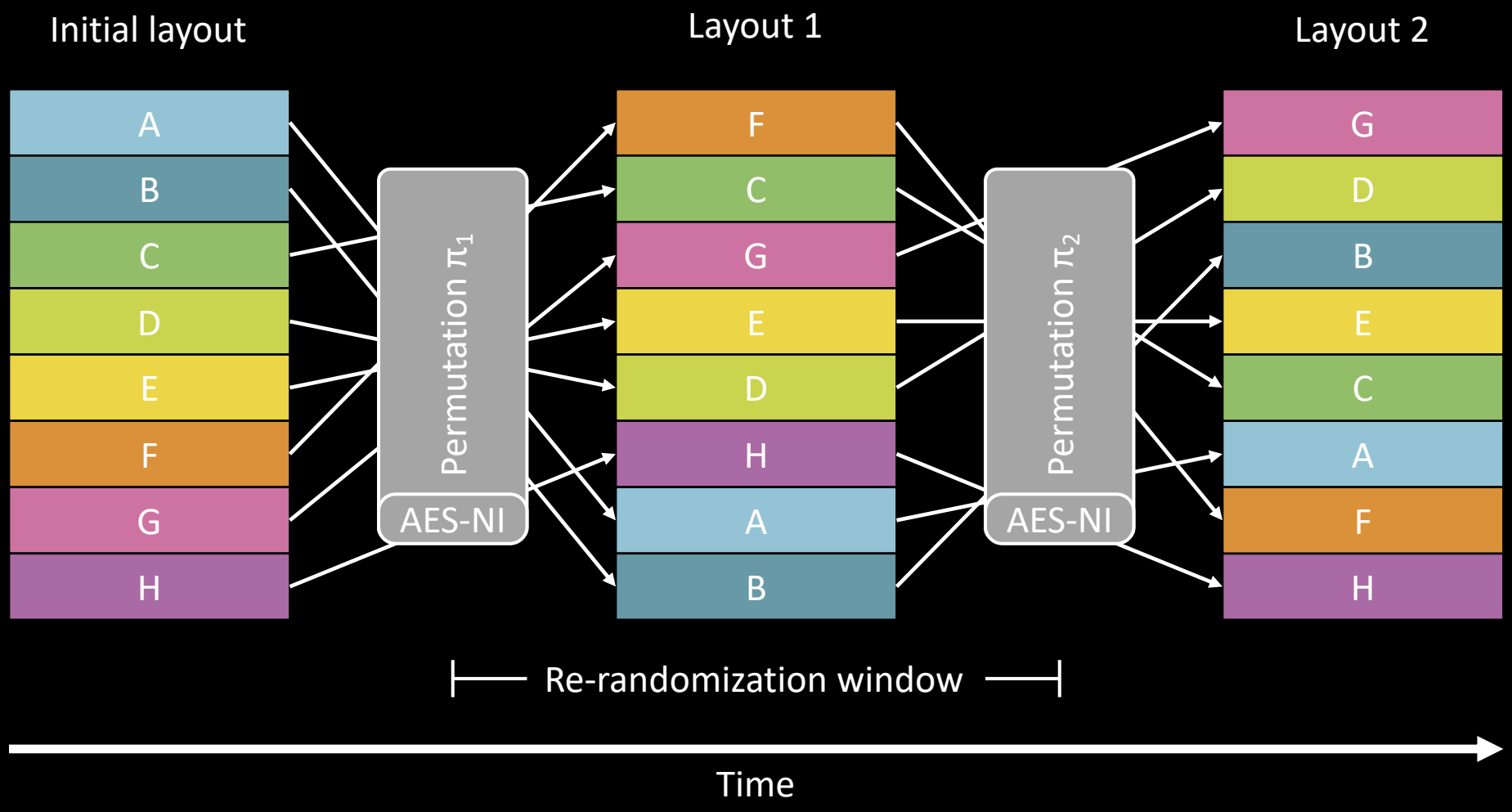


Features


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

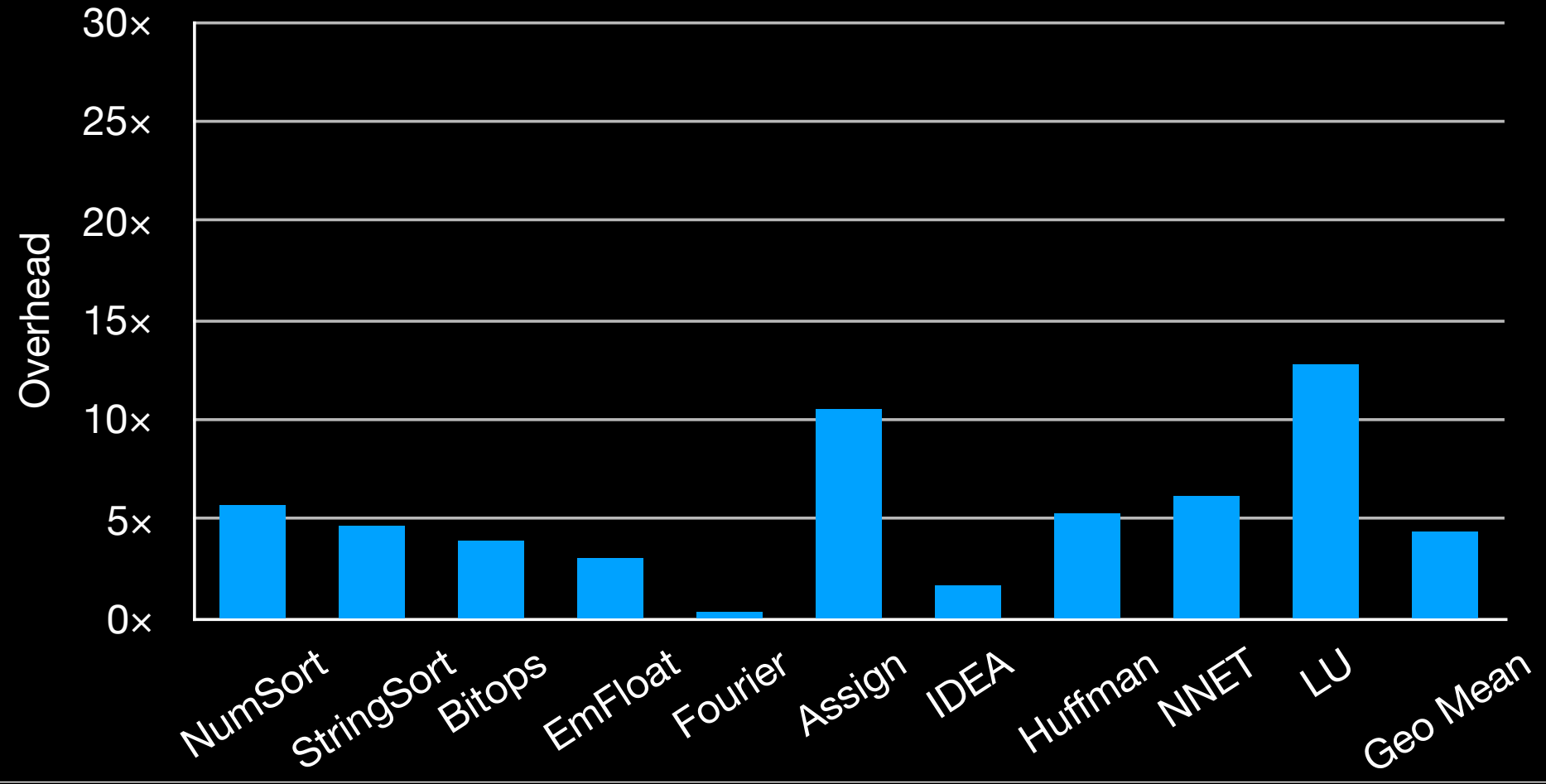
DR.SGX Re-randomization

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



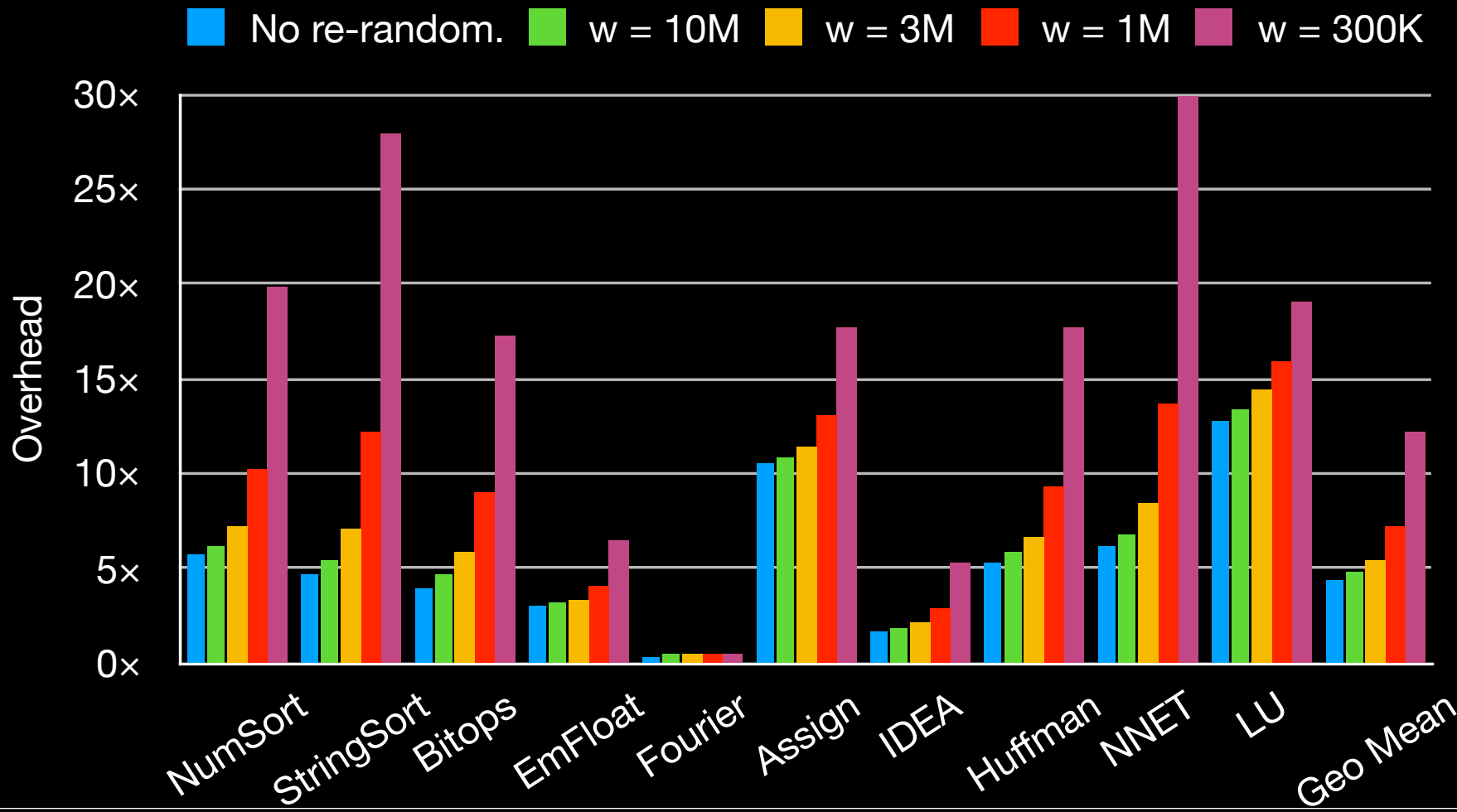
Performance Evaluation using Nbench

- 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


E
?
R
S
D
F