Challenges in the Formal Verification of Attested TLS

Muhammad Usama Sardar[1], Arto Niemi[2], Hannes Tschofenig[3], Thomas Fossati[4]

[1]TU Dresden, Germany

[2]Huawei Technologies, Helsinki, Finland

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

[4]Linaro, Lausanne, Switzerland

May 16, 2024

Agenda

Don't be scared of maths![1]

- Writing is nature's way of letting you know how sloppy your thinking is. (Guindon)

[1] https://www.microsoft.com/en-us/research/publication/2018/05/book-02-08-08.pdf

Don't be scared of maths![1]

- Writing is nature's way of letting you know how sloppy your thinking is. (Guindon)

- Mathematics is nature's way of letting you know how sloppy your writing is. (Leslie Lamport)

[1] https://www.microsoft.com/en-us/research/publication/2018/05/book-02-08-08.pdf

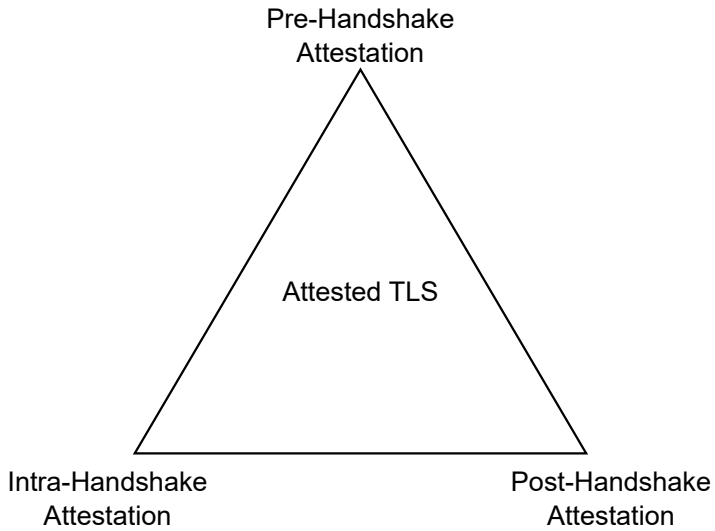
Don't be scared of maths![1]

- Writing is nature's way of letting you know how sloppy your thinking is. (Guindon)
- Mathematics is nature's way of letting you know how sloppy your writing is. (Leslie Lamport)
- Formal mathematics is nature's way of letting you know how sloppy your mathematics is. (Leslie Lamport)

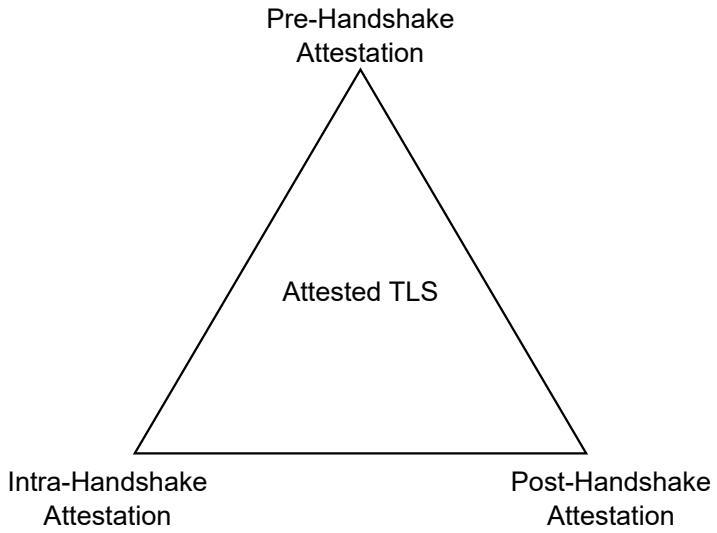
[1] https://www.microsoft.com/en-us/research/publication/2018/05/book-02-08-08.pdf

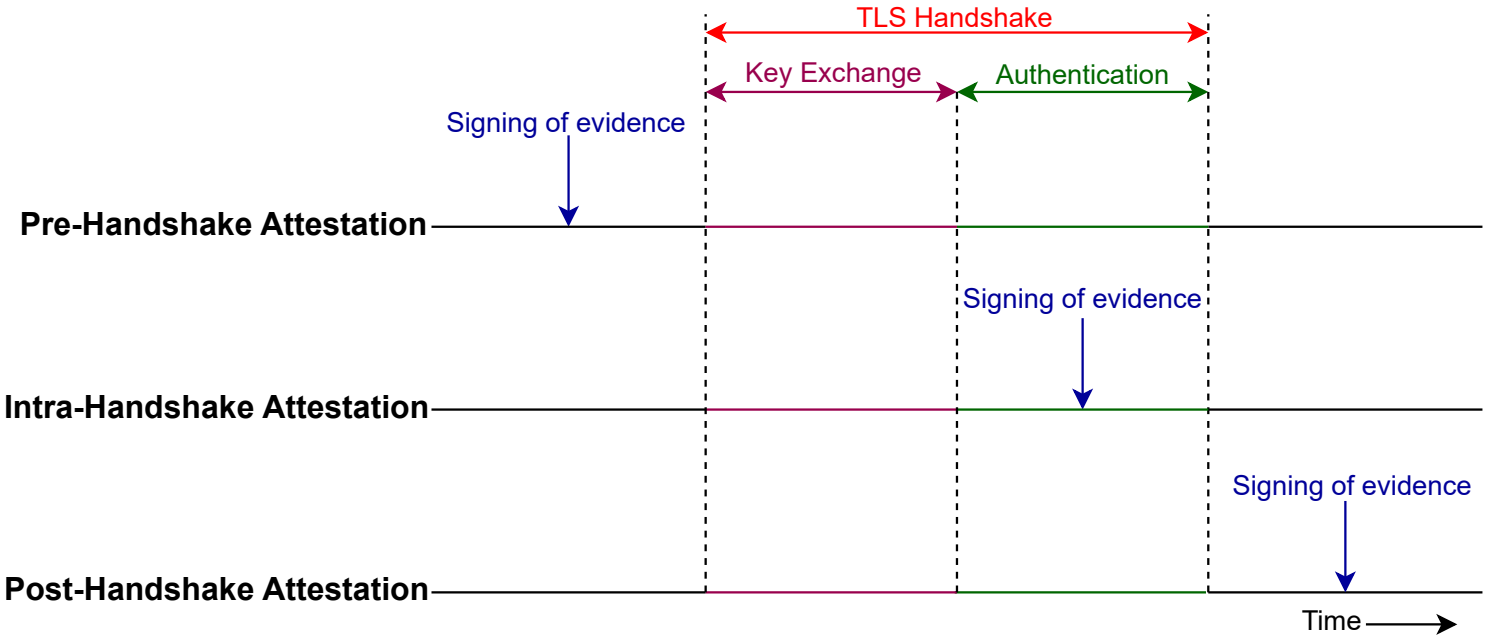
Outline

Attested TLS



Attested TLS





Intel's RA-TLS[2]

- Widely used pre-HS attestation protocol, e.g., in

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

Intel's RA-TLS[2]

- Widely used pre-HS attestation protocol, e.g., in
  - Gramine

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

Intel's RA-TLS[2]

- Widely used pre-HS attestation protocol, e.g., in
  - Gramine
  - RATS-TLS

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

Intel's RA-TLS[2]

- Widely used pre-HS attestation protocol, e.g., in
  - Gramine
  - RATS-TLS
  - Open Enclave Attested TLS

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

Intel's RA-TLS[2]

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

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

Outline

Goal

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

Contributions

- First formal analysis of attested TLS for TEEs (happy to discuss in Hackathon)

[3] https://github.com/Inria-Prosecco/reftls

Contributions

- First formal analysis of attested TLS for TEEs (happy to discuss in Hackathon)
- Validation of formal model[3] of TLS 1.3 Key Schedule, revealing 3 major issues

[3] `https://github.com/Inria-Prosecco/reftls`

Outline

Analysis Approach and Tool

- Approach: Symbolic[4]

[4] Barbosa, Barthe, Karthik Bhargavan, Blanchet, Cremers, Liao, and Parno, "SoK : Computer-Aided Cryptography", 2021.

[5] Blanchet, Cheval, and Cortier, "ProVerif with lemmas, induction, fast subsumption, and much more", 2022.

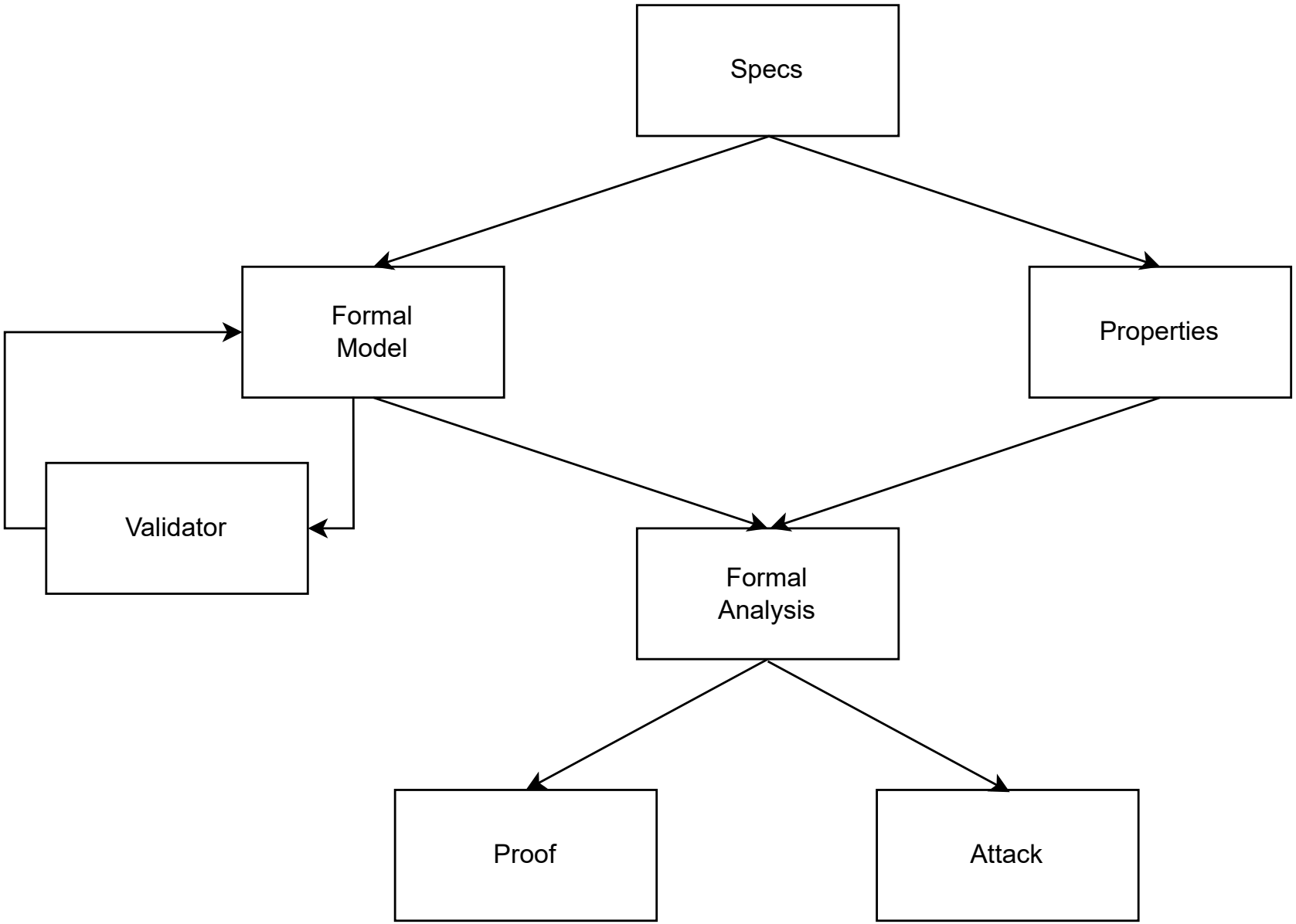
Analysis Approach and Tool

- Approach: Symbolic[4]
- Tool used: ProVerif[5]

[4] Barbosa, Barthe, Karthik Bhargavan, Blanchet, Cremers, Liao, and Parno, "SoK : Computer-Aided Cryptography", 2021.

[5] Blanchet, Cheval, and Cortier, "ProVerif with lemmas, induction, fast subsumption, and much more", 2022.

Approach - Simplified



Challenge in Specification of Intel's RA-TLS[6]

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

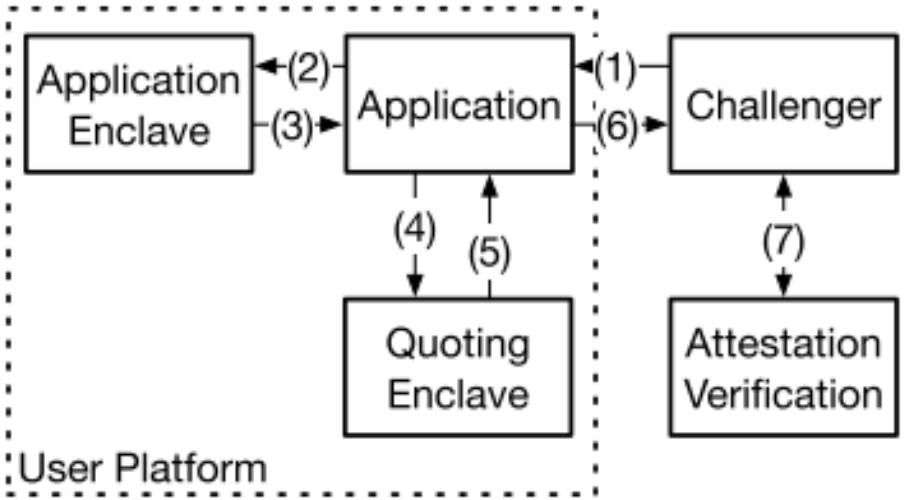


Figure 1: Remote Attestation Example. The challenger is off-platform with respect to the attester.

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

Challenge in Specification of Intel's RA-TLS[6]

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

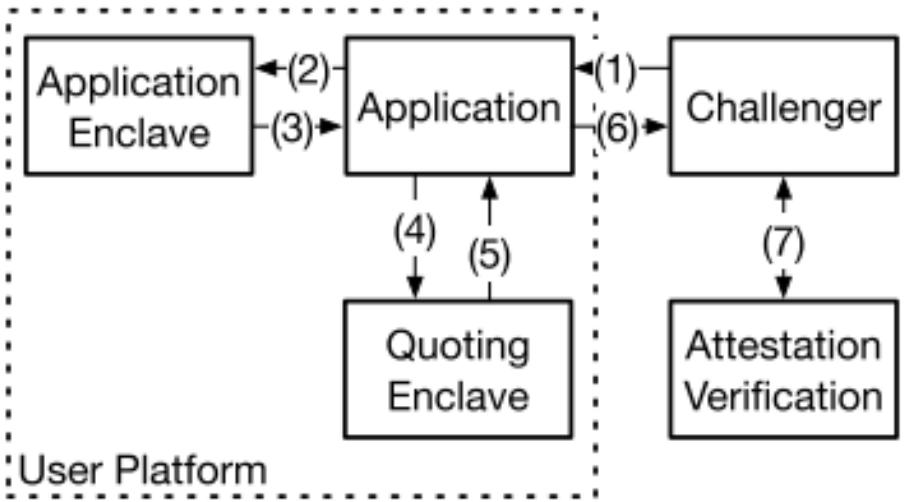


Figure 1: Remote Attestation Example. The challenger is off-platform with respect to the attester.

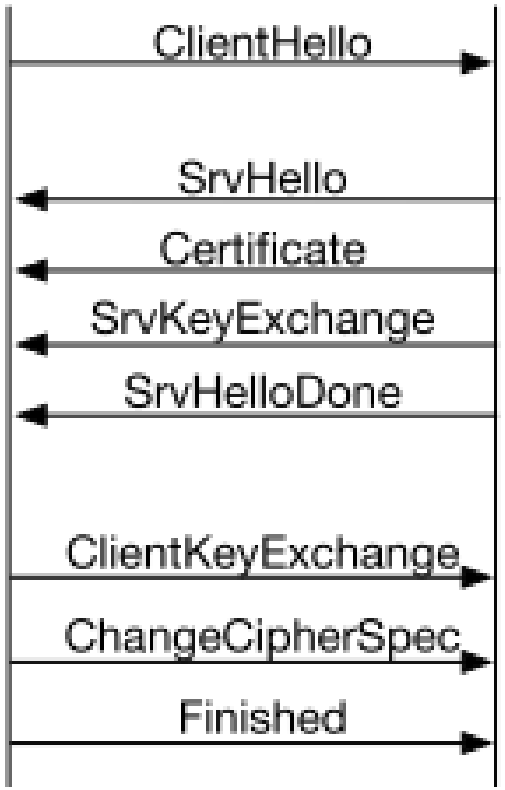


Figure 2: TLS 1.2 Handshake Messages.

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

Challenges from Formal Perspective

- Very few comments in Inria's TLS formal model[7]

[7] https://github.com/Inria-Prosecco/reftls/tree/master/pv

[8] https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrxX8/

Challenges from Formal Perspective

- Very few comments in Inria's TLS formal model[7]
  - Literally no comments at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!

[7] https://github.com/Inria-Prosecco/reftls/tree/master/pv

[8] https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrxX8/

Challenges from Formal Perspective

- Very few comments in Inria's TLS formal model[7]
  - Literally no comments at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
  - Fix: Added extensive comments for future extensions

[7] https://github.com/Inria-Prosecco/reftls/tree/master/pv

[8] https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrxX8/

Challenges from Formal Perspective

- Very few comments in Inria's TLS formal model[7]
  - Literally no comments at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
  - Fix: Added extensive comments for future extensions
- Incomplete validation of draft 20 artifacts[8]

[7] https://github.com/Inria-Prosecco/reftls/tree/master/pv

[8] https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrxX8/

Challenges from Formal Perspective

- Very few comments in Inria's TLS formal model[7]
  - Literally no comments at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
  - Fix: Added extensive comments for future extensions
- Incomplete validation of draft 20 artifacts[8]
  - Fix: Designed an automated validation framework for key schedule

[7] https://github.com/Inria-Prosecco/reftls/tree/master/pv

[8] https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrxX8/

Challenges from Formal Perspective

- Very few comments in Inria's TLS formal model[7]
  - Literally no comments at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
  - Fix: Added extensive comments for future extensions
- Incomplete validation of draft 20 artifacts[8]
  - Fix: Designed an automated validation framework for key schedule
- A simple extension made the artifacts running for 1 month on high-end server (icelake)

[7] https://github.com/Inria-Prosecco/reftls/tree/master/pv

[8] https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrxX8/

Challenges from Formal Perspective

- Very few comments in Inria's TLS formal model[7]
  - Literally no comments at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
  - Fix: Added extensive comments for future extensions
- Incomplete validation of draft 20 artifacts[8]
  - 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

[7] https://github.com/Inria-Prosecco/reftls/tree/master/pv

[8] https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrxX8/

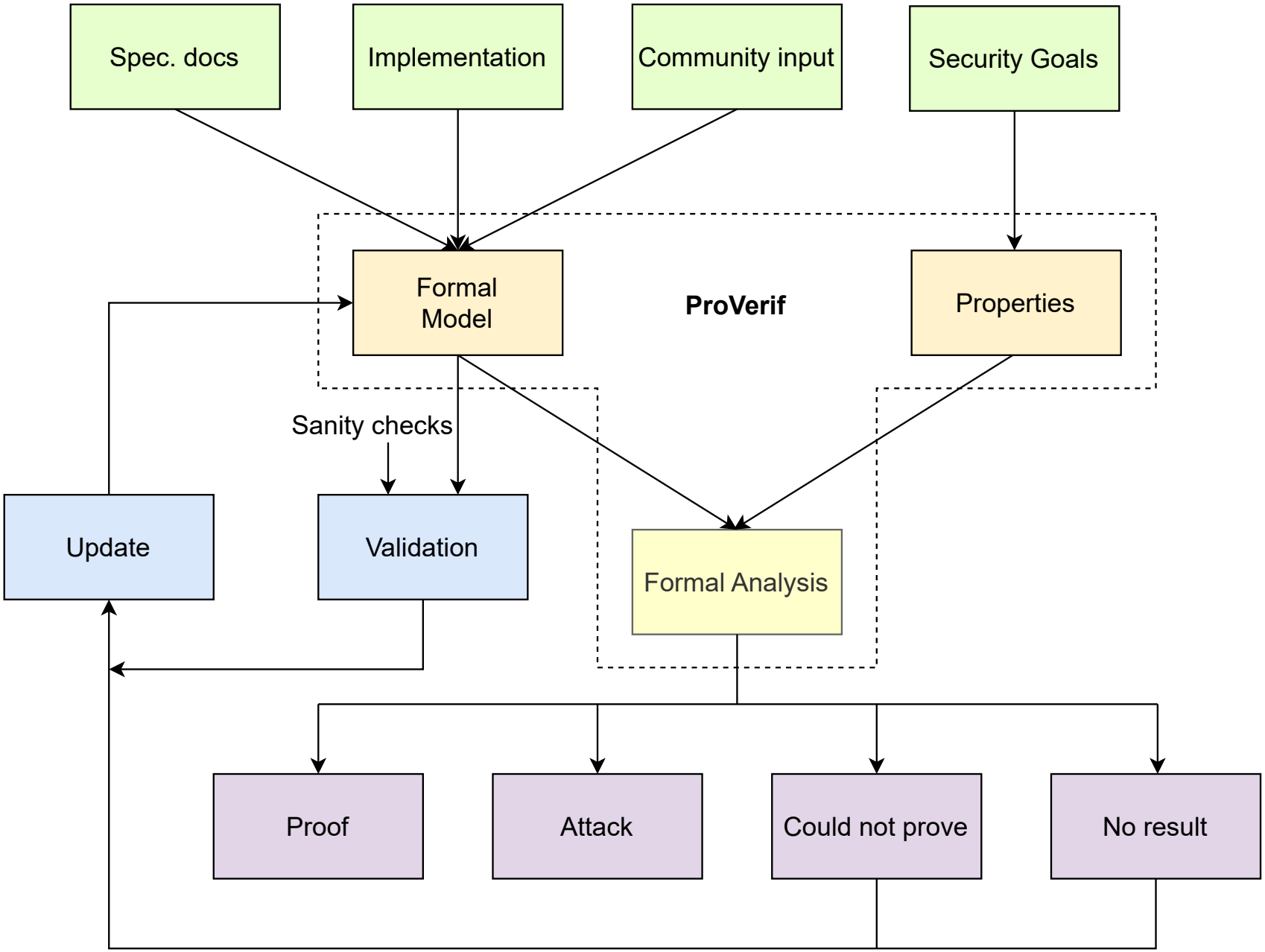
Challenges from Formal Perspective

- Very few comments in Inria's TLS formal model[7]
  - Literally no comments at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
  - Fix: Added extensive comments for future extensions
- Incomplete validation of draft 20 artifacts[8]
  - 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

[7] https://github.com/Inria-Prosecco/reftls/tree/master/pv

[8] https://mailarchive.ietf.org/arch/msg/tls/-nFk9Eu7n-YFsFfGUe9X4JnrxX8/

Approach

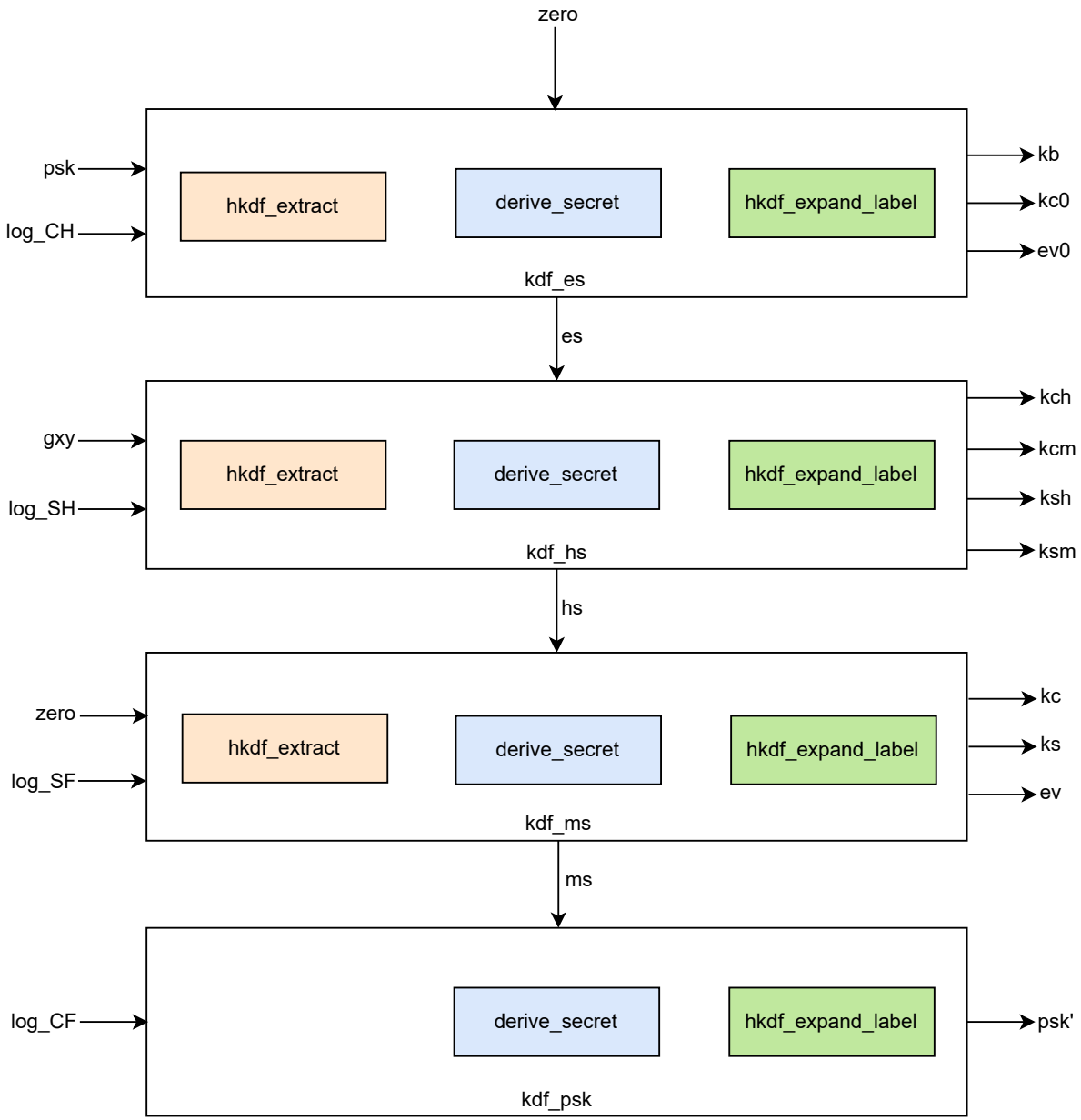

Spec. docs
Implementation
Community input
Security Goals
Formal Model
ProVerif
Properties
Sanity checks
Update
Validation
Formal Analysis
Proof
Attack
Could not prove
No result

Outline

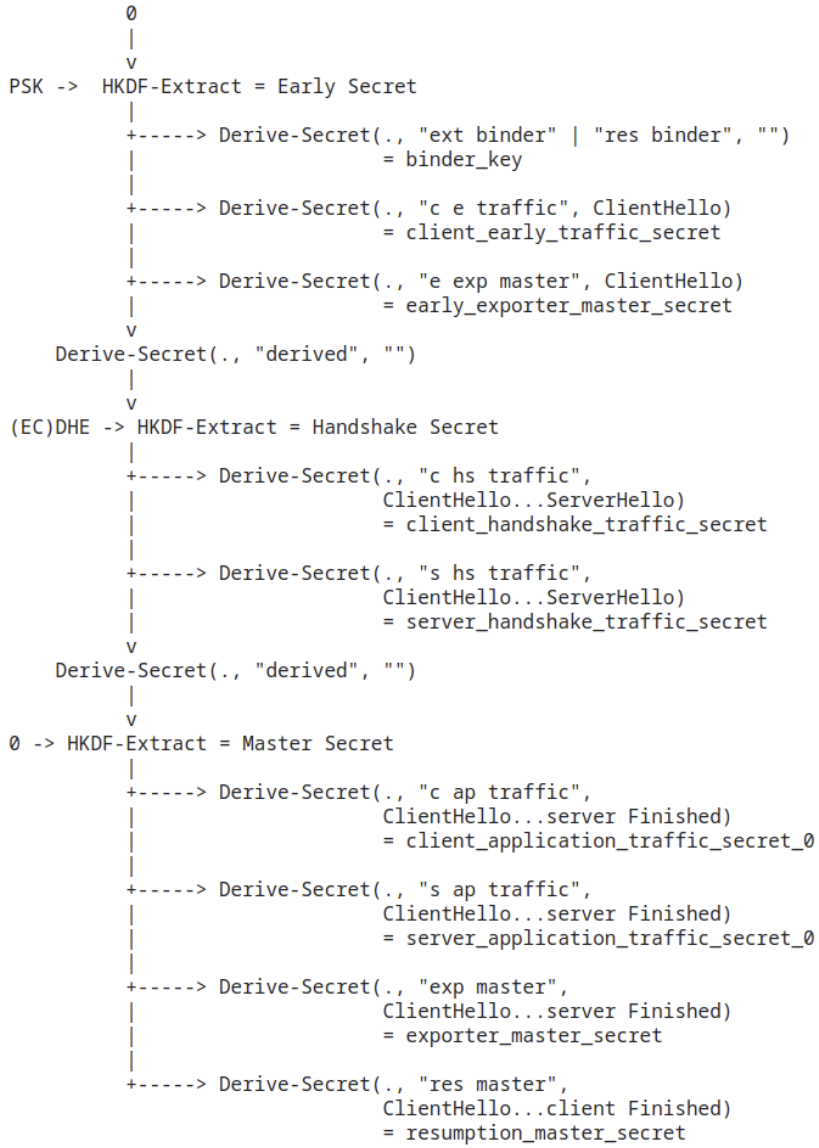
Agenda

5. Validation of TLS 1.3 (Quick overview)
   - Key Schedule
   - Validation of Key Schedule

Key Schedule - Overview

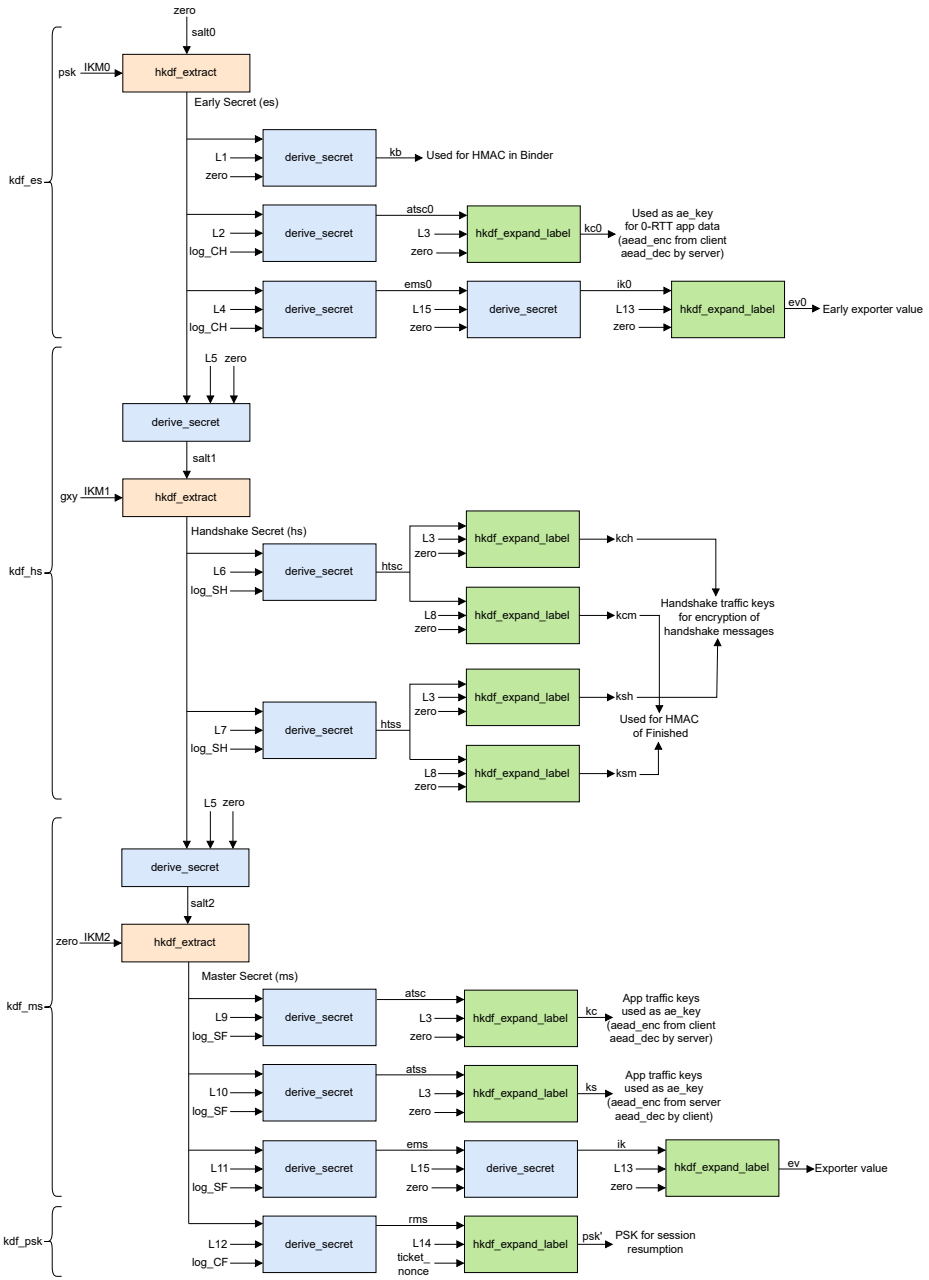


Key Schedule[9]



[9] https://datatracker.ietf.org/doc/html/rfc8446#section-7.1

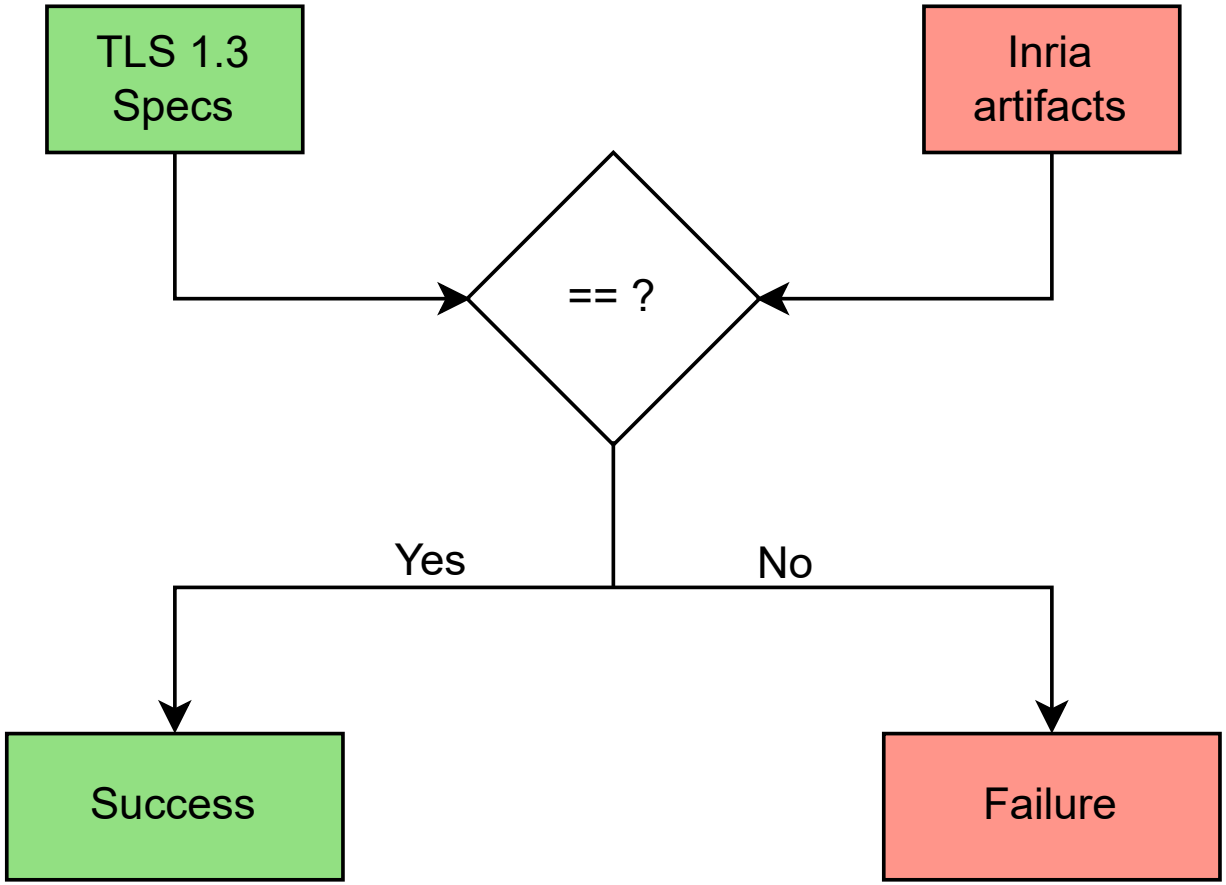
Key Schedule with 2nd Stage



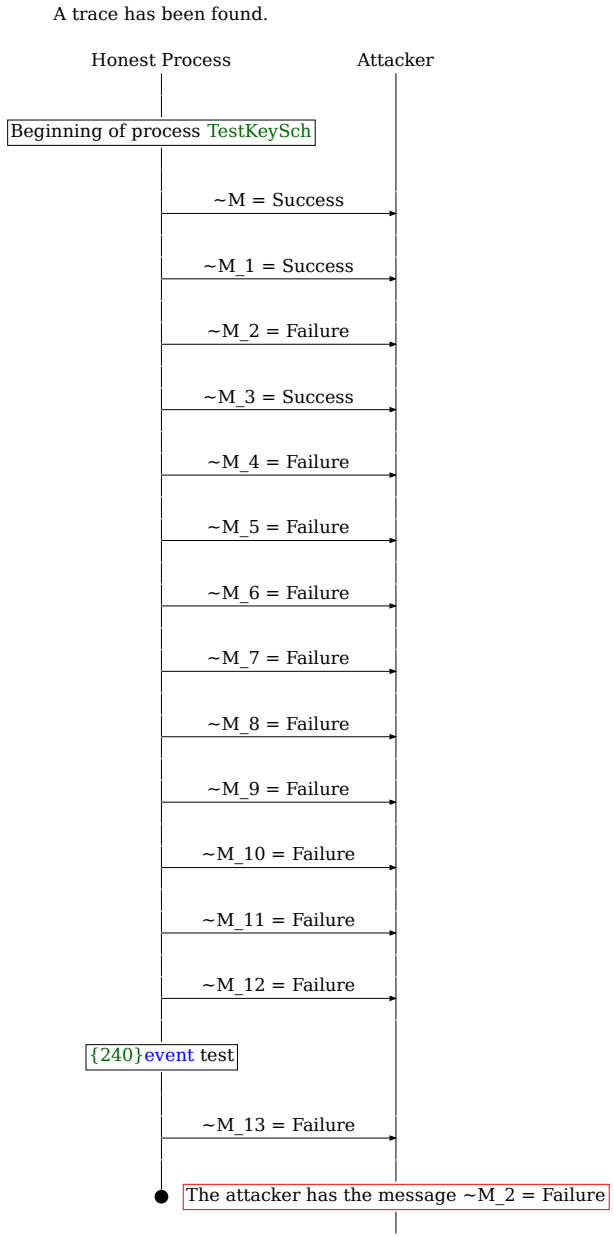
Agenda

5. Validation of TLS 1.3 (Quick overview)
   - Key Schedule
   - Validation of Key Schedule

Validation Framework



Validation Result



Example Issue: Master Secret[10]

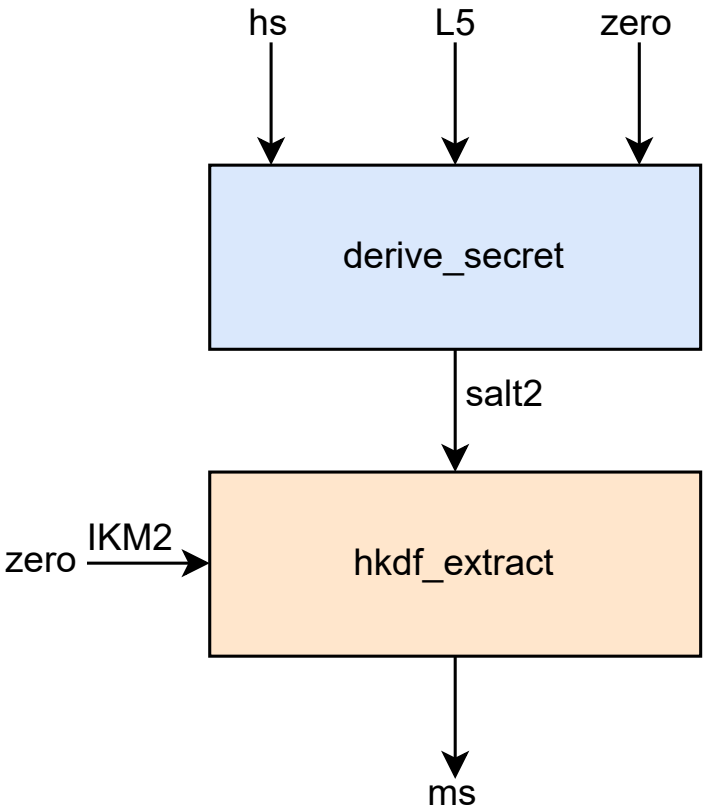


Figure: TLS 1.3 Specs

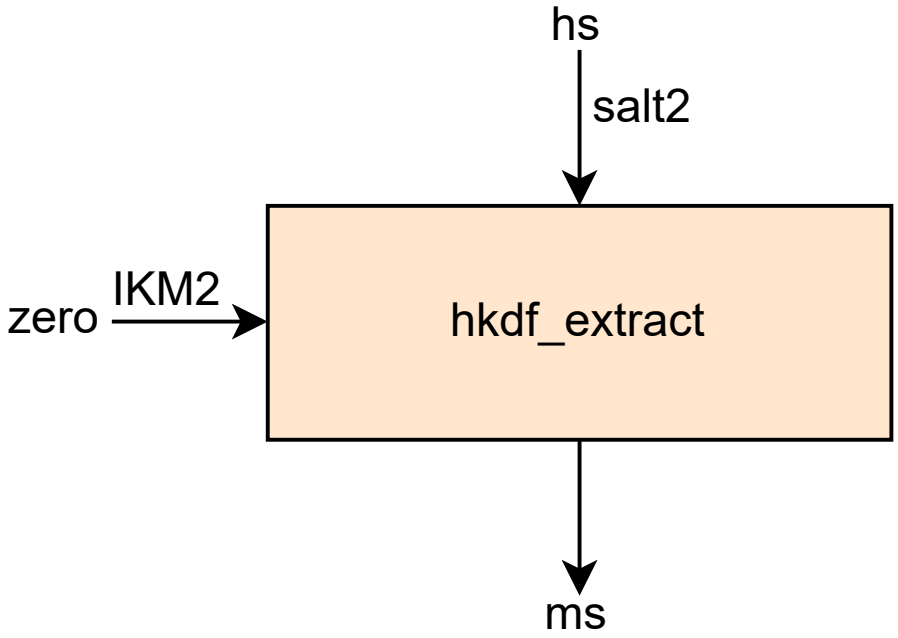


Figure: Inria artifacts

[10] 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 authors[11]

[11] Karthikeyan Bhargavan, Blanchet, and Kobeissi, "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate", 2017.

[12] https://github.com/lurk-t/proverif

[13] https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

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

[15] https://wiki.ietf.org/meeting/119/hackathon

[16] https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00

A "Tale" of Community input

- Paper authors[11]
  - Bruno Blanchet

[11] Karthikeyan Bhargavan, Blanchet, and Kobeissi, "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate", 2017.

[12] https://github.com/lurk-t/proverif

[13] https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

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

[15] https://wiki.ietf.org/meeting/119/hackathon

[16] https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00

A "Tale" of Community input

- Paper authors[11]
  - Bruno Blanchet
  - Karthikeyan Bhargavan

[11] Karthikeyan Bhargavan, Blanchet, and Kobeissi, "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate", 2017.

[12] https://github.com/lurk-t/proverif

[13] https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

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

[15] https://wiki.ietf.org/meeting/119/hackathon

[16] https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00

A "Tale" of Community input

- Paper authors[11]
  - Bruno Blanchet
  - Karthikeyan Bhargavan
  - Nadim Kobeissi

[11] Karthikeyan Bhargavan, Blanchet, and Kobeissi, "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate", 2017.

[12] https://github.com/lurk-t/proverif

[13] https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

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

[15] https://wiki.ietf.org/meeting/119/hackathon

[16] https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00

A "Tale" of Community input

- Paper authors[11]
  - Bruno Blanchet
  - Karthikeyan Bhargavan
  - Nadim Kobeissi
- LURK authors[12]

[11] Karthikeyan Bhargavan, Blanchet, and Kobeissi, "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate", 2017.

[12] https://github.com/lurk-t/proverif

[13] https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

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

[15] https://wiki.ietf.org/meeting/119/hackathon

[16] https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00

A "Tale" of Community input

- Paper authors[11]
  - Bruno Blanchet
  - Karthikeyan Bhargavan
  - Nadim Kobeissi
- LURK authors[12]
- IETF TLS WG[13]

[11] Karthikeyan Bhargavan, Blanchet, and Kobeissi, "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate", 2017.

[12] https://github.com/lurk-t/proverif

[13] https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

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

[15] https://wiki.ietf.org/meeting/119/hackathon

[16] https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00

A "Tale" of Community input

- Paper authors[11]
  - Bruno Blanchet
  - Karthikeyan Bhargavan
  - Nadim Kobeissi
- LURK authors[12]
- IETF TLS WG[13]
- IRTF UFMRG chairs

[11] Karthikeyan Bhargavan, Blanchet, and Kobeissi, "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate", 2017.

[12] https://github.com/lurk-t/proverif

[13] https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

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

[15] https://wiki.ietf.org/meeting/119/hackathon

[16] https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00

A "Tale" of Community input

- Paper authors[11]
  - Bruno Blanchet
  - Karthikeyan Bhargavan
  - Nadim Kobeissi
- LURK authors[12]
- IETF TLS WG[13]
- IRTF UFMRG chairs
- CCC attestation SIG[14]

[11] Karthikeyan Bhargavan, Blanchet, and Kobeissi, "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate", 2017.

[12] https://github.com/lurk-t/proverif

[13] https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

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

[15] https://wiki.ietf.org/meeting/119/hackathon

[16] https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00

A "Tale" of Community input

- Paper authors[11]
  - Bruno Blanchet
  - Karthikeyan Bhargavan
  - Nadim Kobeissi
- LURK authors[12]
- IETF TLS WG[13]
- IRTF UFMRG chairs
- CCC attestation SIG[14]
- ...

[11] Karthikeyan Bhargavan, Blanchet, and Kobeissi, "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate", 2017.

[12] https://github.com/lurk-t/proverif

[13] https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/

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

[15] https://wiki.ietf.org/meeting/119/hackathon

[16] https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00

A "Tale" of Community input

- Paper authors[11]
  - Bruno Blanchet
  - Karthikeyan Bhargavan
  - Nadim Kobeissi
- LURK authors[12]
- IETF TLS WG[13]
- IRTF UFMRG chairs
- CCC attestation SIG[14]
- ...
- IETF 119 Hackathon[15]

[11] Karthikeyan Bhargavan, Blanchet, and Kobeissi, "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate", 2017.

[12] `https://github.com/lurk-t/proverif`

[13] `https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/`

[14] `https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Formal_RA-TLS.pdf`

[15] `https://wiki.ietf.org/meeting/119/hackathon`

[16] `https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00`

A "Tale" of Community input

- Paper authors[11]
  - Bruno Blanchet
  - Karthikeyan Bhargavan
  - Nadim Kobeissi
- LURK authors[12]
- IETF TLS WG[13]
- IRTF UFMRG chairs
- CCC attestation SIG[14]
- ...
- IETF 119 Hackathon[15]
- IRTF Crypto Forum RG @ IETF 119[16]

---

[11] Karthikeyan Bhargavan, Blanchet, and Kobeissi, "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate", 2017.

[12] `https://github.com/lurk-t/proverif`

[13] `https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/`

[14] `https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Formal_RA-TLS.pdf`

[15] `https://wiki.ietf.org/meeting/119/hackathon`

[16] `https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00`

A "Tale" of Community input

- Paper authors[11]
  - Bruno Blanchet
  - Karthikeyan Bhargavan
  - Nadim Kobeissi
- LURK authors[12]
- IETF TLS WG[13]
- IRTF UFMRG chairs
- CCC attestation SIG[14]
- ...
- IETF 119 Hackathon[15]
- IRTF Crypto Forum RG @ IETF 119[16]
- Tool session @ GT MFS'24

[11] Karthikeyan Bhargavan, Blanchet, and Kobeissi, "Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate", 2017.

[12] `https://github.com/lurk-t/proverif`

[13] `https://mailarchive.ietf.org/arch/msg/tls/ZGmyHwTYh2iPwPrirj_rkSTYhDo/`

[14] `https://github.com/CCC-Attestation/meetings/blob/main/materials/MuhammadUsamaSardar_Formal_RA-TLS.pdf`

[15] `https://wiki.ietf.org/meeting/119/hackathon`

[16] `https://datatracker.ietf.org/meeting/119/materials/slides-119-cfrg-formal-analysis-of-ra-tls-00`

Outline

Summary

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

[17] Tschofenig, 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!

[17] Tschofenig, 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 (happy to share paper and discuss in Hackathon)

[17] Tschofenig, 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 (happy to share paper and discuss in Hackathon)
  - Need for standardized and formally verified attested TLS

[17] Tschofenig, 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 (happy to share paper and discuss in Hackathon)
  - Need for standardized and formally verified attested TLS
- Open Questions

[17] Tschofenig, 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 (happy to share paper and discuss in Hackathon)
  - Need for standardized and formally verified attested TLS
- Open Questions
  - Whether a fix for RA-TLS is possible?

[17] Tschofenig, 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 (happy to share paper and discuss in Hackathon)
  - Need for standardized and formally verified attested TLS
- Open Questions
  - Whether a fix for RA-TLS is possible?
  - Security of IETF draft[17]

[17] Tschofenig, 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. Vij. *Integrating Remote Attestation with Transport Layer Security*. Tech. rep. Intel Labs, 2018. URL: https://arxiv.org/abs/1801.05863.

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