Identity Crisis in Attested TLS for Confidential Computing

Muhammad Usama Sardar[1], Mariam Moustafa[2], Tuomas Aura[2] and Henk Birkholz[3]

[1]TU Dresden, Germany

[2]Aalto University, Espoo, Finland

[3]Fraunhofer SIT, Germany

May 2, 2025

Outline

Context

- I-D: draft-fossati-tls-attestation[1]
- Asked for adoption in TLS WG at IETF 121: confidential computing (CC) as main priority
- Formal Analysis Triage Team (FATT[2]) process
- Formal analysis of v8 under CC threat model in ProVerif
  - Breaks server authentication[3]
- Proposed solution
  - New I-D[4] uses post-handshake attestation
- Open problems
- Challenge: *Terminology hell* and several rabbit holes in RATS[5]
  - Very abstracted view: non-exhaustive
  - Verifying RP = Verifier + Relying Party

[1] Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

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

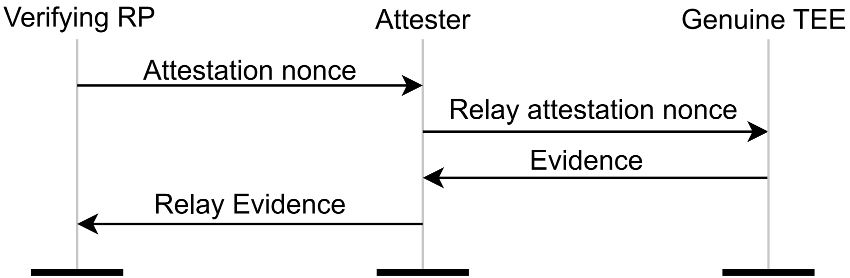
[3] https://mailarchive.ietf.org/arch/msg/tls/Jx_yPoYWMIKaqXmPsytKZBDq23o/

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

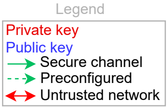
[5] Birkholz, Thaler, Richardson, Smith, and Pan, *Remote ATtestation procedureS (RATS) Architecture*, 2023.

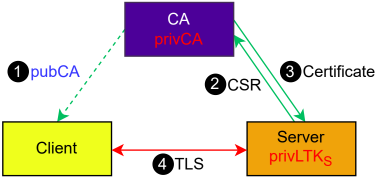
Problem in Remote Attestation

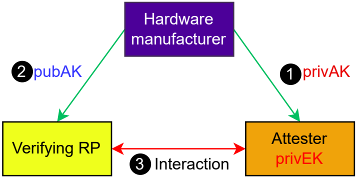
- Privacy: Claims visible to passive adversaries
- Security: Relay attacks
  - Attester is malicious but tricks the Verifying RP to believe that Attester is genuine.



TLS vs. Remote Attestation







- CA as Trust Anchor

- HW manufacturer as Trust Anchor

$$Cert_S = sign(privCA, ID_S \parallel pubLTK_S)$$

ID_S represents identity

$$Evidence = sign(privAK, m \parallel pubEK)$$

m represents measurements

IAB Statements

- IAB statement[6]
- CCC response[7]
- IAB response[8]

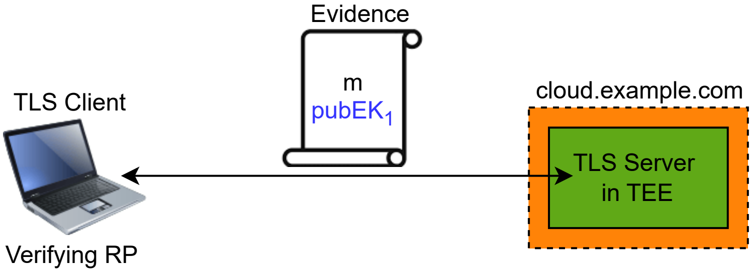
[6] https://datatracker.ietf.org/doc/statement-iab-statement-on-the-risks-of-attestation-of-software-and-hardware-on-the-open-internet/

[7] https://www.ietf.org/lib/dt/documents/LIAISON/liaison-2023-11-07-confidential-computing-consortium-iab-the-confidential-computing-consortiums-response-to-t pdf

[8] https://datatracker.ietf.org/liaison/1897/

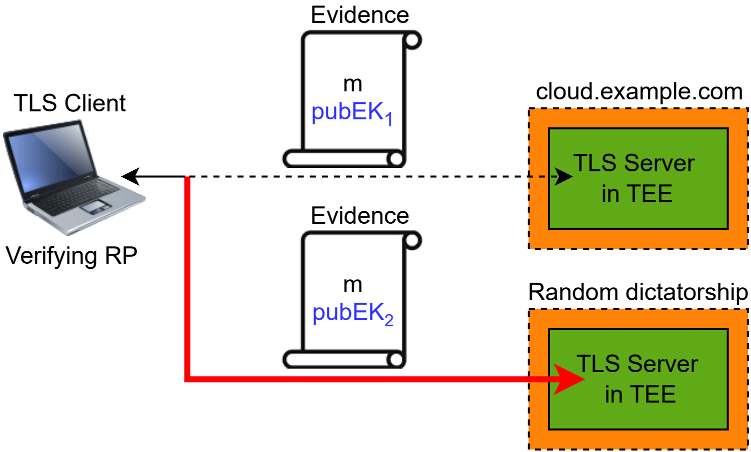
Remote Attestation-only (§6.1 in I-D)

- Evidence with measurements
- Is the average cloud customer happy with this?



Problem with Remote Attestation-only

- No PKI cert $\implies$ No identity authentication
- Hostname not measured $\implies$ Redirection to a different data center

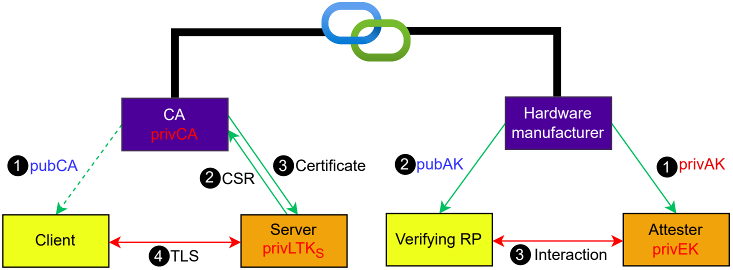


Security Consideration

Using the proposed protocol, the security breaks if there is even one compromised machine (i.e., Attestation Key is compromised) in the world whose corresponding certificate (e.g., Provisioning Certification Key certificate for Intel TDX) has not yet been added to the revocation list.

Solution

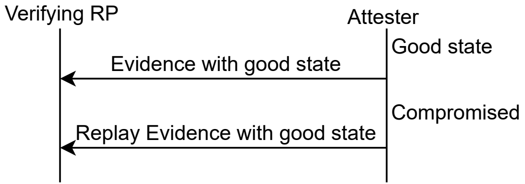
- Augment rather than replace Server Authentication
  - PKI cert for ID, e.g., hostname
  - Evidence to prove integrity of its computing environment



- Challenge: CertificateVerify message is not extensible!

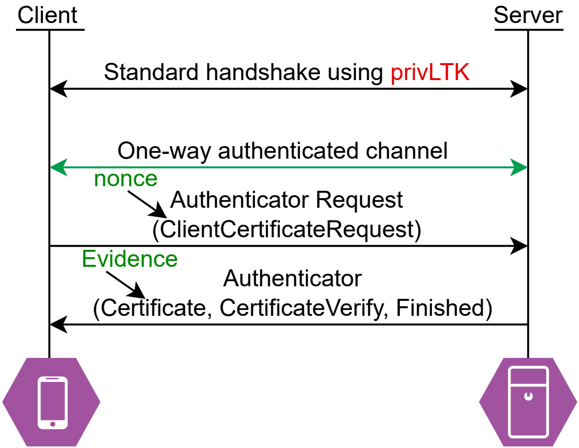
Inherent Limitations of Intra-handshake Attestation

- Inherent complexity
  - Changes in the handshake (potentially as deep as the key schedule)
- Editors claim freshness (§4 in I-D) but in reality
  - (temporally) only at the time of handshake (i.e., not afterwards)
  - and for only the Claims available at the time of handshake (i.e., not afterwards): perhaps the most important for freshness are the runtime measurements, since load-time measurements remain the same. The question remains: how many (if any at all) runtime measurements are available at the time of handshake?
- How would I get a fresh (recent) state whenever I want and for any Claims I want?
  - Post-handshake attestation may be a more reasonable choice.



Potential Solution: Post-Handshake Attestation[10]

- Based on RFC 9261[9]
- Server as Attester



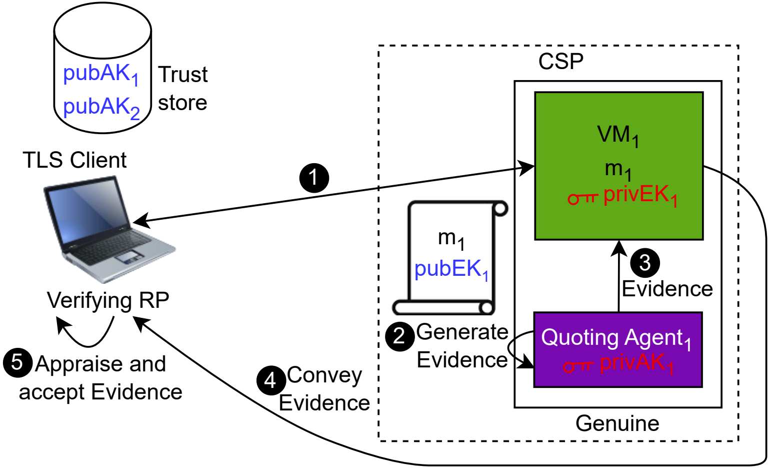
[9]Sullivan, *Exported Authenticators in TLS*, 2022.

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

Outline

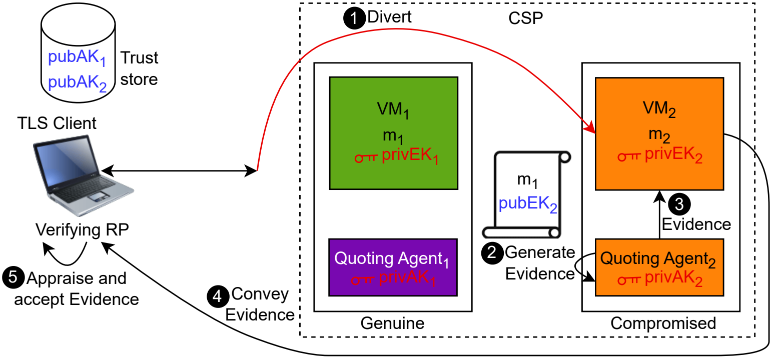
Original Path

- Quoting Agent generates Evidence.



A Diversion Attack Within CSP

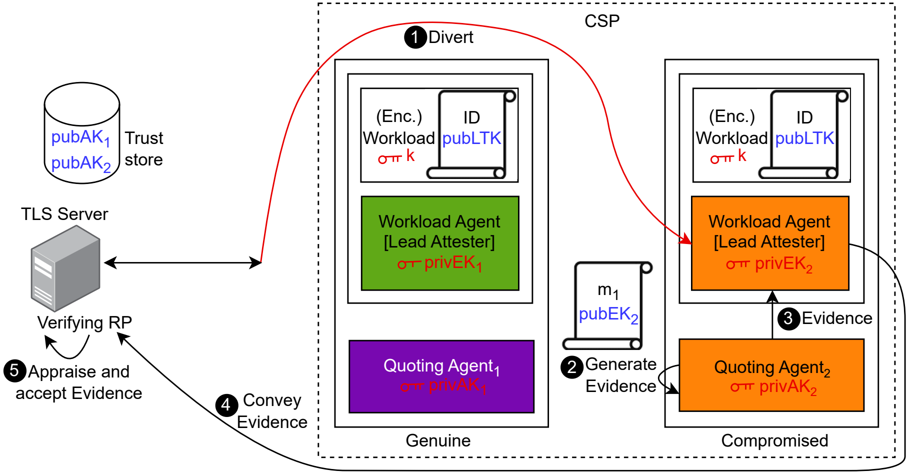
- AK of a specific machine may be compromised. (e.g., $privAK_2$)
  - Transient execution attacks, as demonstrated by Foreshadow[11]
- VM_2 impersonates VM_1



[11] Van Bulck, Minkin, Weisse, Genkin, Kasikci, Piessens, Silberstein, Wenisch, Yarom, and Strackx, "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution", 2018.

B How to Provision ID and LTK based on m?

- Confidential Containers, e.g., Trustee[12]/Key Broker Service (KBS)
- Who owns privLTK?



[12] https://github.com/confidential-containers/trustee

Discussion

- Platform instance identifiers and owner identity fields
  - Typically set to null
  - Operator can still provide the platform instance identifier of the compromised machine
- Security Version Numbers (SVNs)
  - Patch can be applied only when the vulnerability is known

Discussion: Can CSP *really* be out of TCB? (§9.1 in I-D)

- In some cases, CSP is trusted for:
  1. Availability
  2. VM identifier (since it is assigned by CSP)
  3. Location (since CSP is the only source of truth)
  4. Any part of the boot software that is not open source and not independently reproducible (IR)
  5. Early boot measurements by vTPM
  6. Even remote attestation

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

Open Questions for Discussion

- What exactly is the boundary between remote attestation and attested TLS? (channel bindings?)
- Can remote attestation be implemented on its own (without any secure channel) in CC context? Any concrete use case? (key release/KBS?)
- Server's location from regulatory perspective?

Next Steps

- Threat model
- Thorough comparison of intra- and post-handshake attestation

Key References

Birkholz, Henk, Dave Thaler, Michael Richardson, Ned Smith, and Wei Pan. *Remote ATtestation procedureS (RATS) Architecture*. RFC 9334. Jan. 2023. DOI: 10.17487/RFC9334. URL: https://www.rfc-editor.org/info/rfc9334.

Fossati, Thomas, Muhammad Usama Sardar, Yaron Sheffer, Hannes Tschofenig, and Ionuț Mihalcea. *Remote Attestation with Exported Authenticators*. Internet-Draft draft-fossati-tls-exported-attestation-00. Work in Progress. Internet Engineering Task Force, Mar. 2025. 9 pp. URL: https://datatracker.ietf.org/doc/draft-fossati-tls-exported-attestation/00/.

Sullivan, Nick. *Exported Authenticators in TLS*. RFC 9261. July 2022. DOI: 10.17487/RFC9261. URL: https://www.rfc-editor.org/info/rfc9261.

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. Work in Progress. Internet Engineering Task Force, Oct. 2024. 34 pp. URL: https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/08/.

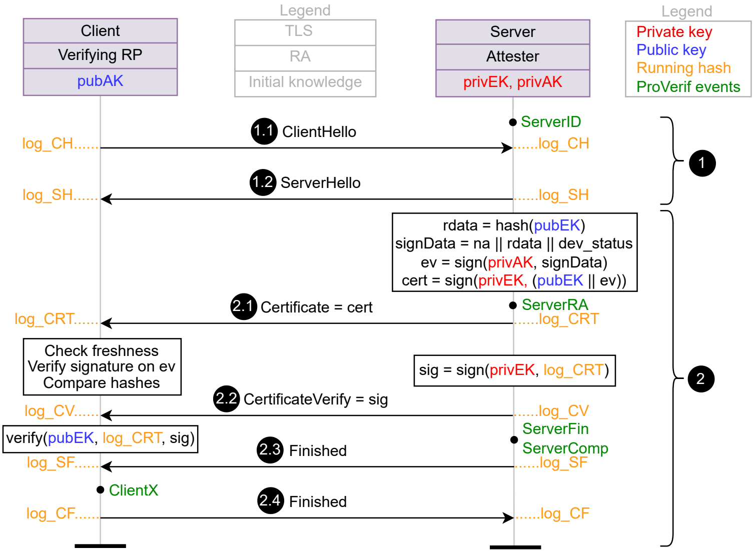
Van Bulck, Jo, Marina Minkin, Ofir Weisse, Daniel Genkin, Baris Kasikci, Frank Piessens, Mark Silberstein, Thomas F. Wenisch, Yuval Yarom, and Raoul Strackx. "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution". In: *Proceedings of the 27th USENIX Security Symposium*. USENIX Association, Aug. 2018.

ACK

- Laurence Lundblade (Security Theory LLC)
- Thomas Fossati (Linaro)
- Hannes Tschofenig (University of Applied Sciences Bonn-Rhein-Sieg and Siemens)
- Ionut Mihalcea (Arm)
- Yaron Sheffer (Intuit)
- Dionna Amalie Glaze (Google)
- Bob Beck (Google)
- Tirumaleswar Reddy K. (Nokia)
- Mike Ounsworth (Entrust)
- Pavel Nikonorov (GENXT)
- John Preuß Mattsson (Ericsson Research)
- Cedric Fournet (Microsoft)
- Thore Sommer (Kiel University)
- Jonathan Hoyland (Cloudflare)
- Jo Van Bulck (KU Leuven)
- Jean-Marie Jacquet (University of Namur)
- Maryam Zarezadeh (Barkhausen Institut)

Outline

TLS-attest Protocol[13]



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