

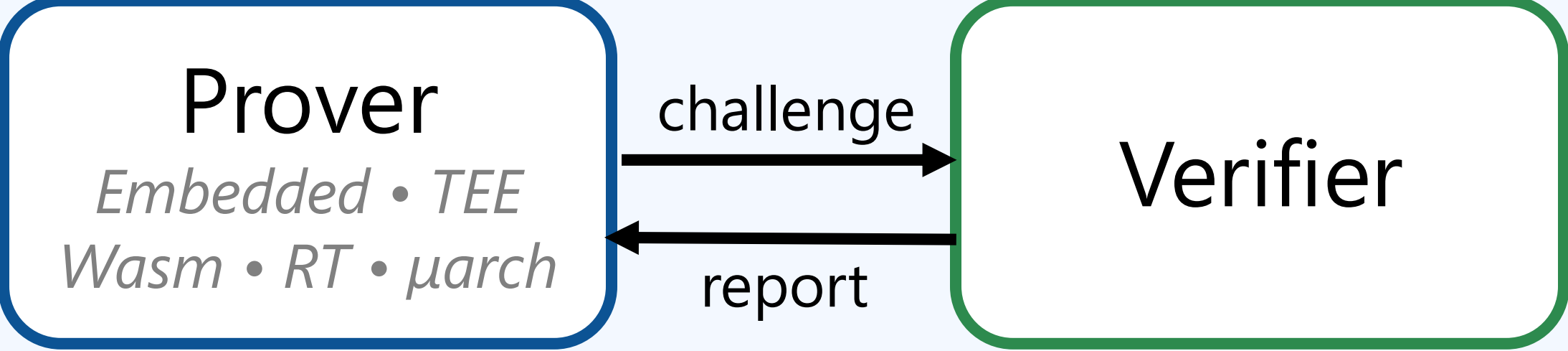
S2 • ATTESTATION PROTOCOLS



REMOTE ATTESTATION FOR COMPLEX SOFTWARE SYSTEMS

A.-R. Sadeghi (TU Darmstadt) • L. Davi (University of Duisburg-Essen) • O. Draissi (University of Duisburg-Essen) • E. Mollakuqe (TU Darmstadt)

► THE VISION



From foundational primitives to data-driven detection.

Twelve years of remote attestation across CROSSING, spanning embedded devices to **complex software systems**:

● Phase 1 Foundations ● Phase 2 Expansion ● Phase 3 Complex Systems

MILESTONES ACROSS THREE PHASES

1

PHASE 1
Foundations

2014–2018

Control-Flow & Hardware Attestation

★ C-Flat • CCS 2016

First control-flow attestation scheme for embedded software

Foundational scheme of S2

SEDA • CCS 2015

First scalable swarm attestation for networks of embedded devices.

Group attestation primitive

LO-FAT • DAC 2017

Low-overhead control-flow attestation in hardware

First HW-accelerated CFA

2

PHASE 2
Expansion

2018–2022

Blockchain, real-time & data-flow attestation

★ RealSWATT • CCS 2021

First software-based attestation for real-time embedded systems

LiteHAX • ICCAD 2018

Hardware-assisted control- & data-flow attestation; covers DOP attacks

★ Sereum • NDSS 2019

Runtime attestation of blockchain transactions

CHASE • ICCAD 2019

Configurable runtime attestation

TeeRex • USENIX 2020

Discovers memory corruption vulnerabilities in SGX enclaves

3

PHASE 3
Complex Systems & ML

2022–2026

Memory, μarch & ML-based attestation

★ RAGE • S&P 2024

GNN-based attestation for embedded devices

↓ see Headline Result

HammerWatch • 2026

First Rowhammer-aware remote attestation protocol

aggressor [red blocks] victim [blue blocks]

DMA'n'Play • ACNS 2023

DMA-based RT attestation

Complements RAGE's CFA view

★ SALSA • SECDEV 2022

SGX control-flow attestation, achieves, 18.9 MB/s on secure video streaming

★ Walma • 2026

First Wasm linear-memory attestation. CNN classifiers on memory-snapshot images.

Dual deployment: TEE for cloud & browser for web modules

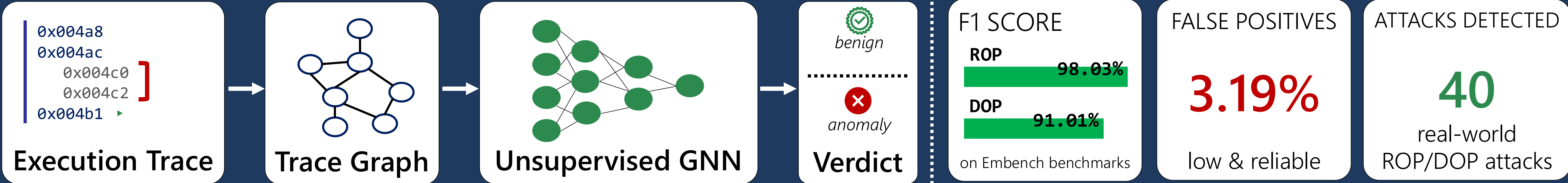
Verifier [checkmark]

Wemby ISSTA'25 • Bento WWW'26 • SGXFuzz USENIX '22 • MPush Cascade '26

► HEADLINE RESULT • IEEE S&P 2024

One for All and All for One: GNN-based control-flow attestation for embedded devices

No prover memory • No complete CFG • No custom hardware



BEYOND CORE • INTEGRITY OF DATA & MODELS

ZORRO • CCS 2025

Privacy for split learning

ZK proofs on partitioned ML training

DEMASQ • NDSS 2024

Fingerprinting AI-generated text

Identifies LLM-authored content

Light2Lie • NDSS 2026

Deepfake detection via physical reflectance laws

COLLABORATIONS WITHIN CROSSING

E4 × S2 • FLAME • USENIX 2022

Backdoor defense for federated learning; clustering + clipping + adaptive noise.

Eliminates backdoors with negligible impact on benign accuracy

E7 × S2 • SCAtt-man • CODASPY 2023

User-observable side channels (sound, light) for software-based IoT attestation.

★ CROSSING Collaboration Award 2023 ★

T1 × S2 • Brigade • ACNS 2026

Cross-chain bridge defense; Tamarin proofs+ runtime monitoring

Against \$2B+ DeFi bridge exploits