Attested TLS

Muhammad Usama Sardar[1], Thomas Fossati[2], Hannes Tschofenig[3], and Simon Frost[4]

[1]TU Dresden, Germany

[2]Linaro, Lausanne, Switzerland

[3]University of Applied Sciences Bonn-Rhein-Sieg and Siemens, Germany

[4]Arm, Cambridge, UK

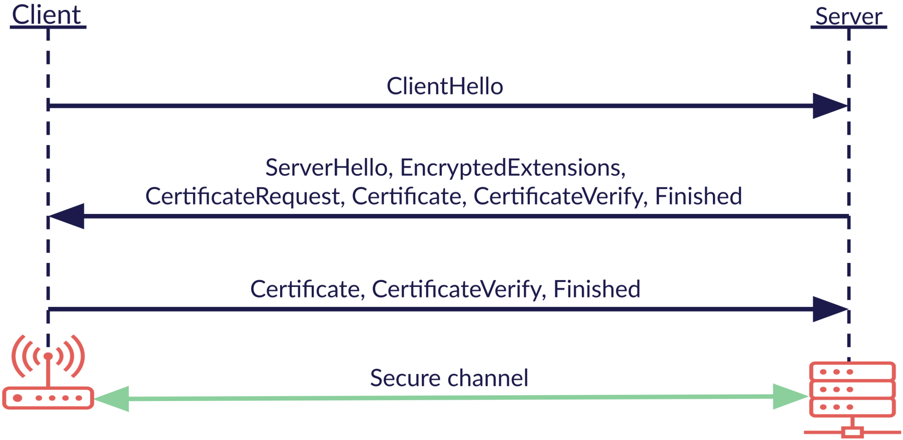
September 20, 2024

Outline

1. Background and Problem Statement

2. Attested TLS (RA+TLS)

TLS Handshake Protocol with Client Authentication


Client
Server
ClientHello
ServerHello, EncryptedExtensions,
CertificateRequest, Certificate, CertificateVerify, Finished
Certificate, CertificateVerify, Finished
Secure channel

Problem Statement

- Good for network security

Problem Statement

- Good for network security
- Not good for endpoint security

Problem Statement

- Good for network security
- Not good for endpoint security
  - Keys

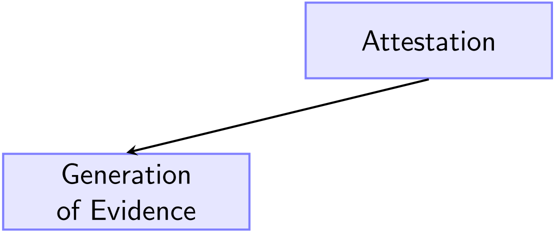
Problem Statement

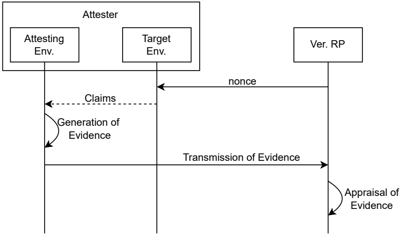
- Good for network security
- Not good for endpoint security
  - Keys
  - Workload

Problem Statement

- Good for network security
- Not good for endpoint security
  - Keys
  - Workload
  - Platform (= HW + Bootloader + FW)

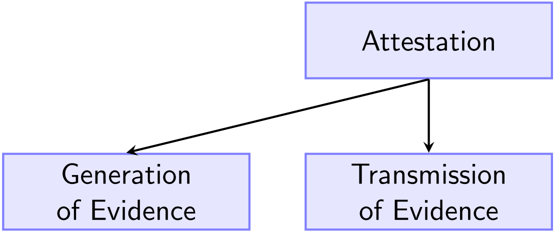
Remote Attestation





Generation of Evidence = Sampling of claims + Collection of claims + (Typically) signing of claims

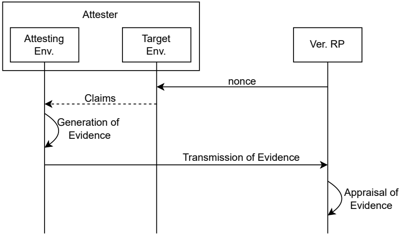
Remote Attestation



Attestation

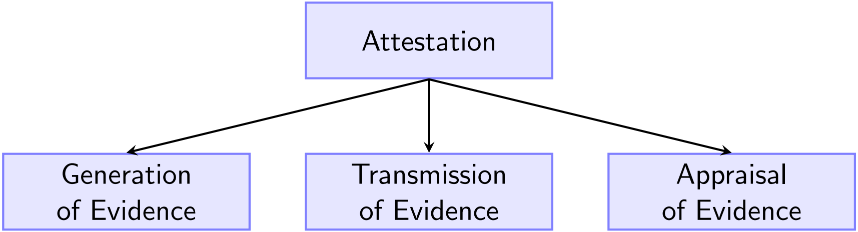
Generation of Evidence

Transmission of Evidence



Generation of Evidence = Sampling of claims + Collection of claims + (Typically) signing of claims

Remote Attestation

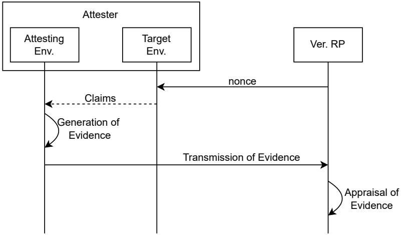


Attestation

Generation of Evidence

Transmission of Evidence

Appraisal of Evidence



Generation of Evidence = Sampling of claims + Collection of claims + (Typically) signing of claims

Problem Statement

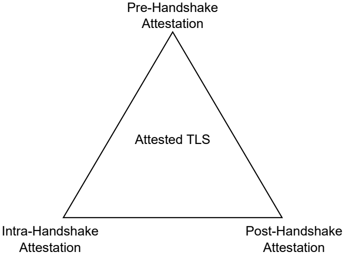
How to combine the two protocols securely in CC context?

Outline

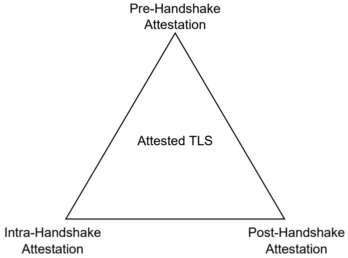
1 Background and Problem Statement

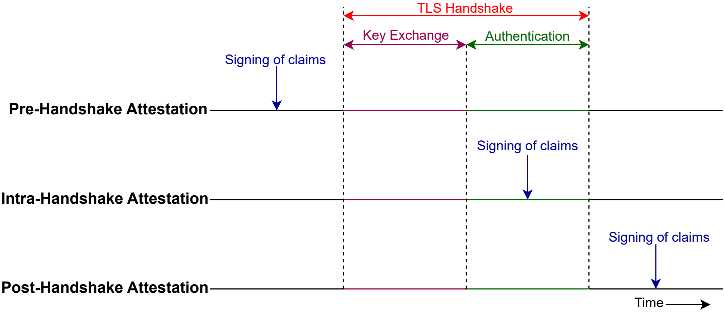
2 Attested TLS (RA+TLS)

Design Options

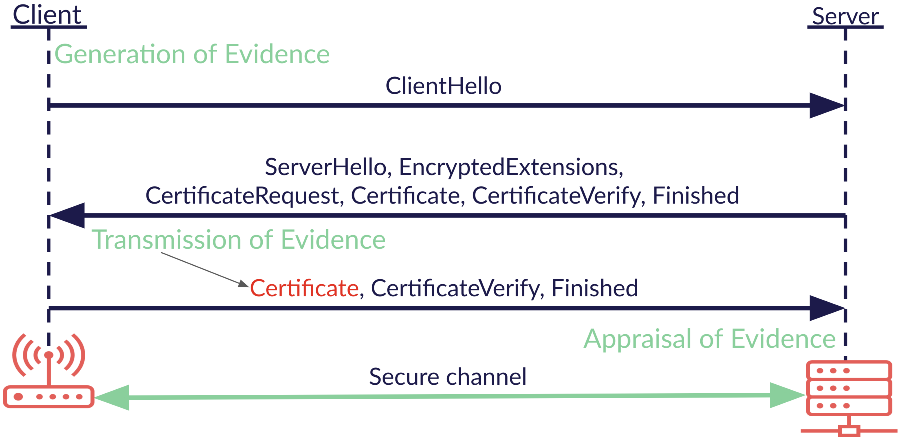


Design Options

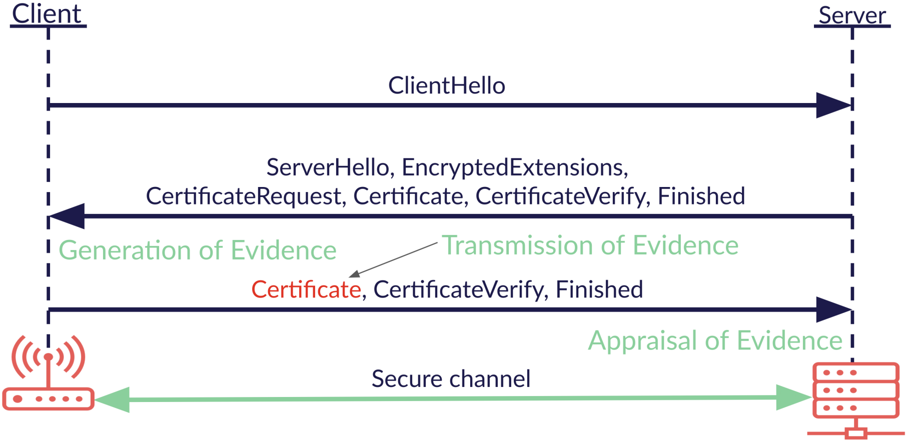

Pre-Handshake Attestation
Attested TLS
Intra-Handshake Attestation
Post-Handshake Attestation



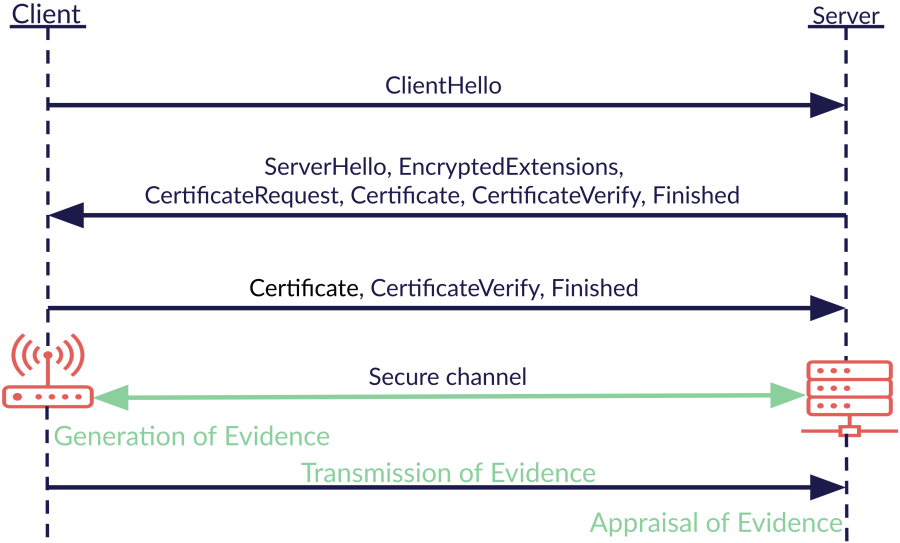
1 Pre-HS Attestation (Client as Attester)


Client
Server
Generation of Evidence
ClientHello
ServerHello, EncryptedExtensions,
CertificateRequest, Certificate, CertificateVerify, Finished
Transmission of Evidence
Certificate, CertificateVerify, Finished
Appraisal of Evidence
Secure channel

2 Intra-HS Attestation (Client as Attester)


Client
Server
ClientHello
ServerHello, EncryptedExtensions,
CertificateRequest, Certificate, CertificateVerify, Finished
Generation of Evidence
Transmission of Evidence
Certificate, CertificateVerify, Finished
Appraisal of Evidence
Secure channel

3 Post-HS Attestation (Client as Attester)



Client

Server

ClientHello

ServerHello, EncryptedExtensions, CertificateRequest, Certificate, CertificateVerify, Finished

Certificate, CertificateVerify, Finished

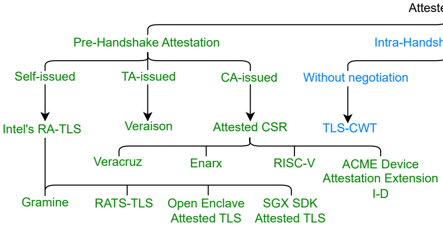
Secure channel

Generation of Evidence

Transmission of Evidence

Appraisal of Evidence

Design Options for Attested TLS



- Attested TLS
  - Pre-Handshake Attestation
    - Self-issued
      - Intel's RA-TLS
        - Gramine
        - RATS-TLS
        - Open Enclave Attested TLS
        - SGX SDK Attested TLS
    - TA-issued
      - Veraison
    - CA-issued
      - Attested CSR
        - Veracruz
        - Enarx
        - RISC-V
        - ACME Device Attestation Extension I-D
  - Intra-Handshake Attestation
    - Without negotiation
      - TLS-CWT
    - With negotiation
      - TLS attest
  - Post-Handshake Attestation
    - TLS Exporters
      - SCONE
    - Exported authenticators
    - Post-handshake exchange

- Discussion: any other fundamental design option?

Specifications in Key Exchange Part

	RA-TLS[1]	TLS attest[2]	SCONE[3]
(a) Extensions	×	✓	×
(b) Attestation nonce	×	✓	×

- Discussion: any other fundamental design option?

[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)*, 2024.

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

Specifications in Authentication Part

	RA-TLS[4]	TLS attest[5]	SCONE[6]
(a) Lifetime of key	Short-term	Short-/Long-term	Short-term
(b)i. Info in Certificate	Evidence	Evidence	Public key
(b)ii. Signer	Self-signed	Self-/CA-signed	Self-signed
(b)iii. Format	X.509	Negotiated	X.509
(c) Extensions	×	✓	×
(d) Exporters	×	✓	✓

- Discussion: any other fundamental design option?

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

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

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

(Typical) Comparison/Tradeoffs

Attestation	Modification	Replay protection	Impact on connection establishment latency	Effective connection establishment latency
Pre-handshake	TA/CA	×	Medium ($t_{hs} + t_a$)	Low
Intra-handshake	TLS	✓	High ($t_{hs} + t_g + t_a$)	Low
Post-handshake	Application	Possible	Low (t_{hs})	High ($\geqslant$0.5RTT)

- Discussion: any other property?