Formal Analysis of Attested TLS for Confidential Computing

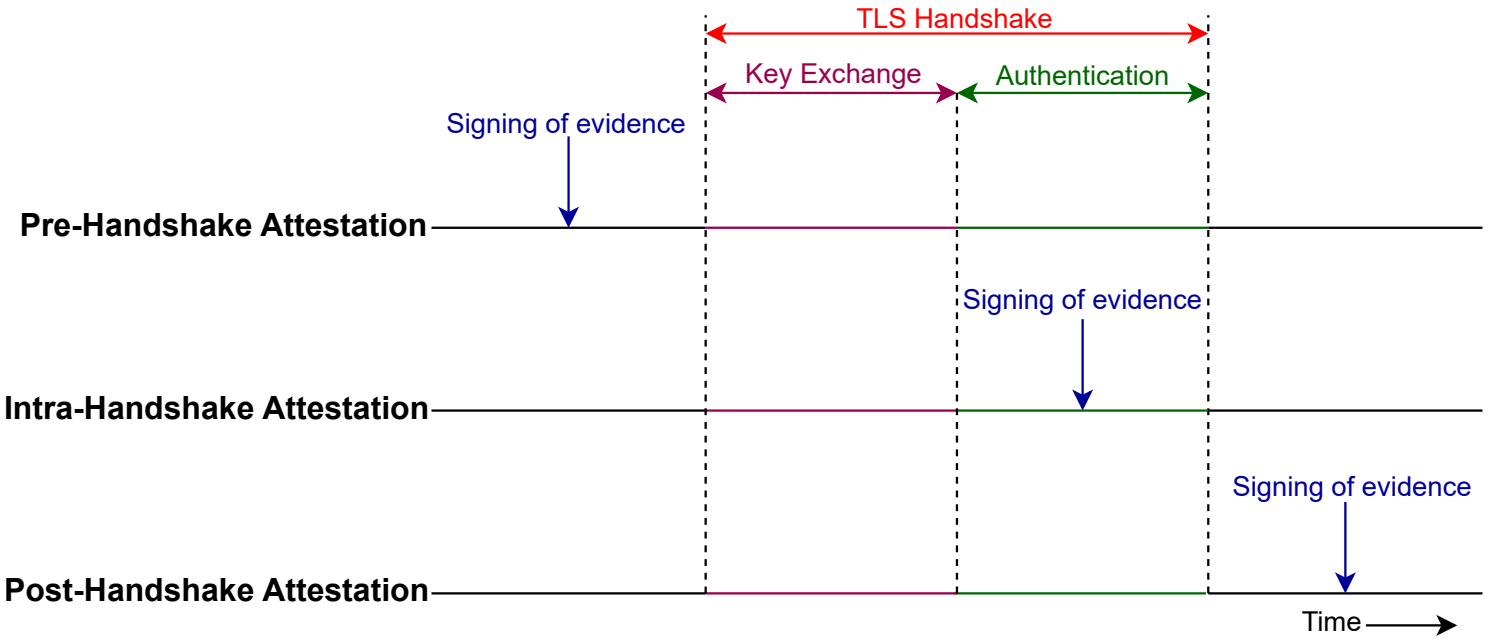
Muhammad Usama Sardar

TU Dresden, Germany

July 21, 2024

Thanks to my sponsor

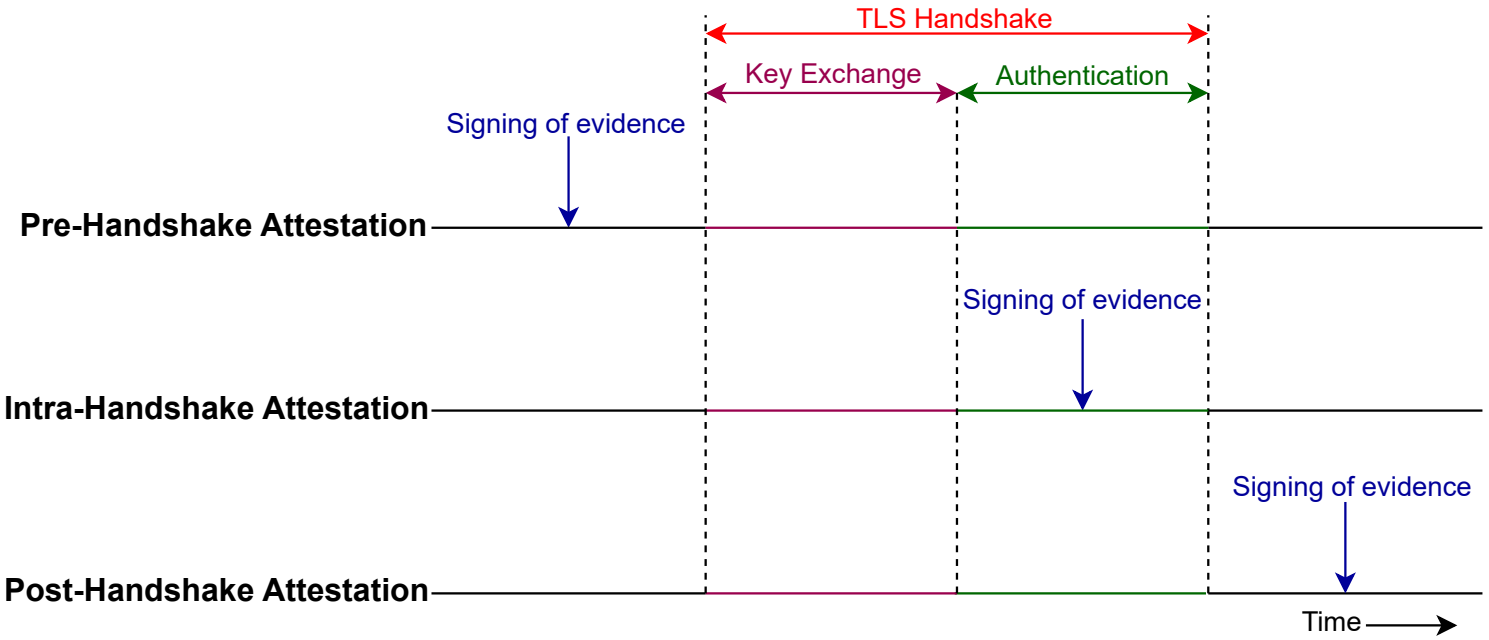
Hackathon Plan



- Involved I-D[1]

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

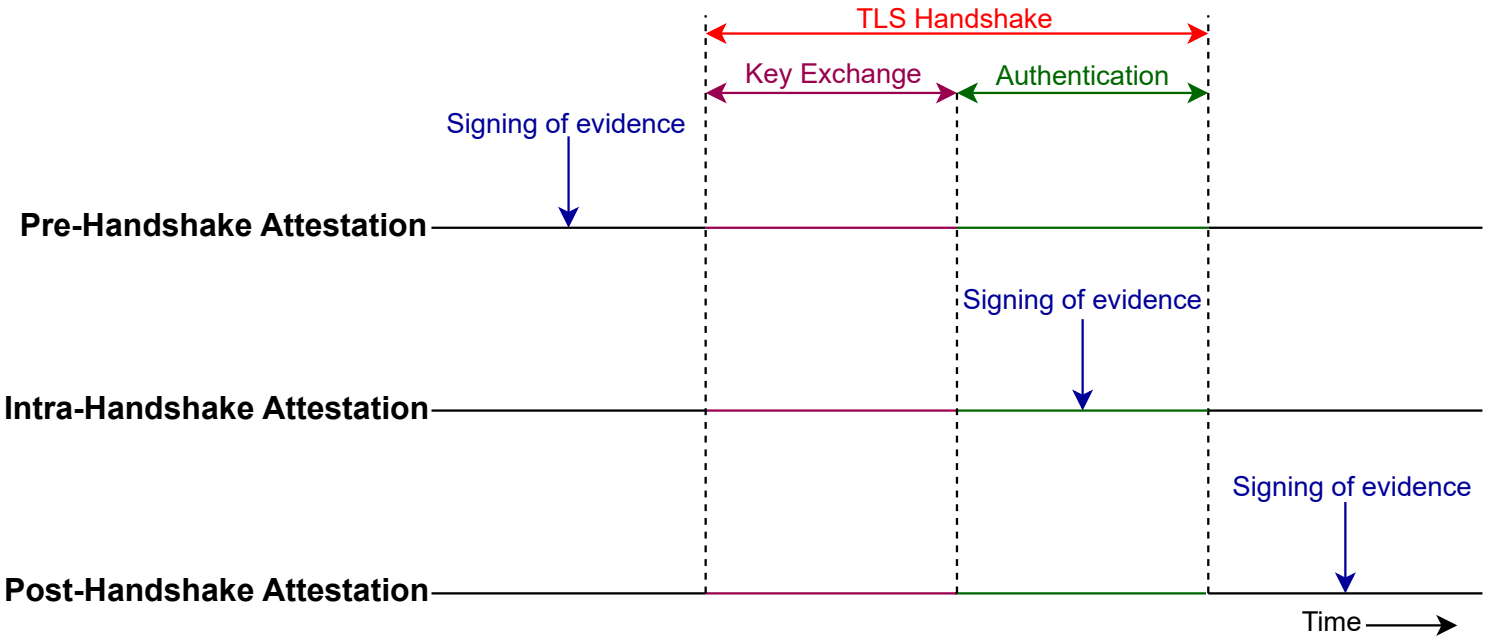
Hackathon Plan



- Involved I-D[1]
- What aspects should be specified for confidential computing?

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

Hackathon Plan



- Involved I-D[1]
- What aspects should be specified for confidential computing?
- How should they be verified?

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

What got done

- Insightful discussions with
  - Monty Wiseman
  - Chunchi Liu
  - Stephen Farrell
  - Sean Turner

What we learned

- Overall direction is correct!

What we learned

- Overall direction is correct!
- New insight: "Attestation" should be precisely specified as "Attestation of what exactly"

Wrap Up

- Side meeting: Tutorial: Attested TLS on Tuesday @ 9:30 - 11:30 in Prince of Wales/Oxford[2]
  - Relevant for RATS, TLS, WIMSE, LAKE, UFMRG and other W/RGs
- Links
  - Design options
    - Pre-HS attestation
    - Intra-HS attestation
    - Post-HS attestation
  - Background on attestation
    - Formal Specs
    - Formal analysis artifacts repo
  - CCC Attestation SIG

[2] https://wiki.ietf.org/en/meeting/120/sidemeetings

Key References

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 draft-fossati-tls-attestation-07. Work in Progress. Internet Engineering Task Force, July 2024. 34 pp. URL: https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/07/.