Formal Specification and Verification of Architecturally-defined Attestation Mechanisms in Arm CCA and Intel TDX

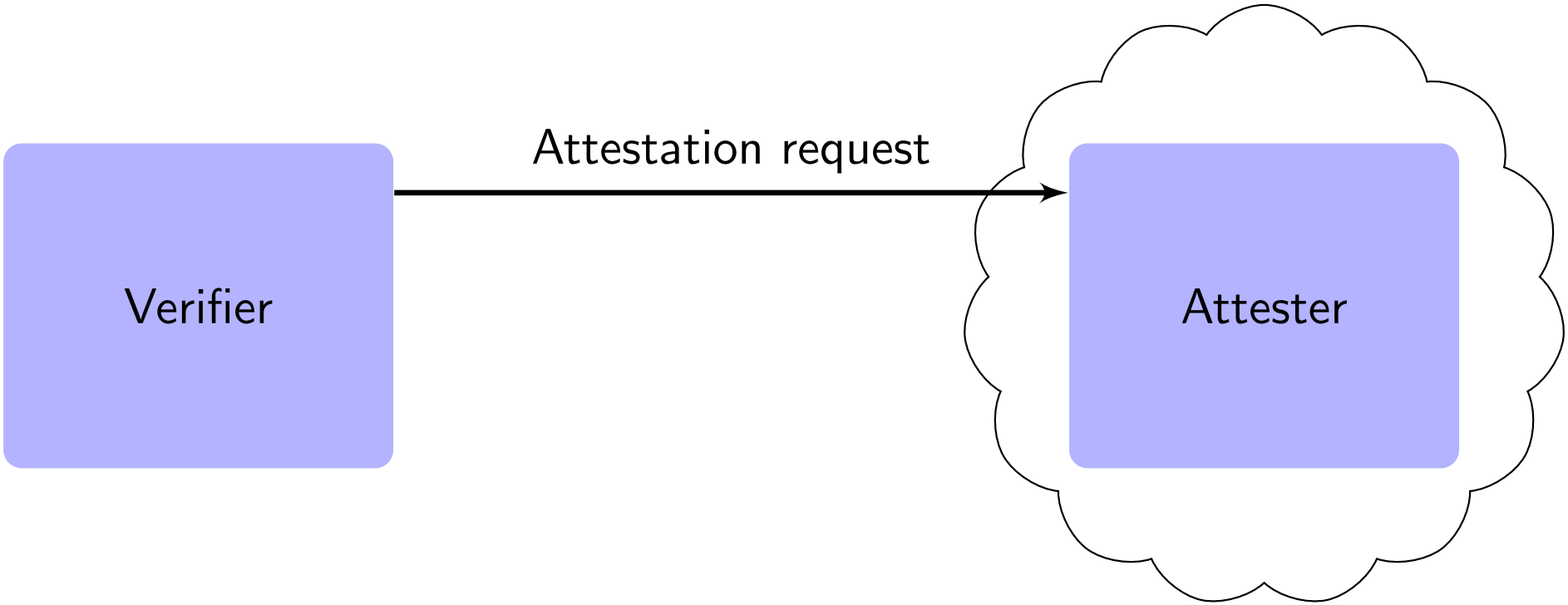
Muhammad Usama Sardar

TU Dresden

April 3, 2024

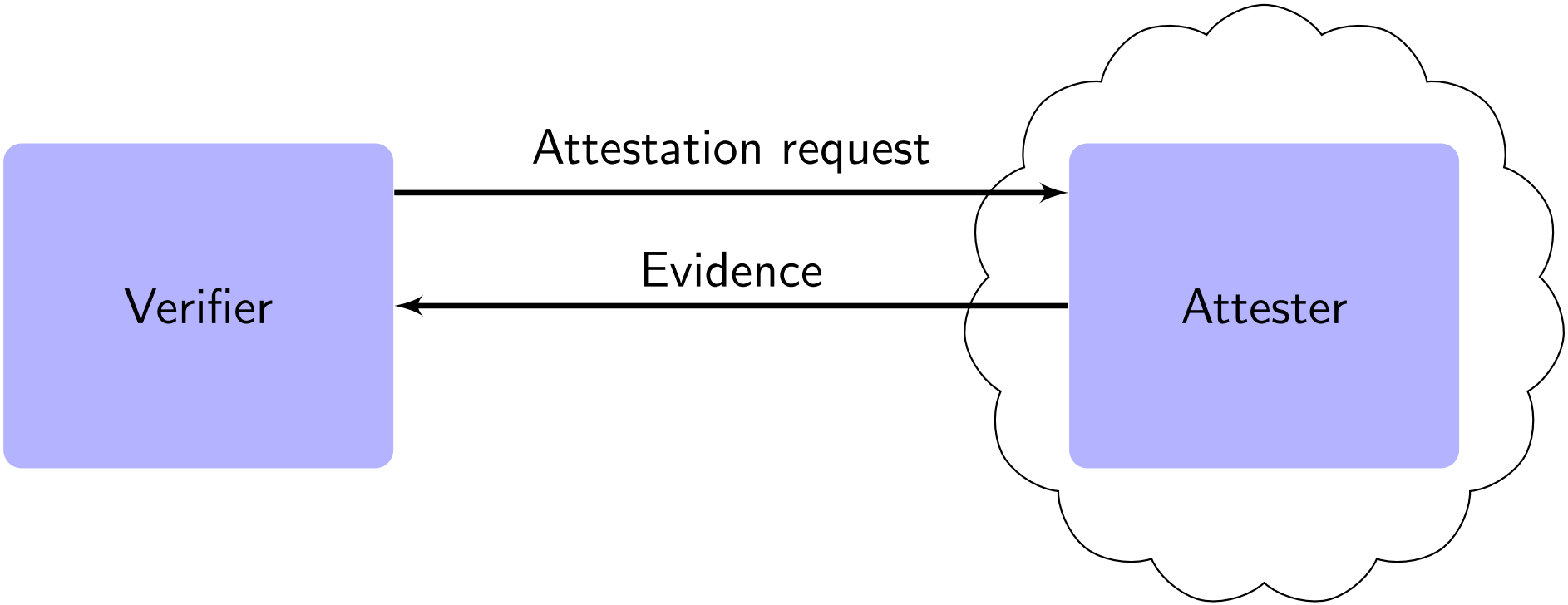
Agenda

Attestation in Confidential Computing[1] (Simplified)



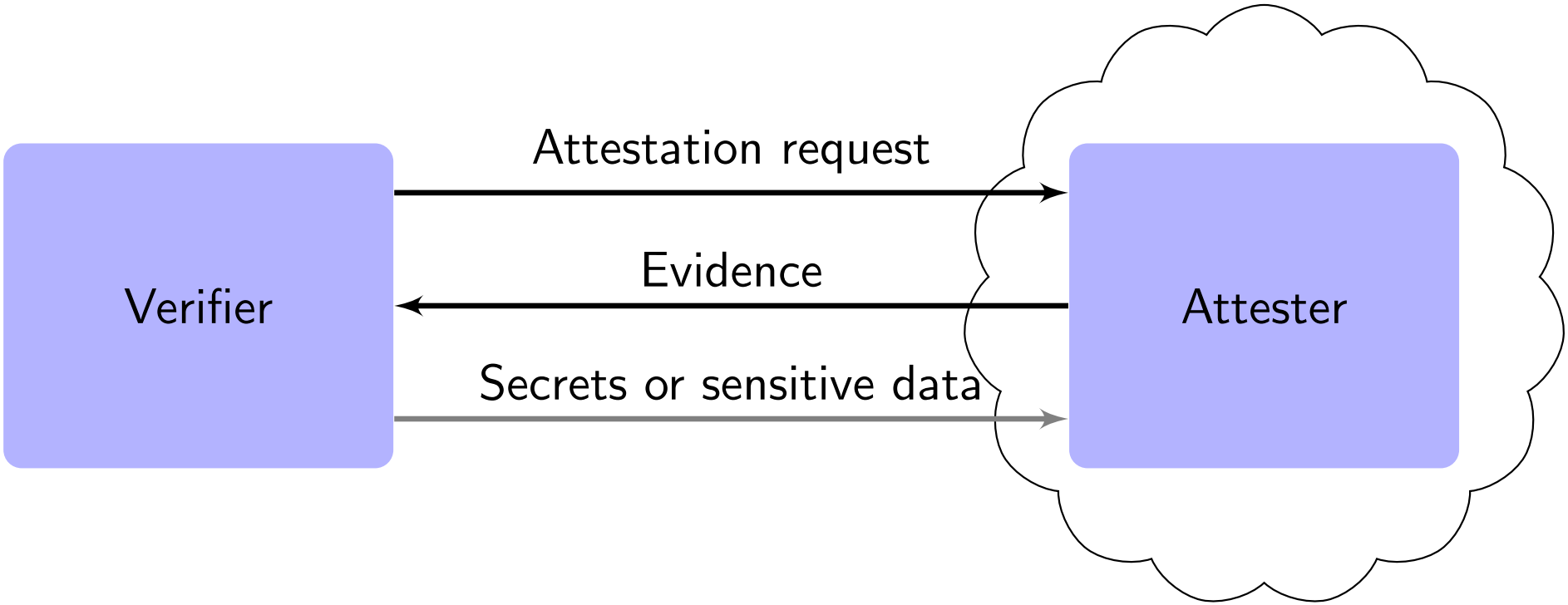
[1] Sardar and Fetzer, "Confidential computing and related technologies: a critical review", 2023.

Attestation in Confidential Computing[1] (Simplified)



[1] Sardar and Fetzer, "Confidential computing and related technologies: a critical review", 2023.

Attestation in Confidential Computing[1] (Simplified)



[1] Sardar and Fetzer, "Confidential computing and related technologies: a critical review", 2023.

Problem: ad-hoc and unverified designs[2]

sgaxe.com

Signing Your Own Quotes

We understand that remote attestion can be very tricky to pass. However, since we already done all the hard work of getting genuine attestation keys, we decided to help you out by developing a Twitter bot that passes SGX attestation for you. Our bot provides Attestation as a Service (AaaS), which allows you to get your own quotes signed with the keys we extracted using SGAxe. This way you can pass attestation without even owning an SGX machine. If you want to make use of our service, you can send a tweet to our bot @SGAxe_AaaS. If you'll tweet it, we'll sign it!

@SGAxe_AaaS

[2] `www.sgaxe.com`

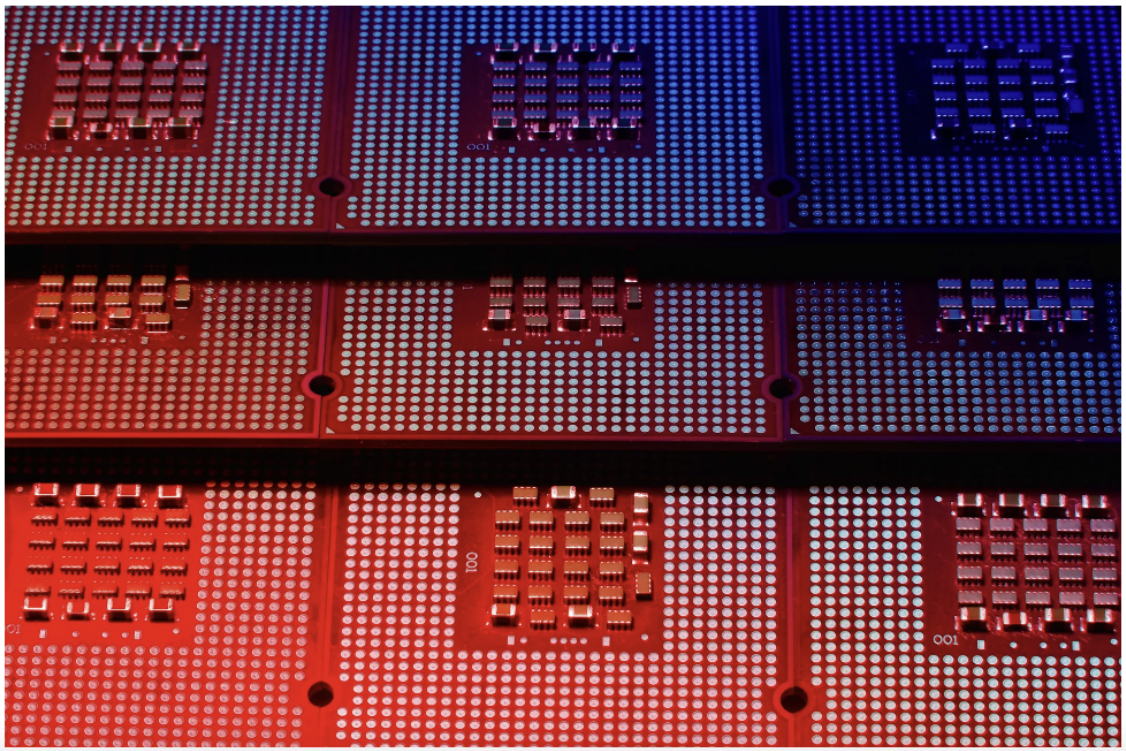
Next-generation TDX[3]

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

LILY HAY NEWMAN SECURITY APR 24, 2023 1:12 PM

Intel Let Google Cloud Hack Its New Secure Chips and Found 10 Bugs

To protect its Confidential Computing cloud infrastructure and gain critical insights, Google leans on its relationships with chipmakers.



PHOTOGRAPH: GETTY IMAGES

[3]Wired, *Intel Let Google Cloud Hack Its New Secure Chips and Found 10 Bugs*, 2023.

Related Work

- Intel SGX EPID[4]

[4] Sardar, Quoc, and Fetzer, "Towards Formalization of EPID-based Remote Attestation in Intel SGX", 2020.

[5] Sardar, Faqeh, and Fetzer, "Formal Foundations for Intel SGX Data Center Attestation Primitives", 2020.

[6] Sardar, Musaev, and Fetzer, "Demystifying Attestation in Intel Trust Domain Extensions via Formal Verification", 2021.

[7] Antonino, Derek, and Woloszyn, *Flexible remote attestation of pre-SNP SEV VMs using SGX enclaves*, 2023.

Related Work

- Intel SGX EPID[4]
- Intel SGX DCAP[5] (Presented at HotSoS'21)

[4] Sardar, Quoc, and Fetzer, "Towards Formalization of EPID-based Remote Attestation in Intel SGX", 2020.

[5] Sardar, Faqeh, and Fetzer, "Formal Foundations for Intel SGX Data Center Attestation Primitives", 2020.

[6] Sardar, Musaev, and Fetzer, "Demystifying Attestation in Intel Trust Domain Extensions via Formal Verification", 2021.

[7] Antonino, Derek, and Woloszyn, *Flexible remote attestation of pre-SNP SEV VMs using SGX enclaves*, 2023.

Related Work

- Intel SGX EPID[4]
- Intel SGX DCAP[5] (Presented at HotSoS'21)
- Intel TDX[6] (Presented at HotSoS'22)

[4] Sardar, Quoc, and Fetzer, "Towards Formalization of EPID-based Remote Attestation in Intel SGX", 2020.

[5] Sardar, Faqeh, and Fetzer, "Formal Foundations for Intel SGX Data Center Attestation Primitives", 2020.

[6] Sardar, Musaev, and Fetzer, "Demystifying Attestation in Intel Trust Domain Extensions via Formal Verification", 2021.

[7] Antonino, Derek, and Woloszyn, *Flexible remote attestation of pre-SNP SEV VMs using SGX enclaves*, 2023.

Related Work

- Intel SGX EPID[4]
- Intel SGX DCAP[5] (Presented at HotSoS'21)
- Intel TDX[6] (Presented at HotSoS'22)
- Intel SGX and AMD SEV[7]

[4] Sardar, Quoc, and Fetzer, "Towards Formalization of EPID-based Remote Attestation in Intel SGX", 2020.

[5] Sardar, Faqeh, and Fetzer, "Formal Foundations for Intel SGX Data Center Attestation Primitives", 2020.

[6] Sardar, Musaev, and Fetzer, "Demystifying Attestation in Intel Trust Domain Extensions via Formal Verification", 2021.

[7] Antonino, Derek, and Woloszyn, *Flexible remote attestation of pre-SNP SEV VMs using SGX enclaves*, 2023.

Contributions

- Most detailed formal model of Intel TDX attestation

Contributions

- Most detailed formal model of Intel TDX attestation
  - Success of FM is how close the model is to reality!

Contributions

- Most detailed formal model of Intel TDX attestation
  - Success of FM is how close the model is to reality!
- Formal proof of insecurity of Intel's claimed TCB

Contributions

- Most detailed formal model of Intel TDX attestation
  - Success of FM is how close the model is to reality!
- Formal proof of insecurity of Intel's claimed TCB
- First formal analysis of Arm CCA attestation

Contributions

- Most detailed formal model of Intel TDX attestation
  - Success of FM is how close the model is to reality!
- Formal proof of insecurity of Intel's claimed TCB
- First formal analysis of Arm CCA attestation
  - Presented at HotSoS'23

Agenda

Formal Verification

$$System \models Property \tag{1}$$

Formal Verification

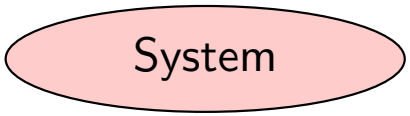
$$System \models Property \tag{1}$$

$$Protocol \parallel Adversary \models Property \tag{2}$$

Formal Verification

$$System \models Property \tag{1}$$

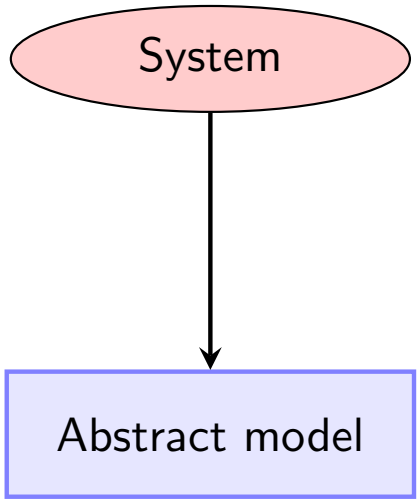
$$Protocol \parallel Adversary \models Property \tag{2}$$



Formal Verification

$$System \models Property \tag{1}$$

$$Protocol \parallel Adversary \models Property \tag{2}$$



Formal Verification

$$System \models Property \tag{1}$$

$$Protocol \parallel Adversary \models Property \tag{2}$$

Formal Verification

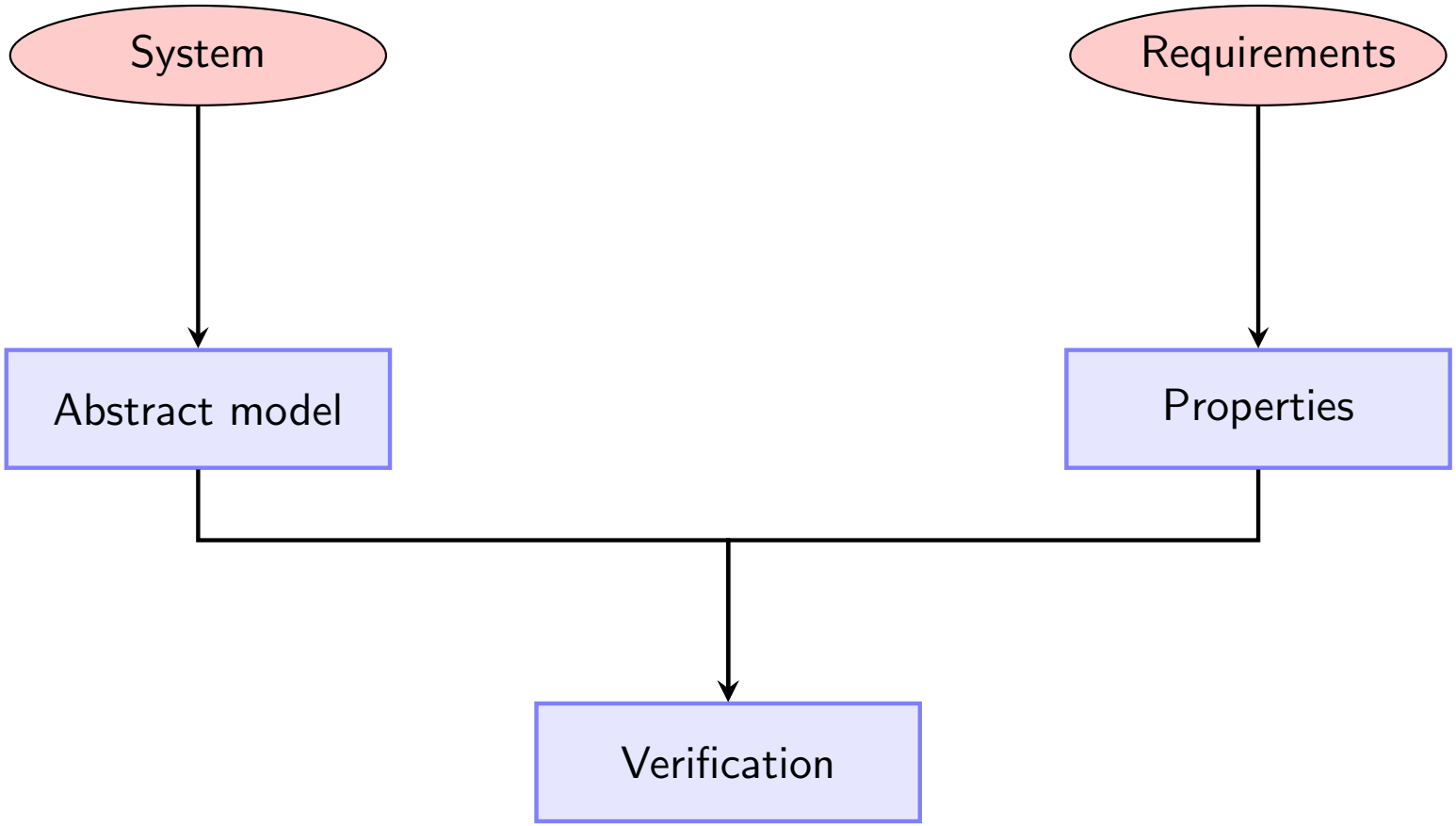
$$System \models Property \tag{1}$$

$$Protocol \parallel Adversary \models Property \tag{2}$$

Formal Verification

$$System \models Property \tag{1}$$

$$Protocol \parallel Adversary \models Property \tag{2}$$



Agenda

2. Approach
   - Model
   - Properties

Challenge 1: Incomplete specs[8]

Wan_Intel
Moderator
09-18-2023 • 07:57 PM • 656Aufrufe

Hello UsamaS,

I've checked with the relevant team.

The "internal specs" that we've mentioned in the thread above are part of an internal document used by our developers and it would not be relevant to customers. Sorry for the inconvenience and thank you for your support.

Regards,

Wan

[8] https://community.intel.com/t5/Intel-Software-Guard-Extensions/Missing-specification-documents-for-TDX/m-p/1527218

Challenge 2: Vague and outdated specs[9]

Peh_Intel 09-14-2023 • 06:04 PM • 397Aufrufe
Moderator

Hi UsamaS,

Thanks for your patience. I just received the updates as follow.

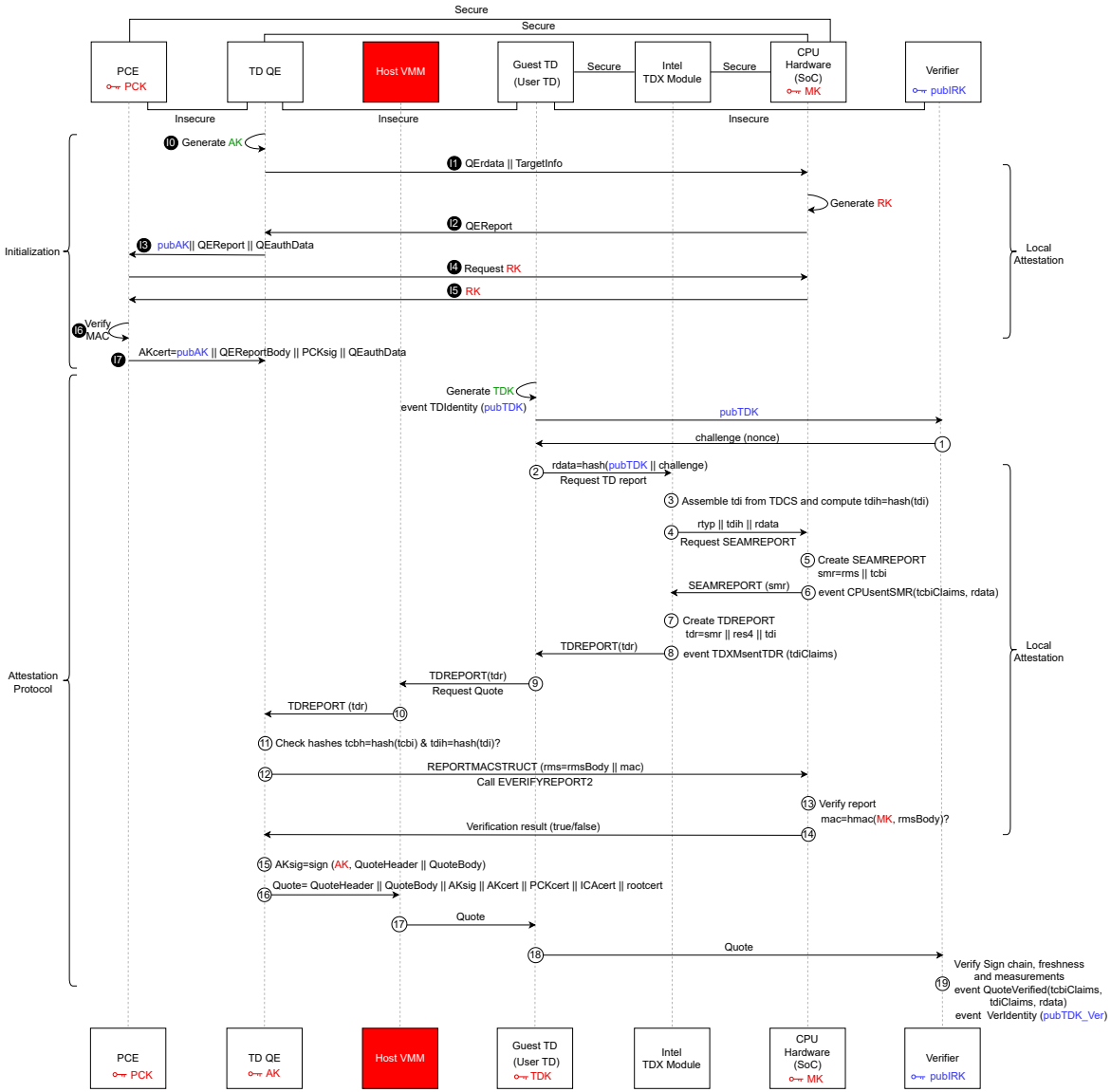
This index 1 SVN is the TDX Module major version. Originally, there was only 1 TDX 1.0 module, so the SVN had to match. Now that we have TDX 1.5 coming, it has a new major version, so the logic has to change, and those steps will also. The API doc will be updated soon to reflect this.

Regards,

Peh

[9] `https://community.intel.com/t5/Intel-Software-Guard-Extensions/index-1-in-tdxtcbcomponents/m-p/1520194`

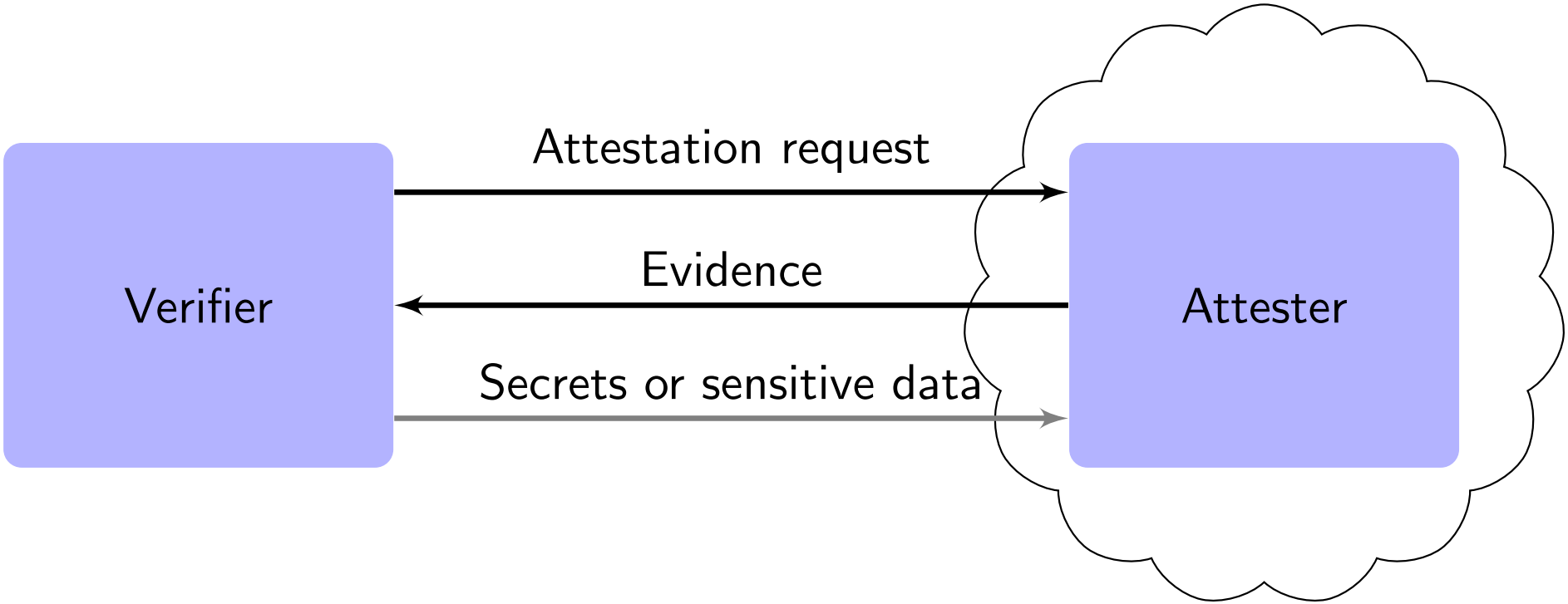
TDX Model with Initialization Phase (PCE)



Agenda

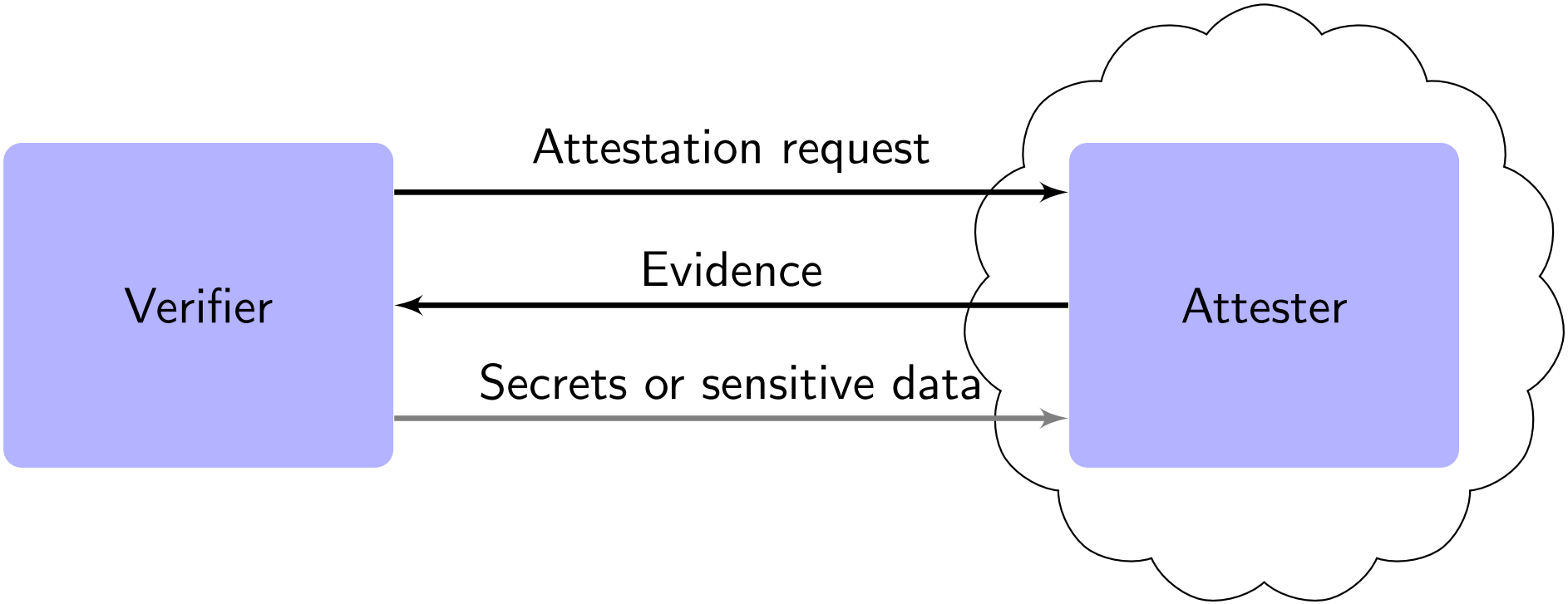
2. Approach
   - Model
   - Properties

Properties



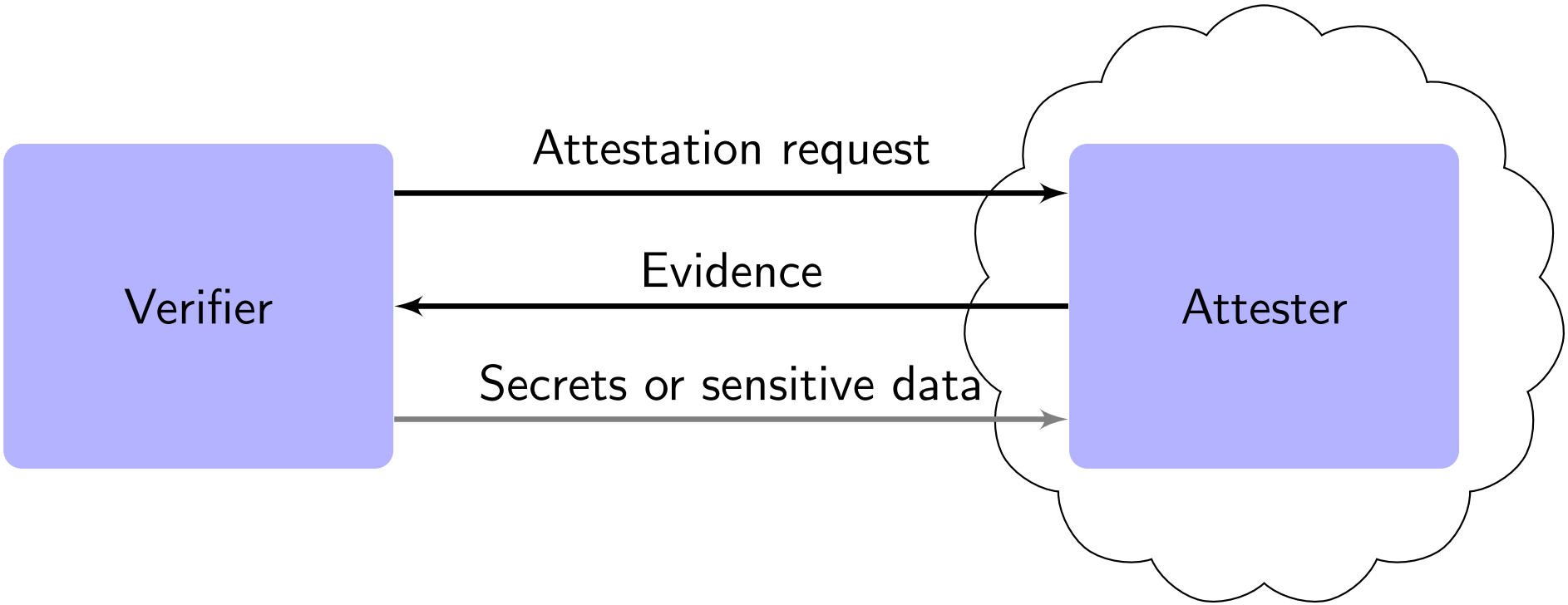
- Sanity checks

Properties



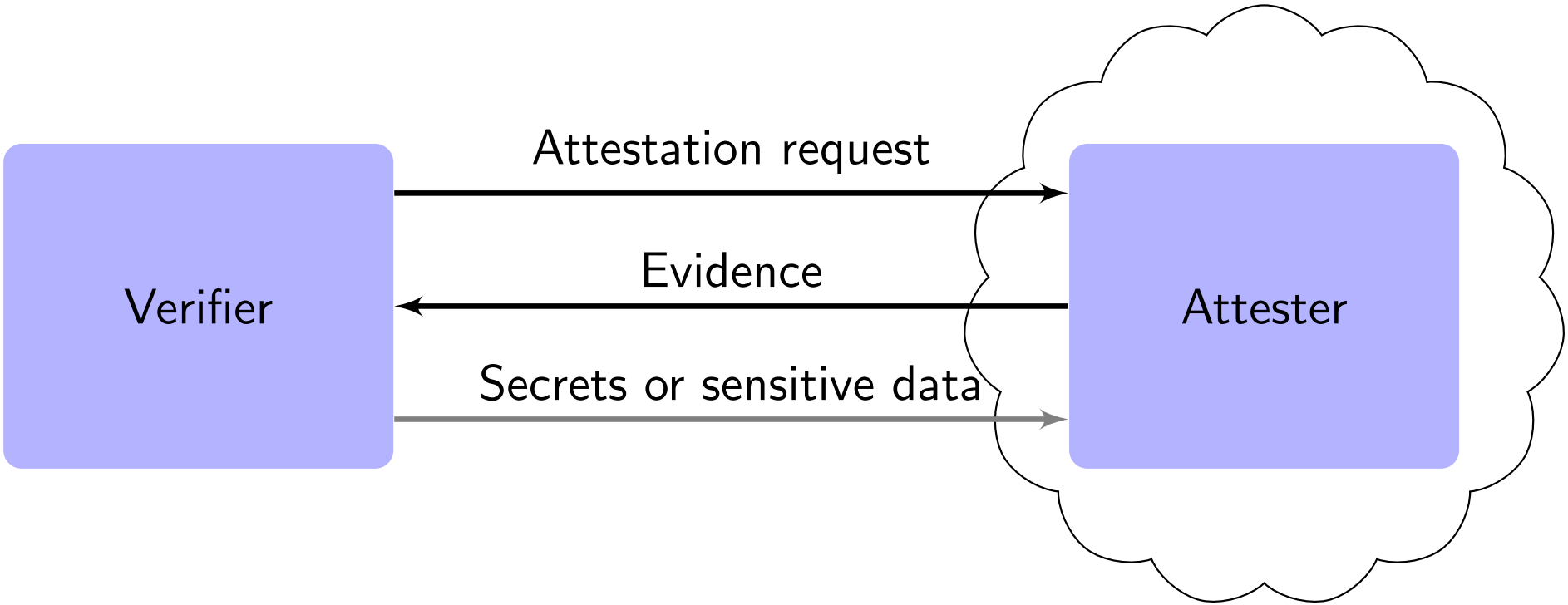
- Sanity checks
- Integrity of Evidence

Properties



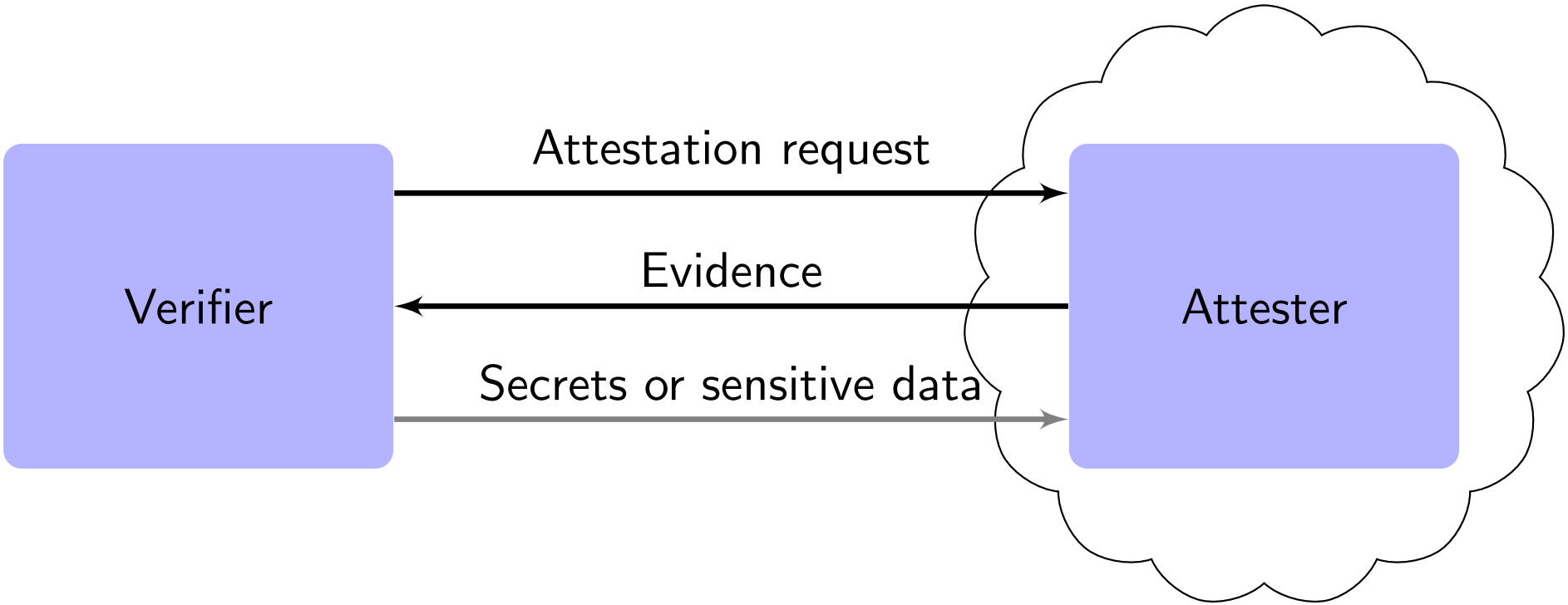
- Sanity checks
- Integrity of Evidence
- Freshness of Evidence

Properties



- Sanity checks
- Integrity of Evidence
- Freshness of Evidence
- Confidentiality/Secrecy of attestation-related keys

Properties



- Sanity checks
- Integrity of Evidence
- Freshness of Evidence
- Confidentiality/Secrecy of attestation-related keys
- Attester Authentication

Agenda

TCB Claimed by Intel[10]

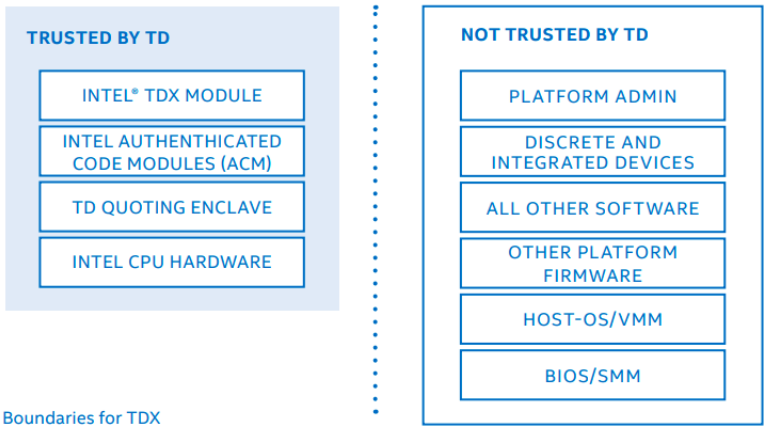
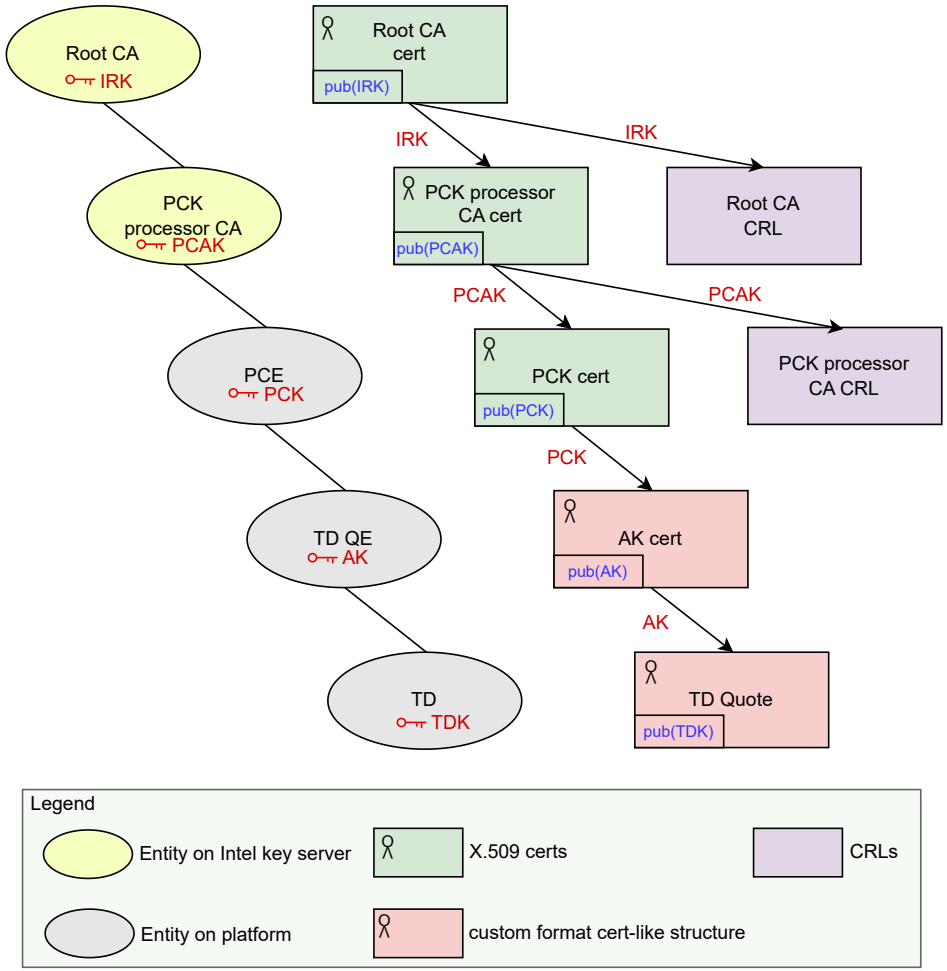


Figure 5.1. Trust Boundaries for TDX



[10] Intel, *Intel ® Trust Domain Extensions*, 2021.

Verification Summary

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

```
------------------------------------------------------------
Verification summary:

Query not event(AKverified(pubAK_1)) is false.

Query not event(CPUsentSMR(tcbiClaims_1,rdata_1)) is false.

Query not event(TDXMsentTDR(tdiClaims_1)) is false.

Query not event(QuoteVerified(tcbiClaims_1,tdiClaims_1,rdata_1)) is false.

Query not (event(TDidentity(pubTDK_1)) && event(VerIdentity(pubTDK_Ver_1))) is false.

Query event(AKverified(pubAK_1)) ==> event(AKsent(pubAK_1)) is true.

Query event(QuoteVerified(tcbiClaims_1,tdiClaims_1,rdata_1)) ==> event(CPUsentSMR(tcbiClaims_1,rdata_1)) is false.

Query event(QuoteVerified(tcbiClaims_1,tdiClaims_1,rdata_1)) ==> event(TDXMsentTDR(tdiClaims_1)) is false.

Query inj-event(QuoteVerified(tcbiClaims_1,tdiClaims_1,rdata_1)) ==> inj-event(CPUsentSMR(tcbiClaims_1,rdata_1)) is false.

Query inj-event(QuoteVerified(tcbiClaims_1,tdiClaims_1,rdata_1)) ==> inj-event(TDXMsentTDR(tdiClaims_1)) is false.

Query secret PCK_1,PCK is false.

Query secret PCAK is true.

Query secret AK_2,AK_1,AK is true.

Query secret MK_1,MK is true.

Query event(AKverified(pubAK_PCE_1)) && event(AKsent(pubAK_1)) ==> pubAK_PCE_1 = pubAK_1 is true.

Query event(VerIdentity(pubTDK_Ver_1)) && event(TDidentity(pubTDK_1)) ==> pubTDK_1 = pubTDK_Ver_1 is false.

------------------------------------------------------------


real    0m55,648s
user    0m55,432s
sys     0m0,132s
```

Reported to Intel[12] and Fixed[13]

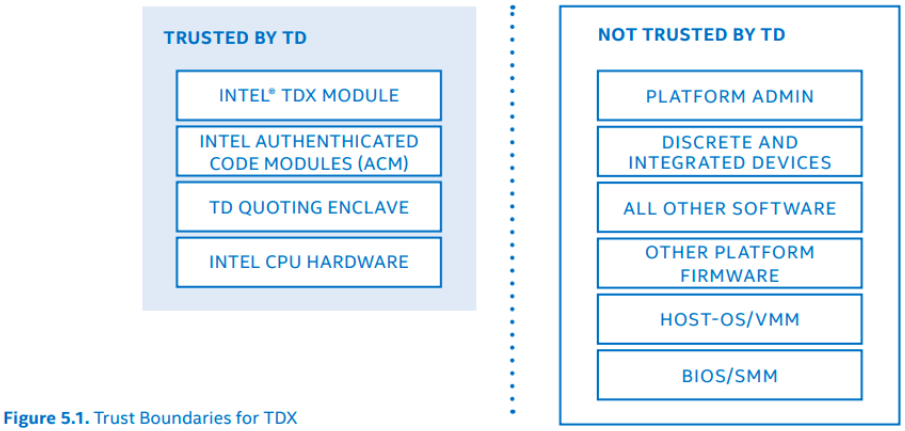


Figure 5.1. Trust Boundaries for TDX

Figure: Old

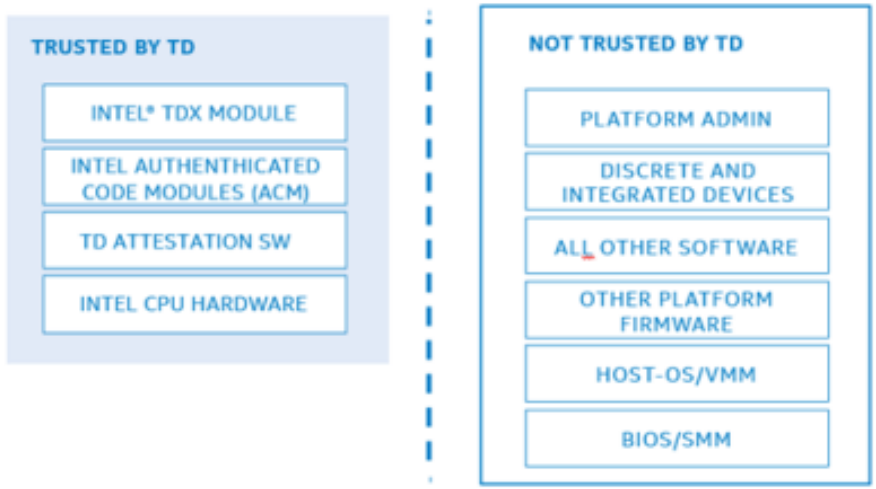


Figure 1 Trust Boundaries for TDX

Figure: Updated

[11] Sardar, *Full transparency of Intel TDX Specifications*, 2023.

[12] Intel, *Intel ® Trust Domain Extensions*, 2021.

[13] Intel, *Intel ® Trust Domain Extensions*, 2023.

Reported to Intel[12] and Fixed[13]

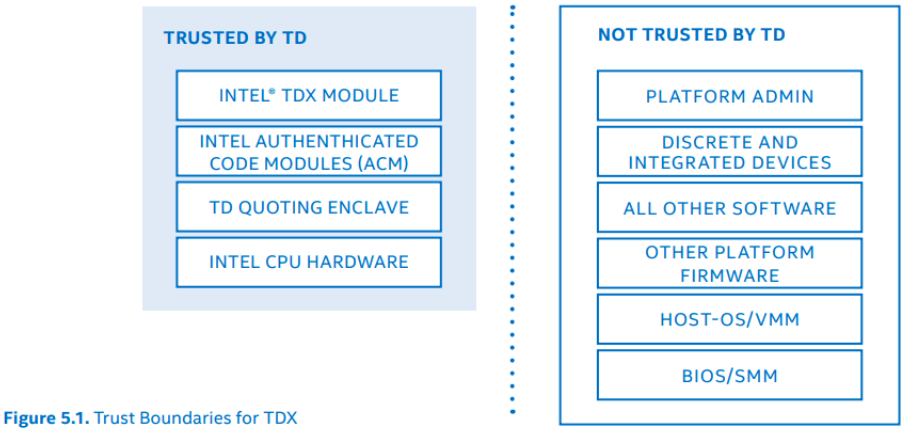


Figure: Old

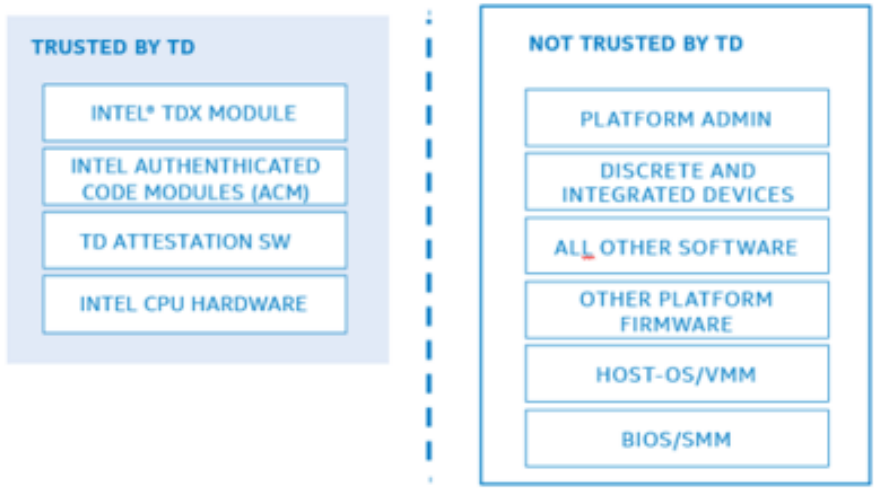


Figure: Updated

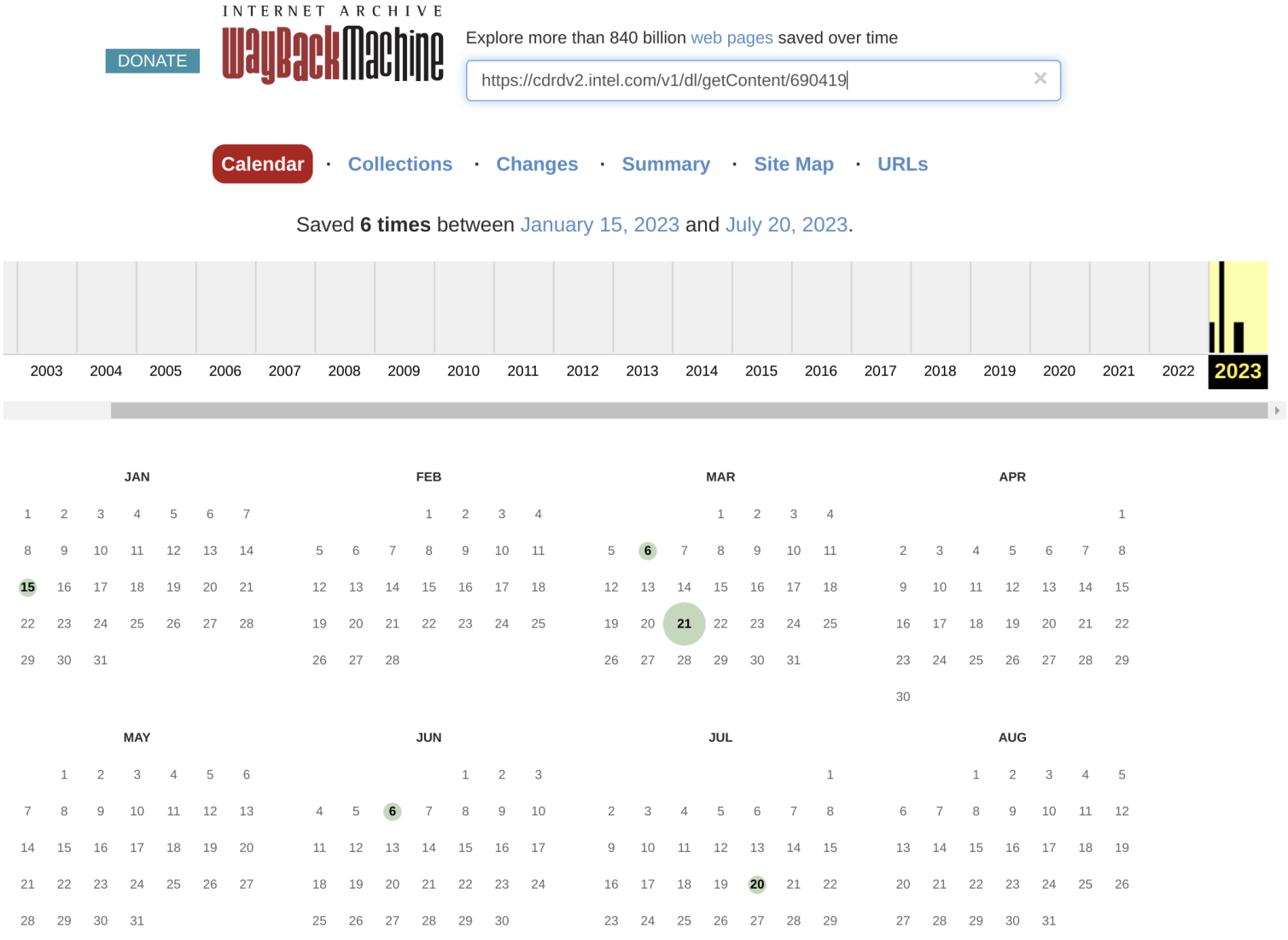
- Warning: on same URL replacing the old white paper: Reported to Intel privately and publicly[11]

[11] Sardar, *Full transparency of Intel TDX Specifications*, 2023.

[12] Intel, *Intel ® Trust Domain Extensions*, 2021.

[13] Intel, *Intel ® Trust Domain Extensions*, 2023.

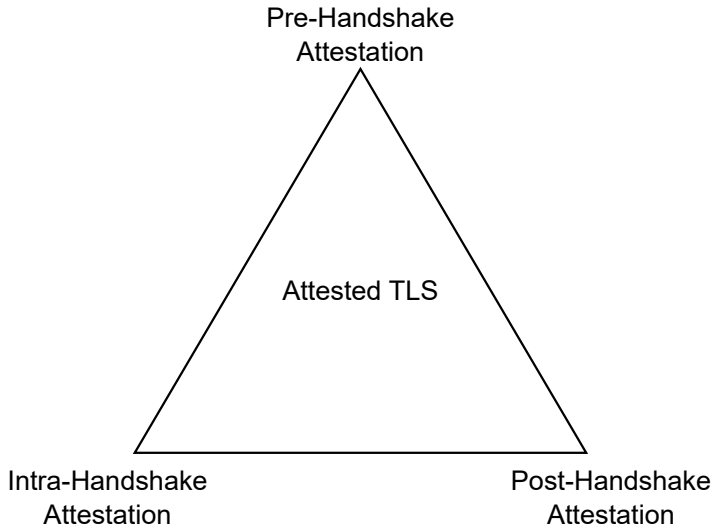
Evidence[14]



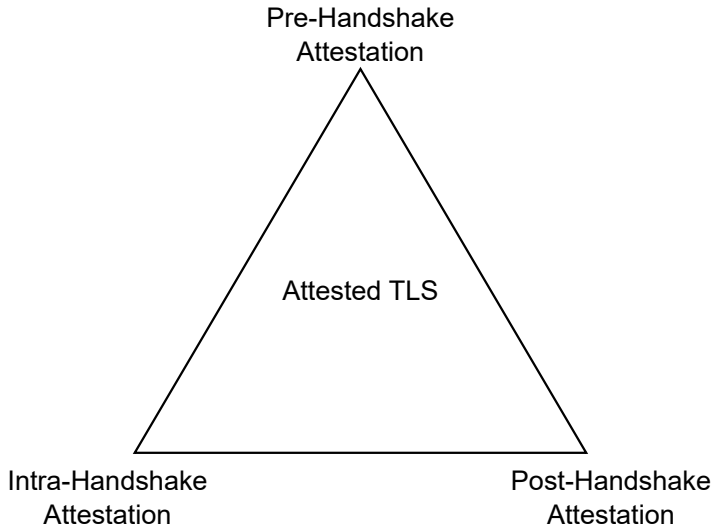
[14] https://web.archive.org/web/20230000000000*/https://cdrdv2.intel.com/v1/dl/getContent/690419

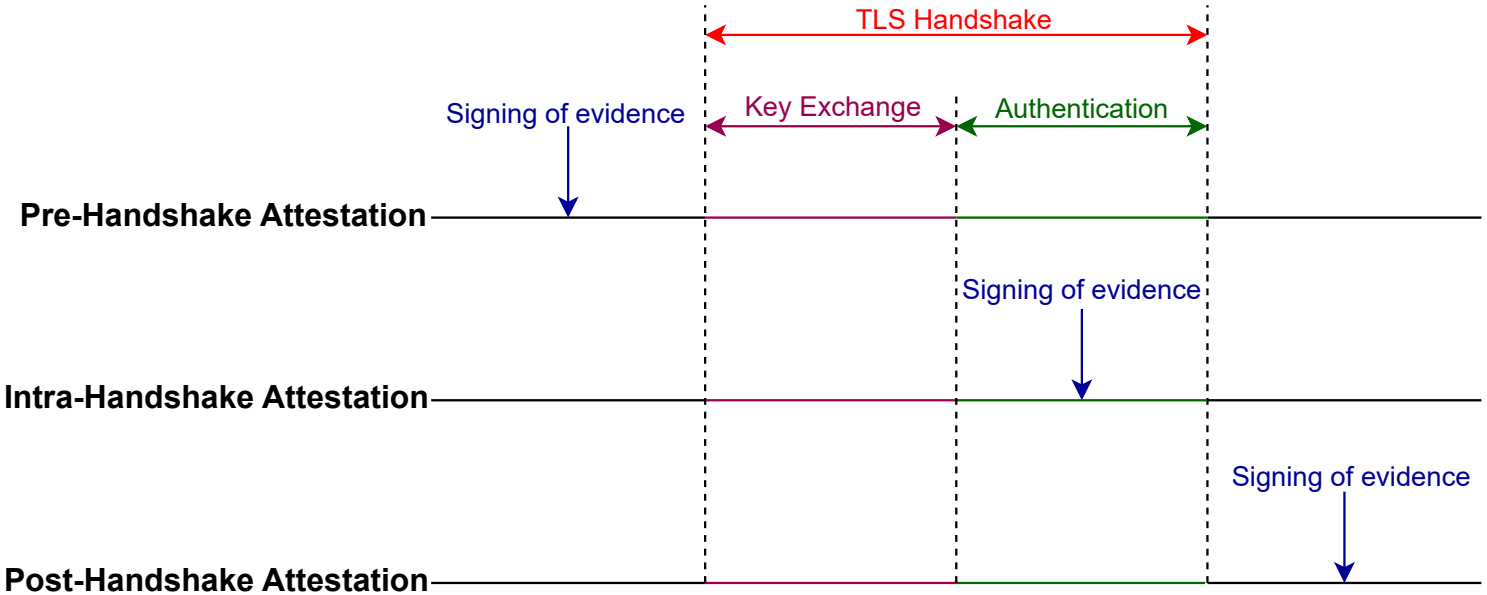
Agenda

Attested TLS



Attested TLS





"Rollercoaster"

- Incomplete and outdated specs for RA-TLS[15]

[15] Knauth et al., *Integrating Remote Attestation with Transport Layer Security*, 2018.

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

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

"Rollercoaster"

- Incomplete and outdated specs for RA-TLS[15]
  - Specs based on TLS 1.2 (TLS 1.3 is RFC since Aug 2018)

[15] Knauth et al., *Integrating Remote Attestation with Transport Layer Security*, 2018.

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

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

"Rollercoaster"

- Incomplete and outdated specs for RA-TLS[15]
  - Specs based on TLS 1.2 (TLS 1.3 is RFC since Aug 2018)
  - Fix: Used implementation and community input for formal model

[15] Knauth et al., *Integrating Remote Attestation with Transport Layer Security*, 2018.

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

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

"Rollercoaster"

- Incomplete and outdated specs for RA-TLS[15]
  - 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 model[16]

[15] Knauth et al., *Integrating Remote Attestation with Transport Layer Security*, 2018.

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

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

"Rollercoaster"

- Incomplete and outdated specs for RA-TLS[15]
  - 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 model[16]
  - Literally no comments at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!

[15] Knauth et al., *Integrating Remote Attestation with Transport Layer Security*, 2018.

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

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

"Rollercoaster"

- Incomplete and outdated specs for RA-TLS[15]
  - 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 model[16]
  - Literally no comments at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
- Incomplete validation of draft 20 artifacts[17]

[15] Knauth et al., *Integrating Remote Attestation with Transport Layer Security*, 2018.

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

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

"Rollercoaster"

- Incomplete and outdated specs for RA-TLS[15]
  - 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 model[16]
  - Literally no comments at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
- Incomplete validation of draft 20 artifacts[17]
  - Fix: Designed an automated validation framework for key schedule

[15] Knauth et al., *Integrating Remote Attestation with Transport Layer Security*, 2018.

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

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

"Rollercoaster"

- Incomplete and outdated specs for RA-TLS[15]
  - 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 model[16]
  - Literally no comments at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
- Incomplete validation of draft 20 artifacts[17]
  - Fix: Designed an automated validation framework for key schedule
- A simple extension made the artifacts running for 1 month on high-end server (icelake)

[15] Knauth et al., *Integrating Remote Attestation with Transport Layer Security*, 2018.

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

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

"Rollercoaster"

- Incomplete and outdated specs for RA-TLS[15]
  - 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 model[16]
  - Literally no comments at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
- Incomplete validation of draft 20 artifacts[17]
  - 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

[15] Knauth et al., *Integrating Remote Attestation with Transport Layer Security*, 2018.

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

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

"Rollercoaster"

- Incomplete and outdated specs for RA-TLS[15]
  - 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 model[16]
  - Literally no comments at all in main processes (such as Client12, Server12, Client13, Server13, appData, channelBindingQuery and secrecyQuery)!
- Incomplete validation of draft 20 artifacts[17]
  - 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

[15] Knauth et al., *Integrating Remote Attestation with Transport Layer Security*, 2018.

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

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

Community input

- Paper authors[18]
  - Bruno Blanchet
  - Karthikeyan Bhargavan
  - Nadim Kobeissi
- LURK[19] authors
- IETF TLS WG[20]
- IRTF UFMRG chairs
- CCC attestation SIG[21]
- ...
- IETF 119 Hackathon[22]
- IRTF Crypto Forum RG @ IETF 119[23]

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

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

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

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

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

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

Outline

Take-home

- Formal proof is as good as the formal model!

Take-home

- Formal proof is as good as the formal model!
- Formal proof of insecurity of Intel's claimed TCB

Take-home

- Formal proof is as good as the formal model!
- Formal proof of insecurity of Intel's claimed TCB
- Arch-def attestation does not provide strong authentication property (see paper)

Take-home

- Formal proof is as good as the formal model!
- Formal proof of insecurity of Intel's claimed TCB
- Arch-def attestation does not provide strong authentication property (see paper)
- Validation of formal model is crucial!

Take-home

- Formal proof is as good as the formal model!
- Formal proof of insecurity of Intel's claimed TCB
- Arch-def attestation does not provide strong authentication property (see paper)
- Validation of formal model is crucial!
- Open question: security of attested TLS

Key References I

Antonino, Pedro, Ante Derek, and Wojciech Aleksander Woloszyn. *Flexible remote attestation of pre-SNP SEV VMs using SGX enclaves*. 2023. URL: https://arxiv.org/pdf/2305.09351.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.

Intel. *Intel ® Trust Domain Extensions*. Aug. 2021. URL: https://cdrdv2.intel.com/v1/dl/getContent/690419.

— .*Intel ® Trust Domain Extensions*. Feb. 2023. URL: https://cdrdv2.intel.com/v1/dl/getContent/690419.

Knauth, T. et al. *Integrating Remote Attestation with Transport Layer Security*. Tech. rep. Intel Labs, 2018. URL: https://arxiv.org/abs/1801.05863.

Sardar, Muhammad Usama. *Full transparency of Intel TDX Specifications*. 2023. URL: https://lists.confidentialcomputing.io/g/attestation/topic/full_transparency_of_intel/99387880 (visited on 06/18/2023).

Sardar, Muhammad Usama, Rasha Faqeh, and Christof Fetzer. "Formal Foundations for Intel SGX Data Center Attestation Primitives". In: *Formal Methods and Software Engineering*. Ed. by Shang-Wei Lin, Zhe Hou, and Brendan Mahoney. Cham: Springer International Publishing, 2020, pp. 268–283. ISBN: 978-3-030-63406-3. DOI: 10.1007/978-3-030-63406-3_16.

Sardar, Muhammad Usama and Christof Fetzer. "Confidential computing and related technologies: a critical review". In: *Cybersecurity* 6.1 (May 2023), p. 10. ISSN: 2523-3246. DOI: 10.1186/s42400-023-00144-1. URL: https://cybersecurity.springeropen.com/articles/10.1186/s42400-023-00144-1.

Key References II

Sardar, Muhammad Usama, Thomas Fossati, et al. *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.

Sardar, Muhammad Usama, Saidgani Musaev, and Christof Fetzer. "Demystifying Attestation in Intel Trust Domain Extensions via Formal Verification". In: *IEEE Access* (2021). URL: https://www.researchgate.net/publication/351699567_Demystifying_Attestation_in_Intel_Trust_Domain_Extensions_via_Formal_Verification.

Sardar, Muhammad Usama, Do Le Quoc, and Christof Fetzer. "Towards Formalization of EPID-based Remote Attestation in Intel SGX". In: *Euromicro Conference on Digital System Design*. 2020, pp. 604–607. DOI: 10.1109/DSD51259.2020.00099.

Wired. *Intel Let Google Cloud Hack Its New Secure Chips and Found 10 Bugs*. 2023. URL: https://www.wired.com/story/intel-google-cloud-chip-security/ (visited on 04/25/2023).

Call to Action

- Bring your expertise: https://github.com/CCC-Attestation/formal-spec-TEE
- Additional information: link here[24]

[24] Sardar, Fossati, et al., *Formal Specification and Verification of Architecturally-defined Attestation Mechanisms in Arm CCA and Intel TDX*, 2023.