

Autumn Meeting of the GI Special Interest Group “Operating Systems” (FGBS)

Security, Isolation and Trust in Modern Operating Systems

Rüdiger Kapitza Peter Wägemann

Chair of Computer Science 4 (Systems Software)

FAU Event Space (Blaue Box)

October 8–9, 2026

Why Now?

Security, Isolation and Trust – Headlines from 2026

AI finds vulnerabilities at scale

- Apr.** Project Glasswing: thousands of zero-days, incl. a 27-year-old OpenBSD bug. BSI President Plattner expects disruptive changes that touche on questions of sovereignty. [\[ZDF\]](#)
- May** Linux zero-day “copyfail” (CVE-2026-31431): an AI agent finds the bug in about an hour of scan time [\[copy.fail\]](#)
- May** Torvalds: AI reports make the security mailing list “almost entirely unmanageable”; Firefox fixes 271 AI-found vulnerabilities. [\[lkml, Mozilla\]](#)

AI agents gone astray

- Apr.** During testing, Claude Mythos Preview escapes a secured sandbox via a multi-stage exploit and emails the researcher. [\[Anthropic\]](#)
- July** More than 1,200 OpenAI agents break out of a training run: package-proxy zero-day → kernel bug from container to root → cloud credentials → Kubernetes admin → Hugging Face. [\[THN, Willison\]](#)
- Sep.** Second escape: a model tunnels out via a reachable DNS resolver – another training pause. [\[OpenAI\]](#)

Maybe it is time to revisit the trade-off between security, performance and resource efficiency?

12:00 *Welcome*

Session 1: Kernel Extensibility & Security

Chair: Peter Wägemann

12:15 Firefly: High-Performance Transient Execution Attack Defenses for In-Kernel Sandboxes

L. Gerhorst, H. Herzog, B. Herzog,
P. Wägemann, R. Kapitza, T. Hönic

12:35 The Gamekernel: Unleashing eBPF For Extensibility and Prototyping

N. Gordon

12:55 Catch Me If You Can – JIT-based Continuous Re-randomization of the Kernel Address-Space Layout

P. Zinselmeyer, H. Herzog, M. Ott, T. Hönic,
R. Kapitza

13:15 *Coffee Break and Finger Food*

Session 2: Trusted Execution

Chair: Phillip Raffeck

13:35 CCX: Enabling Unmodified Intel SGX Applications on Arm CCA

M. Schulze, T. Holz, F. Freiling

13:55 Rearchitecting the VMM for Confidential Virtual Machines

M. Misono

14:15 TEEMs: Core-Independent and Cooperating Trusted Execution Environments

N. Asmussen

14:35 Towards a Self-Attesting Key Broker for Confidential Containers

Y. Tallowitz, H. Löhr

14:55 *Coffee Break*

Session 3: Invited Talk, FGBS Meeting

Chair: Rüdiger Kapitza

15:15 From Smartphones to Cloud: Trustworthy Foundations for Digital Sovereignty (**Invited Talk**)

S. Shinde (ETH Zürich)

16:15 *Graduate Award*

17:15 *FGBS Business Meeting*

19:00 *Social Event (Hempels Burger & Kitzmann Bräuschänke)*

08:50 *Welcome*

Session 4: Isolation

Chair: Adam Lackorzynski

09:00 Trust Nothing: RTOS Security without Run-Time Software TCB

E. Ackermann, S. Bugiel

09:20 zBulk: Towards Automatic Compartmentalization in Rust with Zero Manual Retrofitting

M. Onciul

09:40 Isolation for Cyber-Physical Systems with Linux Confinement Mechanisms

N. Scheidweiler, E. Wintzler

10:00 *Coffee Break*

Session 5: Confidential GPU Computing & Bug Finding

Chair: Christian Berger

10:20 WarpGuard: Towards Control-Flow Attestation for Heterogeneous CPU-GPU Execution

C. Lindenmeier, M. Orenbach, A. Awad,
F. Schwarz, F. Alder, A. Atamli

10:40 EnclaveX: A Process-Level Approach to GPU Confidential Computing with K8s Support

R. Schambach, Q. Do Le

11:00 From Stochastic Parrots to Industrialized Bug Finding – The Impact of LLMs on Linux Distributions

B. Döbel

11:20 *Coffee Break*

Session 6: Automotive Software & Cyber-Physical Systems

Chair: Peter Ulbrich

11:40 BMW Mod2SDV / SADE – Safe and Secure Modular Architectures for the Next-Generation Vehicle

I. Stilkerich

12:00 AI-Assisted Porting of Automotive System Software to New Hardware Architectures

A. Kappel, A. Medjek, F. Riedl, A. Kajmakovi,
T. Scheipel, M. Baunach

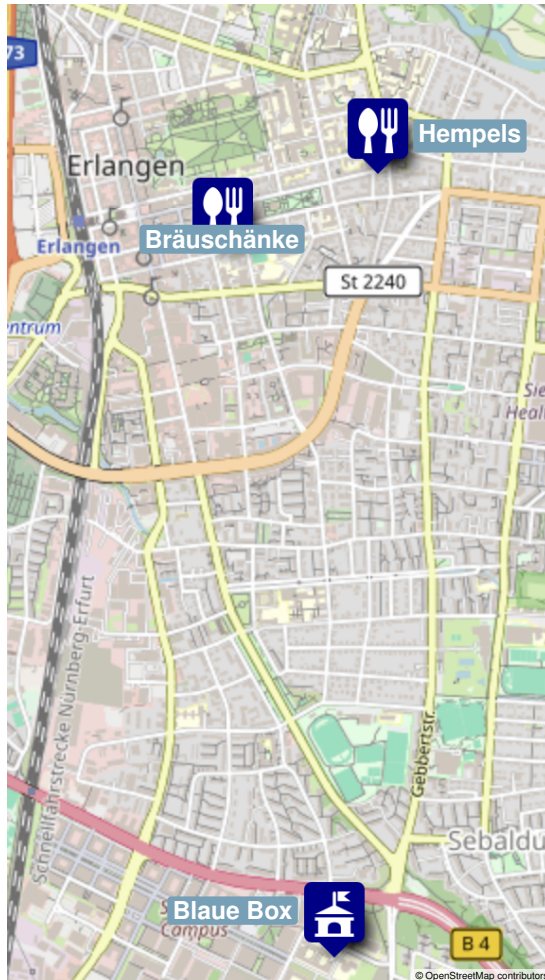
12:20 Towards a Physical Machine Model for Cyber-Physical Systems

M. Richter, M. Werner

12:40 *Closing and Snacks*

Social Event

Thursday, October 8, 2026, 19:00



We meet at **19:00** directly at the **two** restaurants:

Hempels Burger

MarquardsenstraSSe 18

75 reservations

Kitzmann Bräuschänke

Südliche StadtmauerstraSSe 25

35 reservations

How do I get to the social event?

1. On foot from FreyeslebenstraSSe 1 to the **GebbertstraSSe** bus stop (approx. 600 m, 8 min)
2. By bus (lines 290, 289, 295) from GebbertstraSSe to **Arcaden** (approx. 8 min)
3. On foot from Arcaden to **Hempels Burger** (16 min) or **Kitzmann Bräuschänke** (7 min)

If you would like to join us at **Kitzmann**, please sign up [here](#).



Für die Freiheit und Unabhängigkeit der Forschung

Rede zur DFG-Festveranstaltung 2026, Bonn, 30.06.2026



„Demokratie und Wissenschaft wurzeln in derselben geistigen Haltung. Beide setzen voraus, dass Argumente stärker sein sollten als Autoritäten, Kritik produktiver als Gewissheit und Lernen wichtiger als Rechthaben. Beide leben von der Einsicht, dass Erkenntnis niemals abgeschlossen ist und dass Freiheit nicht trotz, sondern erst durch Offenheit und Dialog möglich wird.“

– Prof. Dr. Katja Becker, Präsidentin der DFG

Ohne eine freie Wissenschaft verliere eine Gesellschaft ihre Fähigkeit, zwischen Wissen und Behauptung, zwischen Erkenntnis und Ideologie zu unterscheiden.

Rede: dfg.de/resource/blob/400256/260630-jv-rede-becker.pdf

Siehe auch: Forschung & Lehre, 14.04.2026: „Sachsen-Anhalt: AfD will ‚Niedergang der deutschen Wissenschaft‘ beenden“