

Towards Formal Verification of Attested TLS: Potential Replay Attacks on RA-TLS

Muhammad Usama Sardar¹, Arto Niemi², Hannes Tschofenig³,
Thomas Fossati⁴

¹TU Dresden, Germany

²Huawei Technologies, Helsinki, Finland

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

⁴Linaro, Lausanne, Switzerland

April 5, 2024



Agenda

- 1 TLS
- 2 Attestation (RA)
- 3 Attested TLS (RA+TLS)
- 4 Goal and Contributions
- 5 Approach and Tool
- 6 Validation of TLS 1.3
- 7 Formal Analysis of Attested TLS
- 8 Summary

Data-in-transit: Transport Protocols

- TLS¹: world's most-used cryptographic protocol

¹<https://datatracker.ietf.org/doc/html/rfc8446>

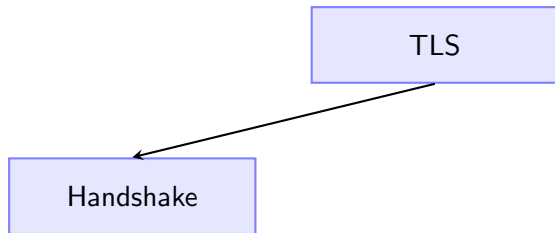
Data-in-transit: Transport Protocols

- TLS¹: world's most-used cryptographic protocol
- Conceptually 2 main subprotocols:

¹<https://datatracker.ietf.org/doc/html/rfc8446>

Data-in-transit: Transport Protocols

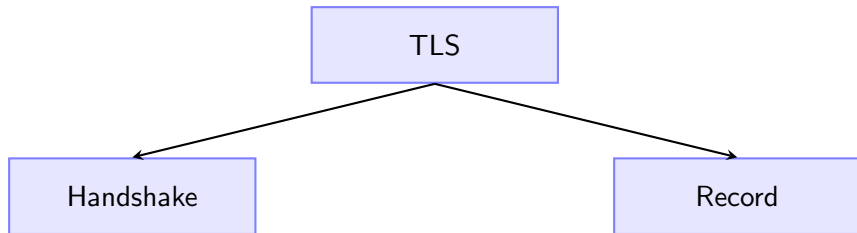
- TLS¹: world's most-used cryptographic protocol
- Conceptually 2 main subprotocols:



¹<https://datatracker.ietf.org/doc/html/rfc8446>

Data-in-transit: Transport Protocols

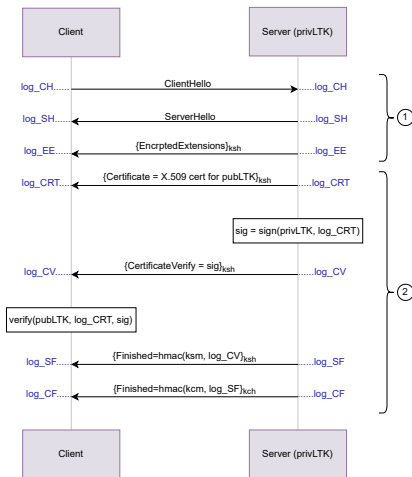
- TLS¹: world's most-used cryptographic protocol
- Conceptually 2 main subprotocols:



¹<https://datatracker.ietf.org/doc/html/rfc8446>

TLS Handshake Protocol

- Most complex part of TLS
 1. Unauthenticated **key exchange** (and parameter negotiation)
 2. **Authentication** (inc. key confirmation)



Problem in TLS

- No validation of security state of endpoint software and platform

Problem in TLS

- No validation of security state of endpoint software and platform
 - Need a **more comprehensive** set of security metrics in some use cases, e.g., CC

Problem in TLS

- No validation of security state of endpoint software and platform
 - Need a **more comprehensive** set of security metrics in some use cases, e.g., CC
- Very complex: at least 15 different exploits

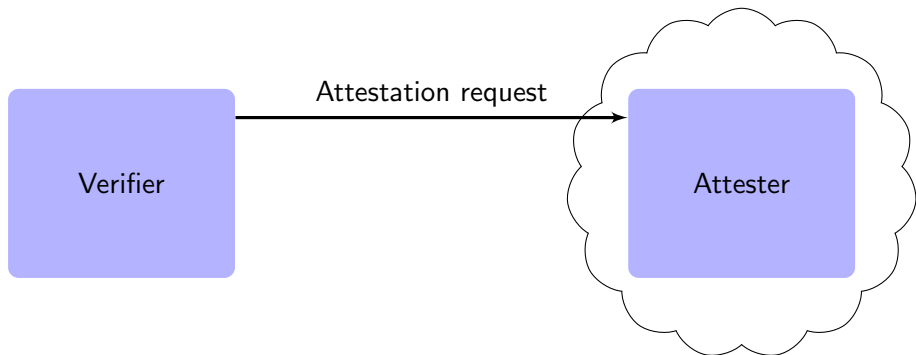
Problem in TLS

- No validation of security state of endpoint software and platform
 - Need a **more comprehensive** set of security metrics in some use cases, e.g., CC
- Very complex: at least 15 different exploits
 - Is all complexity (e.g., of key schedule) **justified**?

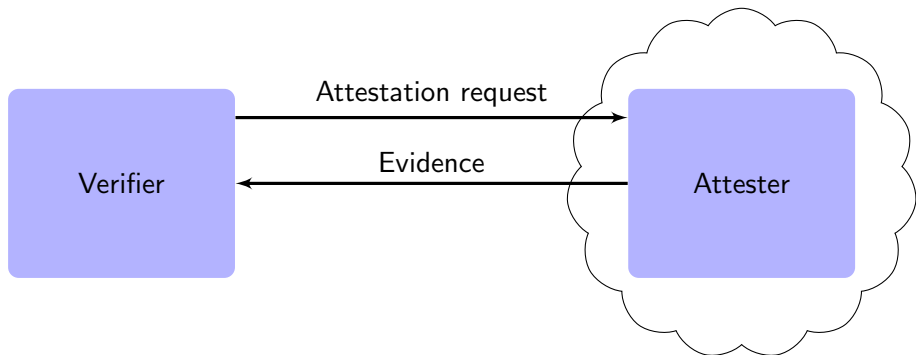
Outline

- 1 TLS
- 2 Attestation (RA)
- 3 Attested TLS (RA+TLS)
- 4 Goal and Contributions
- 5 Approach and Tool
- 6 Validation of TLS 1.3
 - Key Schedule
 - Validation of Key Schedule
- 7 Formal Analysis of Attested TLS
 - Flow
 - Property
- 8 Summary

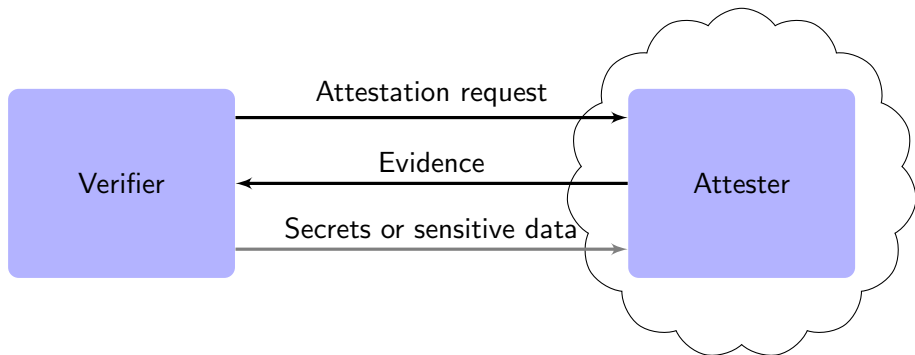
Architecturally-defined Attestation (GT MFS'23)



Architecturally-defined Attestation (GT MFS'23)



Architecturally-defined Attestation (GT MFS'23)



Data-in-use: Architecturally-defined attestation²

- Intel TDX

	Integrity	Freshness	Confidentiality	Authentication
Intel's claimed TCB	×	×	×	×
Our proposed TCB	✓	✓	✓	×

- Arm CCA

Attester	Integrity	Freshness	Confidentiality	Authentication
Platform	✓	×	✓	×
Realm	✓	✓	✓	×

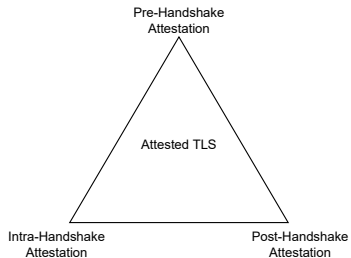
- Problem 1: **No server authentication** (e.g., misconfiguration)
- Problem 2: No standard way of implementation

²Sardar, Fossati, Frost, and Xiong, *Formal Specification and Verification of Architecturally-defined Attestation Mechanisms in Arm CCA and Intel TDX*, 2023.

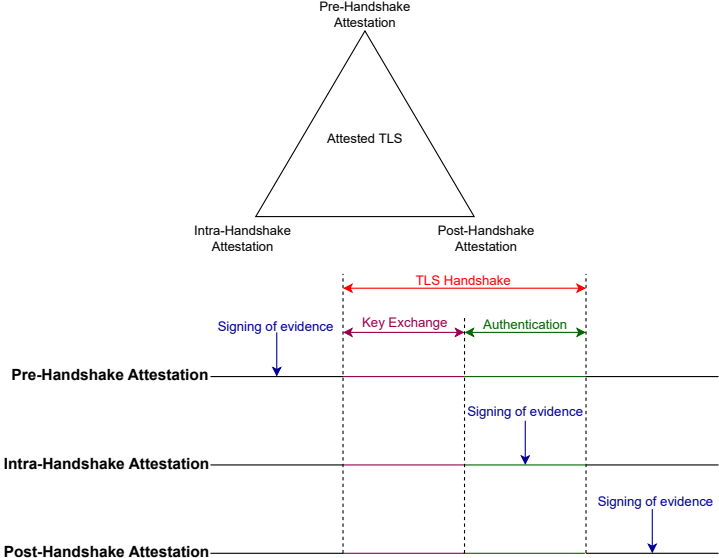
Outline

- 1 TLS
- 2 Attestation (RA)
- 3 Attested TLS (RA+TLS)**
- 4 Goal and Contributions
- 5 Approach and Tool
- 6 Validation of TLS 1.3
 - Key Schedule
 - Validation of Key Schedule
- 7 Formal Analysis of Attested TLS
 - Flow
 - Property
- 8 Summary

Data-in-transit + Data-in-use



Data-in-transit + Data-in-use



Intel's RA-TLS³

- Widely used protocol, e.g., in Gramine, RATS-TLS, Open Enclave Attested TLS, and SGX SDK Attested TLS

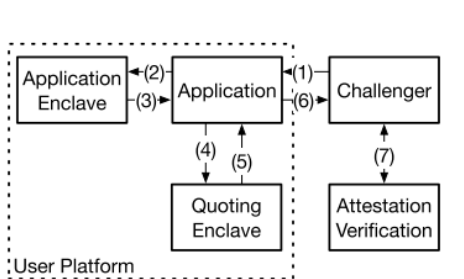


Figure 1: Remote Attestation Example. The challenger is off-platform with respect to the attester.

³Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

Intel's RA-TLS³

- Widely used protocol, e.g., in Gramine, RATS-TLS, Open Enclave Attested TLS, and SGX SDK Attested TLS

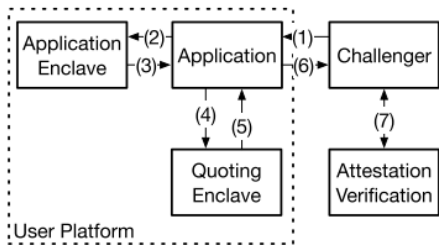


Figure 1: Remote Attestation Example. The challenger is off-platform with respect to the attester.



Figure 2: TLS 1.2 Handshake Messages.

³Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

Outline

- 1 TLS
- 2 Attestation (RA)
- 3 Attested TLS (RA+TLS)
- 4 Goal and Contributions**
- 5 Approach and Tool
- 6 Validation of TLS 1.3
 - Key Schedule
 - Validation of Key Schedule
- 7 Formal Analysis of Attested TLS
 - Flow
 - Property
- 8 Summary

Goal

- Formally analyze the security of Intel's RA-TLS

Contributions

- First formal analysis of attested TLS for TEEs

⁴<https://github.com/Inria-Prosecco/reftls>

Contributions

- First formal analysis of attested TLS for TEEs
- Validation of formal model⁴ of TLS 1.3 Key Schedule, revealing 3 major issues

⁴<https://github.com/Inria-Prosecco/reftls>

Outline

- 1 TLS
- 2 Attestation (RA)
- 3 Attested TLS (RA+TLS)
- 4 Goal and Contributions
- 5 Approach and Tool**
- 6 Validation of TLS 1.3
 - Key Schedule
 - Validation of Key Schedule
- 7 Formal Analysis of Attested TLS
 - Flow
 - Property
- 8 Summary

Analysis Approach and Tool

- Approach: Symbolic⁵

⁵Barbosa, Barthe, Karthik Bhargavan, Blanchet, Cremers, Liao, and Parno, “SoK : Computer-Aided Cryptography”, 2021.

⁶Blanchet, Cheval, and Cortier, “ProVerif with lemmas, induction, fast subsumption, and much more”, 2022.

Analysis Approach and Tool

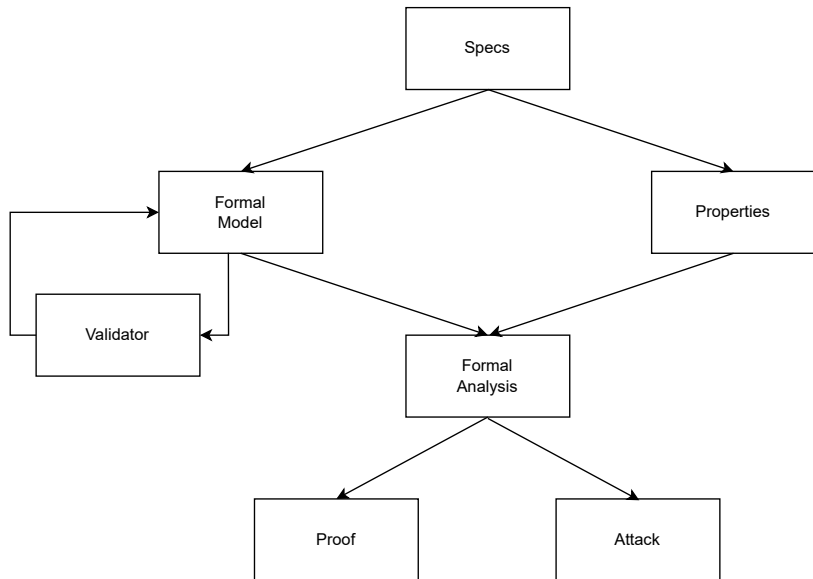
- Approach: Symbolic⁵
- Tool used: [ProVerif](#)⁶



⁵Barbosa, Barthe, Karthik Bhargavan, Blanchet, Cremers, Liao, and Parno, “SoK : Computer-Aided Cryptography”, 2021.

⁶Blanchet, Cheval, and Cortier, “ProVerif with lemmas, induction, fast subsumption, and much more”, 2022.

Approach - Simplified



“Rollercoaster”

- **Incomplete** and **outdated** specs for RA-TLS⁷

⁷Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

⁸<https://github.com/Inria-Prosecco/reftls/tree/master/pv>

⁹<https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrX8/>

“Rollercoaster”

- **Incomplete** and **outdated** specs for RA-TLS⁷
 - Specs based on TLS 1.2 (TLS 1.3 is RFC since Aug 2018)

⁷Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

⁸<https://github.com/Inria-Prosecco/reftls/tree/master/pv>

⁹<https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrX8/>

“Rollercoaster”

- **Incomplete** and **outdated** specs for RA-TLS⁷
 - Specs based on TLS 1.2 (TLS 1.3 is RFC since Aug 2018)
 - Fix: Used **implementation** and **community input** for formal model

⁷Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

⁸<https://github.com/Inria-Prosecco/reftls/tree/master/pv>

⁹<https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrX8/>

“Rollercoaster”

- **Incomplete** and **outdated** specs for RA-TLS⁷
 - Specs based on TLS 1.2 (TLS 1.3 is RFC since Aug 2018)
 - Fix: Used **implementation** and **community input** for formal model
- Very **few comments** in Inria’s TLS formal model⁸

⁷Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

⁸<https://github.com/Inria-Prosecco/reftls/tree/master/pv>

⁹<https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrX8/>

“Rollercoaster”

- **Incomplete** and **outdated** specs for RA-TLS⁷
 - Specs based on TLS 1.2 (TLS 1.3 is RFC since Aug 2018)
 - Fix: Used **implementation** and **community input** for formal model
- Very **few comments** in Inria’s TLS formal model⁸
 - Literally **no comments** at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!

⁷Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

⁸<https://github.com/Inria-Prosecco/reftls/tree/master/pv>

⁹<https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrX8/>

“Rollercoaster”

- **Incomplete** and **outdated** specs for RA-TLS⁷
 - Specs based on TLS 1.2 (TLS 1.3 is RFC since Aug 2018)
 - Fix: Used **implementation** and **community input** for formal model
- Very **few comments** in Inria’s TLS formal model⁸
 - Literally **no comments** at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
- **Incomplete validation** of draft 20 artifacts⁹

⁷Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

⁸<https://github.com/Inria-Prosecco/reftls/tree/master/pv>

⁹<https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrX8/>

“Rollercoaster”

- **Incomplete** and **outdated** specs for RA-TLS⁷
 - Specs based on TLS 1.2 (TLS 1.3 is RFC since Aug 2018)
 - Fix: Used **implementation** and **community input** for formal model
- Very **few comments** in Inria’s TLS formal model⁸
 - Literally **no comments** at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
- **Incomplete validation** of draft 20 artifacts⁹
 - Fix: Designed an **automated validation framework** for key schedule

⁷Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

⁸<https://github.com/Inria-Prosecco/reftls/tree/master/pv>

⁹<https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrX8/>

“Rollercoaster”

- **Incomplete** and **outdated** specs for RA-TLS⁷
 - Specs based on TLS 1.2 (TLS 1.3 is RFC since Aug 2018)
 - Fix: Used **implementation** and **community input** for formal model
- Very **few comments** in Inria’s TLS formal model⁸
 - Literally **no comments** at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
- **Incomplete validation** of draft 20 artifacts⁹
 - Fix: Designed an **automated validation framework** for key schedule
- A **simple extension** made the artifacts running for **1 month** on high-end server (icelake)

⁷Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

⁸<https://github.com/Inria-Prosecco/reftls/tree/master/pv>

⁹<https://mailarchive.ietf.org/arch/msg/tls/~nFk9Eu7n-YFsFfGUe9X4JnrX8/>

“Rollercoaster”

- **Incomplete** and **outdated** specs for RA-TLS⁷
 - Specs based on TLS 1.2 (TLS 1.3 is RFC since Aug 2018)
 - Fix: Used **implementation** and **community input** for formal model
- Very **few comments** in Inria’s TLS formal model⁸
 - Literally **no comments** at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
- **Incomplete validation** of draft 20 artifacts⁹
 - Fix: Designed an **automated validation framework** for key schedule
- A **simple extension** made the artifacts running for **1 month** on high-end server (icelake)
 - Submitted to ProVerif developers for analysis

⁷Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

⁸<https://github.com/Inria-Prosecco/reftls/tree/master/pv>

⁹<https://mailarchive.ietf.org/arch/msg/tls/~nFk9Eu7n-YFsFfGUe9X4JnrX8/>

“Rollercoaster”

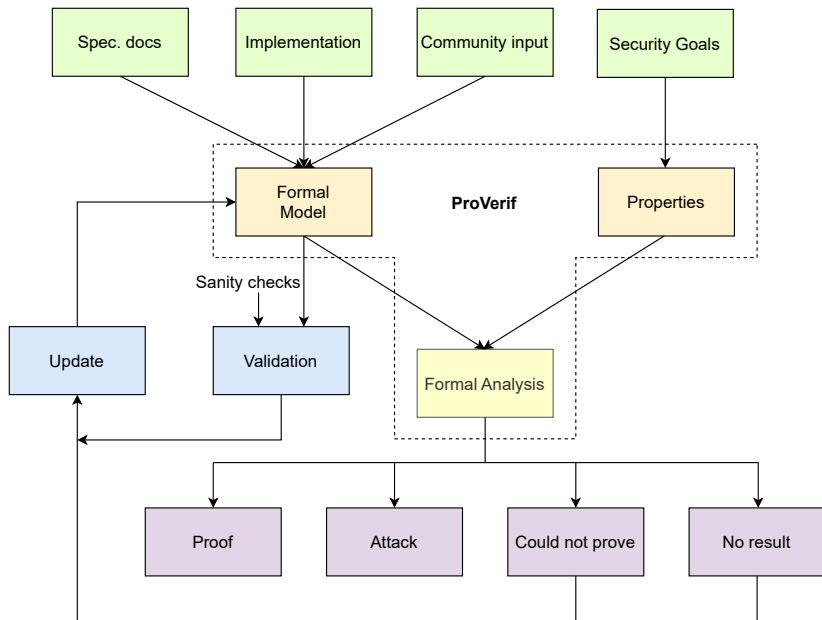
- **Incomplete** and **outdated** specs for RA-TLS⁷
 - Specs based on TLS 1.2 (TLS 1.3 is RFC since Aug 2018)
 - Fix: Used **implementation** and **community input** for formal model
- Very **few comments** in Inria’s TLS formal model⁸
 - Literally **no comments** at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
- **Incomplete validation** of draft 20 artifacts⁹
 - Fix: Designed an **automated validation framework** for key schedule
- A **simple extension** made the artifacts running for **1 month** on high-end server (icelake)
 - Submitted to ProVerif developers for analysis
 - Fix: Formal model from **scratch**

⁷Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

⁸<https://github.com/Inria-Prosecco/reftls/tree/master/pv>

⁹<https://mailarchive.ietf.org/arch/msg/tls/~nFk9Eu7n-YFsFfGUe9X4JnrX8/>

Approach



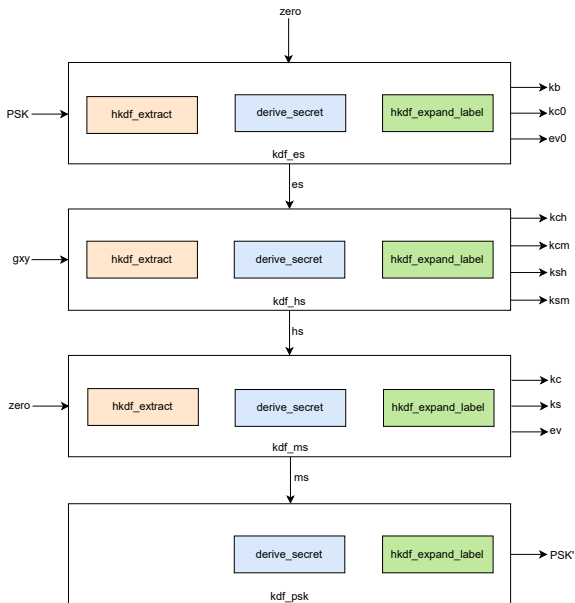
Outline

- 1 TLS
- 2 Attestation (RA)
- 3 Attested TLS (RA+TLS)
- 4 Goal and Contributions
- 5 Approach and Tool
- 6 Validation of TLS 1.3**
 - Key Schedule
 - Validation of Key Schedule
- 7 Formal Analysis of Attested TLS
 - Flow
 - Property
- 8 Summary

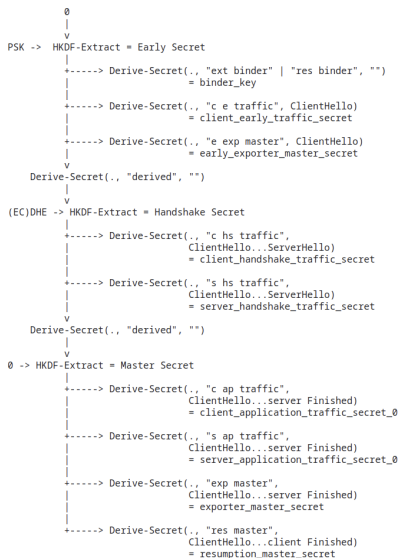
Agenda

- 6 Validation of TLS 1.3
 - Key Schedule
 - Validation of Key Schedule

Key Schedule - Overview



Key Schedule¹⁰

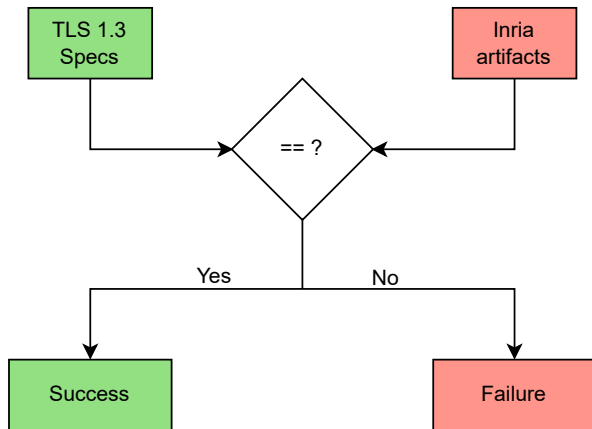


¹⁰<https://datatracker.ietf.org/doc/html/rfc8446#section-7.1>

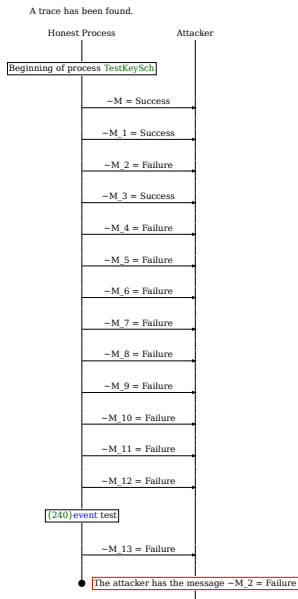
Agenda

- 6 Validation of TLS 1.3
 - Key Schedule
 - Validation of Key Schedule

Validation Framework



Validation Result



Issue 1: Salt for Handshake Secret¹¹

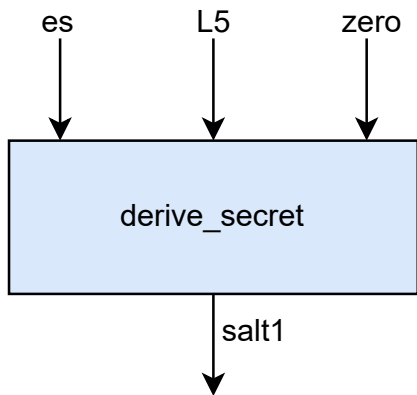


Figure: TLS 1.3 Specs

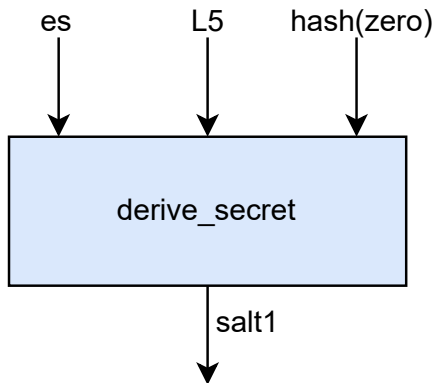


Figure: Inria artifacts

¹¹<https://github.com/Inria-Prosecco/reftls/issues/7>

Issue 2: Salt for Master Secret¹²

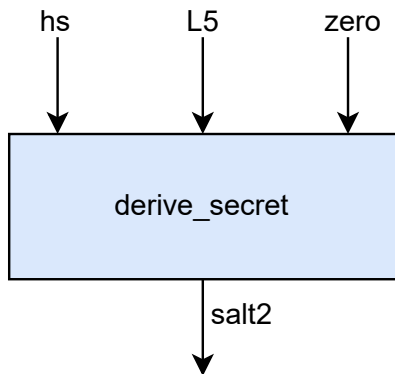


Figure: TLS 1.3 Specs

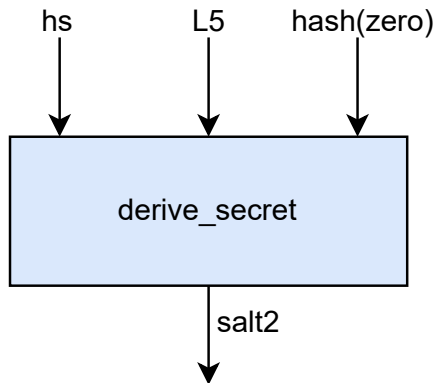


Figure: Inria artifacts

¹²<https://github.com/Inria-Prosecco/reftls/issues/7>

Issue 3: Master Secret¹³

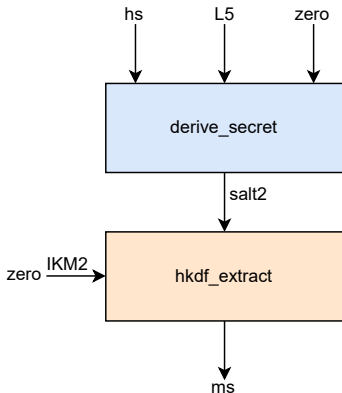


Figure: TLS 1.3 Specs

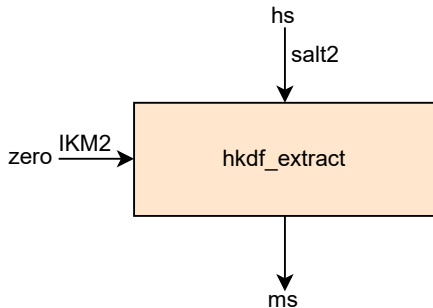


Figure: Inria artifacts

¹³<https://github.com/Inria-Prosecco/reftls/issues/6>

Ruling out Abstractions

- Ubuntu 20.04 LTS on an Intel Core i7-11800H processor with 64 GB of RAM

Code	ProVerif 2.04	ProVerif 2.05
Original	6 min 06.634 s	6 min 02.256 s
With issue 1 fixed	5 min 51.682 s	6 min 03.335 s
With issue 2 fixed	7 min 04.472 s	6 min 14.954 s
With issue 3 fixed	7 min 11.434 s	6 min 41.872 s
With all 3 issues fixed	6 min 40.010 s	6 min 31.887 s

A “Tale” of Community input

- Paper authors¹⁴

¹⁴Karthikeyan Bhargavan, Blanchet, and Kobeissi, “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”, 2017.

¹⁵<https://github.com/lurk-t/proverif>

¹⁶https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

¹⁷https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Formal_RA-TLS.pdf

¹⁸<https://wiki.ietf.org/meeting/119/hackathon>

¹⁹<https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00>

A “Tale” of Community input

- Paper authors¹⁴
 - Bruno Blanchet

¹⁴Karthikeyan Bhargavan, Blanchet, and Kobeissi, “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”, 2017.

¹⁵<https://github.com/lurk-t/proverif>

¹⁶https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

¹⁷https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Forma1_RA-TLS.pdf

¹⁸<https://wiki.ietf.org/meeting/119/hackathon>

¹⁹<https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00>

A “Tale” of Community input

- Paper authors¹⁴
 - Bruno Blanchet
 - Karthikeyan Bhargavan

¹⁴Karthikeyan Bhargavan, Blanchet, and Kobeissi, “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”, 2017.

¹⁵<https://github.com/lurk-t/proverif>

¹⁶https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

¹⁷https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Forma1_RA-TLS.pdf

¹⁸<https://wiki.ietf.org/meeting/119/hackathon>

¹⁹<https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00>

A “Tale” of Community input

- Paper authors¹⁴
 - Bruno Blanchet
 - Karthikeyan Bhargavan
 - Nadim Kobeissi

¹⁴Karthikeyan Bhargavan, Blanchet, and Kobeissi, “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”, 2017.

¹⁵<https://github.com/lurk-t/proverif>

¹⁶https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

¹⁷https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Forma1_RA-TLS.pdf

¹⁸<https://wiki.ietf.org/meeting/119/hackathon>

¹⁹<https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00>

A “Tale” of Community input

- Paper authors¹⁴
 - Bruno Blanchet
 - Karthikeyan Bhargavan
 - Nadim Kobeissi
- LURK authors¹⁵

¹⁴Karthikeyan Bhargavan, Blanchet, and Kobeissi, “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”, 2017.

¹⁵<https://github.com/lurk-t/proverif>

¹⁶https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

¹⁷https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Forma1_RA-TLS.pdf

¹⁸<https://wiki.ietf.org/meeting/119/hackathon>

¹⁹<https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00>

A “Tale” of Community input

- Paper authors¹⁴
 - Bruno Blanchet
 - Karthikeyan Bhargavan
 - Nadim Kobeissi
- LURK authors¹⁵
- IETF TLS WG¹⁶

¹⁴Karthikeyan Bhargavan, Blanchet, and Kobeissi, “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”, 2017.

¹⁵<https://github.com/lurk-t/proverif>

¹⁶https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

¹⁷https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Forma1_RA-TLS.pdf

¹⁸<https://wiki.ietf.org/meeting/119/hackathon>

¹⁹<https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00>

A “Tale” of Community input

- Paper authors¹⁴
 - Bruno Blanchet
 - Karthikeyan Bhargavan
 - Nadim Kobeissi
- LURK authors¹⁵
- IETF TLS WG¹⁶
- IRTF UFRMG chairs

¹⁴Karthikeyan Bhargavan, Blanchet, and Kobeissi, “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”, 2017.

¹⁵<https://github.com/lurk-t/proverif>

¹⁶https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

¹⁷https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Forma1_RA-TLS.pdf

¹⁸<https://wiki.ietf.org/meeting/119/hackathon>

¹⁹<https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00>

A “Tale” of Community input

- Paper authors¹⁴
 - Bruno Blanchet
 - Karthikeyan Bhargavan
 - Nadim Kobeissi
- LURK authors¹⁵
- IETF TLS WG¹⁶
- IRTF UFMRG chairs
- CCC attestation SIG¹⁷

¹⁴Karthikeyan Bhargavan, Blanchet, and Kobeissi, “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”, 2017.

¹⁵<https://github.com/lurk-t/proverif>

¹⁶https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

¹⁷https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Formal_RA-TLS.pdf

¹⁸<https://wiki.ietf.org/meeting/119/hackathon>

¹⁹<https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00>

A “Tale” of Community input

- Paper authors¹⁴
 - Bruno Blanchet
 - Karthikeyan Bhargavan
 - Nadim Kobeissi
- LURK authors¹⁵
- IETF TLS WG¹⁶
- IRTF UFMRG chairs
- CCC attestation SIG¹⁷
- ...

¹⁴Karthikeyan Bhargavan, Blanchet, and Kobeissi, “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”, 2017.

¹⁵<https://github.com/lurk-t/proverif>

¹⁶https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

¹⁷https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Formal_RA-TLS.pdf

¹⁸<https://wiki.ietf.org/meeting/119/hackathon>

¹⁹<https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00>

A “Tale” of Community input

- Paper authors¹⁴
 - Bruno Blanchet
 - Karthikeyan Bhargavan
 - Nadim Kobeissi
- LURK authors¹⁵
- IETF TLS WG¹⁶
- IRTF UFMRG chairs
- CCC attestation SIG¹⁷
- ...
- IETF 119 Hackathon¹⁸

¹⁴Karthikeyan Bhargavan, Blanchet, and Kobeissi, “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”, 2017.

¹⁵<https://github.com/lurk-t/proverif>

¹⁶https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

¹⁷https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Forma1_RA-TLS.pdf

¹⁸<https://wiki.ietf.org/meeting/119/hackathon>

¹⁹<https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00>

A “Tale” of Community input

- Paper authors¹⁴
 - Bruno Blanchet
 - Karthikeyan Bhargavan
 - Nadim Kobeissi
- LURK authors¹⁵
- IETF TLS WG¹⁶
- IRTF UFMRG chairs
- CCC attestation SIG¹⁷
- ...
- IETF 119 Hackathon¹⁸
- IRTF Crypto Forum RG @ IETF 119¹⁹

¹⁴Karthikeyan Bhargavan, Blanchet, and Kobeissi, “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”, 2017.

¹⁵<https://github.com/lurk-t/proverif>

¹⁶https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

¹⁷https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Forma1_RA-TLS.pdf

¹⁸<https://wiki.ietf.org/meeting/119/hackathon>

¹⁹<https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00>

A “Tale” of Community input

- Paper authors¹⁴
 - Bruno Blanchet
 - Karthikeyan Bhargavan
 - Nadim Kobeissi
- LURK authors¹⁵
- IETF TLS WG¹⁶
- IRTF UFMRG chairs
- CCC attestation SIG¹⁷
- ...
- IETF 119 Hackathon¹⁸
- IRTF Crypto Forum RG @ IETF 119¹⁹
- Tool session @ GT MFS'24

¹⁴Karthikeyan Bhargavan, Blanchet, and Kobeissi, “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”, 2017.

¹⁵<https://github.com/lurk-t/proverif>

¹⁶https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

¹⁷https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Formal_RA-TLS.pdf

¹⁸<https://wiki.ietf.org/meeting/119/hackathon>

¹⁹<https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00>

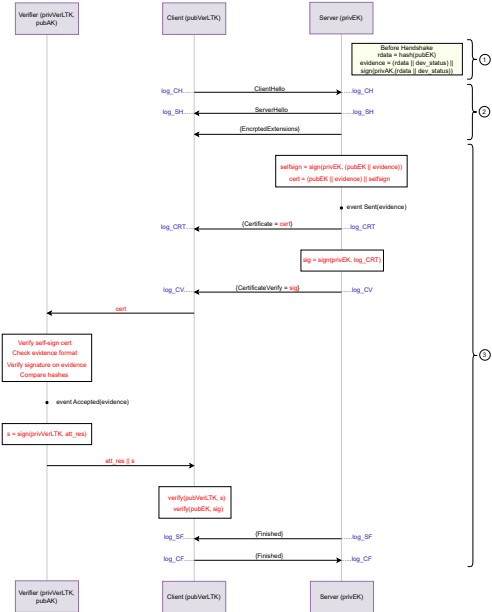
Outline

- 1 TLS
- 2 Attestation (RA)
- 3 Attested TLS (RA+TLS)
- 4 Goal and Contributions
- 5 Approach and Tool
- 6 Validation of TLS 1.3
 - Key Schedule
 - Validation of Key Schedule
- 7 Formal Analysis of Attested TLS**
 - Flow
 - Property
- 8 Summary

Agenda

- 7 Formal Analysis of Attested TLS
 - Flow
 - Property

RA-TLS in BC Model



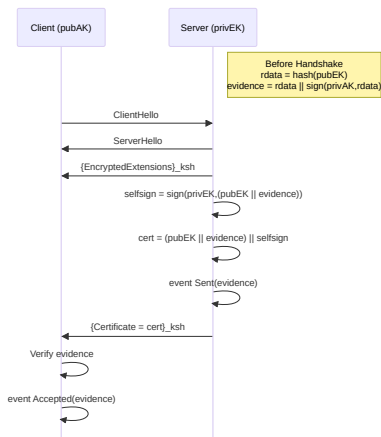
Agenda

- 7 Formal Analysis of Attested TLS
 - Flow
 - Property

Replay Protection of Evidence

$\forall ev.$

$$inj - event(Accepted(ev)) \implies inj - event(Sent(ev)) \quad (1)$$



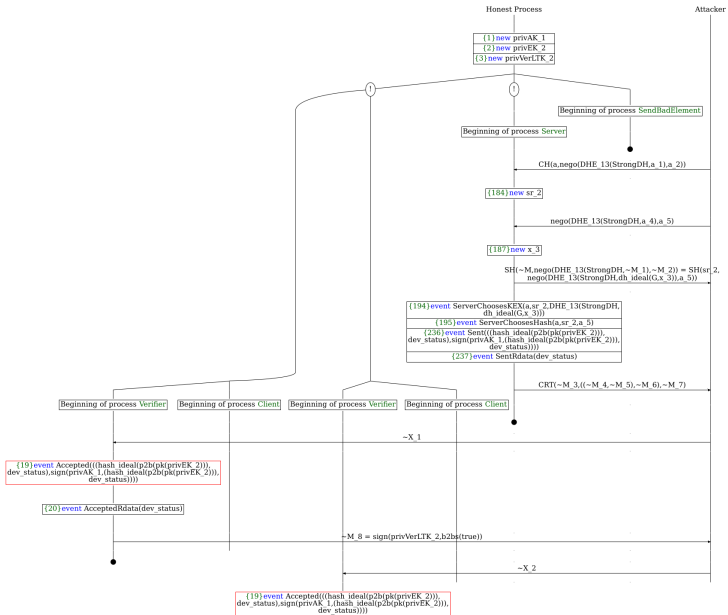
Eliminate Reasons of Failure

$\forall ev.$

$\exists cr, sr, e.$

$inj - event(Accepted(ev)) \implies inj - event(Sent(ev)) \parallel$
 $event(ServerChoosesKEX(cr, sr, DHE_{13}(WeakDH, e))) \parallel$
 $event(ServerChoosesHash(cr, sr, WeakHash)) \parallel$
 $event(SentBadElement).$

Attack Trace (BC with one-way authenticated channel)



Outline

- 1 TLS
- 2 Attestation (RA)
- 3 Attested TLS (RA+TLS)
- 4 Goal and Contributions
- 5 Approach and Tool
- 6 Validation of TLS 1.3
 - Key Schedule
 - Validation of Key Schedule
- 7 Formal Analysis of Attested TLS
 - Flow
 - Property
- 8 Summary

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!

²⁰Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!
 - Validation of formal model is crucial!

²⁰Tschofenig, Sheffer, Howard, Mihalea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!
 - Validation of formal model is crucial!
- Intel's RA-TLS is potentially vulnerable to replay attacks

²⁰Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!
 - Validation of formal model is crucial!
- Intel's RA-TLS is potentially vulnerable to replay attacks
 - Need for standardized and formally verified attested TLS

²⁰Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!
 - Validation of formal model is crucial!
- Intel's RA-TLS is potentially vulnerable to replay attacks
 - Need for standardized and formally verified attested TLS
- Lessons learnt

²⁰Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!
 - Validation of formal model is crucial!
- Intel's RA-TLS is potentially vulnerable to replay attacks
 - Need for standardized and formally verified attested TLS
- Lessons learnt
 1. Comments in formal models (best practices)

²⁰Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!
 - Validation of formal model is crucial!
- Intel's RA-TLS is potentially vulnerable to replay attacks
 - Need for standardized and formally verified attested TLS
- Lessons learnt
 1. Comments in formal models (best practices)
 2. Validation of formal models

²⁰Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!
 - Validation of formal model is crucial!
- Intel's RA-TLS is potentially vulnerable to replay attacks
 - Need for standardized and formally verified attested TLS
- Lessons learnt
 1. Comments in formal models (best practices)
 2. Validation of formal models
 3. Keep formal verification artifacts up to date (IRTF UFMRG)

²⁰Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!
 - Validation of formal model is crucial!
- Intel's RA-TLS is potentially vulnerable to replay attacks
 - Need for standardized and formally verified attested TLS
- Lessons learnt
 1. Comments in formal models (best practices)
 2. Validation of formal models
 3. Keep formal verification artifacts up to date (IRTF UFMRG)
 4. Usability of tools for formal analysis

²⁰Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!
 - Validation of formal model is crucial!
- Intel's RA-TLS is potentially vulnerable to replay attacks
 - Need for standardized and formally verified attested TLS
- Lessons learnt
 1. Comments in formal models (best practices)
 2. Validation of formal models
 3. Keep formal verification artifacts up to date (IRTF UFMRG)
 4. Usability of tools for formal analysis
- Plan

²⁰Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!
 - Validation of formal model is crucial!
- Intel's RA-TLS is potentially vulnerable to replay attacks
 - Need for standardized and formally verified attested TLS
- Lessons learnt
 1. Comments in formal models (best practices)
 2. Validation of formal models
 3. Keep formal verification artifacts up to date (IRTF UFMRG)
 4. Usability of tools for formal analysis
- Plan
 - Client-side attestation

²⁰Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!
 - Validation of formal model is crucial!
- Intel's RA-TLS is potentially vulnerable to replay attacks
 - Need for standardized and formally verified attested TLS
- Lessons learnt
 1. Comments in formal models (best practices)
 2. Validation of formal models
 3. Keep formal verification artifacts up to date (IRTF UFMRG)
 4. Usability of tools for formal analysis
- Plan
 - Client-side attestation
 - Propose and verify the fixed version for RA-TLS

²⁰Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!
 - Validation of formal model is crucial!
- Intel's RA-TLS is potentially vulnerable to replay attacks
 - Need for standardized and formally verified attested TLS
- Lessons learnt
 1. Comments in formal models (best practices)
 2. Validation of formal models
 3. Keep formal verification artifacts up to date (IRTF UFMRG)
 4. Usability of tools for formal analysis
- Plan
 - Client-side attestation
 - Propose and verify the fixed version for RA-TLS
 - IETF draft for intra-HS attestation²⁰

²⁰Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!
 - Validation of formal model is crucial!
- Intel's RA-TLS is potentially vulnerable to replay attacks
 - Need for standardized and formally verified attested TLS
- Lessons learnt
 1. Comments in formal models (best practices)
 2. Validation of formal models
 3. Keep formal verification artifacts up to date (IRTF UFMRG)
 4. Usability of tools for formal analysis
- Plan
 - Client-side attestation
 - Propose and verify the fixed version for RA-TLS
 - IETF draft for intra-HS attestation²⁰
- Call to action

²⁰Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Summary

- Inria's formal model of TLS 1.3 draft-20 key schedule is wrong!
 - Validation of formal model is crucial!
- Intel's RA-TLS is potentially vulnerable to replay attacks
 - Need for standardized and formally verified attested TLS
- Lessons learnt
 1. Comments in formal models (best practices)
 2. Validation of formal models
 3. Keep formal verification artifacts up to date (IRTF UFMRG)
 4. Usability of tools for formal analysis
- Plan
 - Client-side attestation
 - Propose and verify the fixed version for RA-TLS
 - IETF draft for intra-HS attestation²⁰
- Call to action
 - anyone interested?

²⁰Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

Key References



Barbosa, Manuel, Gilles Barthe, Karthik Bhargavan, Bruno Blanchet, Cas Cremers, Kevin Liao, and Bryan Parno. “SoK : Computer-Aided Cryptography”. In: *42nd IEEE Symposium on Security and Privacy*. 2021. URL: <https://eprint.iacr.org/2019/1393.pdf>.



Bhargavan, Karthikeyan, Bruno Blanchet, and Nadim Kobeissi. “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”. In: *2017 IEEE Symposium on Security and Privacy (SP)*. 2017, pp. 483–502. DOI: 10.1109/SP.2017.26.



Blanchet, Bruno, Vincent Cheval, and Véronique Cortier. “ProVerif with lemmas, induction, fast subsumption, and much more”. In: *IEEE Symposium on Security and Privacy (S&P’22)*. Los Alamitos, CA, USA: IEEE Computer Society, May 2022, pp. 205–222. DOI: 10.1109/SP46214.2022.00013.



Knauth, T., M. Steiner, S. Chakrabarti, L. Lei, C. Xing, and M. Vj. *Integrating Remote Attestation with Transport Layer Security*. Tech. rep. Intel Labs, 2018. URL: <https://arxiv.org/abs/1801.05863>.



Sardar, Muhammad Usama, Thomas Fossati, Simon Frost, and Shale Xiong. *Formal Specification and Verification of Architecturally-defined Attestation Mechanisms in Arm CCA and Intel TDX*. Nov. 2023. URL: https://www.researchgate.net/publication/375592777_Formal_Specification_and_Verification_of_Architecturally-defined_Attestation_Mechanisms_in_Arm_CCA_and_Intel_TDX.



Tschofenig, Hannes, Yaron Sheffer, Paul Howard, Ionuț Mihălcea, 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-06. Work in Progress. Internet Engineering Task Force, Mar. 2024. 34 pp. URL: <https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/06/>.

ACK

- Ionut Mihalcea (Arm)

ACK

- Ionut Mihalcea (Arm)
- Yaron Sheffer (Intuit)

ACK

- Ionut Mihalcea (Arm)
- Yaron Sheffer (Intuit)
- Yogesh Deshpande (Arm)

ACK

- Ionut Mihalcea (Arm)
- Yaron Sheffer (Intuit)
- Yogesh Deshpande (Arm)
- Anonymous HCVS reviewer # 3

Shameless plug: 4th PAVeTrust @ FM 2024

- Program Analysis and Verification on Trusted Platforms (PAVeTrust) Workshop
- Paper submission: 5 July
- Notification: 26 July
- Workshop: 9 September
- Milan, Italy
- <https://pavetrust.github.io/>