Comprehensive Formal Analysis of Attested TLS Protocols

Muhammad Usama Sardar

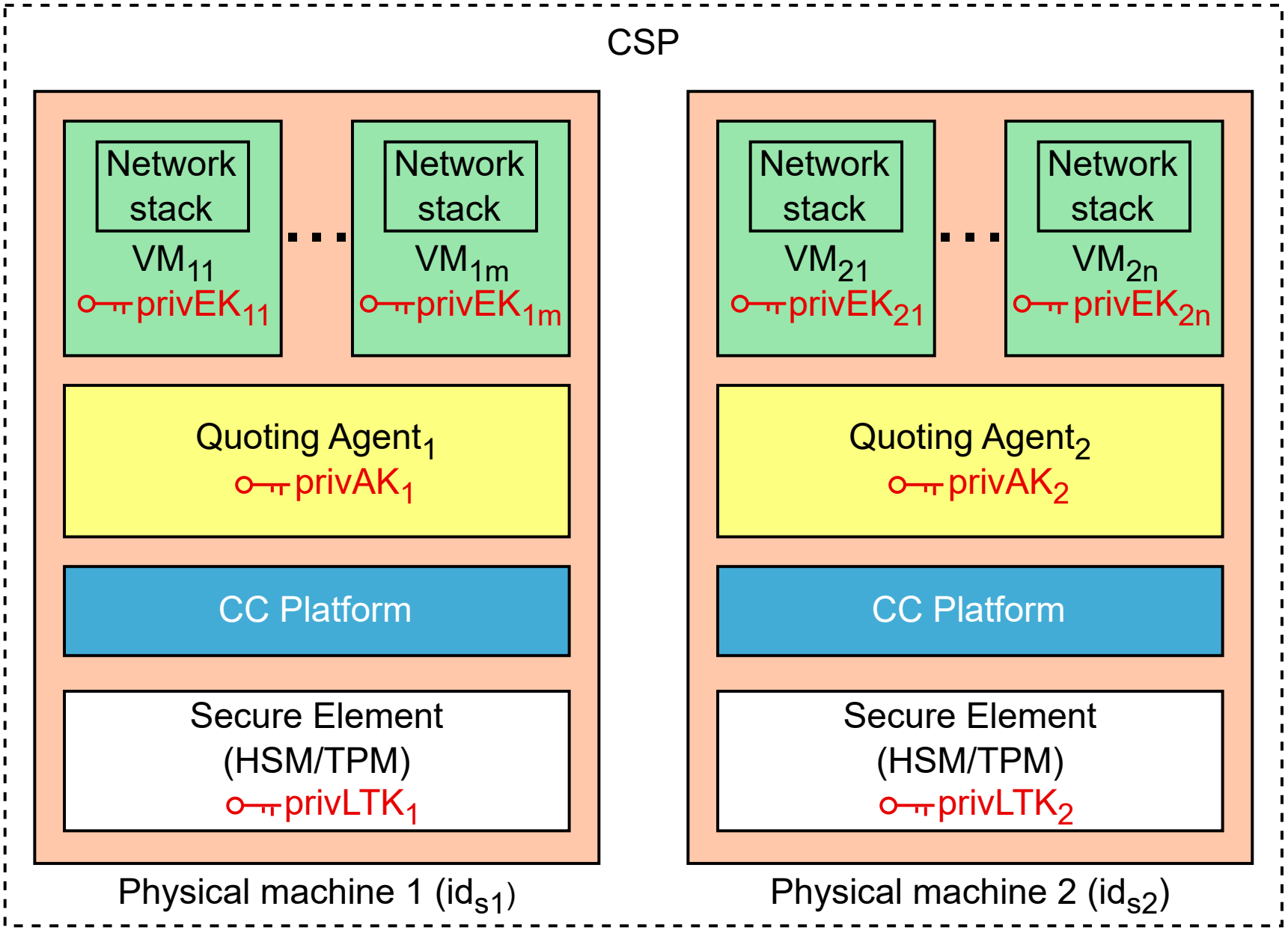
Based on joint works with Arto Niemi, Hannes Tschofenig, Thomas Fossati, Simon Frost, Ned Smith, Ionut Mihalcea, Yaron Sheffer, Mariam Moustafa, Tuomas Aura, Jean-Marie Jacquet, Tirumaleswar Reddy, Carsten Weinhold and Michael Roitzsch

TU Dresden, Germany

October 7, 2025

Outline

System Model



Informal Security Goals

- Standard TLS properties, in particular
  - Server authentication
  - Secrecy of session keys

Informal Security Goals

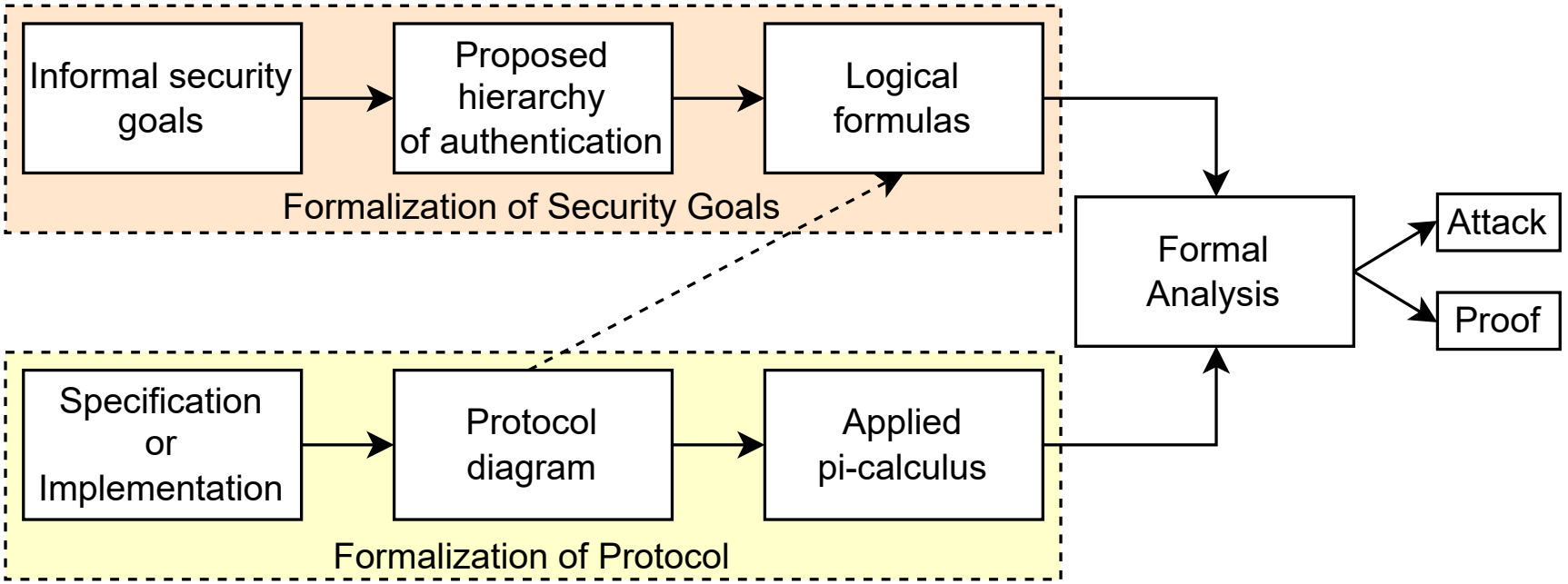
- Standard TLS properties, in particular
  - Server authentication
  - Secrecy of session keys

- Remote Attestation
  - Integrity of Evidence
  - Freshness of Evidence
    - Binding Evidence to a specific RA interaction
    - Recentness of Evidence generation
  - Refresh of Evidence: repeatedly track runtime state

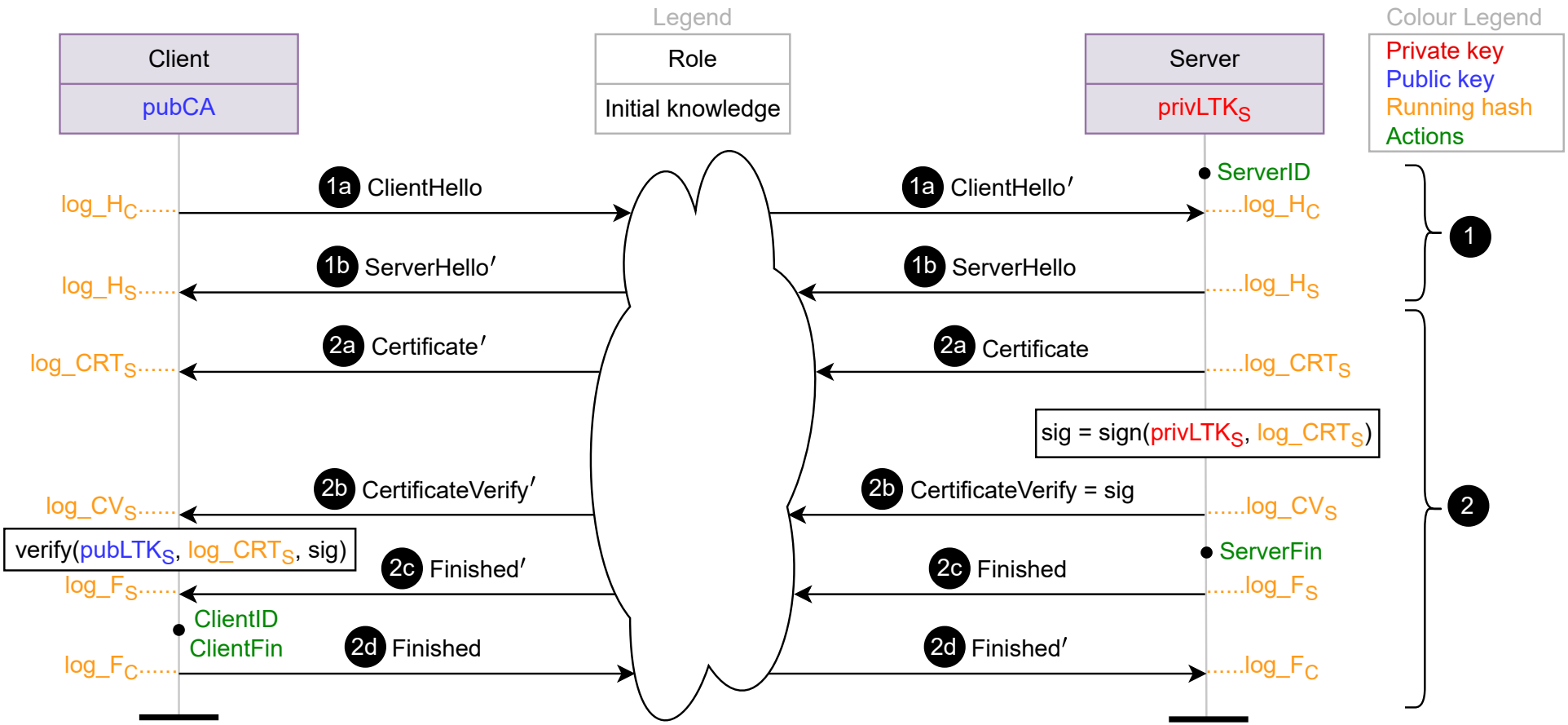
Informal Security Goals

- Standard TLS properties, in particular
  - Server authentication
  - Secrecy of session keys
- Remote Attestation
  - Integrity of Evidence
  - Freshness of Evidence
    - Binding Evidence to a specific RA interaction
    - Recentness of Evidence generation
  - Refresh of Evidence: repeatedly track runtime state
- Composition goals
  - Binding of Remote Attestation and TLS
    - Binding Evidence to a specific TLS connection: g^{xy}, *htsc*, *atsc*
  - Evidence is generated by the same server that is authenticated.

Overview of Approach

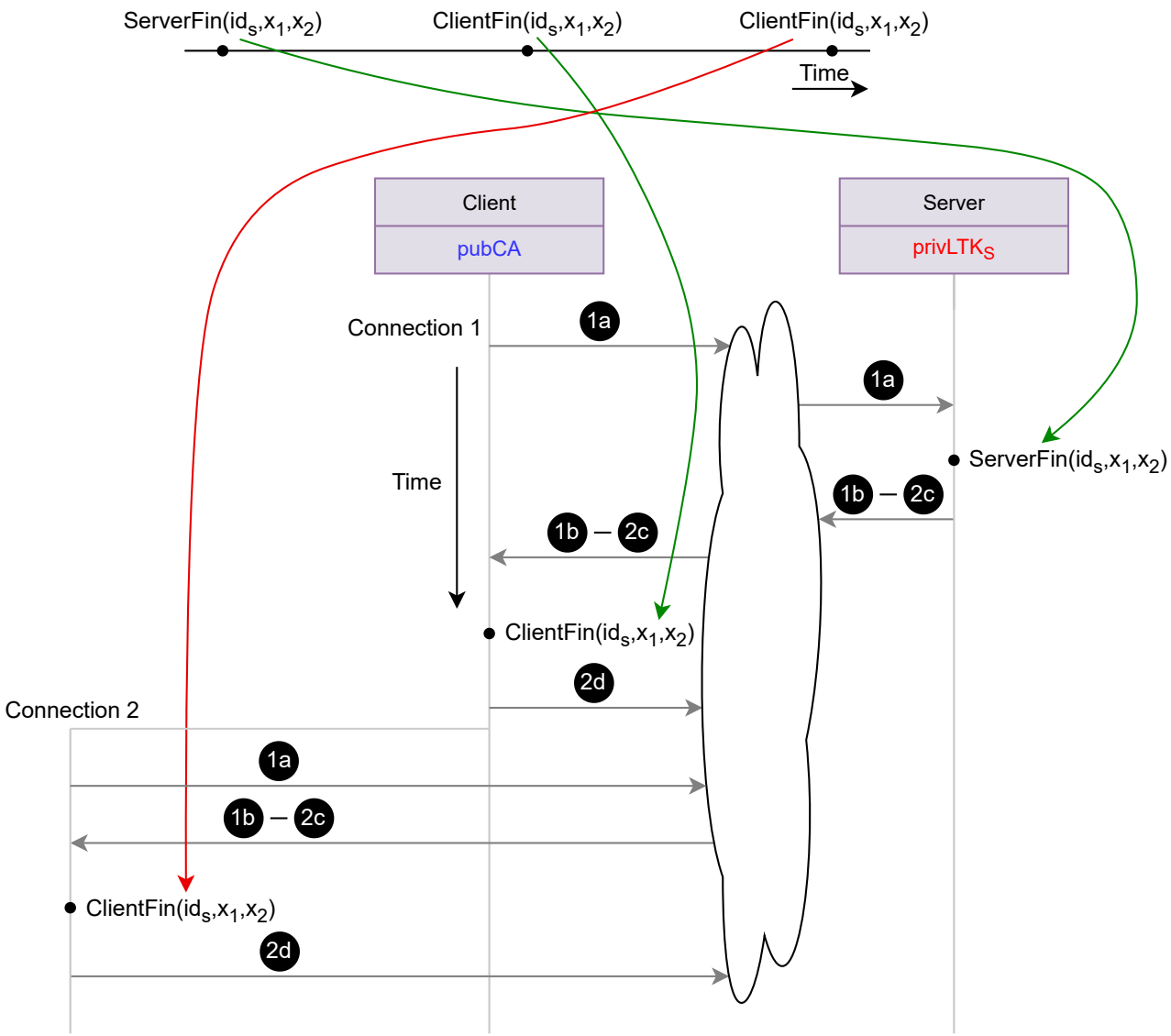


Overview of Approach



Outline

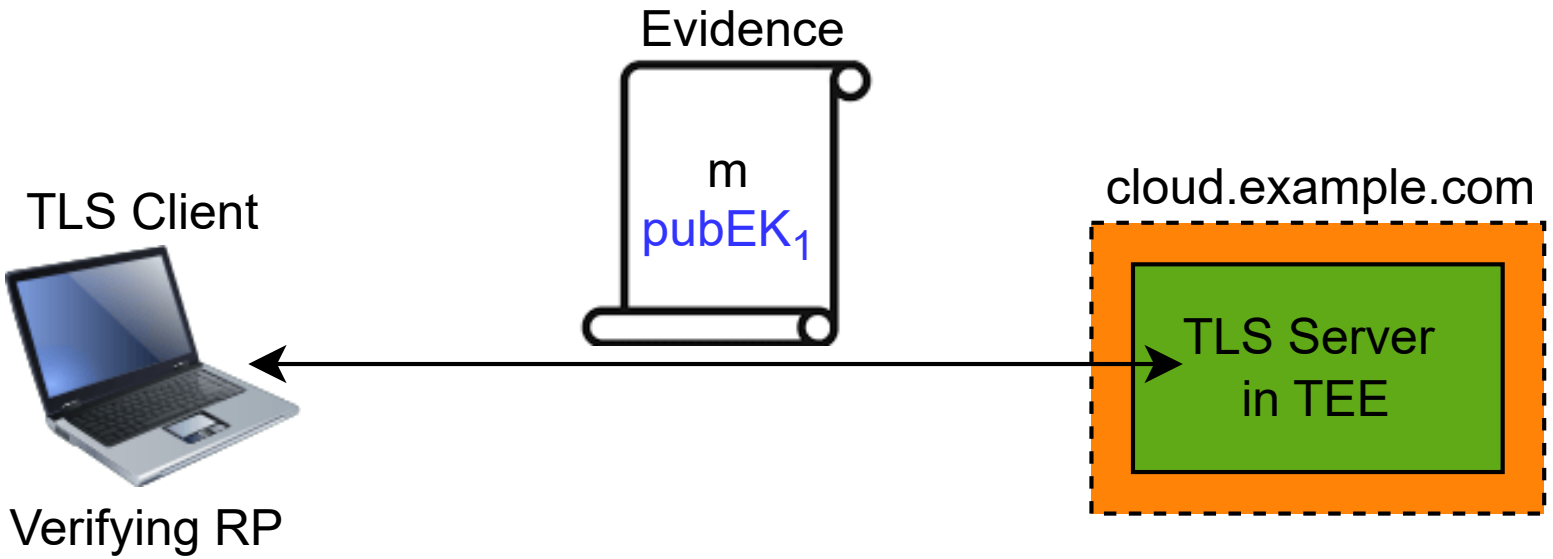
1 Replay Attack in Interoperable RA-TLS[1]



[1] https://github.com/ccc-attestation/interoperable-ra-tls

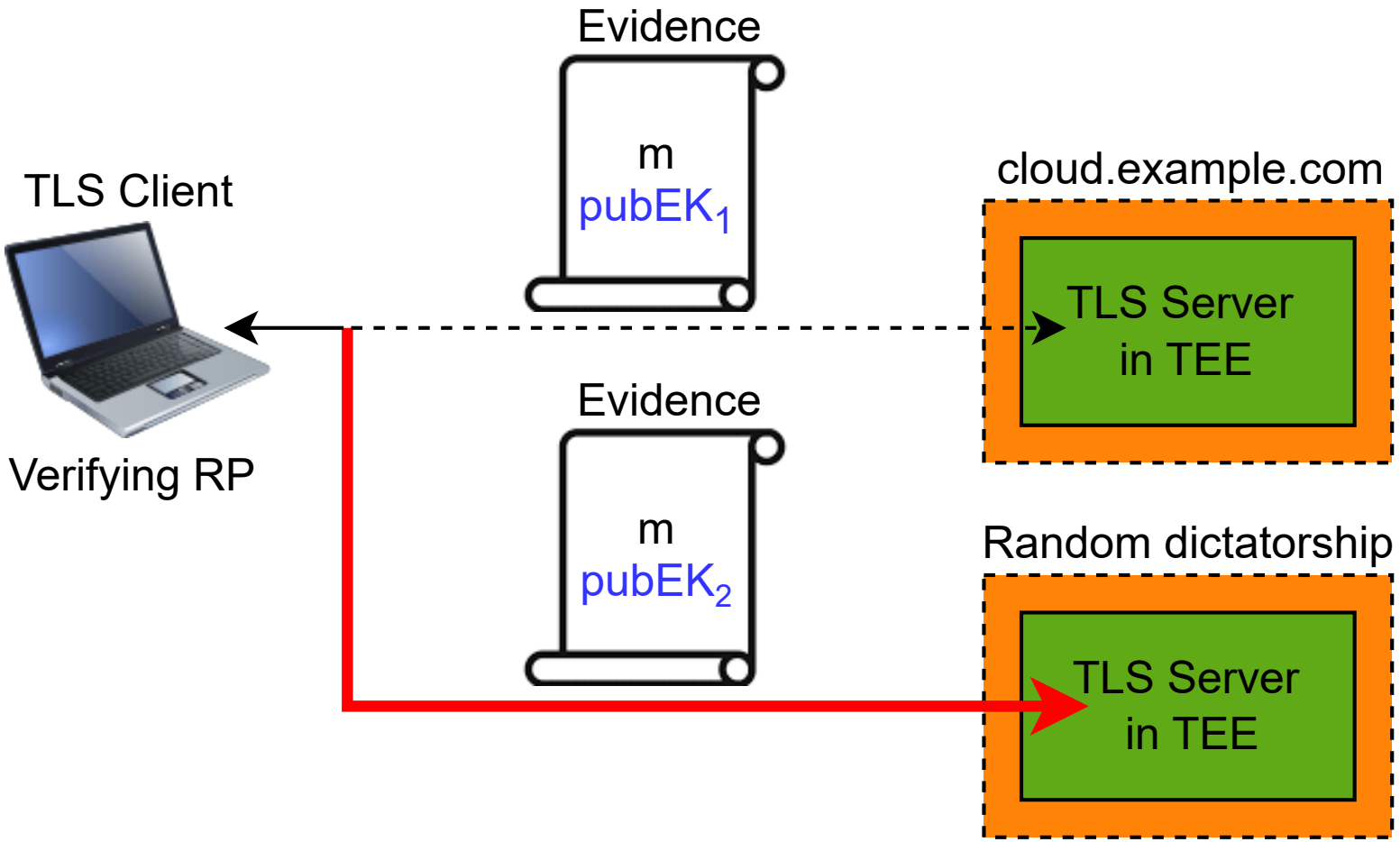
2 Remote Attestation-only (§6.1 in TLS-attestation draft)

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



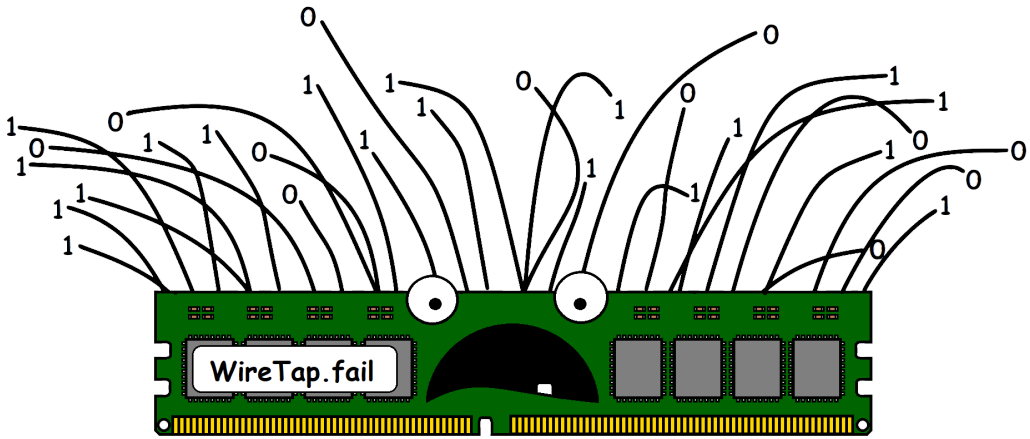
Diversion to Different Data Center

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

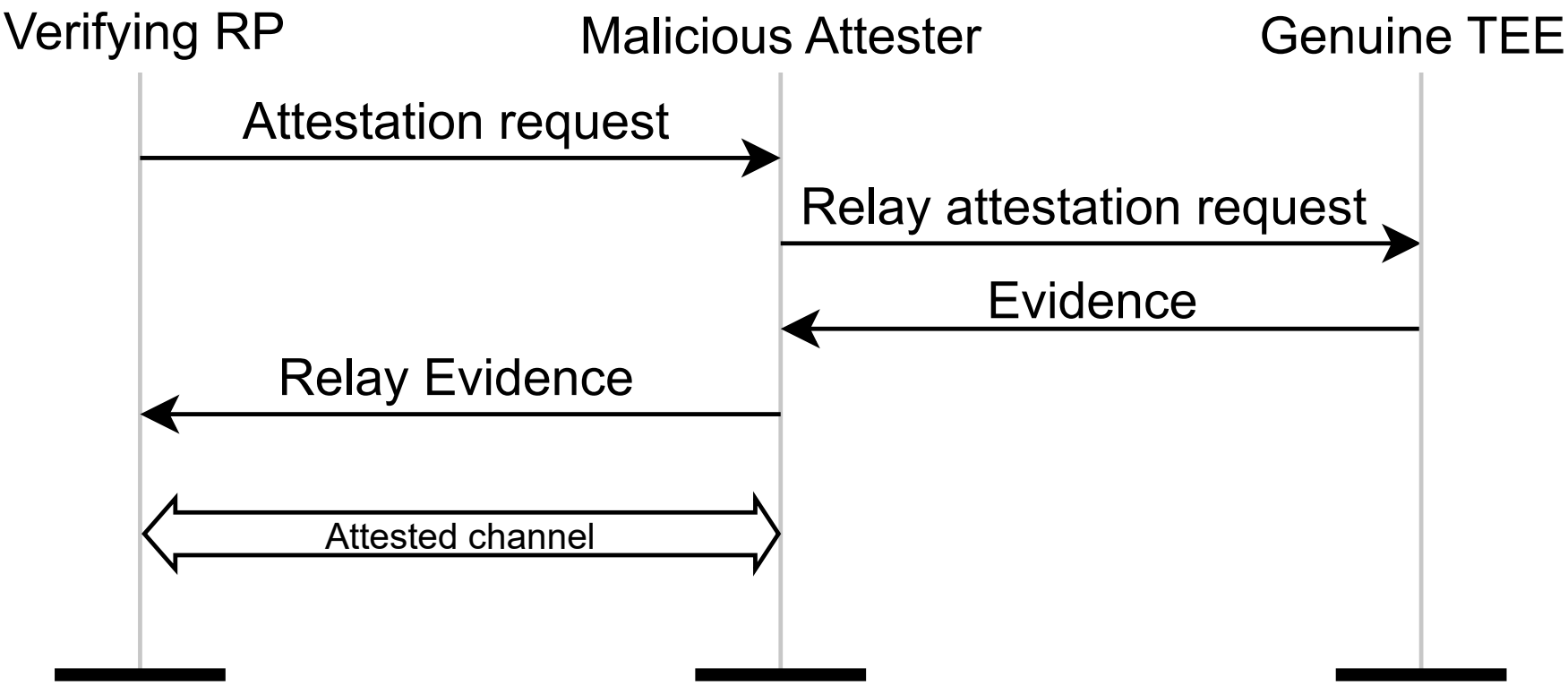


Security Consideration: Identity Crisis

Using the proposed protocols, 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.



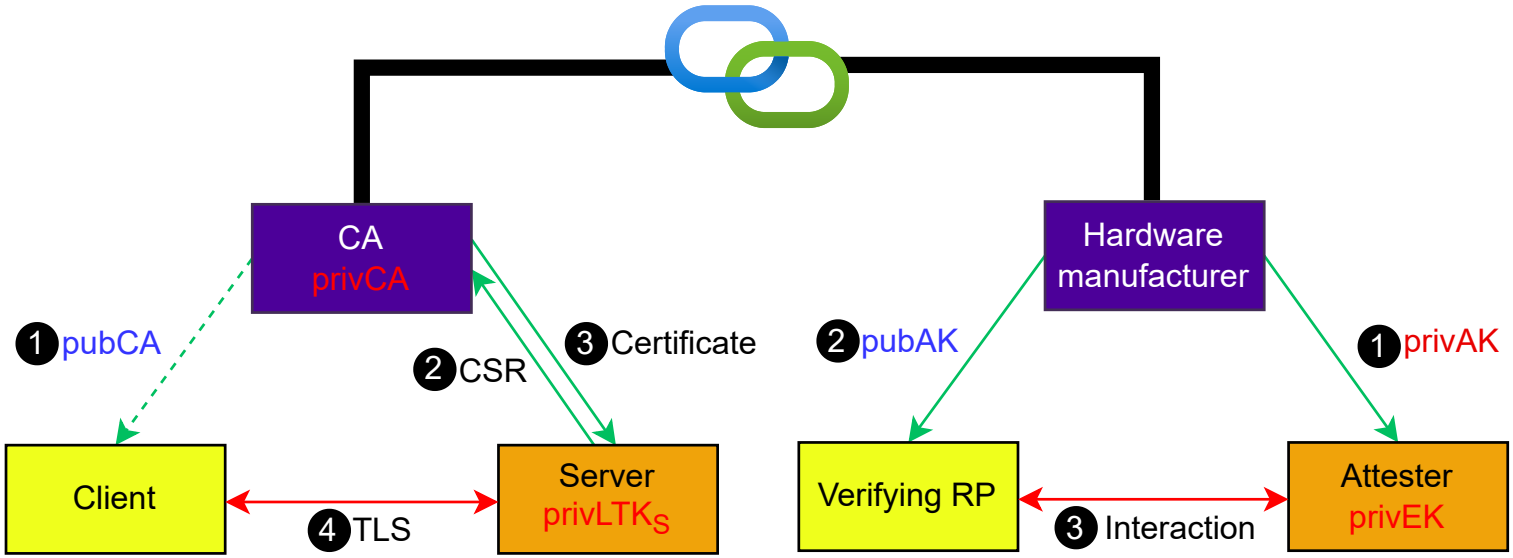
3 Relay Attack



Outline

Solution

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



Links to Resources

- Paper on identity crisis
  - https://www.researchgate.net/publication/398839141_Identity_Crisis_in_Confidential_Computing_Formal_Analysis_of_Attested_TLS
- Wiki page
  - https://github.com/EuroProofNet/ProgramVerification/wiki/AttestedTLS
- Formal proof of insecurity of pre- and intra-handshake attestation
  - https://github.com/CCC-Attestation/formal-spec-id-crisis
- Post-handshake attestation draft
  - https://datatracker.ietf.org/doc/draft-fossati-seat-expat/
- Attestation in Arm CCA and Intel TDX
  - https://github.com/CCC-Attestation/formal-spec-TEE
- Security considerations of remote attestation
  - https://datatracker.ietf.org/doc/draft-sardar-rats-sec-cons/
- IETF SEAT WG
  - https://datatracker.ietf.org/wg/seat/about/
- Technical Concepts
  - https://www.researchgate.net/publication/396199290_Perspicuity_of_Attestation_Mechanisms_in_Confidential_Computing_Technical_Concepts
- Validation of TLS 1.3 Key Schedule
  - https://www.researchgate.net/publication/396245726_Perspicuity_of_Attestation_Mechanisms_in_Confidential_Computing_Validation_of_TLS_13_Key_Schedule
- General Approach
  - https://www.researchgate.net/publication/396593308_Perspicuity_of_Attestation_Mechanisms_in_Confidential_Computing_General_Approach
- Weekly meetings
  - https://github.com/tls-attestation#meetings

ACK

Co-authors

- Arto Niemi (Huawei)
- Thomas Fossati (Linaro)
- Simon Frost (Arm)
- Ned Smith (Intel)
- Ionut Mihalcea (Arm)
- 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)

Contributors

- Christopher Patton (Cloudflare)
- Jean-Marie Jacquet (University of Namur)
- 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)
- Nikolaus Thümmel (Scontain)
- Giridhar Mandyam (Mediatek)
- Jonathan Hoyland (Cloudflare)
- Jo Van Bulck (KU Leuven)
- Eric Rescorla (Independent)
- Richard Barnes (Cloudflare)
- Martin Thomson (Mozilla)
- Britta Hale (Naval Postgraduate School)