

SysTEX 2026 Workshop Program

Monday, April 27th — Room Ochil 1, Level 1

9:00 – 10:30	Session 1: Attacks on TEEs	
09:00 – 09:10	Opening and Welcome	
09:10 – 09:50	Keynote 1	30 + 10 min
	■ ■ Attacks ■ ■	
09:50 – 10:10	StepOverflow: PMC Overflows on AMD SEV <i>Anja Rabich (University of Luebeck), Jonah Heller (University of Luebeck), Florian Sieck (University of Luebeck), Thomas Eisenbarth (University of Luebeck)</i> Artifact: ✓ Available - ✓ Reusable	15 + 5 min
10:10 – 10:30	Breaking Isolation: Last-level Cache Side-Channel Attacks on AWS Nitro Enclaves <i>Monder Rammouz (TU Munich), Quoc Do Le (Huawei Munich Research Center)</i> Artifact: ✓ Available - ✓ Reusable	15 + 5 min
10:30 – 11:00	Coffee Break	
11:00 – 12:30	Session 2: TEE Platforms & Systems	
	■ ■ Embedded TEEs ■ ■	
11:00 – 11:20	Control-Flow Balancing for Texas Instruments IPE <i>Marton Bognar (DistriNet, KU Leuven), Alexander Croes (DistriNet, KU Leuven), Hans Winderix (DistriNet, KU Leuven), Jo Van Bulck (DistriNet, KU Leuven)</i> Artifact: ✓ Available - ✓ Reusable	15 + 5 min
11:20 – 11:40	Keystone with Linux PREEMPT_RT: Real-Time Enclaves on RISC-V? <i>Oscar Van Slijpe (Université Libre de Bruxelles), Jean-Michel Dricot (Université libre de Bruxelles), Jan Tobias Mühlberg (Université libre de Bruxelles)</i> Artifact: ✓ Available - ✓ Reusable	15 + 5 min
	■ ■ TEE Performance ■ ■	
11:40 – 12:00	Optimizing Launch Latency for Confidential VMs with Device Passthrough in the Linux KVM Hypervisor <i>Hao-Jung Wei (National Taiwan University), Shih-Wei Li (National Taiwan University)</i> Artifact: ✓ Available - ✓ Functional	15 + 5 min
12:00 – 12:20	Performance and Security of TEE-Based Threshold Cryptography <i>Marius Haller (Karlsruhe Institute of Technology (KIT)), Marc Leinweber (Karlsruhe Institute of Technology (KIT)), Tilo Spannagel (Karlsruhe Institute of Technology (KIT)), Markus Raiber (Karlsruhe Institute of Technology (KIT)), Hannes Hartenstein (Karlsruhe Institute of Technology (KIT))</i>	15 + 5 min
12:30 – 14:00	Lunch Break	
14:00 – 15:30	Session 3: Attestation & Trust	
14:00 – 14:40	Keynote 2	30 + 10 min
	■ ■ Attestation ■ ■	
14:40 – 14:50	[Short] On Attestation Dilution <i>Charly Castes (EPFL)</i>	10 min
14:50 – 15:00	[Short] Mind the Gap: Where TEE Attestations Fall Short and Why We Need Proof of Cloud <i>Filip Rezacsek (Technical University of Munich), Jonathan Passerat-Palmbach (Flashbots)</i>	10 min
	■ ■ Trusted Services ■ ■	
15:00 – 15:20	Trusted and Transparent Time-Stamping Through TEEs and Network Time Security <i>Tobias Nießen (TU Wien), Andrew Pavard (Microsoft Security Response Center)</i>	15 + 5 min
15:30 – 16:00	Coffee Break	

16:00 – 17:30	Session 4: TEE Applications	
	■■ Trust & Certification ■■	
16:00 – 16:20	CACTEE: Confidential Asset Certification using Trusted Execution Environments <i>Istemi Ekin Akkus (Nokia Bell Labs), Ivica Rimac (Nokia Bell Labs)</i> Artifact: ✓ Available - ✓ Reusable	15 + 5 min
	■■ Platforms & AI ■■	
16:20 – 16:40	[Tool] Epsilon: A Bring-Your-Own-Data Research Platform with Trusted Verification <i>Khajiev Nizomjon (Action Lab, Monash University), Aare Puusaar (Action Lab, Monash University), Chu Lee Shen (Action Lab, Monash University Malaysia), Patrick Olivier (Action Lab, Monash University), Lay-Ki Soon (Action Lab, Monash University Malaysia), Delvin Varghese (Action Lab, Monash University)</i> Artifact: ✓ Available - ✓ Reusable	15 + 5 min
16:40 – 16:50	[Short] AI Agents Need Both Hardware-Backed Security and Application-Level Guardrails <i>Shichen Hu (Technical University of Munich), Quoc Do Le (Huawei Research)</i> Artifact: ✓ Available - ✓ Reusable	10 min
16:50 – 17:10	Open Discussion & Closing Remarks	
17:30 – 19:30	<i>Welcome Reception</i>	

■ Short Paper (10 min)

■ Tool Paper (15+5 min)

Regular Paper (15+5 min)