CCRI: ENS: Enhancement of Trust-Hub, a Web-based Portal to support the Cybersecurity Research Community

Mark Tehranipoor
Domenic Forte

Farinaz Koushanfar

Ramesh Karri

Acknowledgements

Top Trust-Hub Community Contributors

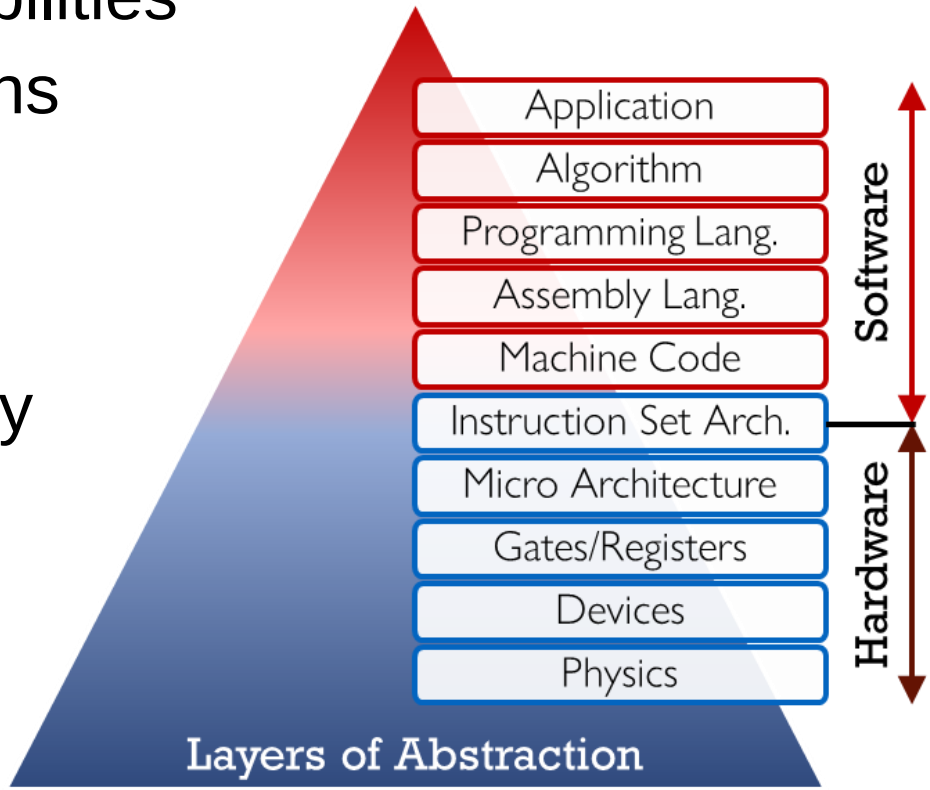
- Dr. Sohrab Aftabjahani, Intel
- Dr. Navid Asadi, University of Florida
- Dr. Fatemeh Ganji, Worcester Polytechnic Institute
- Dr. Farimah Farahmandi, University of Florida
- Dr. Hassan Salmani, Howard University
- Dr. Shahin Tajik Worcester Polytechnic Institute
- Dr. Damon Woodard, University of Florida

National Science Foundation and PMs

- Dr. Almadena Chtchelkanova
- Dr. Nina Amla
- Dr. Marilyn McClure

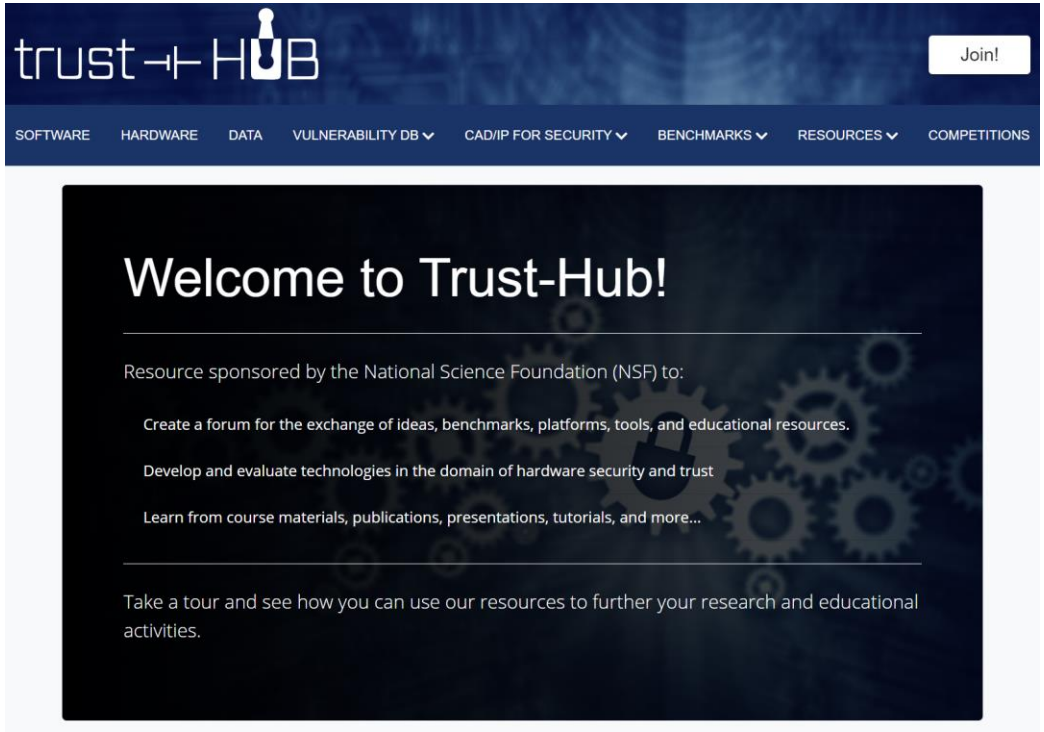
Why Hardware Security and Trust (HS&T)?

- Resilience to software vulnerabilities
- Secure cryptographic operations and sensitive data
- Guarantee hardware performs as intended, without being compromised in a global supply chain and free from vulnerabilities
- Protect against physical attacks
- Prevent counterfeiting and Intellectual Property (IP) theft



Challenge: Benchmarking in hardware security is challenging, i.e., lack of standard metrics, diverse threat landscape, limited publicly available data, etc.

What is Trust-Hub?

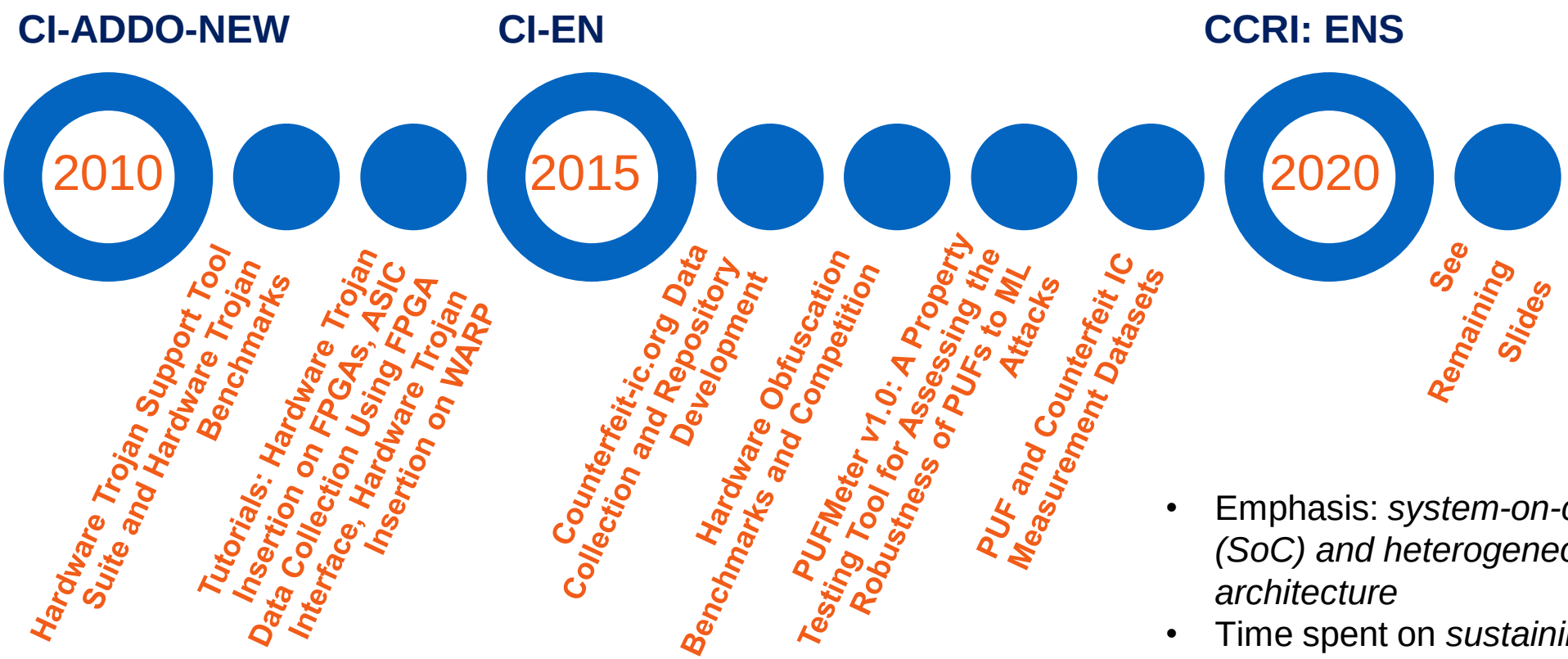


- 14 software tools, 14 datasets, and 400+ benchmarks available on web
- Physical and SoC vulnerability databases
- Catalogue containing 60+ CAD solutions and 50+ IP solutions from nearly 100 researchers and/or companies
- 500+ Facebook group members

Website Stats (Jul 20 – Mar 23)

- 44 users per day
- Users from 147 countries
  - *Top 10:* USA, China, Indonesia, India, Japan, South Korea, Germany, Taiwan, Hong Kong, Singapore
- 36 downloads per day
  - *Top Categories - items*
    - Trojan Benchmarks
    - Datasets – FPIC and FICS-PCB
    - Obfuscation Benchmarks
    - Software – SynthGen and PUFMeter

History of Trust-Hub and Major Contributions



- Emphasis: level S&T (hardware Trojans, obfuscation, piracy, counterfeit, etc.)
- Time spent on building and refining web interface and communication networks, e.g., social media
- Contributions from Trust-Hub team (T), i.e., from Principal Investigators (PIs) and their students

- Emphasis: *system-on-chip (SoC) and heterogeneous architecture*
- Time spent on *sustaining* web interface, increasing e-mail communication, and creating consistent influx of tools, datasets, etc.
- Expanding external outreach to *obtain contributions from wider community (C)*, including colleagues in both academia and industry

Trust-Hub has played a major role in the HS&T community's growth

CCRI: ENS: Enhancement Goals

CI-ADDO-NEW and CI-EN

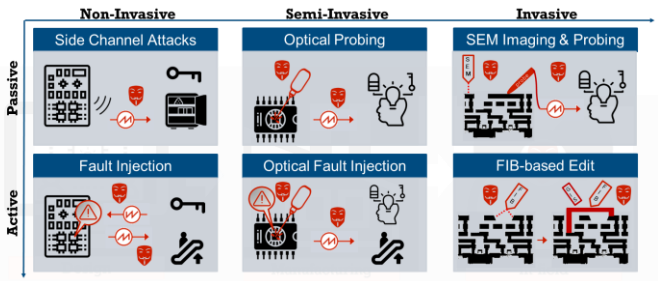
- Emphasis on IP level S&T (hardware Trojans, obfuscation, piracy, counterfeit, etc.)
- Time spent on building and refining web interface and communication networks, e.g., social media
- Contributions from Trust-Hub team (T), i.e., from Principal Investigators (PIs) and their students

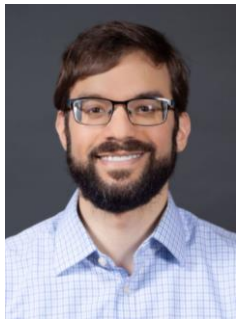
CCRI: ENS

- Emphasis on *system-on-chip (SoC) and heterogeneous architecture S&T*
- Time spent on *sustaining* web interface, increasing e-mail communication, and creating consistent influx of tools, datasets, competitions, etc.
- Expand external outreach to *obtain contributions from wider community (C)*, including colleagues in both academia and industry

CCRI: ENS: Enhancement Tasks and Leads

1. Physical SoC Security Tools & Benchmarking





Lead: Domenic Forte

2. AI Security Tools & Benchmarking

Lead: Farinaz Koushanfar

3. RTL/Gate SoC CAD Tools & Benchmarking

CAD FOR SECURITY
CAD4SEC

Lead: Mark Tehranipoor

4. Cybersecurity Games & Conference (CSAW)

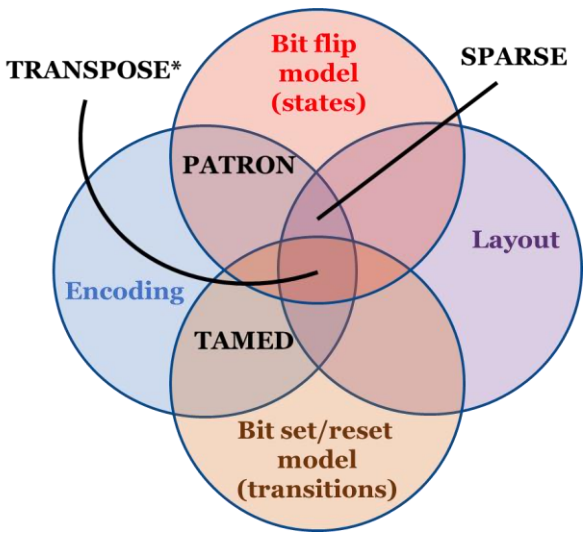
SCAN ME

Lead: Ramesh Karri

Task 1 – Physical Attack Tools, Datasets, etc.

Physical SoC Security Assessment and Mitigation Tools – C/T

- 4 FSM design tools



- 1 layout analysis tool – Detour
- 1 LFI standard cell analysis tool*

** In Progress*

Remote Access to Side Channel (RASC) - T

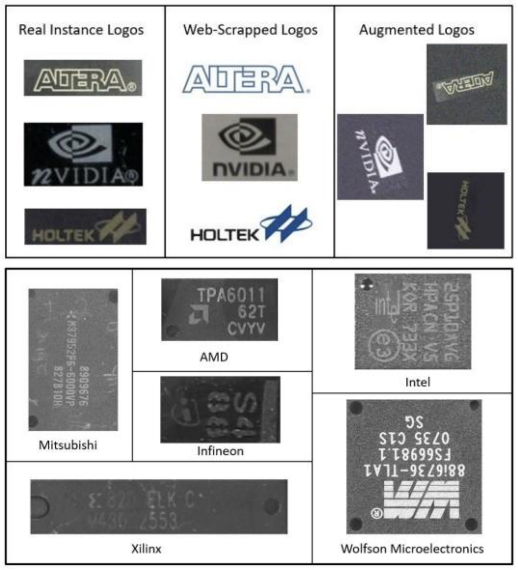
- Power and EM measurements for two datasets*
  - Offense: AES key extraction
  - Defense: Instruction disassembly (e.g., malware detection)
- RASC design files to be shared upon release

CAPEC - T

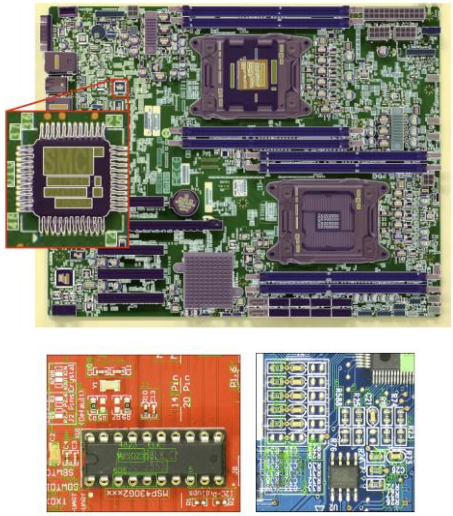
- 6 new physical attack entries developed:
  - Optical side-channel attacks (EOP, EOFM, LLSI, TLS)
  - Invasive Attacks (FIB probing, fault injection, and circuit edit)
  - Laser fault injection (LFI)
- To be shared with Hardware CWE Special Interest Group (HW CWE SIG)

Task 1 – New Counterfeit and Reverse Engineering Image Datasets

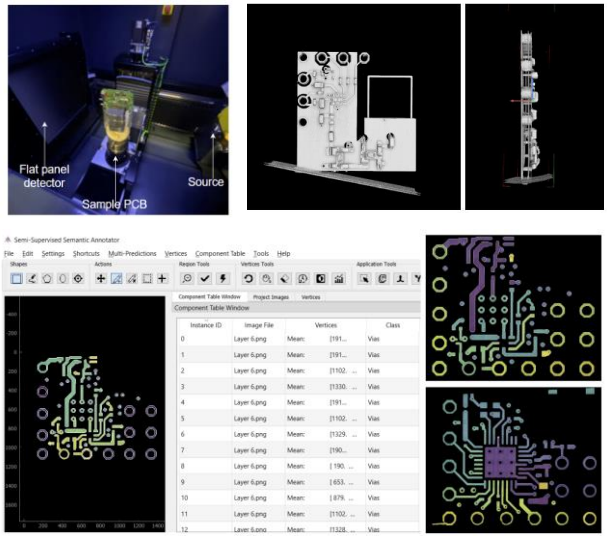
Real and Synthetic Chip Logo Datasets – C/T



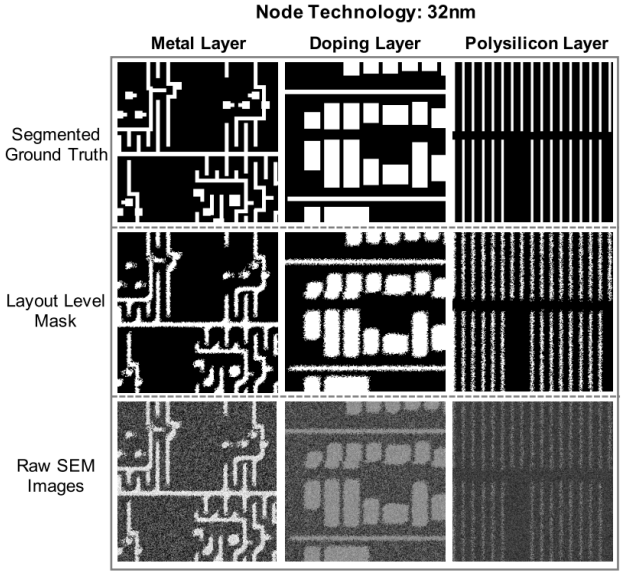
Raw and Annotated PCB Component and Test Datasets – C/T

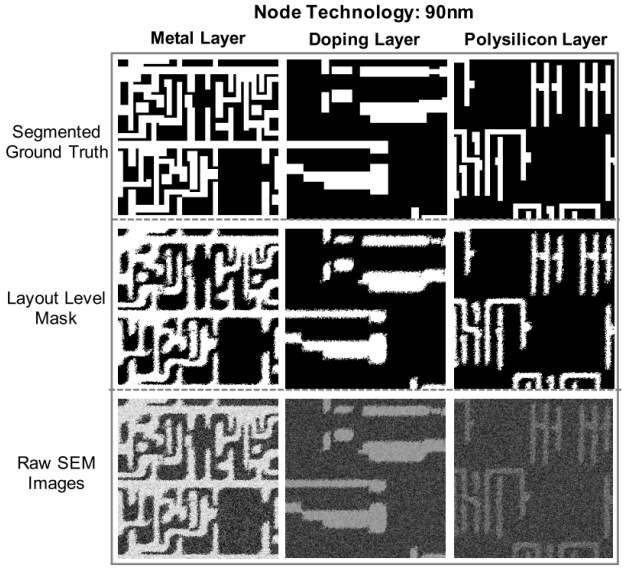


Raw and Annotated PCB X-ray Datasets – C/T



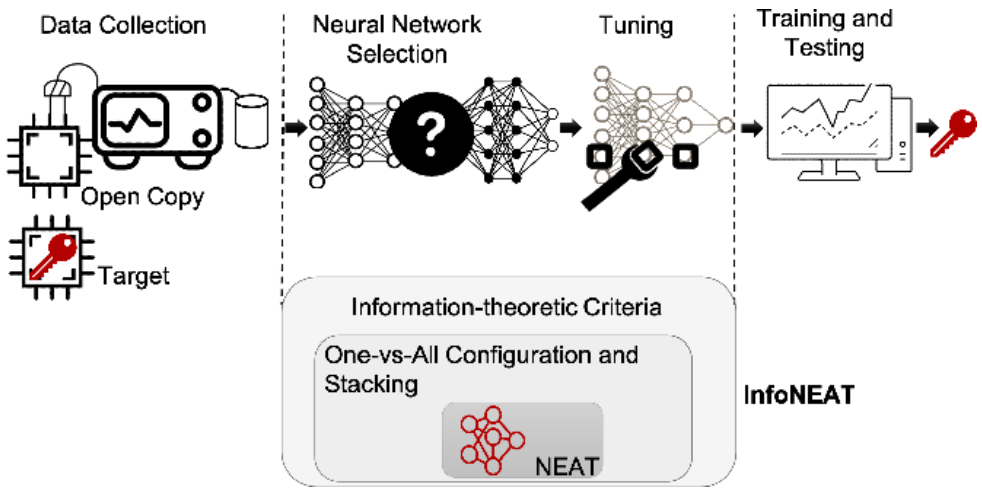
Real and Synthetic Chip SEM Image Datasets – C/T (90nm and 32nm)





Task 2 – AI HW Assessment Tools and Datasets

InfoNEAT – C/T



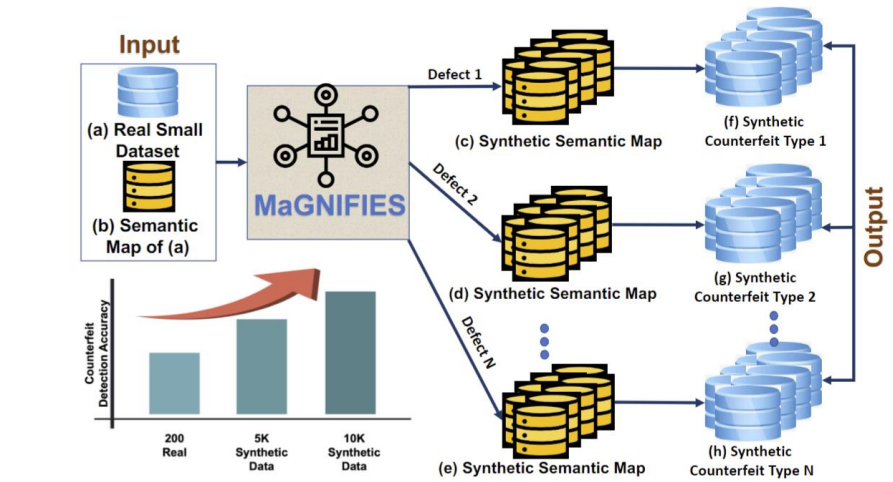
Uses information-theoretic based criteria (Conditional Mutual Information – CMI) for hyperparameter tuning:

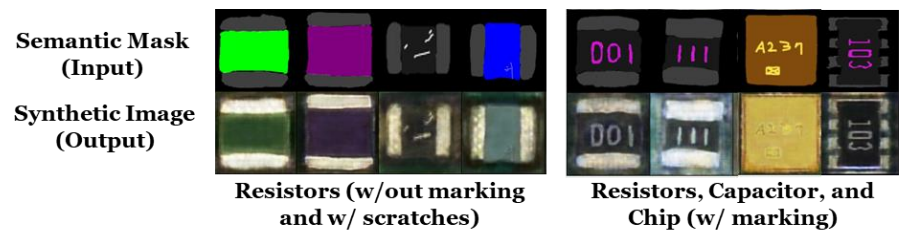
- **Selection criteria:** add only useful nodes
- **Stopping criteria:** stop the evolution at the correct time

MLP	# of layers	# of nodes	Epochs	Training traces
[1]	6	200	400	40k
[2]	[2,8]	[100, 1000]	-	50k
[3]	6	300	200	20k
[4]	[2,10]	[100, 400]	10	50k
InfoNEAT	**2**	**15**	**8**	**38.4k**

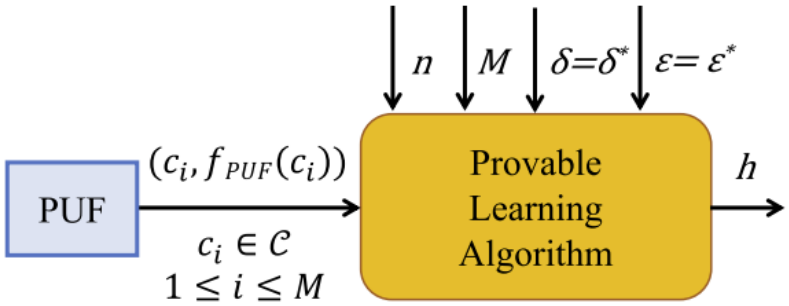
[1] Benadjila et al., JCEN 2020; [2] Perin et al, TCHES 2020.
[3] Weissbart et al, .ACNS 2020; [4] Wu et al. IEEE TECS 2022.

MaGNIFIES – C/T (Release Pending)



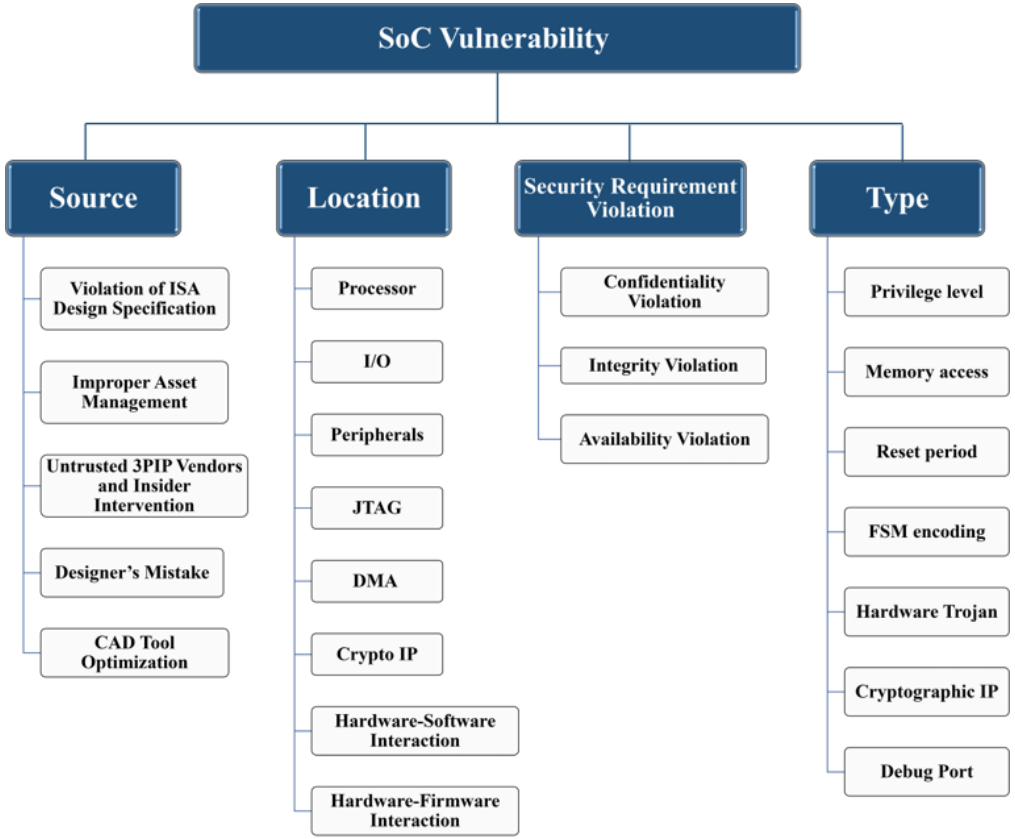


PUFMeter v2.0 – C/T (In Progress)



Task 3 – SoC Vulnerability Database & Benchmarks

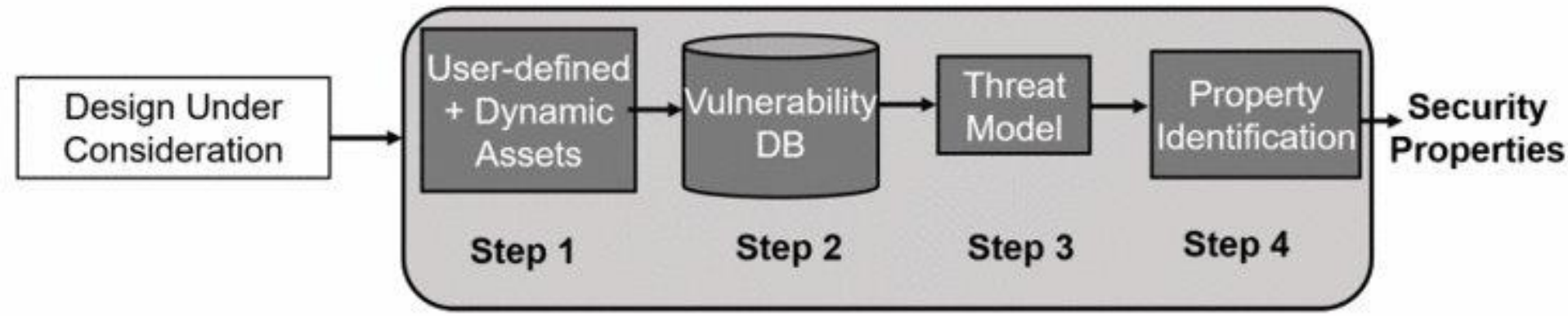
- Provides researchers and practitioners from academia and industry with a set of SoC vulnerabilities based on security objectives in hardware to perform various experimental analyses.
- Includes 23 SoC vulnerabilities (identified and categorized). – C/T
- 6 SoC vulnerability benchmarks listed with threat model and description. – C/T



Two Benchmark Generators

- MEXT-SE: Multi-processor Exploration with Security Extension – C
- SynthGen: Synthetic Circuit Benchmark Generator v1.0 and v2.0 – T

Task 3 – SoC Property/Rule Database



- Includes 100+ security properties and rules for a number of designs and design components, their respective vulnerabilities, and threat models – C/T
- Supports formal verification of SoC designs at RTL, Gate and Physical layout levels.
- Each security property or rule is formally represented to verify different design implementations.
  - *Example 1:* Signals ready and load cannot be true at the same time.
  - *Example 2:* No path should exist between points A and B.

```
assertion_1: assert property (@(posedge
clk) (!(ready && load)));
```

```
assertion_2: assert property
(No_path_between_A_B);
```

Task 4 – CSAW Hardware Competitions

Year	2020	2021	2022	2023
Venues	Virtual	Virtual	In-person	In-person
# of Total (HW) Competitions	8 (3)	9 (3)	10 (3)	11 (3)
Regions	EU, India, Israel, MENA, Mexico, US-CAN	EU, India, Israel, MENA, Mexico, US-CAN	EU, India, MENA, US-CAN	EU, India, MENA, Mexico, US-CAN
Embedded Systems Challenge (ESC): # Teams	10, 6, 0, 0, 0, 12	6, 7, 5, 0, 0, 10	3, 5, 0, 0, 4	In progress
Logic Locking Competition (LLC): # Participants (Finalists)	0, 3 (2), 0, 0, 0, 8 (4)	1 (!), 2 (1), 0, 0, 0, 8 (4)	0, 5 (0), 1 (1), 11 (7)	In progress
Academic Research Competition (ARC): Total # Participants (Finalists)	N/A	N/A	80 (10)	160 (10)