Security Analysis of Attested TLS and Attested EDHOC

Muhammad Usama Sardar[1,2], Viacheslav Dubeyko[3], and Jean-Marie Jacquet[4]

[1]TU Dresden, Germany

[2]Co-chair, Trusted Research Environment (TRE) Open Suite, Global Alliance for Genomics and Health (GA4GH)

[3]IBM, San Jose, CA, USA

[4]Nadi Research Institute, University of Namur, Belgium

September 3, 2026

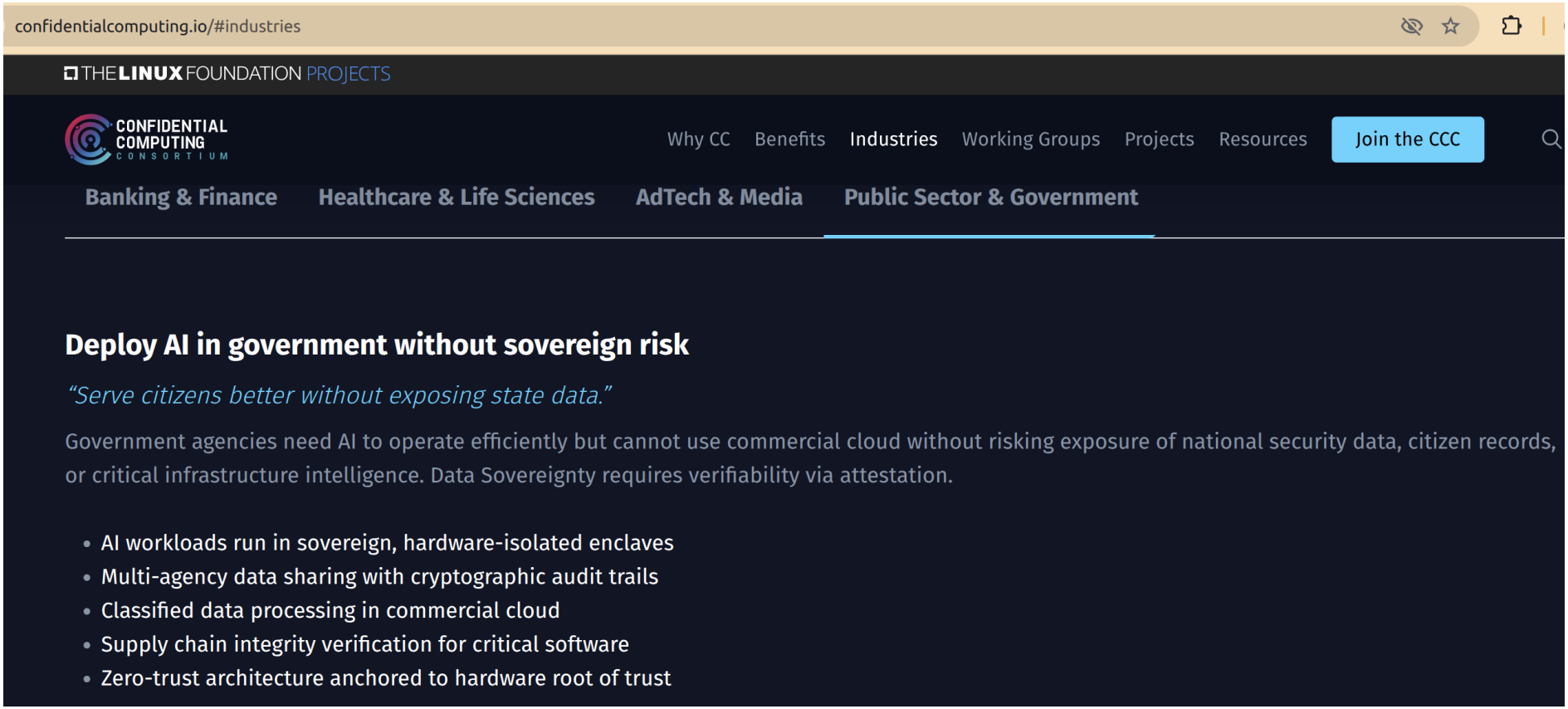
Use case: Trusted Research Environment (TRE) Scenario



- Background
  - See recording at RIoT 2024 (link)
  - See recording at RIoT 2025 (link)
- (D)TLS + Attestation = Attested (D)TLS
- We discovered high-severity vulnerability intra-handshake attestation
  - CVE-2026-33697 published: Severity = HIGH (7.5/10)
  - EUVD-2026-16488 published: Severity = HIGH (7.5/10)
  - Accepted at ESORICS[1] (CORE Rank A)

[1] https://sites.google.com/di.uniroma1.it/esorics2026/

The Claim of Confidential Computing[2]



[2] `https://confidentialcomputing.io/#industries`

The Reality[3] of Confidential Computing

Vulnerability	CVE	CVSS	Severity
wiretap.fail	No CVE (Intel and AMD announcements)	-	None
TEE.fail	No CVE	-	None
TDXdown	Intel	2.5	Low
Staleus	CVE-2025-54509	4.0	Medium
BreakFAST	CVE-2025-61972	4.2	Medium
BadRAM	AMD	5.3	Medium
BreakFAST	CVE-2025-61971	5.9	Medium
Fabricked	CVE-2025-54510	5.9	Medium
Intra-handshake.fail	[CVE-2026-33697]	7.5	High

[3] https://nvd.nist.gov/vuln-metrics/cvss

Team Credits

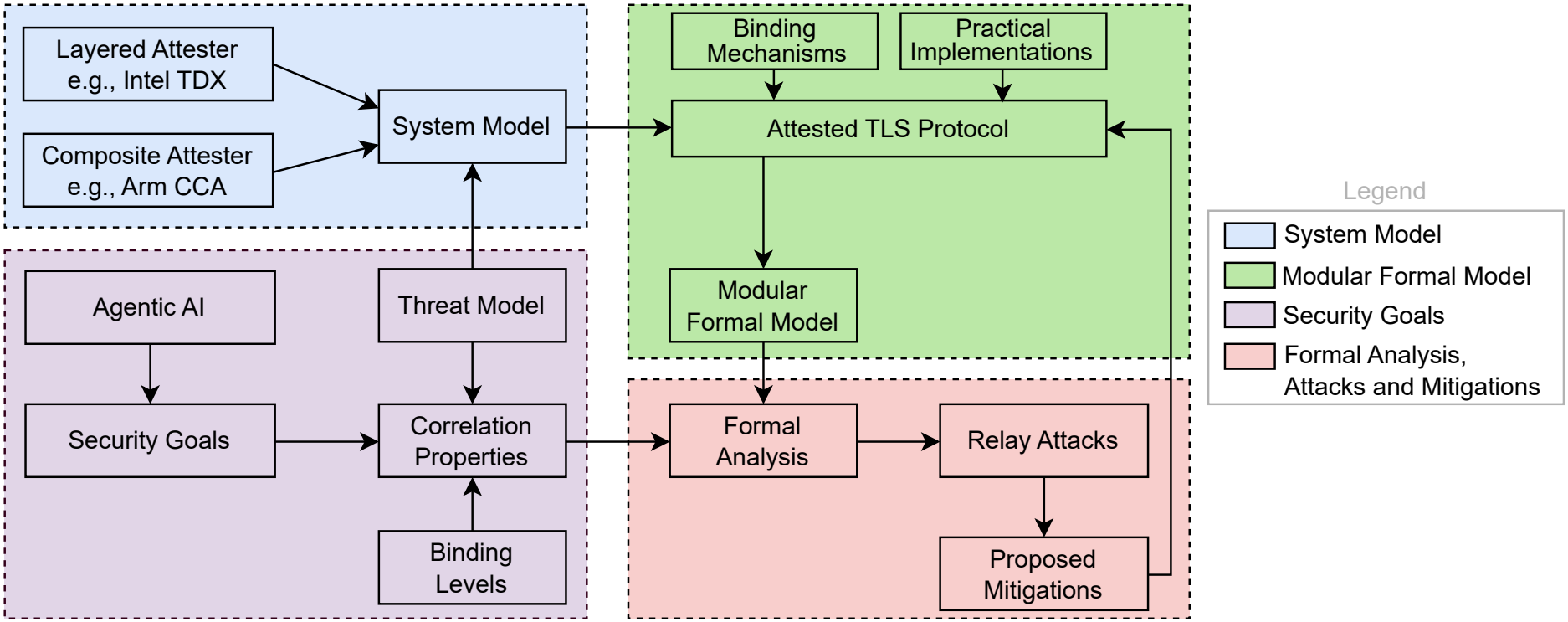
GHSA/CVE	Finders
[CVE-2026-33697]	Muhammad Usama Sardar, Viacheslav Dubeyko, and Jean-Marie Jacquet
[EUVD-2026-16488]	Muhammad Usama Sardar, Viacheslav Dubeyko, and Jean-Marie Jacquet
[GHSA-Cocos-AI]	Muhammad Usama Sardar, Viacheslav Dubeyko, and Jean-Marie Jacquet
[GHSA-Edgeless-Systems]	Muhammad Usama Sardar
[GHSA-Cocos-AI2]	Muhammad Usama Sardar and Songbo Bu
[GHSA-Cocos-AI3]	Muhammad Usama Sardar and Songbo Bu
TBA	Songbo Bu and Muhammad Usama Sardar

Currently in Process

CVSS	Severity	Number of CVEs
9.8	Critical	1
9.1	Critical	3 (confirmed by developers)
8.7	High	1
7.5	High	2
7.4	High	2
6.3	Medium	2

Approach

- TLS 1.3 as the transport protocol
- AI agents as motivational use case
- Formalization tool: ProVerif



Potential Binding Mechanisms (TLS Server as Attester)

S. No.	Binding material	Value of rdata field
1	Client's TLS nonce	nc
2	Client's attestation nonce	na
3	Early exporter	exp_0
4	Server's public key	pubEK
5	Client's attestation nonce and early exporter	na $\|\|$ exp_0
6	Client's attestation nonce and server's public key	na $\|\|$ pubEK
7	Nonce, early exporter, and server's public key	na $\|\|$ exp_0 $\|\|$ pubEK

- Industry implementations: all are vulnerable
  - #1: Meta's AI[4]
  - #6: Edgeless Systems Contrast[5], Cocos AI[6] and CCC PoC[7]
  - #7: draft-fossati-tls-attestation-06

[4] https://ai.meta.com/static-resource/private-processing-technical-whitepaper

[5] https://github.com/CCC-Attestation/meetings/blob/main/materials/MarkusRudy.contrast-atls-ccc-attestation.pdf

[6] https://github.com/ultravioletrs/cocos

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

Binding Levels

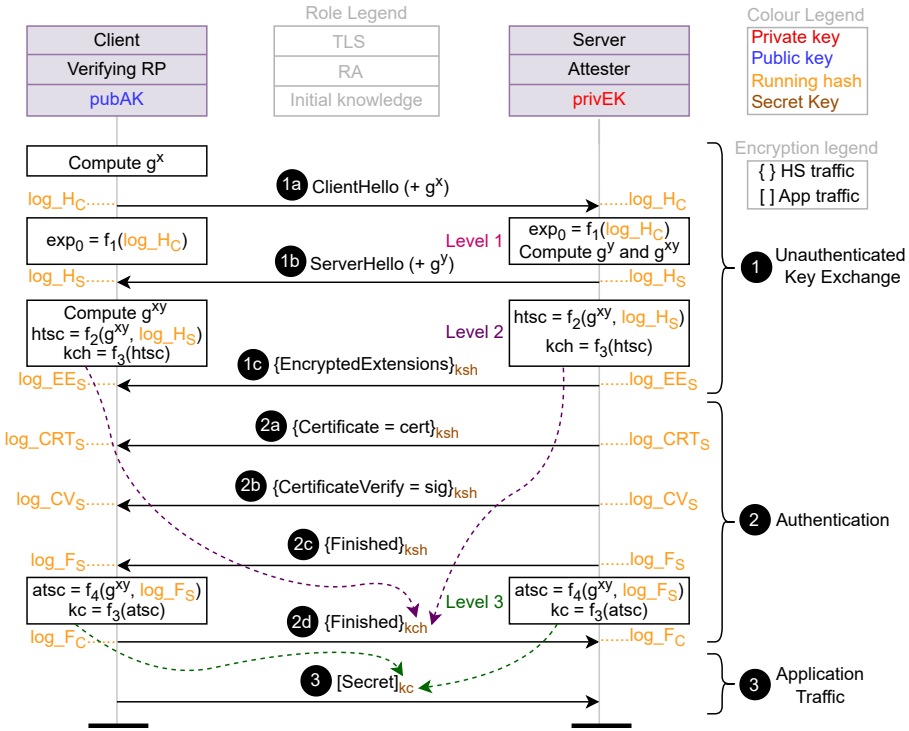
$$\forall\ ev, x, y.\ action(ClientX(ev, x)) \wedge action(ServerX(ev, y)) \rightarrow x = y \tag{1}$$

Level	Secret	Handshake state
1	DH shared secret (g^{xy})	g^x from ClientHello and g^y from Server
2	Client's handshake traffic key (*htsc*)	complete ClientHello and ServerHello
3	Client's application traffic key (*atsc*)	ClientHello up to ServerFinished

$$G_3 \Rightarrow G_2 \Rightarrow G_1 \tag{2}$$

Binding to Client Handshake Traffic Secret is Not Sufficient

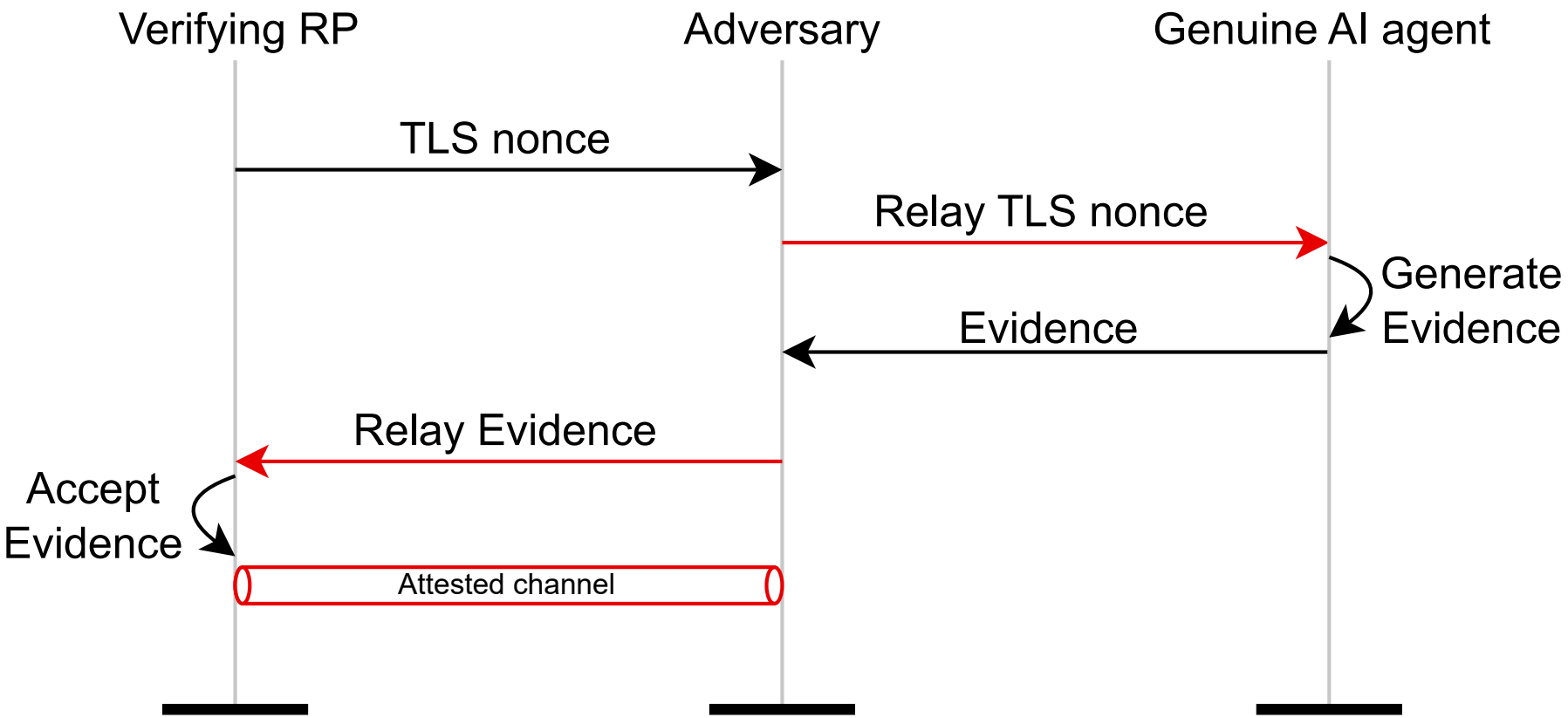
Devil is in the Details!



- `htsc`: used for encryption of clientFinished message (2d).
  - Irrelevant for security goals
  - Server not yet authenticated at this point
- `atsc`: used for encryption of application data (client's secret, e.g., decryption key)
  - Relevant for security goals

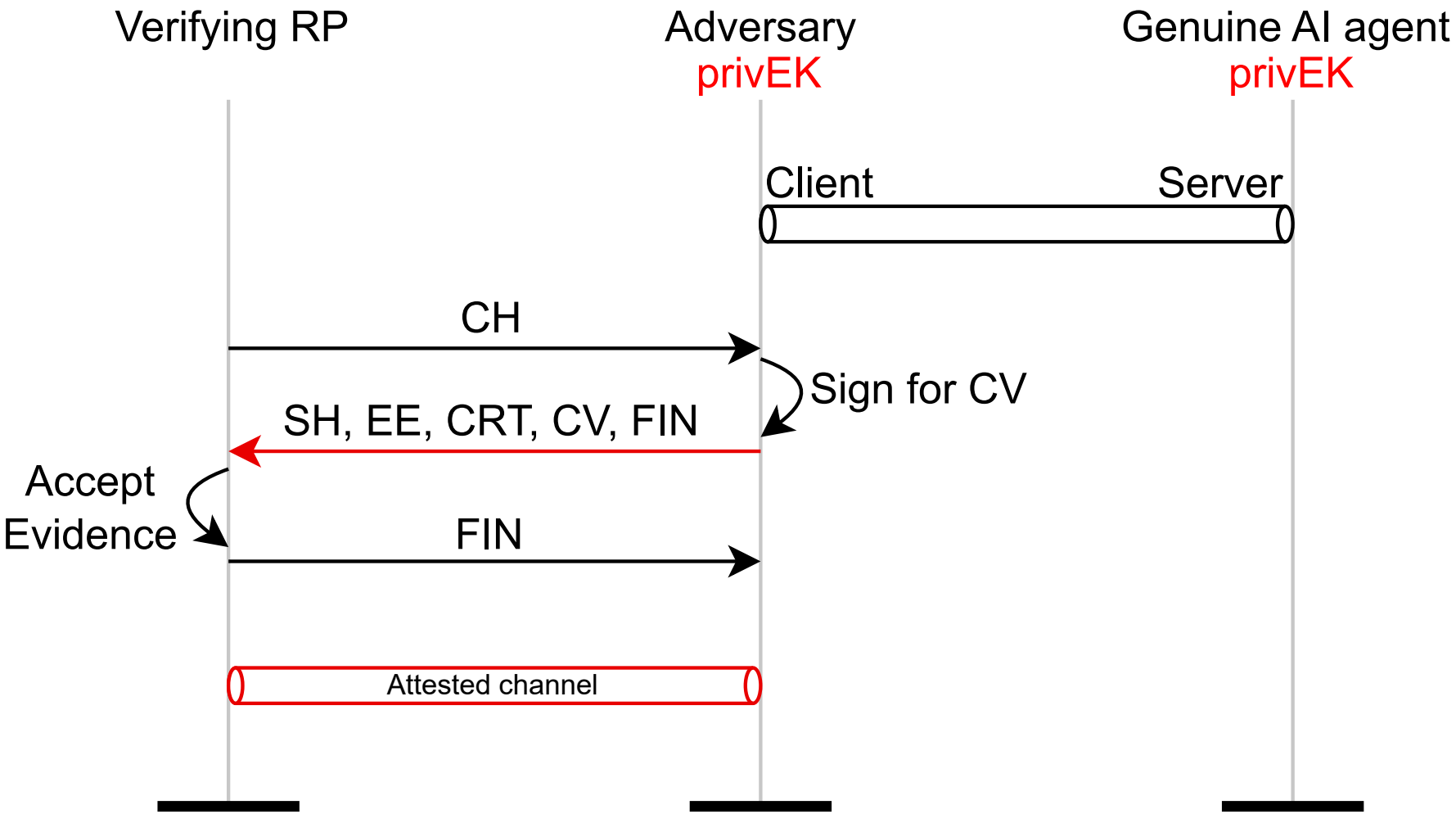
Relay Attack 1 (Abstracted): Mechanism # 1 (nc)

- Adversary can relay nonce to a genuine Attester



Relay Attack 2 (Abstracted): Mechanism # 4 (pubEK)

- No protection if privEK is accessible to some entity other than an AI agent (e.g., provisioning at runtime) or leaked via vulnerability in code
- Adversary gets signed Evidence from genuine AI agent (server)



High-severity CVE Published

CWE 2 Total

Learn more

- CWE-322: CWE-322: Key Exchange without Entity Authentication
- CWE-346: CWE-346: Origin Validation Error

CVSS 1 Total

Learn more

Score	Severity	Version	Vector String
7.5	HIGH	3.1	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N

- Drafts vulnerable to CVE-2026-33697
  - draft-fossati-tls-attestation[8] (draft withdrawn after CVE)
  - draft-fossati-seat-early-attestation[9] (extension of withdrawn draft)
  - draft-ritz-seat-facts[10]
- Similar issues in draft-ietf-lake-ra
  - Awaiting implementation from authors to report CVEs :)

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

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

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

Implementations Vulnerable to CVE-2026-33697

- Meta's AI: [CVE-2026-33697] and [EUVD-2026-16488] [**Severity = HIGH (CVSS 7.5)**]
- Cocos AI: [GHSA-Cocos-AI] [**Severity = HIGH (CVSS 7.8)**], [CVE-2026-33697] and [EUVD-2026-16488] [**Severity = HIGH (CVSS 7.5)**]
- Edgeless Systems Contrast: [GHSA-Edgeless-Systems] [**Severity = HIGH (CVSS 7.4)**]
- CCC Attestation SIG's adopted project intra-handshake attestation: declared vulnerable to relay attacks and **archived**
- Privasys rustls: Acknowledgment of applicability of [CVE-2026-33697] [**Severity = HIGH (CVSS 7.5)**]
- Pirvasys go: Acknowledgment of applicability of [CVE-2026-33697] [**Severity = HIGH (CVSS 7.5)**]

Core Problem

Binding Evidence to
unauthenticated peer (Server)

Other Problems of Intra-handshake Attestation

- Hardware-level Information of Server
- Only Boot-time Claims
- Re-attestation (Continuous Attestation)
- High Handshake Latency and Timeouts
- Unnecessary complexity within the handshake

Summary of Security Analysis So Far

- Pre-handshake attestation: replay and diversion attacks
- Intra-handshake attestation: diversion, replay, and relay attacks
  - draft-fossati-tls-attestation[11]
  - draft-fossati-seat-early-attestation[12]
  - draft-ritz-seat-facts[13]
  - draft-ietf-lake-ra[14]
- Post-handshake attestation
  - draft-fossati-seat-expat[15]

- Intra-handshake attestation can achieve at most level 2 binding

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

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

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

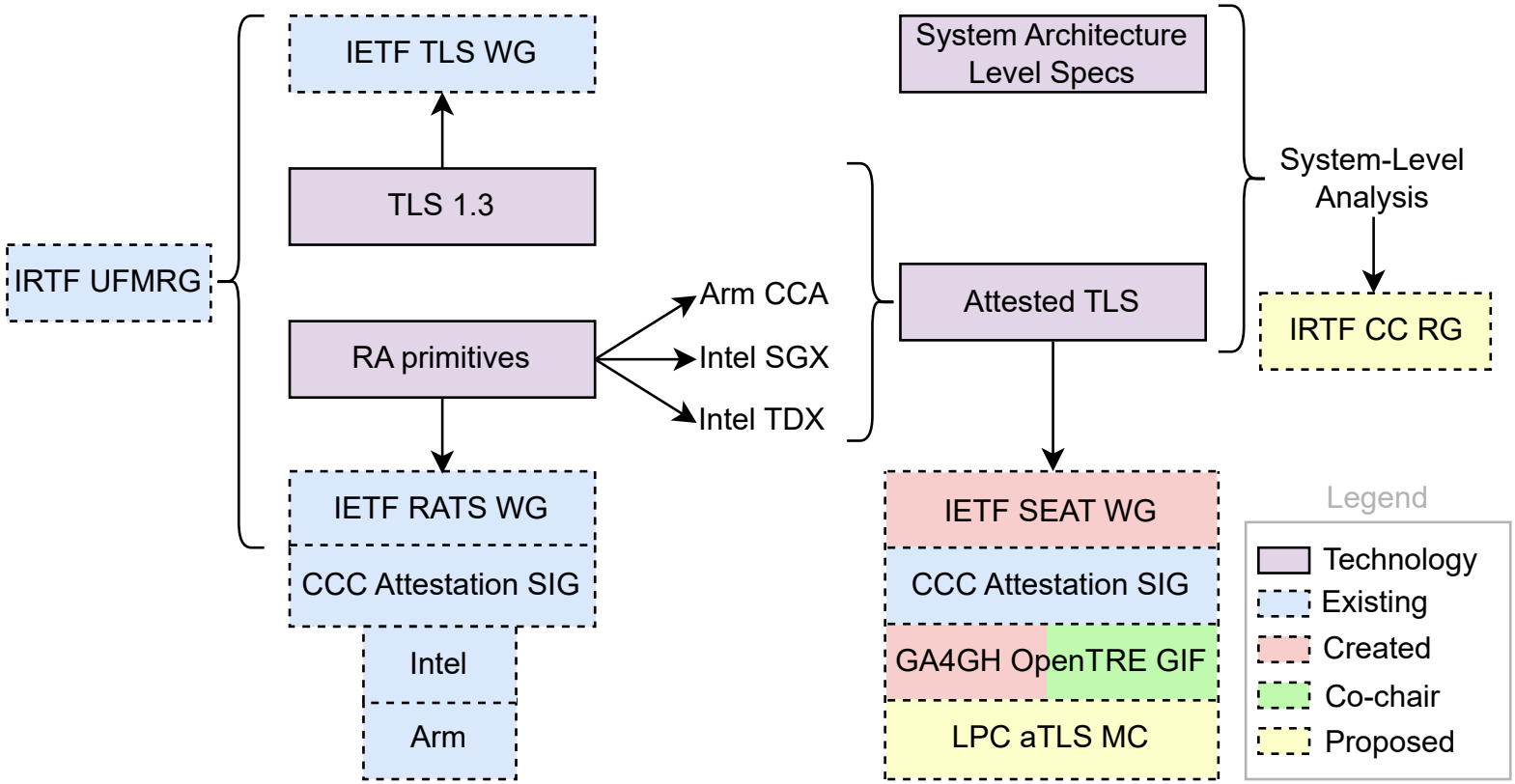
[14] https://datatracker.ietf.org/doc/draft-ietf-lake-ra/

[15] https://datatracker.ietf.org/doc/draft-fossati-seat-expat/

Ask for RIoT Community

Too many vulnerabilities for our small team; we need your help!

Big Picture and Next Steps



- IETF: Internet Engineering Task Force
- IRTF: Internet Research Task Force
- CCC: Confidential Computing Consortium
- GA4GH: Global Alliance for Genomics and Health
- RATS: Remote ATtestation ProcedureS
- TLS: Transport Layer Security
- SEAT: Secure Evidence and Attestation Transport

- UFMRG: Usable Formal Methods Research Group
- CC: Confidential Computing
- WG: Working Group
- RG: Research Group
- aTLS: Attested TLS
- SIG: Special Interest Group
- OpenTRE: Trusted Research Environment Open Suite

Links to Resources

- Paper
  - https://www.researchgate.net/publication/408219182_Intra-handshakefail_CVE-2026-33697_High-severity_CVE_in_Attested_TLS
- ProVerif artifacts
  - https://www.github.com/muhammad-usama-sardar/intra-handshake.fail
- Internet-Draft
  - https://datatracker.ietf.org/doc/draft-intra-handshake-fail/

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)
- Venkat Malladi (Quest Diagnostics)
- Alistair Woodman
- and many others...