SoK: Attestation in Confidential Computing

Muhammad Usama Sardar[1] Thomas Fossati[2] Simon Frost[2]

[1]TU Dresden

[2]Arm Ltd.

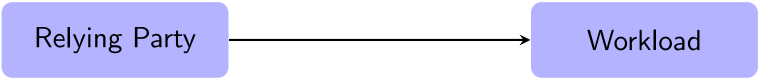
March 29, 2023

Outline

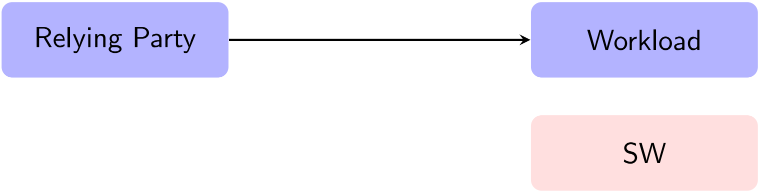
Confidential Computing

Relying Party

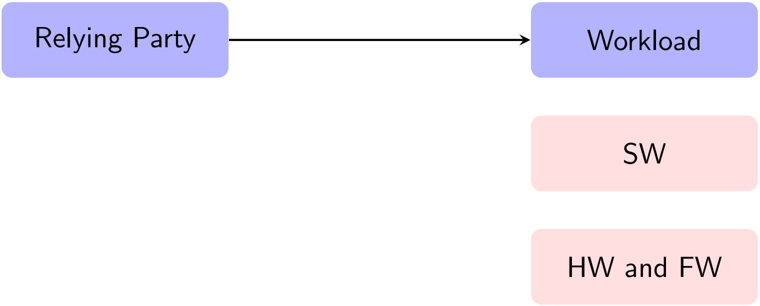
Confidential Computing



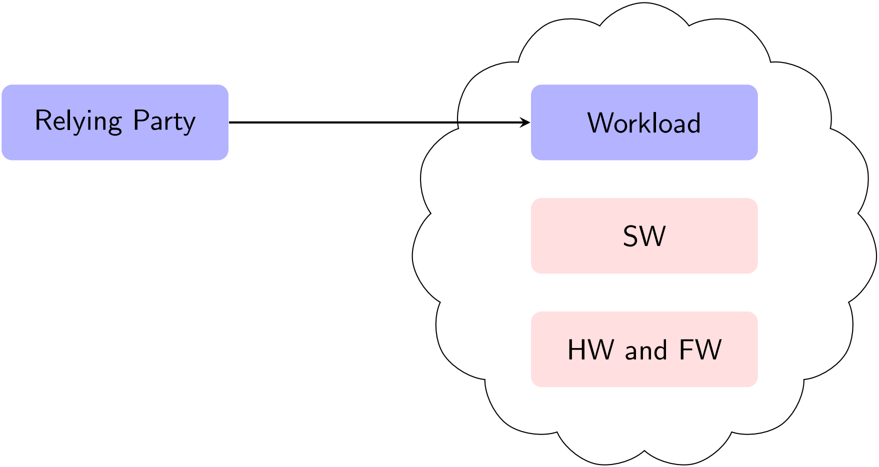
Confidential Computing



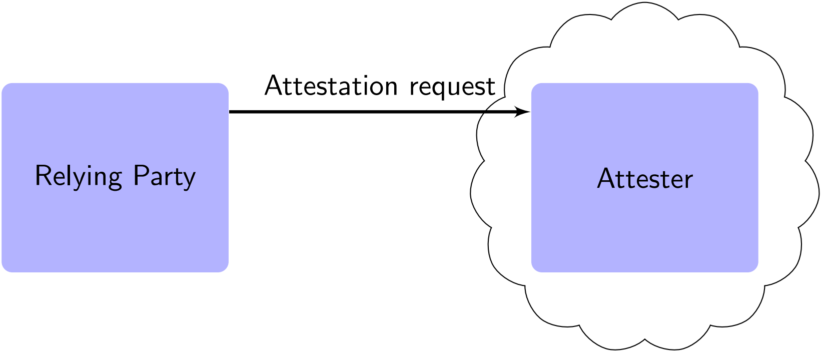
Confidential Computing



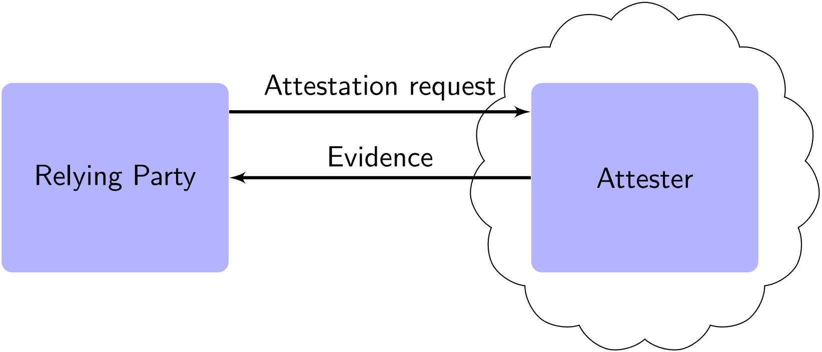
Confidential Computing



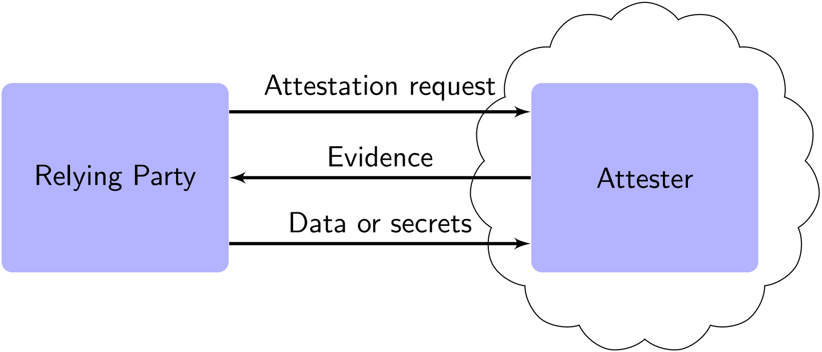
Attestation



Attestation



Attestation



Problem Statement

Holistic view of attestation

Problem Statement

Holistic view of attestation

TEE-agnostic attestation architecture

Problem Statement

Holistic view of attestation

TEE-agnostic attestation architecture

Mappings to attestation architecture

Problem Statement

Holistic view of attestation

TEE-agnostic attestation architecture

Mappings to attestation architecture

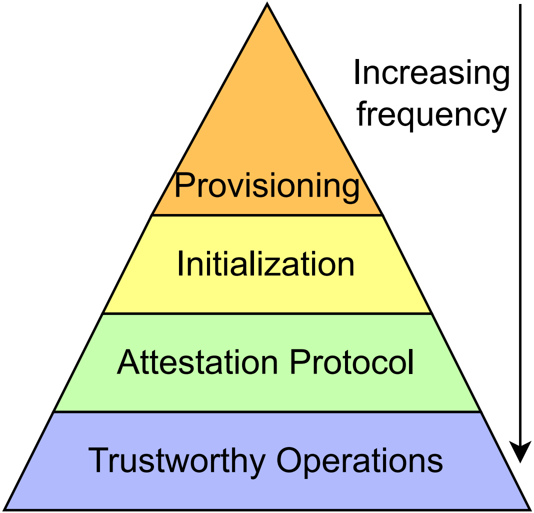
Formal specs

Outline

Outline

2. Contributions
   - Holistic View
   - TEE-agnostic Architecture
   - Mappings
   - Formal Specs
   - Design and Security Issues: TDX
   - Design and Security Issues: SCONE

Holistic View of Attestation



Outline

2 Contributions
- Holistic View
- TEE-agnostic Architecture
- Mappings
- Formal Specs
- Design and Security Issues: TDX
- Design and Security Issues: SCONE

Attestation Architecture

- Limitations of RATS[1]

[1] Birkholz et al., *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Attestation Architecture

- Limitations of RATS[1]
  - Local attestation out of scope (cannot express Intel's attestation mechanisms)

[1] Birkholz et al., *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Attestation Architecture

- Limitations of RATS[1]
  - Local attestation out of scope (cannot express Intel's attestation mechanisms)
  - Cannot express anonymous attestation (Intel EPID)

[1] Birkholz et al., *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Attestation Architecture

- Limitations of RATS[1]
  - Local attestation out of scope (cannot express Intel's attestation mechanisms)
  - Cannot express anonymous attestation (Intel EPID)
  - Various ambiguities, e.g., role vs. entity

[1] Birkholz et al., *Remote ATtestation procedureS (RATS) Architecture*, 2023.

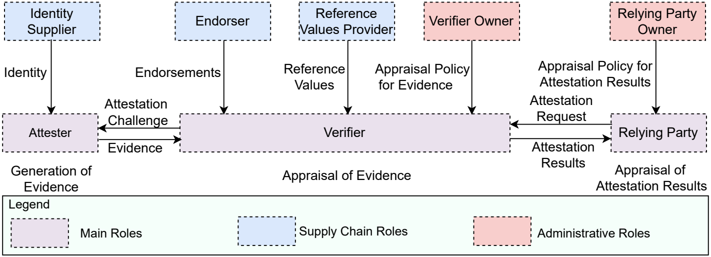
Attestation Architecture

- Limitations of RATS[1]
  - Local attestation out of scope (cannot express Intel's attestation mechanisms)
  - Cannot express anonymous attestation (Intel EPID)
  - Various ambiguities, e.g., role vs. entity
- Errata submitted for RATS

[1] Birkholz et al., *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Attestation Architecture

- Limitations of RATS[1]
  - Local attestation out of scope (cannot express Intel's attestation mechanisms)
  - Cannot express anonymous attestation (Intel EPID)
  - Various ambiguities, e.g., role vs. entity
- Errata submitted for RATS
- TEE-agnostic architecture

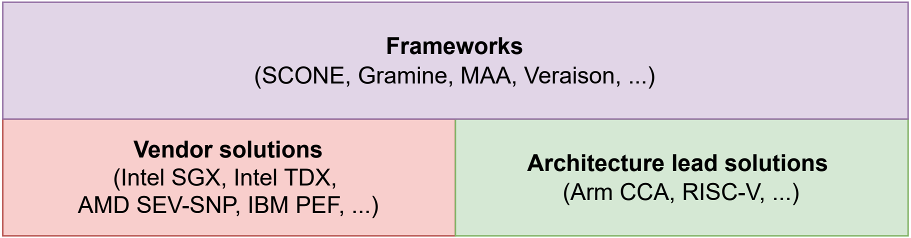


[1] Birkholz et al., *Remote ATtestation procedureS (RATS) Architecture*, 2023.

Outline

2. Contributions
   - Holistic View
   - TEE-agnostic Architecture
   - Mappings
   - Formal Specs
   - Design and Security Issues: TDX
   - Design and Security Issues: SCONE

Main Groups for Attestation



Overview of Related Work

Related work				
IETF RATS[2]				
Ménétrey et al.[3,4]				
Niemi et al.[5]				

[2] Birkholz et al., *Remote ATtestation procedureS (RATS) Architecture*, 2023.

[3] Ménétrey, Göttel, Pasin, et al., "An Exploratory Study of Attestation Mechanisms for Trusted Execution Environments", 2022.

[4] Ménétrey, Göttel, Khurshid, et al., "Attestation Mechanisms for Trusted Execution Environments Demystified", 2022.

[5] Niemi, Sovio, and Ekberg, "Towards Interoperable Enclave Attestation: Learnings from Decades of Academic Work", 2022.

Overview of Related Work

Related work	Architecture			
IETF RATS[2]	Co-developed with DICE[3]			
Ménétrey et al.[4,5]	Use RATS			
Niemi et al.[6]	Adapted from RATS			

[2] Birkholz et al., *Remote ATtestation procedureS (RATS) Architecture*, 2023.

[3] Trusted Computing Group, *DICE Attestation Architecture*, 2021.

[4] Ménétrey, Göttel, Pasin, et al., "An Exploratory Study of Attestation Mechanisms for Trusted Execution Environments", 2022.

[5] Ménétrey, Göttel, Khurshid, et al., "Attestation Mechanisms for Trusted Execution Environments Demystified", 2022.

[6] Niemi, Sovio, and Ekberg, "Towards Interoperable Enclave Attestation: Learnings from Decades of Academic Work", 2022.

Overview of Related Work

Related work	Architecture	Mapping to group 1		
IETF RATS[2]	Co-developed with DICE[3]	No		
Ménétrey et al.[4,5]	Use RATS	Inaccurate for SGX		
Niemi et al.[6]	Adapted from RATS	Very high level for SGX		

[2] Birkholz et al., *Remote ATtestation procedureS (RATS) Architecture*, 2023.

[3] Trusted Computing Group, *DICE Attestation Architecture*, 2021.

[4] Ménétrey, Göttel, Pasin, et al., "An Exploratory Study of Attestation Mechanisms for Trusted Execution Environments", 2022.

[5] Ménétrey, Göttel, Khurshid, et al., "Attestation Mechanisms for Trusted Execution Environments Demystified", 2022.

[6] Niemi, Sovio, and Ekberg, "Towards Interoperable Enclave Attestation: Learnings from Decades of Academic Work", 2022.

Overview of Related Work

Related work	Architecture	Mapping to group 1	Mapping to group 2	
IETF RATS[2]	Co-developed with DICE[3]	No	No	
Ménétrey et al.[4,5]	Use RATS	Inaccurate for SGX	No	
Niemi et al.[6]	Adapted from RATS	Very high level for SGX	High level summary for CCA	

[2] Birkholz et al., *Remote ATtestation procedureS (RATS) Architecture*, 2023.

[3] Trusted Computing Group, *DICE Attestation Architecture*, 2021.

[4] Ménétrey, Göttel, Pasin, et al., "An Exploratory Study of Attestation Mechanisms for Trusted Execution Environments", 2022.

[5] Ménétrey, Göttel, Khurshid, et al., "Attestation Mechanisms for Trusted Execution Environments Demystified", 2022.

[6] Niemi, Sovio, and Ekberg, "Towards Interoperable Enclave Attestation: Learnings from Decades of Academic Work", 2022.

Overview of Related Work

Related work	Architecture	Mapping to group 1	Mapping to group 2	Mapping to group 3
IETF RATS[2]	Co-developed with DICE[3]	No	No	No
Ménétrey et al.[4,5]	Use RATS	Inaccurate for SGX	No	No
Niemi et al.[6]	Adapted from RATS	Very high level for SGX	High level summary for CCA	No

[2] Birkholz et al., *Remote ATtestation procedureS (RATS) Architecture*, 2023.

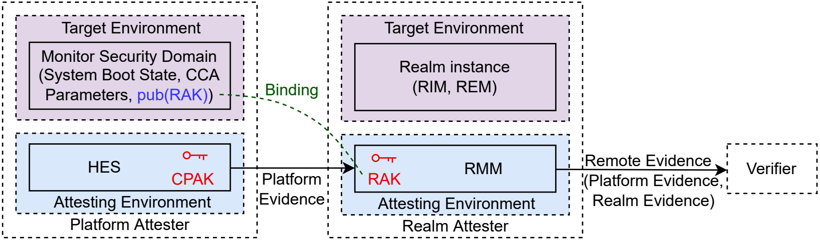
[3] Trusted Computing Group, *DICE Attestation Architecture*, 2021.

[4] Ménétrey, Göttel, Pasin, et al., "An Exploratory Study of Attestation Mechanisms for Trusted Execution Environments", 2022.

[5] Ménétrey, Göttel, Khurshid, et al., "Attestation Mechanisms for Trusted Execution Environments Demystified", 2022.

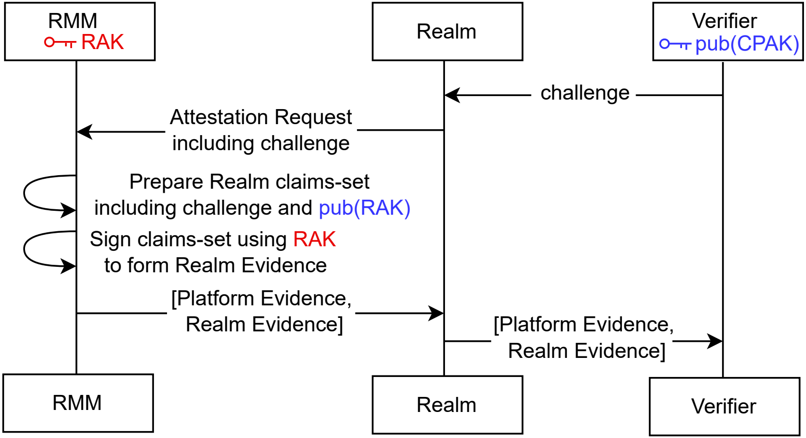
[6] Niemi, Sovio, and Ekberg, "Towards Interoperable Enclave Attestation: Learnings from Decades of Academic Work", 2022.

Arm CCA Attestation Architecture Overview



Outline

Arm CCA Evidence Generation



Formal Analysis in ProVerif

- Assumptions
  - Verifier has preconfigured pub(CPAK) for signature verification
  - Secure channel between HES and RMM to transport the RAK key pair
- Integrity of Platform and Realm Evidence

$$\texttt{query } \mathit{data} : \mathit{bitstring} \,; \quad \texttt{event } (\mathit{accepted}(\mathit{data})) \texttt{ ==> } \texttt{inj-event } (\mathit{sent}(\mathit{data})). \tag{1}$$

Outline

2. Contributions
   - Holistic View
   - TEE-agnostic Architecture
   - Mappings
   - Formal Specs
   - Design and Security Issues: TDX
   - Design and Security Issues: SCONE

Claimed TCB

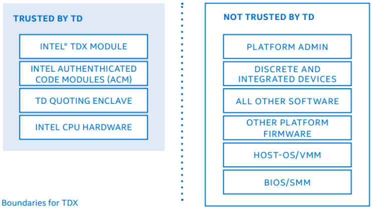
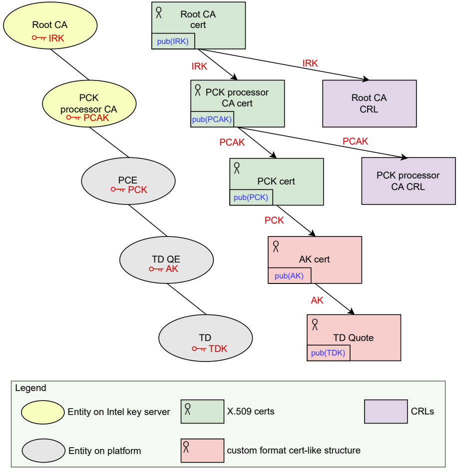


Figure 5.1. Trust Boundaries for TDX



TCB Fixed

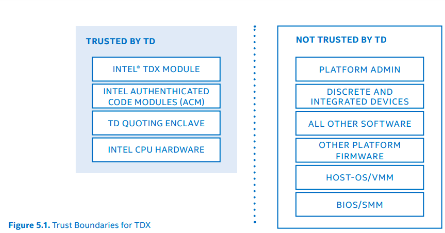


Figure: Old

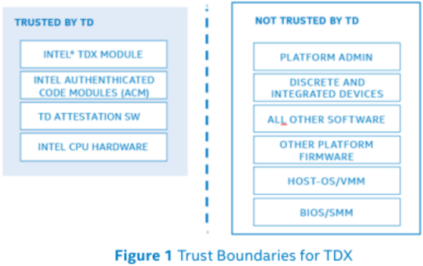
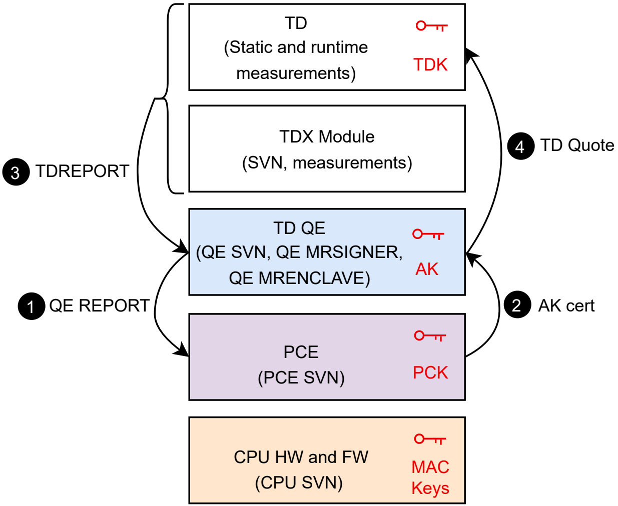


Figure: Updated

SVN for TD?


TD
(Static and runtime
measurements)
TDK
TDX Module
(SVN, measurements)
TD QE
(QE SVN, QE MRSIGNER,
QE MRENCLAVE)
AK
PCE
(PCE SVN)
PCK
CPU HW and FW
(CPU SVN)
MAC
Keys
3 TDREPORT
1 QE REPORT
4 TD Quote
2 AK cert

Missing Specs

Provisioning phase

Missing Specs

Provisioning phase

Structure of Remote Evidence (TD Quote)

Missing Specs

Provisioning phase

Structure of Remote Evidence (TD Quote)

Structure of AK cert

Missing Specs

Provisioning phase

Structure of Remote Evidence (TD Quote)

Structure of AK cert

KDF for Local Evidence

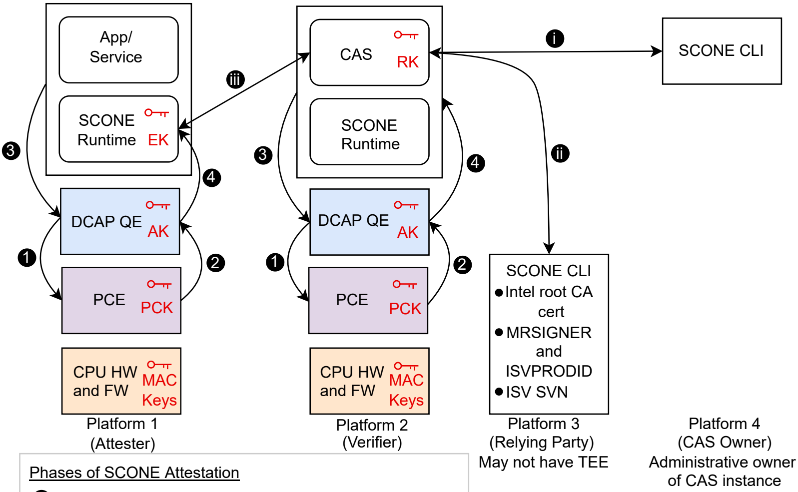
Outline

Order of QE selection

Chosen based on platform capabilities (not by app owner)

- Perspective 1
    1. DCAP QE (qe3)
    2. SCONE QE + EPID QE
    3. EPID QE
- Perspective 2
    1. DCAP QE (qe3)
    2. EPID QE
    3. SCONE QE (can use only if platform ID is known)
- Perspective 3
    - Everything (out of EPID, DCAP, SCONE Quote) that Platform 1 supports is sent to the CAS. So order is not important. CAS decides based on the policy.
        - food for thought: what do we gain?
        - unnecessary overhead without any apparent gain

LA vs. RA



Phases of SCONE Attestation

- (i) SCONE CLI (Platform 4) verifies CAS remotely
- (ii) SCONE CLI (Platform 3) verifies CAS remotely
- (iii) CAS verifies App enclave (Platform 1) remotely

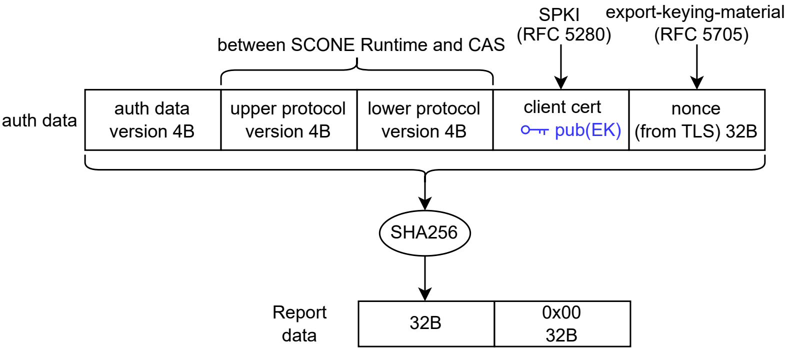
Initialization

- (1) QE REPORT
- (2) AK cert

Attestation Protocol

- (3) REPORT
- (4) Quote

When is a property attested?



Outline

Challenges

ca. 1500 pages of specs of TDX

Challenges

ca. 1500 pages of specs of TDX

Inherits specs from SGX (SDM alone ca. 5000 pages)

Challenges

ca. 1500 pages of specs of TDX

Inherits specs from SGX (SDM alone ca. 5000 pages)

Specs in natural language

Challenges

ca. 1500 pages of specs of TDX

Inherits specs from SGX (SDM alone ca. 5000 pages)

Specs in natural language

Closed-source nature of SCONE

Take-home

- Towards TEE-agnostic *verification* infrastructure for transparency and interoperability

Take-home

- Towards TEE-agnostic *verification* infrastructure for transparency and interoperability

- TDX: how do we precisely express trust boundaries?

Take-home

- Towards TEE-agnostic *verification* infrastructure for transparency and interoperability

- TDX: how do we precisely express trust boundaries?

- SCONE: when do we say that something is attested?

Take-home

- Towards TEE-agnostic *verification* infrastructure for transparency and interoperability
- TDX: how do we precisely express trust boundaries?
- SCONE: when do we say that something is attested?
- Lots of work required for precise specification and standardization for understanding underlying assumptions

Take-home

- Towards TEE-agnostic *verification* infrastructure for transparency and interoperability
- TDX: how do we precisely express trust boundaries?
- SCONE: when do we say that something is attested?
- Lots of work required for precise specification and standardization for understanding underlying assumptions
  - Integration with TLS (RA-TLS)

Take-home

- Towards TEE-agnostic *verification* infrastructure for transparency and interoperability
- TDX: how do we precisely express trust boundaries?
- SCONE: when do we say that something is attested?
- Lots of work required for precise specification and standardization for understanding underlying assumptions
  - Integration with TLS (RA-TLS)
  - Integration with vTPM

Key References

Birkholz, Henk et al. *Remote ATtestation procedureS (RATS) Architecture*. RFC 9334. Jan. 2023. DOI: 10.17487/RFC9334. URL: https://www.rfc-editor.org/info/rfc9334.

Ménétrey, Jämes, Christian Göttel, Anum Khurshid, et al. "Attestation Mechanisms for Trusted Execution Environments Demystified". In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 13272 LNCS (2022), pp. 95–113. ISSN: 16113349. DOI: 10.1007/978-3-031-16092-9_7.

Ménétrey, Jämes, Christian Göttel, Marcelo Pasin, et al. "An Exploratory Study of Attestation Mechanisms for Trusted Execution Environments". In: *5th Workshop on System Software for Trusted Execution (SysTEX 2022)*. 2022. URL: https://systex22.github.io/papers/systex22-final79.pdf.

Niemi, Arto, Sampo Sovio, and Jan Erik Ekberg. "Towards Interoperable Enclave Attestation: Learnings from Decades of Academic Work". In: *Conference of Open Innovation Association, FRUCT*. Vol. 2022-April. IEEE Computer Society, 2022, pp. 189–200. ISBN: 9789526924472. DOI: 10.23919/FRUCT54823.2022.9770907.

Trusted Computing Group. *DICE Attestation Architecture*. Tech. rep. 2021. URL: https://trustedcomputinggroup.org/wp-content/uploads/DICE-Attestation-Architecture-r23-final.pdf.

Call to Action

- Get involved: https://github.com/CCC-Attestation/formal-spec-TEE
- Additional information: link here
- Specify your attestation designs using presented architecture and proposed formalism