Security Considerations for Confidential Computing

Muhammad Usama Sardar

TU Dresden, Germany

July 20, 2025

Teleport

Can Cloud Service Provider (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

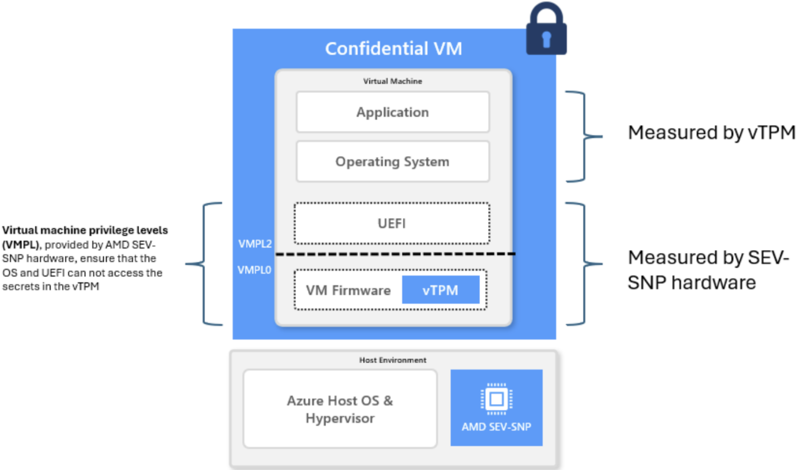
Can CSP *really* be out of TCB?

- 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[1]

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



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

What we are looking for?

- Seek collaborators knowledgeable in at least one of:
  - TLS
  - Remote attestation
  - Formal methods (Symbolic security analysis)
  - Confidential computing

  and interested in precisely stating the security considerations for confidential computing

- Side meetings
  - Attested TLS (Fundamentals): Monday 11:00 - 13:00, , El Escorial
  - Attested TLS (Deep dive): Wednesday 11:00 - 13:00, Segovia

- BoF: Monday 14:30 - 16:30, Tapices

Pointers to resources

- Wiki page[2]
- 3 main ways to combine attestation in TLS:
  - Pre-handshake attestation[3]
  - Intra-handshake attestation[4]
  - Post-handshake attestation: I-D[5] and Sec. 4 in this paper[6]
- Remote Attestation for Confidential Computing[7]
- Repo for attestation[8]
- Some recent slides and videos[9]
- Slides from side-meeting at IETF 122[10]
- #attested-tls on IETF slack

[2] https://github.com/EuroProofNet/ProgramVerification/wiki/AttestedTLS

[3] https://www.researchgate.net/publication/385384309_Towards_Validation_of_TLS_13_Formal_Model_and_Vulnerabilities_in_Intel's_RA-TLS_Protocol

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

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

[6] https://www.researchgate.net/publication/367284929_SoK_Attestation_in_Confidential_Computing

[7] https://www.researchgate.net/publication/375592777_Formal_Specification_and_Verification_of_Architecturally-defined_Attestation_Mechanisms_in_Arm_CCA_and_Intel_TDX

[8] https://github.com/CCC-Attestation/formal-spec-TEE

[9] https://github.com/CCC-Attestation/formal-spec-KBS

[10] https://www.researchgate.net/publication/390121641_Presentation_Attested_TLS_Fundamentals