Formal Analysis of Attested TLS for Confidential Computing

Muhammad Usama Sardar

TU Dresden, Germany

July 21, 2024

Thanks to my sponsor
• Involved I-D\textsuperscript{1}

\textsuperscript{1}Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, \textit{Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)}, 2024
**Involved I-D**

**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
- What aspects should be **specified** for confidential computing?
- How should they be **verified**?

---

What got done

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

- Overall direction is correct!

New insight: "Attestation" should be precisely specified as "Attestation of what exactly".
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

  • 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

---

https://wiki.ietf.org/en/meeting/120/sidemeetings

Muhammad Usama Sardar (TUD)
Key References