Formal Analysis of Attested TLS for Confidential Computing

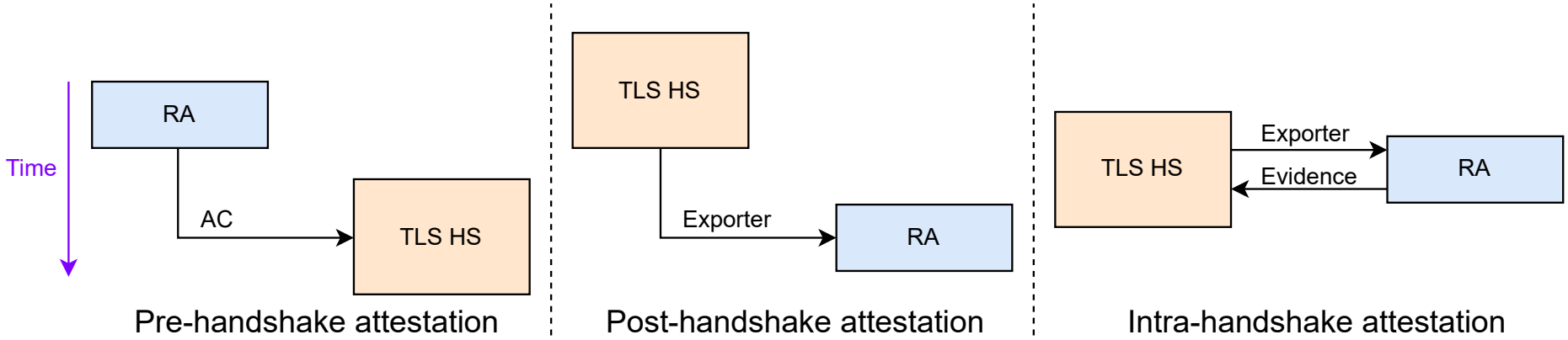
Muhammad Usama Sardar

TU Dresden, Germany

November 3, 2024

Thanks to my sponsor

Hackathon Plan



- Involved I-Ds[1,2]
- 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

[2] Ounsworth, Tschofenig, Birkholz, Wiseman, and Smith, *Use of Remote Attestation with Certification Signing Requests*, 2024

Thank you for discussions

- Cedric Fournet
- Thomas Fossati
- Ionut Mihalcea
- Hannes Tschofenig
- Monty Wiseman
- Göran Selander
- Michael Richardson
- Ned Smith
- Yogesh Deshpande
- Ayoub Messous
- Gergely Buday

What we learned

- Better understanding of channel bindings
- Tradeoffs: Attested CSR[3] vs. TLS attest[4]
- Optimization: can CertificateVerify be removed for intra-HS?
- New properties:
  - If connection is established, client and server agree on attestation (evidence).
  - If RA verification succeeds, client and server agree on all connection parameters (TLS transcript).

[3] Ounsworth, Tschofenig, Birkholz, Wiseman, and Smith, *Use of Remote Attestation with Certification Signing Requests*, 2024

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

Wrap Up

- Side meetings relevant for RATS, TLS, WIMSE, LAKE, UFMRG and other W/RGs
  - Basic attested TLS tutorial: Tuesday 9:30-11:30, Wicklow Hall 2A
  - Advanced attested TLS tutorial: Wednesday 9:30-11:30, Wicklow Hall 2A
- Pointers
  - Design options
    - Pre-HS attestation
    - Intra-HS attestation
    - Post-HS attestation
  - Background on attestation
    - Formal Specs
    - Formal analysis artifacts repo
  - CCC Attestation SIG