Gaps in Attested TLS Protocols for Confidential Computing

Muhammad Usama Sardar

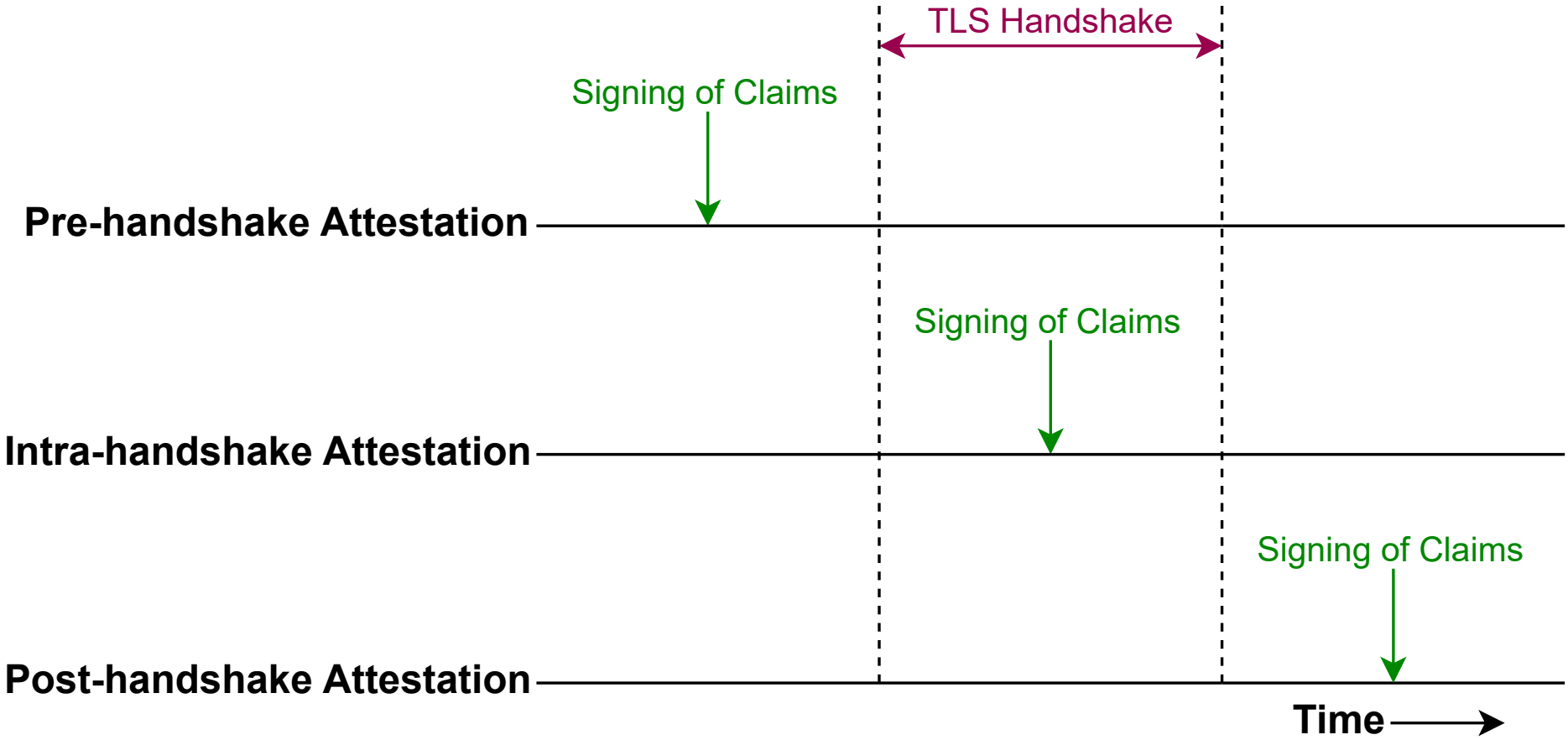
TU Dresden, Germany

June 27, 2025

Outline

Design Options for Attested TLS

- Temporal ordering of RA and TLS at Attester side



Levels of Assurance for Attested TLS Protocols

	RA-TLS[1] (Pre-HS)	TLS attest[2] (Intra-HS)	SCONE[3] (Post-HS)
(a) Open-source implementation	✓[4]	✓[5]	×
(b) Informal specifications available	×	✓	×
(c) Formal specifications	✓[6]	×	×
(d) Formal analysis of specifications	✓	×	×
(e) Formal verification of implementation	×	×	×

- Open source is a MUST for confidential computing!
- Formal analysis: a requirement at TLS WG[7]

[1] T. Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

[2] Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2025.

[3] Arnautov, Trach, Gregor, Thomas Knauth, Martin, Priebe, Lind, Muthukumaran, O'keeffe, Stillwell, et al., "SCONE: Secure Linux Containers with Intel SGX", 2016.

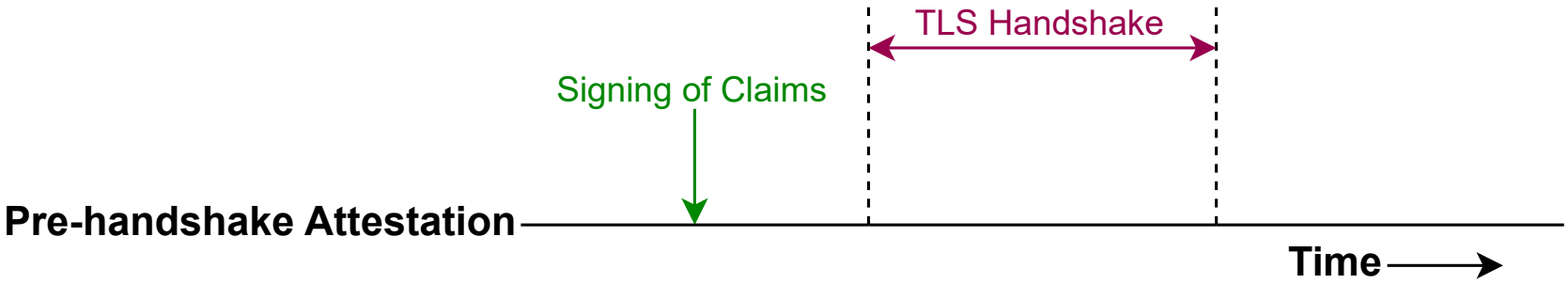
[4] `https://github.com/gramineproject/gramine/tree/master/CI-Examples/ra-tls-mbedtls`

[5] `https://github.com/CCC-Attestation/attested-tls-poc`

[6] Sardar, Niemi, Tschofenig, and Fossati, "Towards Validation of TLS 1.3 Formal Model and Vulnerabilities in Intel's RA-TLS Protocol", 2024.

[7] `https://github.com/tlswg/tls-fatt`

Pre-handshake Attestation



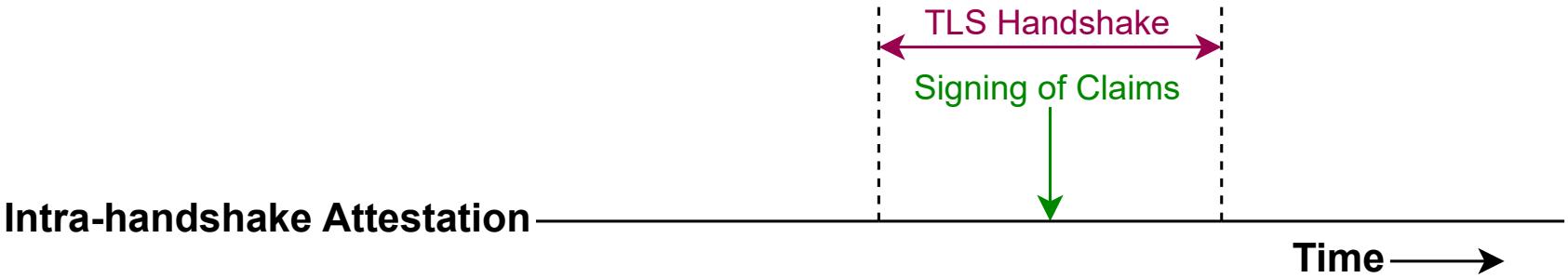
- General limitations
  - Limited claim set available (Runtime integrity not provided)
  - Per-session Evidence freshness[8] is not provided.
- CSR attestation[9]
  - Reliance on CA
- Intel's RA-TLS: diversion attacks[10]
  - Diversion to different data center
  - Diversion within data center

[8] Sardar, Niemi, Tschofenig, and Fossati, "Towards Validation of TLS 1.3 Formal Model and Vulnerabilities in Intel's RA-TLS Protocol", 2024.

[9] Ounsworth, Tschofenig, Birkholz, Wiseman, and Smith, *Use of Remote Attestation with Certification Signing Requests*, 2025.

[10] `https://datatracker.ietf.org/meeting/interim-2025-rats-01/materials/slides-interim-2025-rats-01-sessa-identity-crisis-in-attested-tls-for-confidential-computing-01.pdf`

Intra-handshake Attestation

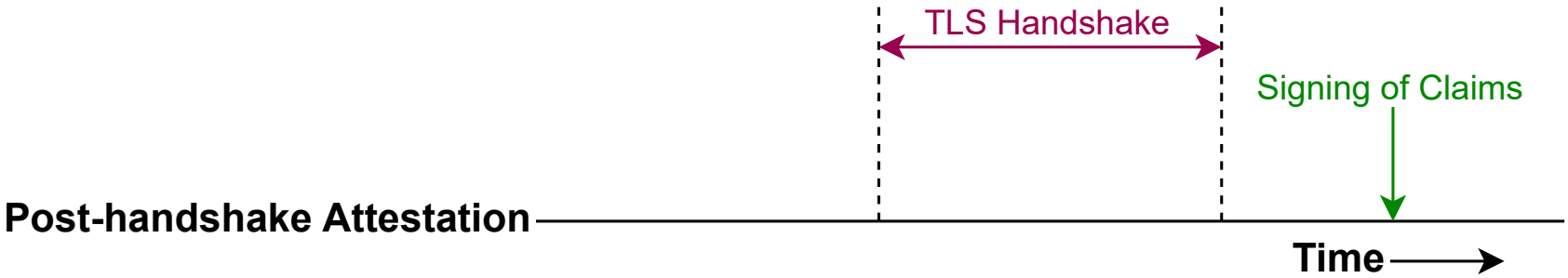


- General limitations
  - Limited claim set available (Runtime integrity not provided)
  - Invasive changes in TLS protocol (potentially as deep as key schedule)
- TLS attest I-D[11]: diversion attacks[12]
  - Diversion to different data center
  - Diversion within data center

[11] Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2025.

[12] `https://datatracker.ietf.org/meeting/interim-2025-rats-01/materials/slides-interim-2025-rats-01-sessa-identity-crisis-in-attested-tls-for-confidential-computing-01.pdf`

Post-handshake Attestation



- General limitations
  - Requires application-layer changes
  - Small latency impact (only for first authentication request)
- SCONE[13]
  - Closed source
  - Several missing specifications and contradictions
  - Breaks standard TLS server authentication property (TLS server as Attester)
  - Potentially replay attacks (Reuse of Exported Keying Material)
- draft-fossati-tls-exported-attestation[14]

[13] Arnautov, Trach, Gregor, Thomas Knauth, Martin, Priebe, Lind, Muthukumaran, O'keeffe, Stillwell, et al., "SCONE: Secure Linux Containers with Intel SGX", 2016.

[14] Fossati, Sardar, Reddy.K, Sheffer, Tschofenig, and Mihalcea, *Remote Attestation with Exported Authenticators*, 2025.

Outline

Can CSP *really* be out of TCB?

- In all public cloud cases, CSP is trusted for:
  1. Availability
  2. Machine identifier
     - Violates host-affinity requirement of *data sovereignty* regulations
  3. Location
     - CSP is the only source of truth for location.
     - Violates location-affinity requirement of *data residency* regulations

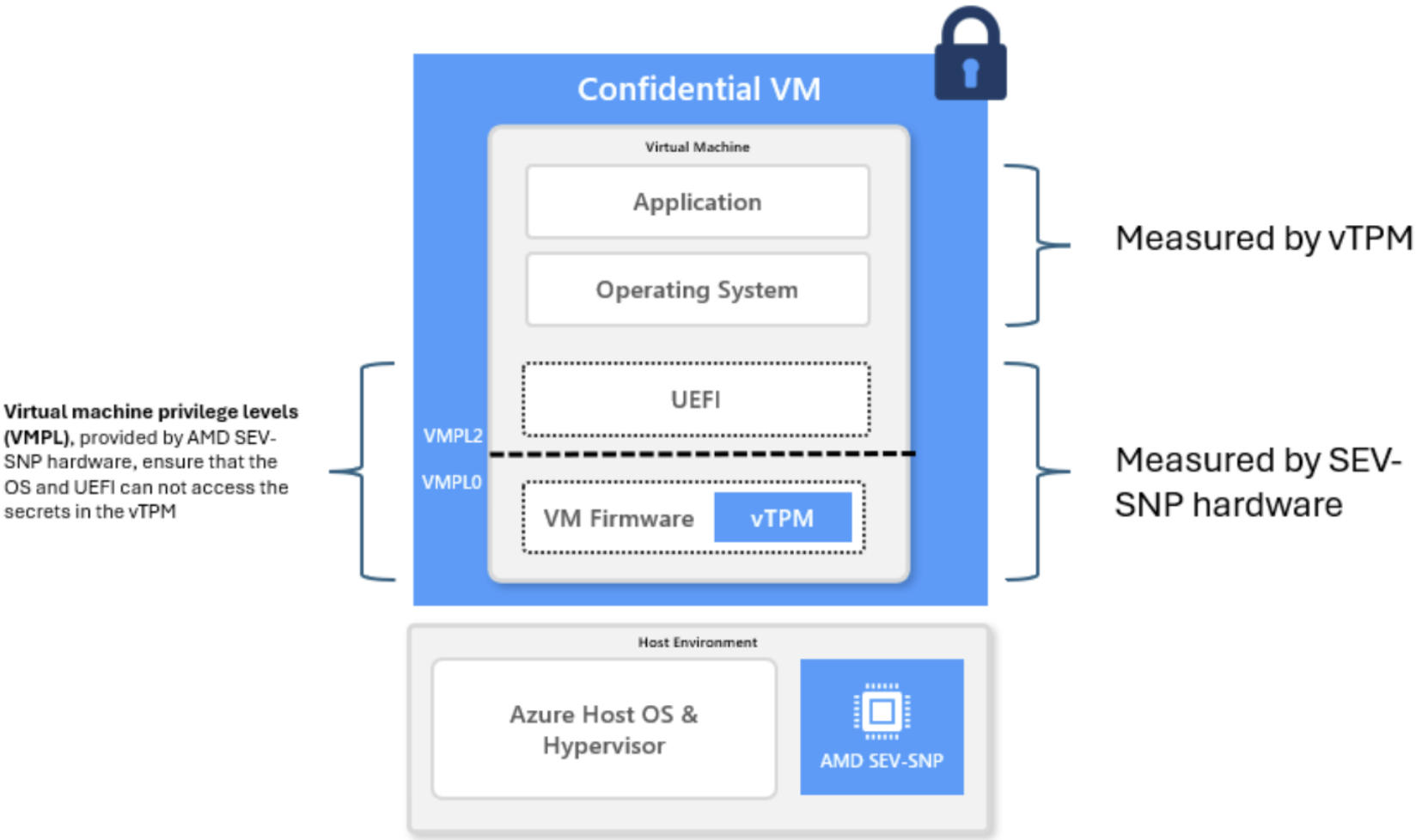
Can CSP *really* be out of TCB?

- In most cases, CSP is trusted for:
  1. Any part of the boot software that is not open source and not independently reproducible (IR)
     - Closed-source code may contain backdoors.
     - Cannot ensure configs of vTPM, e.g., non-migratability of keys
  2. Early boot measurements stored in vTPM
  3. Even remote attestation

Criteria	AWS	Microsoft	Google
VM firmware: open-source & IR	✓	×	×
vTPM inside confidential VM	×	✓	×
Ability to fetch raw Evidence directly	✓	×	✓

Example: Microsoft Azure[15]

- Who owns the seed for the Endorsement Key of vTPM?
- Who signs the Endorsement Key of vTPM?



[15] https://learn.microsoft.com/en-us/azure/confidential-computing/virtual-tpms-in-azure-confidential-vm

Next Steps

WG-forming BoF[16] at IETF 123

[16] https://datatracker.ietf.org/doc/bofreq-fossati-tls-exported-attestation-expat/

Key References

Arnautov, Sergei, Bohdan Trach, Franz Gregor, Thomas Knauth, Andre Martin, Christian Priebe, Joshua Lind, Divya Muthukumaran, Dan O'keeffe, Mark L Stillwell, et al. "SCONE: Secure Linux Containers with Intel SGX". In: *USENIX Symposium on Operating Systems Design and Implementation*. 2016, pp. 689–703. URL: https://www.usenix.org/conference/osdi16/technical-sessions/presentation/arnautov.

Fossati, Thomas, Muhammad Usama Sardar, Tirumaleswar Reddy.K, Yaron Sheffer, Hannes Tschofenig, and Ionuț Mihalcea. *Remote Attestation with Exported Authenticators*. Internet-Draft draft-fossati-tls-exported-attestation-01. Work in Progress. Internet Engineering Task Force, May 2025. 15 pp. URL: https://datatracker.ietf.org/doc/draft-fossati-tls-exported-attestation/01/.

Knauth, T., M. Steiner, S. Chakrabarti, L. Lei, C. Xing, and M. Vij. *Integrating Remote Attestation with Transport Layer Security*. Tech. rep. Intel Labs, 2018. URL: https://arxiv.org/abs/1801.05863.

Ounsworth, Mike, Hannes Tschofenig, Henk Birkholz, Monty Wiseman, and Ned Smith. *Use of Remote Attestation with Certification Signing Requests*. Internet-Draft draft-ietf-lamps-csr-attestation-19. Work in Progress. Internet Engineering Task Force, May 2025. 51 pp. URL: https://datatracker.ietf.org/doc/draft-ietf-lamps-csr-attestation/19/.

Sardar, Muhammad Usama, Arto Niemi, Hannes Tschofenig, and Thomas Fossati. "Towards Validation of TLS 1.3 Formal Model and Vulnerabilities in Intel's RA-TLS Protocol". In: *IEEE Access* 12 (2024), pp. 173670–173685. DOI: 10.1109/ACCESS.2024.3497184.

Tschofenig, Hannes, Yaron Sheffer, Paul Howard, Ionuț Mihalcea, Yogesh Deshpande, Arto Niemi, and Thomas Fossati. *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*. Internet-Draft draft-fossati-tls-attestation-09. Work in Progress. Internet Engineering Task Force, Apr. 2025. 34 pp. URL: https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/09/.

ACK

Co-authors/Co-editors

- Arto Niemi (Huawei)
- Ionut Mihalcea (Arm)
- Mariam Moustafa (Aalto University)
- Tuomas Aura (Aalto University)
- Thomas Fossati (Linaro)
- 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)

Others

- Henk Birkholz (Fraunhofer SIT)
- Pavel Nikonorov (GENXT)
- Laurence Lundblade (Security Theory LLC)
- Dionna Amalie Glaze (Google)
- Bob Beck (Google)
- Mike Ounsworth (Entrust)
- John Preuß Mattsson (Ericsson Research)
- Cedric Fournet (Microsoft)
- Thore Sommer (TU Munich)
- Jonathan Hoyland (Cloudflare)
- Jo Van Bulck (KU Leuven)
- Jean-Marie Jacquet (University of Namur)
- Maryam Zarezadeh (Barkhausen Institut)