7th Workshop on System Software for Trusted Execution (SysTEX 2024)

Opening and Welcome

Jo Van Bulck, Nuno Santos

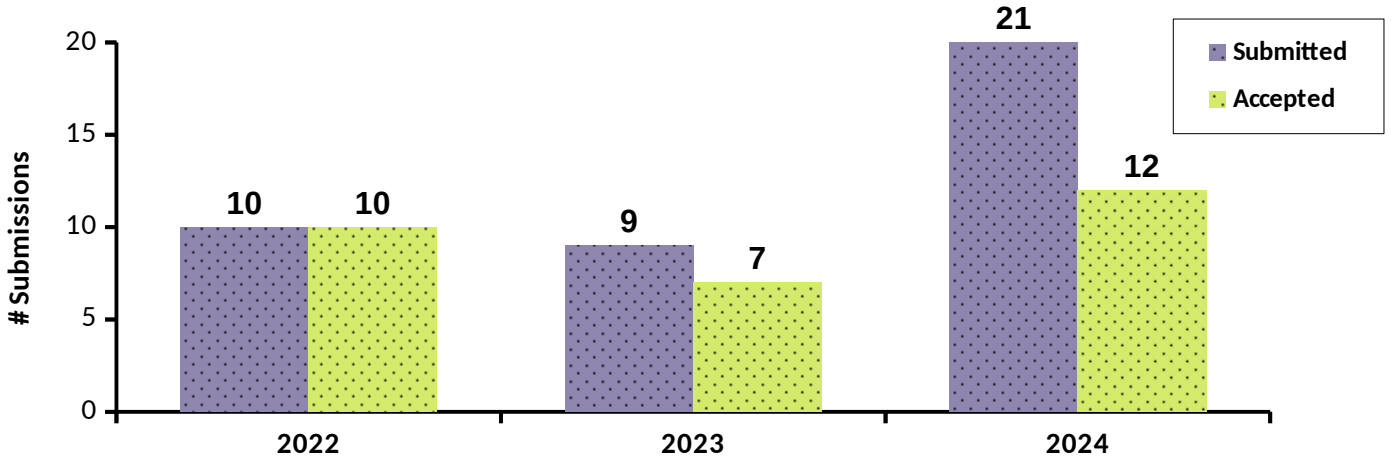
July 8, 2024, Vienna

DistriNet

KU LEUVEN

Submission Stats

- **Record:** 21 submissions *(× 2.3 vs. last year!)*
- **Accepted:** 12 papers *(≈ 57 % AR)*
  - 10× “regular research papers”
  - 1× “short research statement”
  - 1× “tool paper” *(new ★)*



Program Committee: Thank You!

3 × 21 = 63 reviews!

- Andreas Kogler, TU Graz
- Andrew Paverd, Microsoft Research
- Cristiano Rodrigues, University of Minho
- Daniel Castro, University of Lisbon
- Daniel Gruss, TU Graz
- Daniel Moghimi, Google Research
- David Oswald, University of Birmingham
- Dimitra Giantsidi, University of Edinburgh
- Fritz Alder, NVIDIA
- Ghada Dessouky, Google
- Lesly-Ann Daniel, KU Leuven
- Luca Wilke, University of Lübeck
- Masanori Misono, Technical University of Munich
- Michael Schwarz, CISPA Helmholtz Center for Information Security
- Pierre-Louis Aublin, IIJ Research Lab
- Robert Buhren, AMD
- Rüdiger Kapitza, FAU Erlangen-Nürnberg
- Sandro Pinto, University of Minho
- Shweta Shinde, ETH Zurich
- Thomas Eisenbarth, University of Lübeck

New: Artifact Evaluation

- **Optional** and constructive:
  - 1 (single-blind) review per artifact
- **Participation:** 7 out of 12 accepted papers
  - 1× *"Artifacts Available"*

  - 3× *"Artifacts Available + Functional"*

  - 3× *"Artifacts Available + Functional + Reusable"*

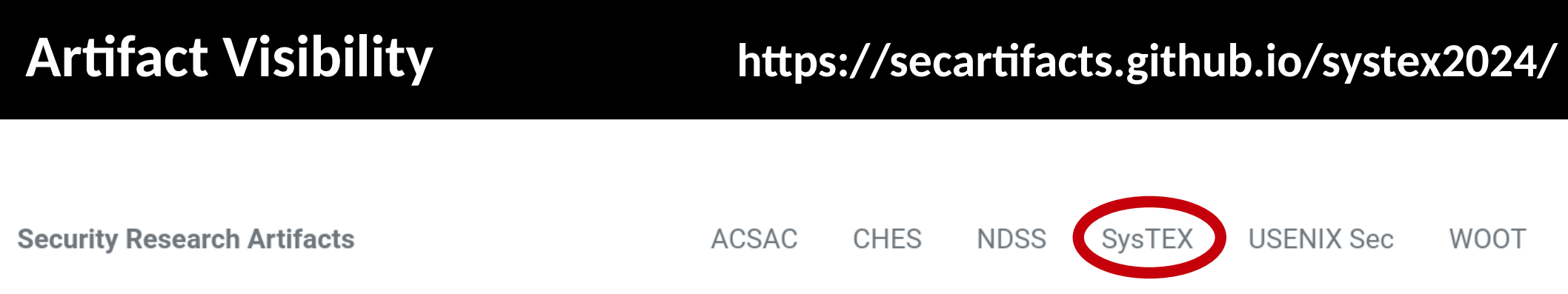
    

Artifact Evaluation Committee: Thank You!

- Anna Pätschke, University of Lübeck
- Cristiano Rodrigues, University of Minho
- Daniel Castro, INESC-ID / IST, University of Lisbon
- Gianluca Scopelliti, Ericsson Security Research and DistriNet, KU Leuven
- Jan Wichelmann, University of Lübeck
- Luca Wilke, University of Lübeck
- Marton Bognar, DistriNet, KU Leuven
- Tom Van Eyck, DistriNet, KU Leuven

Artifact Visibility

https://secartifacts.github.io/systex2024/



Best Paper Awards

1) **Best Paper Award**
   - Overall best-rated reviewer's score on hotcrp
   - ```
     SELECT * FROM hotcrp
     ORDER BY overall_reviewer_score;
     ```

2) **Best Paper with Artifacts Award**
   - "Reusable"-rated artifact with highest reviewer score
   - ```
     SELECT * FROM hotcrp
     ORDER BY reusable, overall_reviewer_score;
     ```

DALL·E, please announce the winners…

DALL·E 3

The 7th Workshop on System Software for Trusted Execution (SysTEX 2024)

is honored to present the Best Paper Award to

Gianluca Scopelliti, Christoph Baumann, Jan Tobias Mühlberg

for their work entitled

Understanding Trust Relationships in Cloud-Based Confidential Computing

Jo Van Bulck
PC co-chair

Nuno Santos
PC co-chair

July 8th, 2024, Vienna, Austria

DALL·E 3

The 7th Workshop on System Software for Trusted Execution (SysTEX 2024)

is honored to present the Best Paper with Artifacts Award to

Istemi Ekin Akkus, Ivica Rimac

for their work entitled

duet: Combining a Trustworthy Controller with a Confidential Computing Environment

Jo Van Bulck
PC co-chair

Nuno Santos
PC co-chair

July 8th, 2024, Vienna, Austria

09:30-09:45	Opening and Welcome
09:45-11:00	**Technical Paper Sessions 1: ARM TrustZone**
	09:45: Secure Intermittent Computing with ARM TrustZone on the Cortex-M
	10:10: Conditional Network Availability: Enhancing Connectivity Guarantees for TEE-Based Services
	10:35: NetReach: Guaranteed Network Availability and Reachability to enable Resilient Networks for Embedded Systems
11:00-11:15	Coffee Break
11:15-12:30	**Technical Paper Sessions 2: Intel SGX**
	11:15: duet: Combining a Trustworthy Controller with a Confidential Computing Environment
	11:40: PraaS: Verifiable Proofs of Property as-a-Service with Intel SGX
	12:05: Revisiting Rollbacks on Smart Contracts in TEE-protected Private Blockchains
12:30-13:30	Lunch
13:30-14:45	**Technical Paper Sessions 3: Remote Attestation**
	13:30: Understanding Trust Relationships in Cloud-Based Confidential Computing
	13:55: Delegating Verification for Remote Attestation using TEE
	14:20: SNPGuard: Remote Attestation of SEV-SNP VMs Using Open Source Tools
14:45-15:00	Coffee Break
15:00-16:15	**Technical Paper Sessions 4: Enhanced and Future TEEs**
	15:00: Minimal Partitioning Kernel with Time Protection and Predictability
	15:25: SyncEmu: Enabling Dynamic Analysis of Stateful Trusted Applications
	15:50: BarriCCAde: Isolating Closed-Source Drivers with ARM CCA
16:15-16:30	Closing Remarks

No keynote speaker this year..
(maximize #accepted papers)