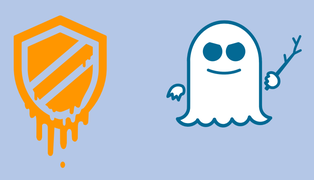
Unique Program Execution Checking: Formal Security Guarantees for RISC-V Systems

Alex Wezel[1], Lucas Deutschmann[1], Tobias Jauch[1], Dino Mehmedagić[1], Johannes Müller[1], Mohamed Ali[1],
Anna Lena Duque Antón[1], Philipp Schmitz[1], Mohammad Rahmani Fadiheh[2], Dominik Stoffel[1], Wolfgang Kunz[1]
[1]RPTU Kaiserslautern-Landau, Germany; [2]Stanford University, USA

Motivation

- Discovery of Meltdown and Spectre sparked interest in hardware security



- Industry and academia found various vulnerabilities

- Need for exhaustive security guarantees

Unique Program Execution Checking

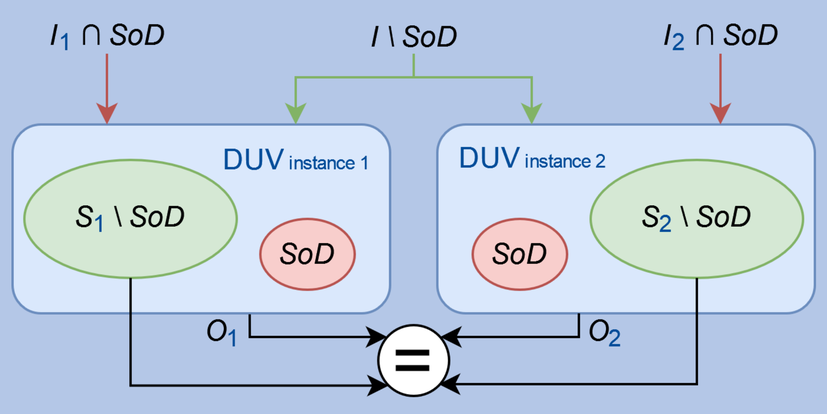
UPEC exhaustively detects all propagation of information from or to critical locations in a given RTL design:

- Possible leakage of confidential information
- Malicious interference with protected data (integrity)

UPEC proves that a system executes uniquely w.r.t. the signals of interest called Source of Discrepancy (SoD)

Computational Model

- Duplicate the DUV to construct a miter circuit
- Choose the Source of Discrepancy (SoD) to determine which signals should be observed
- Since the SoD is the only difference between the two DUVs, all resulting differences originate from the SoD



DUV: Design under Verification

SoD: Source of Discrepancy

I: Inputs

O: Outputs

S: Microarchitectural State Variables

Generic UPEC Property

```
assume:
  at t:              S1\SoD == S2\SoD;
  during[t, t+k]:    I1\SoD == I2\SoD;
  at t:              threat_model();
prove:
  during[t, t+k]:    S1\SoD == S2\SoD;
  during[t, t+k]:    O1 == O2;
```

- Prove the property and inspect counterexamples
  - Harmless propagation → refine SoD
  - Propagation violating security → apply appropriate mitigation
- Repeat until no more counterexample appears
- DUV is guaranteed to be secure w.r.t. the threat model

Case Studies

- ✓ UPEC exhaustively verifies confidentiality even in deep out-of-order pipelines and entire SoCs
- ✓ UPEC detects data-dependent timing in accelerators and qualifies individual instructions in a processor as data-oblivious
- ✓ UPEC guarantees system integrity for integration of untrusted 3rd-Party-IPs in SoCs

Security Target	DUV	Detected Vulnerabilities	Reference
Transient-Execution-Attacks	*BOOM*	*Multiple Spectre variants, Meltdown*	
Data-Independent-Timing	*Ibex*	*Timing dependency for misaligned memory accesses*	
Functional Security Bugs in SoCs	*Pulpissimo*	*Confused deputy attack using an accelerator ignoring PMP*	
Operation Integrity in SoCs	*OpenTitan*	*Denial-of-Service attack using an untrusted IP*	

Summary

- ✓ UPEC is a scalable methodology for exhaustively detecting malicious information flows
- ✓ Independent of functional correctness of the DUV
- ✓ Case studies show the versatility of UPEC and its easy adaptibility to different threat models
- ✓ UPEC enables to provide a hardware root of trust for higher levels of the system stack

Publications

- Mohammad Rahmani Fadiheh, Alex Wezel, Johannes Müller, Jörg Bormann, Sayak Ray, Jason M. Fung, Subhasish Mitra, Dominik Stoffel, Wolfgang Kunz. *An Exhaustive Approach to Detecting Transient Execution Side Channels in RTL Designs of Processors*, IEEE Transactions on Computers, 2023
- Tobias Jauch, Alex Wezel, Mohammad R. Fadiheh, Philipp Schmitz, Sayak Ray, Jason M. Fung, Christopher W. Fletcher, Dominik Stoffel, and Wolfgang Kunz. *Secure-by-Construction Design Methodology for CPUs: Implementing Secure Speculation on the RTL*, IEEE/ACM International Conference on Computer-Aided Design, 2023
- Lucas Deutschmann, Johannes Müller, Mohammad R. Fadiheh, Dominik Stoffel, Wolfgang Kunz. *A Scalable Formal Verification Methodology for Data-Oblivious Hardware*, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2024
- Johannes Müller, Mohammad Rahmani Fadiheh, Anna Lena Duque Antón, Thomas Eisenbarth, Dominik Stoffel, Wolfgang Kunz. *A Formal Approach to Confidentiality Verification in SoCs at the Register Transfer Level*, ACM/IEEE Design Automation Conference, 2021
- Dino Mehmedagic, Mohammad Rahmani Fadiheh, Johannes Müller, Anna Lena Duque Antón, Dominik Stoffel, Wolfgang Kunz. *Design of Access Control Mechanisms in Systems-on-Chip with Formal Integrity Guarantees*, USENIX Security Conference, 2023

RPTU Rheinland-Pfälzische Technische Universität Kaiserslautern Landau

Stanford University

The reported research was supported in part by **BMBF** ZuSe (Scale4Edge), 16ME0122K-16ME0140+16ME0465, in part by **DFG** SPP Nano Security, KU 1051/11-2, in part by **Intel** Corporation (Scalable Assurance), and in part by **Siemens EDA**

RISC-V Summit Europe, Munich
June 24th – June 28th 2024