Intra-handshake.fail: CVE-2026-33697 (CVSS 7.5)

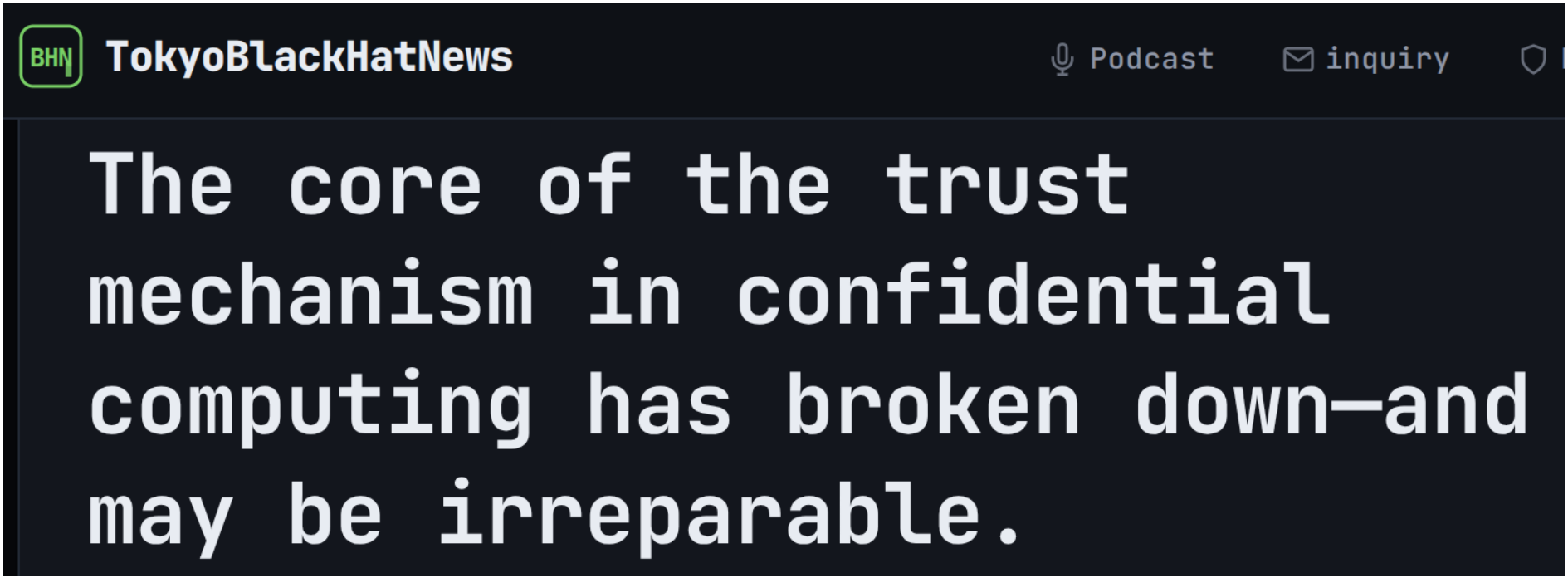
Muhammad Usama Sardar

TU Dresden, Germany

July 19, 2026

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

Motivation for Hackathon[1]



- Attestation protocol is the core trust mechanism of CC.

[1] https://blackhatnews.tokyo/archives/119915

Motivation for Hackathon[2]



[2] https://thenextgentechinsider.com/pulse/critical-flaw-discovered-in-confidential-computing-attestation-protocols

Motivation for Hackathon[3]

Confidential Computing: The proof of authenticity that confirms the fake machine

[3] translated from German: `https://www.blogspan.net/confidential-computing-attestierung-relay-luecke/`

Motivation for Hackathon[4]

A flaw breaks trust in confidential computing

New formal analyses challenge attested TLS, a key mechanism for confidential computing. The problem also affects production systems.

[4] translated from Italian `https://data4biz.com/articles/una-falla-rompe-la-fiducia-del-confidential-computing`

Why is it a Substantial Technical Concern?

- wiretap.fail: No CVE (Intel and AMD announcements)
- TEE.fail: No CVE
- TDXdown: CVSS **2.5** by Intel
- Staleus: CVE-2025-54509: 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!

No physical access required!

Thank You for Discussions

- Viacheslav Dubeyko
- Jean-Marie Jacquet
- Songbo Bu
- Werner Staub
- Alistair Woodman
- Göran Selander
- Pavel Nikonorov
- Tom Sato
- Davyd Okaianchenko

What We Learned

- A confirmation of vulnerability of drafts to CVE-2026-33697
  - draft-fossati-tls-attestation[5]
  - draft-fossati-seat-early-attestation[6]
  - draft-ritz-seat-facts[7]

Intra-handshake attestation is not a suitable choice for standardization.

[5] https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/

[6] https://datatracker.ietf.org/doc/draft-fossati-seat-early-attestation/

[7] https://datatracker.ietf.org/doc/draft-ritz-seat-facts/

Next Steps

- Discuss code and details at Hackdemo Happy Hour: Monday 18:30 - 19:30 Uhr
- SEAT WG: Tuesday 11:00 - 12:30 Uhr
- Side meetings: Proposal for new RGs
  - Confidential Computing, Monday; 11:00-12:00 Uhr @ Park Suite 4 and online
  - Agentic AI, Tuesday; 15:00-16:00 Uhr @ Park Suite 4 and online
- Complete the responsible disclosure before sharing on list
  - 3 more CVEs, each of CVSS 9.1!
  - 2 more CVEs, each of CVSS 7.5!

Links to Resources

- Paper
  - https://www.researchgate.net/publication/408219182_Intra-handshakefail_CVE-2026-33697_High-severity_CVE_in_Attested_TLS
- ProVerif artifacts, slides and video recordings
  - https://www.github.com/muhammad-usama-sardar/intra-handshake.fail
- 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)
- Camilo A. Posada (ULISSY s.r.l.)

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...