Confidential Computing and Digital Sovereignty

Muhammad Usama Sardar

TU Dresden, Germany

July 19, 2026

Thanks to ULISSY s.r.l. for travel sponsorship!

Example Motivation for RG[1]

Sovereignty in the Cloud is an Illusion

For years, the tech industry has sold Confidential Computing as the ultimate shield for data sovereignty and cloud security.

Akber A Choudhry

06 Jul 2026 • 4 min read

Share

[1] https://akber.com/sovereignty-in-the-cloud-is-an-illusion/

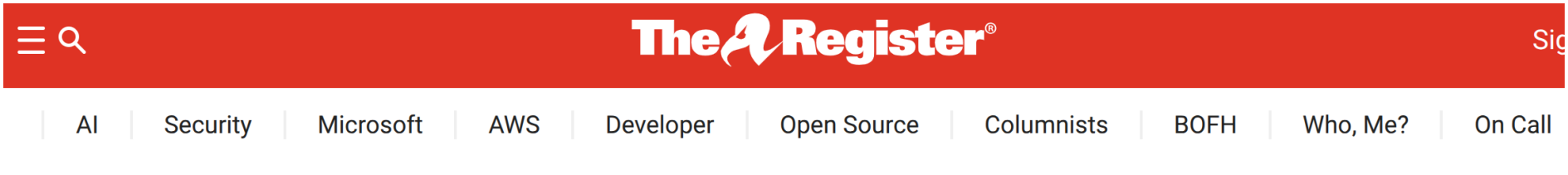
Example Motivation for RG[2]

The Handshake That Can't Keep Its Promise: Why Confidential Computing's Flaw Changes the Data Sovereignty Conversation

Jul 8, 2026

[2] https://blogs.groupware.org.uk/01-Quantum-Inc/the-handshake-that-cant-keep-its-promise-why-confidential-computings-flaw-changes-the-data-sovereignty-conver

Example Motivation for RG[3]



[3] https://www.theregister.com/security/2026/07/04/confidential-computings-trust-mechanism-is-broken-the-fix-may-not-exist/5266056

Potential Core Problem: Systematic Lack of Assurance of Accountability in Confidential Computing

- Example: European sovereignty is broken
  - Trust in chip manufacturers outside of Europe; supply chain attacks possible.
- Example: USA sovereignty is broken
  - Connection can be relayed to anywhere in the world
- Who is sovereign in current Confidential Computing?

Attackers are!

Why RG Now?

- wiretap.fail: No CVE (Intel and AMD announcements)
- TEE.fail: No CVE
- TDXdown: CVSS **2.5** by Intel
- Staleus: : CVSS **4.0**
- BreakFAST: CVE-2025-61972: CVSS **4.2** and CVE-2025-61971: CVSS **5.9**
- BadRAM: CVSS **5.3** by AMD
- Fabricked: CVE-2025-54510: CVSS **5.9**

CVE-2026-33697 of CVSS 7.5!

What Are We Looking For?

- Collaborators who can help in at least one of:
  - identification of research gaps/challenges/questions
  - setting a reasonable scope (open to discussion)
  - drafting charter

  for the proposed RG.

- Researchers, industry and all others who are interested in related topics.

Side Meeting

11:00-12:00 Uhr (CEST) on
20th July (Monday)
at Park Suite 4
and online

Links to Resources

- Pre-handshake attestation
  - https://www.researchgate.net/publication/385384309_Towards_Validation_of_TLS_13_Formal_Model_and_Vulnerabilities_in_Intel's_RA-TLS_Protocol
- Intra-handshake attestation
  - https://www.researchgate.net/publication/408219182_Intra-handshakefail_CVE-2026-33697_High-severity_CVE_in_Attested_TLS
  - https://www.github.com/muhammad-usama-sardar/intra-handshake.fail
- Attestation in Arm CCA and Intel TDX
  - https://www.researchgate.net/publication/375592777_Formal_Specification_and_Verification_of_Architecturally-defined_Attestation_Mechanisms_in_Arm_CCA_and_Intel_TDX
  - www.github.com/CCC-Attestation/formal-spec-TEE
- Identity Crisis
  - https://www.researchgate.net/publication/398839141_Identity_Crisis_in_Confidential_Computing_Formal_Analysis_of_Attested_TLS
  - https://www.researchgate.net/publication/398839141_Identity_Crisis_in_Confidential_Computing_Formal_Analysis_of_Attested_TLS
- Wiki page
  - www.github.com/EuroProofNet/ProgramVerification/wiki/AttestedTLS

ACK: Co-authors (in papers/IETF drafts)

- Viacheslav Dubeyko (IBM)
- Jean-Marie Jacquet (University of Namur)
- Songbo Bu (Shanghai Guan An Information Technology)
- Ionut Mihalcea (Arm)
- Thomas Fossati (Linaro)
- Arto Niemi (Huawei)
- Hannes Tschofenig (University of Applied Sciences Bonn-Rhein-Sieg and Siemens)
- Simon Frost (Arm)
- Ned Smith (Intel)
- Carsten Weinhold (Barkhausen Institut)
- Michael Roitzsch (Barkhausen Institut)
- Yogesh Deshpande (Arm)
- Yaron Sheffer (Intuit)
- Tirumaleswar Reddy K. (Nokia)
- Henk Birkholz (Fraunhofer SIT)
- Mariam Moustafa (Aalto University)
- Tuomas Aura (Aalto University)
- Liang Xia (Huawei)
- Weiyu Jiang (Huawei)
- Jun Zhang (Huawei)
- Houda Labiod (Huawei)
- Yuning Jiang (Huawei International)
- Meiling Chen (China Mobile)
- Minghui Xu (Shandong University)
- Pavel Nikonorov (GENXT)

ACK: Contributors

- Eric Rescorla (Independent)
- Laurence Lundblade (Security Theory LLC)
- Göran Selander (Ericsson AB)
- Marco Tiloca (RISE AB)
- Richard Barnes (Cloudflare)
- Giridhar Mandyam (AMD)
- Christopher Patton (Cloudflare)
- Dionna Amalie Glaze (Google)
- Bob Beck (Google)
- Mike Ounsworth (Cryptic Forest Software)
- John Preuß Mattsson (Ericsson Research)
- Cedric Fournet (Microsoft)
- Thore Sommer (TU Munich)
- Nikolaus Thümmel (Scontain)
- Jonathan Hoyland (Cloudflare)
- Jo Van Bulck (KU Leuven)
- Martin Thomson (Mozilla)
- Britta Hale (Naval Postgraduate School)
- Werner Staub (CORE Association)
- Christian Simmen (DENIC)
- Dennis Jackson (Mozilla)
- Paul Wouters (Aiven)
- Matthias Wählisch (TU Dresden)
- Andrey Ruzhanskiy (Telekom MMS)
- Muuhh Ikede (Cybertrust)
- Mike Bursell (CCC)
- Ravi Sahita (Rivos)
- Samuel Ortiz (Rivos)
- Mathieu Poirier (Linaro)
- Hannes Reinecke (SUSE)
- Alexander Graf (AWS)
- Elena Reshetova (Intel)
- Jon Lange (Microsoft)
- Daniel Kiper
- David Woodhouse (AWS)
- David Kaplan (AMD)
- Tiziano Santoro (Google)
- Juho Forsén
- Ira McDonald
- Markus Rudy (Edgeless Systems)
- Ayoub Benaissa (Zama)
- Greg Kostal (Microsoft)
- Mike Stunes (Microsoft)
- David Altobelli (Microsoft)
- Alistair Woodman
- and many others...