Inconsistencies in Specification of Intel TDX Remote Attestation

Muhammad Usama Sardar, Saidgani Musaev and Christof Fetzer
Ack: Anna Galanou, Amna Shahab, Bruno Blanchet
Funding: CPEC, CeTI

Chair of Systems Engineering
Institute of Systems Architecture
Technische Universität Dresden

Dresden, Germany

April 5, 2022

Promise of talk

- Need of science of security in an emerging and important domain

Promise of talk

- Need of science of security in an emerging and important domain
- CCC: more marketing than scientific[1,2] (highlights only)

[1] Confidential Computing Consortium, *Whitepaper feedback from Muhammad Usama Sardar, Issue #77*, 2020

[2] Sardar and Fetzer, *Confidential Computing and Related Technologies : A Review*, 2021

Promise of talk

- Need of science of security in an emerging and important domain
- CCC: more marketing than scientific[1,2] (highlights only)
- Attestation: one of the most critical and essential parts of TEE

[1] Confidential Computing Consortium, *Whitepaper feedback from Muhammad Usama Sardar, Issue #77*, 2020

[2] Sardar and Fetzer, *Confidential Computing and Related Technologies : A Review*, 2021

Promise of talk

- Need of science of security in an emerging and important domain
- CCC: more marketing than scientific[1,2] (highlights only)
- Attestation: one of the most critical and essential parts of TEE
- Complexity is the worst enemy of security (B. Schneier)

[1] Confidential Computing Consortium, *Whitepaper feedback from Muhammad Usama Sardar, Issue #77*, 2020

[2] Sardar and Fetzer, *Confidential Computing and Related Technologies : A Review*, 2021

Promise of talk

- Need of science of security in an emerging and important domain
- CCC: more marketing than scientific[1,2] (highlights only)
- Attestation: one of the most critical and essential parts of TEE
- Complexity is the worst enemy of security (B. Schneier)
- Complexity is the best friend of Intel!

[1] Confidential Computing Consortium, *Whitepaper feedback from Muhammad Usama Sardar, Issue #77*, 2020

[2] Sardar and Fetzer, *Confidential Computing and Related Technologies : A Review*, 2021

Outline

TEE

- "an environment that provides a level of assurance of the three properties: data confidentiality, data integrity, code integrity"[3]

[3] Confidential Computing Consortium, *A Technical Analysis of Confidential Computing, v1.1*, 2021

TEE

- "an environment that provides a level of assurance of the three properties: data confidentiality, data integrity, code integrity"[3]
- Quite vague, e.g.,

[3] Confidential Computing Consortium, *A Technical Analysis of Confidential Computing, v1.1*, 2021

TEE

- "an environment that provides a level of assurance of the three properties: data confidentiality, data integrity, code integrity"[3]
- Quite vague, e.g.,
  - "a level of assurance"

[3] Confidential Computing Consortium, *A Technical Analysis of Confidential Computing, v1.1*, 2021

TEE

- "an environment that provides a level of assurance of the three properties: data confidentiality, data integrity, code integrity"[3]
- Quite vague, e.g.,
  - "a level of assurance"
  - Def. satisfied by HSM also

[3] Confidential Computing Consortium, *A Technical Analysis of Confidential Computing, v1.1*, 2021

TEE

- "an environment that provides a level of assurance of the three properties: data confidentiality, data integrity, code integrity"[3]
- Quite vague, e.g.,
  - "a level of assurance"
  - Def. satisfied by HSM also
- Trusted HW and SW argument: need for RA

[3] Confidential Computing Consortium, *A Technical Analysis of Confidential Computing, v1.1*, 2021

TEE

- “an environment that provides a level of assurance of the three properties: data confidentiality, data integrity, code integrity”[3]
- Quite vague, e.g.,
  - “a level of assurance”
  - Def. satisfied by HSM also
- Trusted HW and SW argument: need for RA
- Without attestation, no better than conventional computing for possible threat models

[3] Confidential Computing Consortium, *A Technical Analysis of Confidential Computing, v1.1*, 2021

TEE

- "an environment that provides a level of assurance of the three properties: data confidentiality, data integrity, code integrity"[3]
- Quite vague, e.g.,
  - "a level of assurance"
  - Def. satisfied by HSM also
- Trusted HW and SW argument: need for RA
- Without attestation, no better than conventional computing for possible threat models
  - Remote user cannot distinguish a malicious platform and a genuine one

[3] Confidential Computing Consortium, *A Technical Analysis of Confidential Computing, v1.1*, 2021

TEE

- "an environment that provides a level of assurance of the three properties: data confidentiality, data integrity, code integrity"[3]
- Quite vague, e.g.,
  - "a level of assurance"
  - Def. satisfied by HSM also
- Trusted HW and SW argument: need for RA
- Without attestation, no better than conventional computing for possible threat models
  - Remote user cannot distinguish a malicious platform and a genuine one
  - Even with alternative of attestation: authentication

[3] Confidential Computing Consortium, *A Technical Analysis of Confidential Computing, v1.1*, 2021

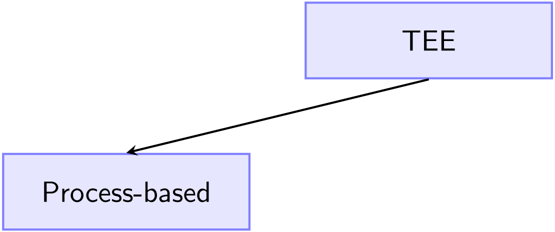
TEE

- "an environment that provides a level of assurance of the three properties: data confidentiality, data integrity, code integrity"[3]
- Quite vague, e.g.,
  - "a level of assurance"
  - Def. satisfied by HSM also
- Trusted HW and SW argument: need for RA
- Without attestation, no better than conventional computing for possible threat models
  - Remote user cannot distinguish a malicious platform and a genuine one
  - Even with alternative of attestation: authentication
- "Any attack that could compromise the attestation of a TEE instance could lead to a workload or data being compromised in turn."[4]

[3] Confidential Computing Consortium, *A Technical Analysis of Confidential Computing, v1.1*, 2021

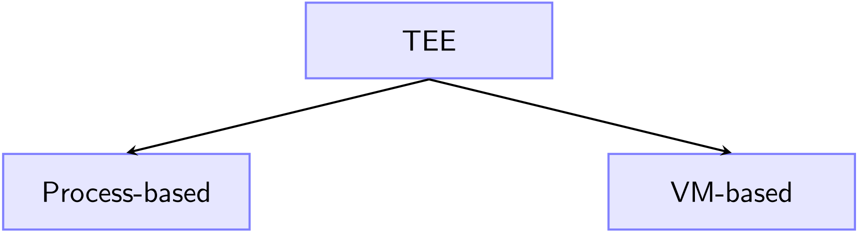
[4] Confidential Computing Consortium, *A Technical Analysis of Confidential Computing, v1.1*, 2021

TEEs Granularity (Public cloud commercial solutions)



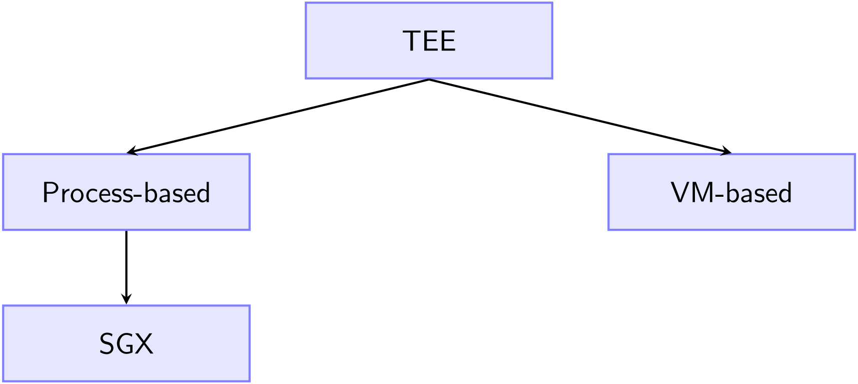
- Smaller TCB

TEEs Granularity (Public cloud commercial solutions)

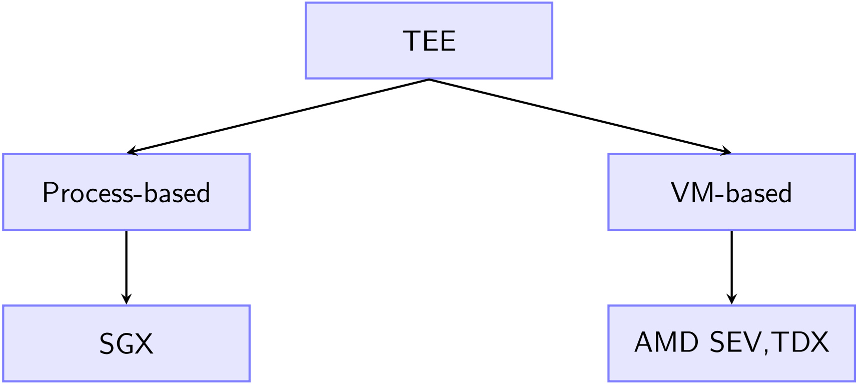


- Ease of use

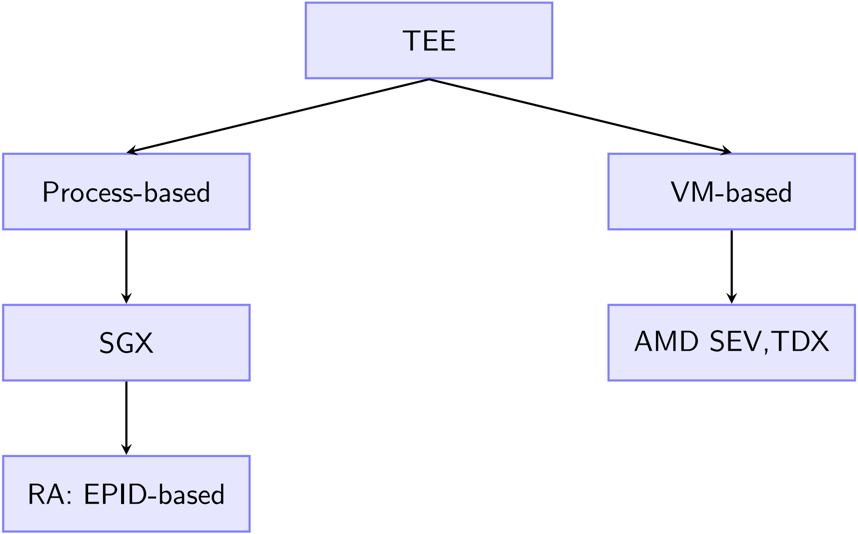
TEEs Granularity (Public cloud commercial solutions)



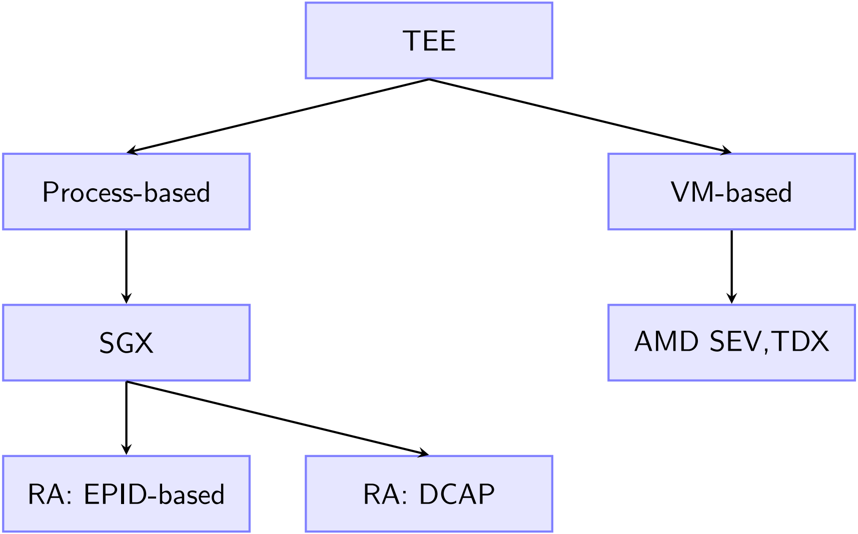
TEEs Granularity (Public cloud commercial solutions)



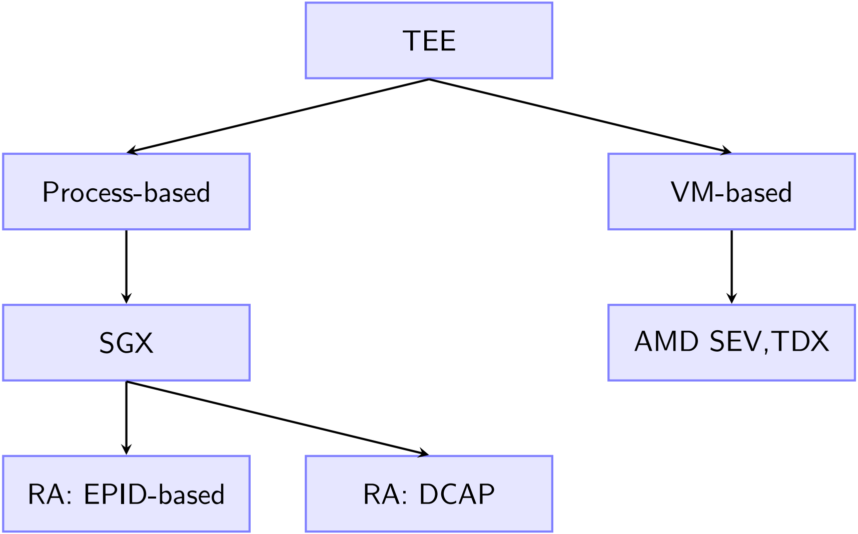
TEEs Granularity (Public cloud commercial solutions)



TEEs Granularity (Public cloud commercial solutions)



TEEs Granularity (Public cloud commercial solutions)



- Different report generation mechanism
- Runtime TD measurements

Outline

ProVerif vs. Tamarin prover

- More automation vs. user interaction

ProVerif vs. Tamarin prover

- More automation vs. user interaction
  - Tamarin accepts ProVerif-like input but not vice versa

ProVerif vs. Tamarin prover

- More automation vs. user interaction
  - Tamarin accepts ProVerif-like input but not vice versa
- Computational security analysis on same model (CryptoVerif[5])

[5] Blanchet, "CryptoVerif: A computationally-sound security protocol verifier", 2017

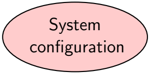
ProVerif vs. Tamarin prover

- More automation vs. user interaction
  - Tamarin accepts ProVerif-like input but not vice versa
- Computational security analysis on same model (CryptoVerif[5])
- Faster[6]

[5] Blanchet, "CryptoVerif: A computationally-sound security protocol verifier", 2017

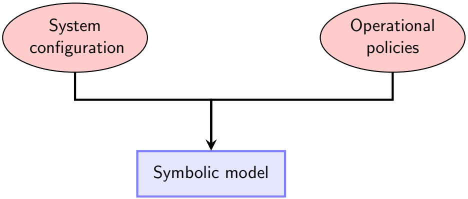
[6] Lafourcade and Puys, "Performance Evaluations of Cryptographic Protocols Verification Tools Dealing with Algebraic Properties", 2016

Workflow of the Analysis Approach

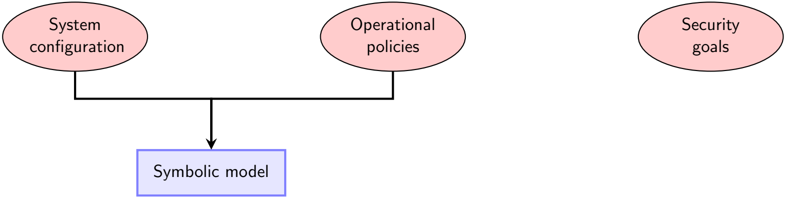


Workflow of the Analysis Approach

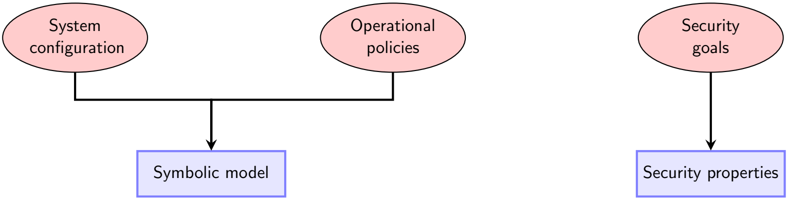
Workflow of the Analysis Approach



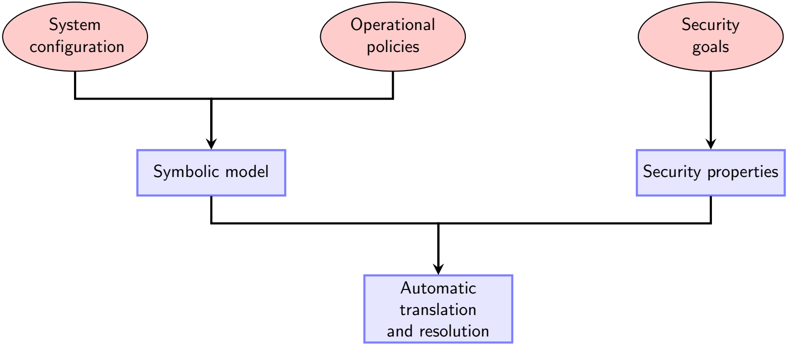
Workflow of the Analysis Approach



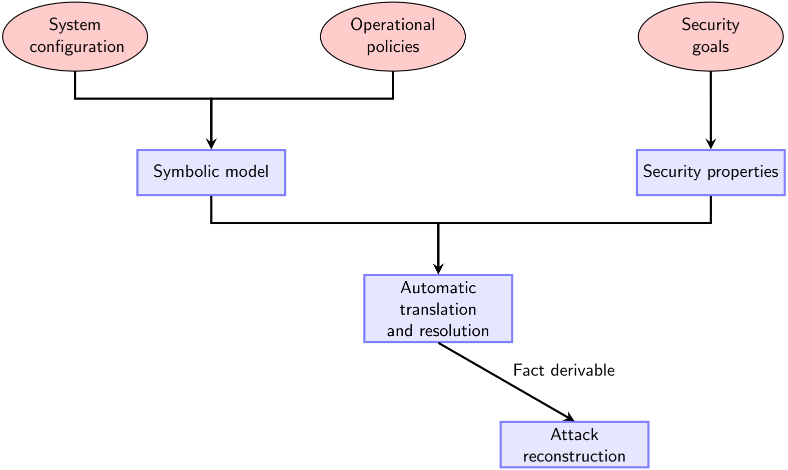
Workflow of the Analysis Approach



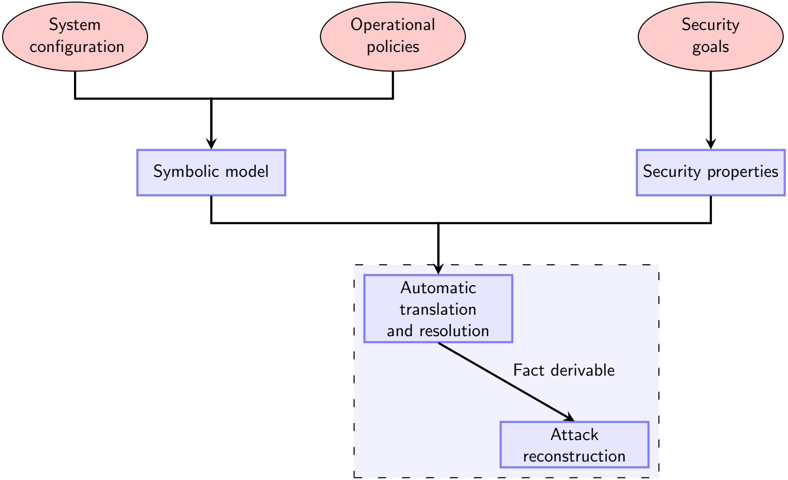
Workflow of the Analysis Approach



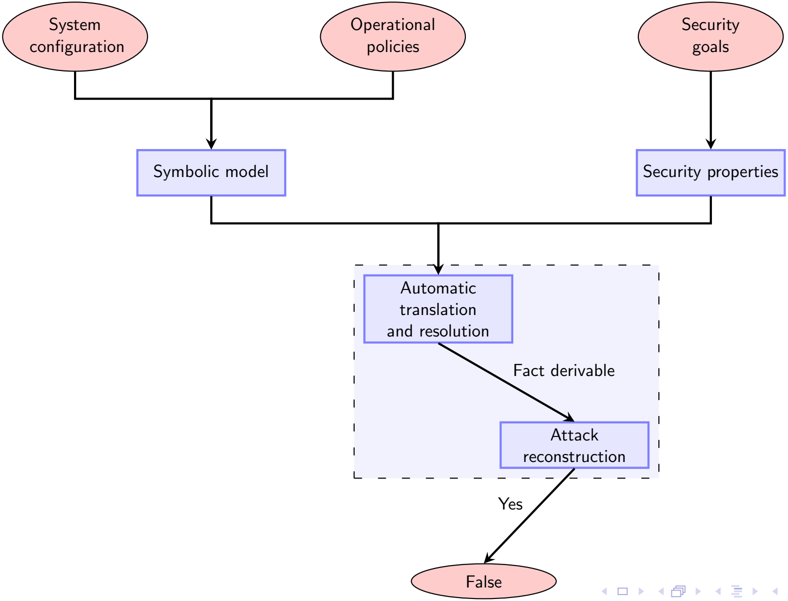
Workflow of the Analysis Approach



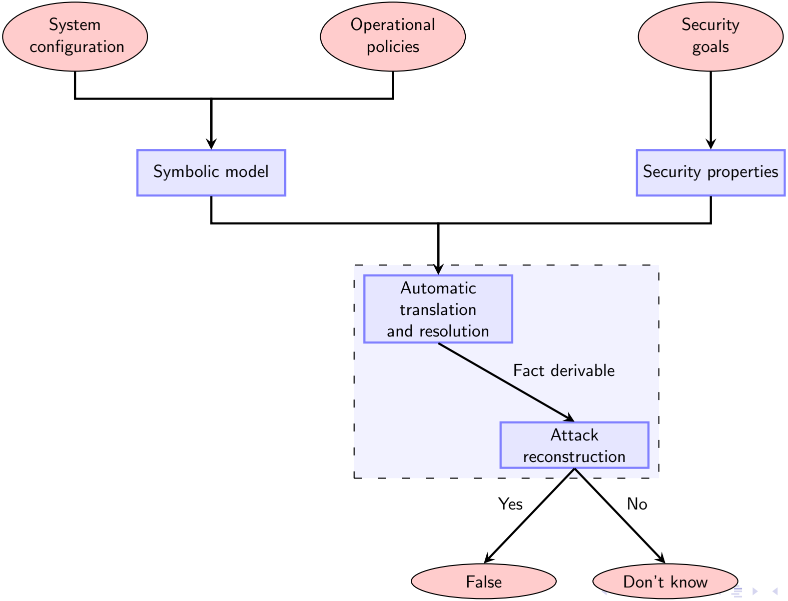
Workflow of the Analysis Approach



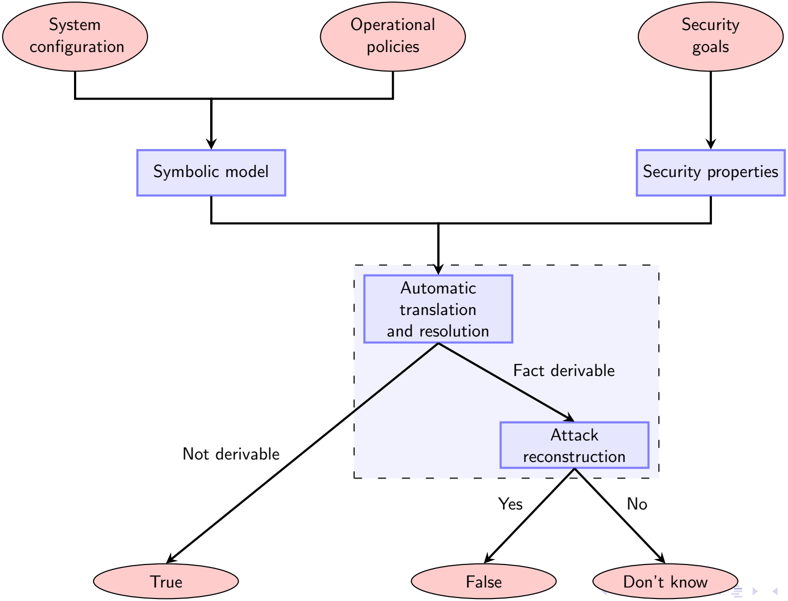
Workflow of the Analysis Approach



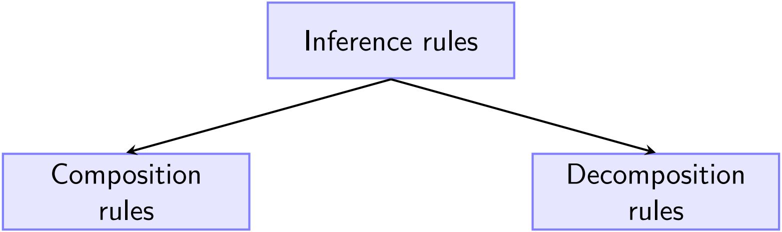
Workflow of the Analysis Approach



Workflow of the Analysis Approach



Inference System



Inference System and Horn Clauses (Simplified)

- Composition rules

Inference System and Horn Clauses (Simplified)

- Composition rules
  - pair $\frac{x \quad y}{\langle x, y \rangle}$ $\quad att(x) \bigwedge att(y) \rightarrow att(\langle x, y \rangle)$

Inference System and Horn Clauses (Simplified)

- Composition rules
  - pair $\frac{x \quad y}{\langle x,y \rangle}$ $\quad att(x) \bigwedge att(y) \rightarrow att(\langle x, y \rangle)$
  - hash $\frac{m}{h(m)}$ $\quad att(m) \rightarrow att(h(m))$

Inference System and Horn Clauses (Simplified)

- Composition rules
  - pair $\frac{x \quad y}{\langle x,y \rangle}$ $\quad att(x) \bigwedge att(y) \rightarrow att(\langle x, y \rangle)$
  - hash $\frac{m}{h(m)}$ $\quad att(m) \rightarrow att(h(m))$
  - hmac $\frac{mk \quad m}{hmac(mk,m)}$ $\quad att(mk) \bigwedge att(m) \rightarrow att(hmac(mk, m))$

Inference System and Horn Clauses (Simplified)

- Composition rules
  - pair $\frac{x \quad y}{\langle x,y \rangle}$ $att(x) \bigwedge att(y) \rightarrow att(\langle x, y \rangle)$
  - hash $\frac{m}{h(m)}$ $att(m) \rightarrow att(h(m))$
  - hmac $\frac{mk \quad m}{hmac(mk,m)}$ $att(mk) \bigwedge att(m) \rightarrow att(hmac(mk, m))$
  - senc $\frac{sek \quad m}{senc(sek,m)}$ $att(sek) \bigwedge att(m) \rightarrow att(senc(sek, m))$

Inference System and Horn Clauses (Simplified)

- Composition rules
  - pair $\frac{x \quad y}{\langle x, y \rangle}$ $\quad att(x) \bigwedge att(y) \rightarrow att(\langle x, y \rangle)$
  - hash $\frac{m}{h(m)}$ $\quad att(m) \rightarrow att(h(m))$
  - hmac $\frac{mk \quad m}{hmac(mk, m)}$ $\quad att(mk) \bigwedge att(m) \rightarrow att(hmac(mk, m))$
  - senc $\frac{sek \quad m}{senc(sek, m)}$ $\quad att(sek) \bigwedge att(m) \rightarrow att(senc(sek, m))$
  - aenc $\frac{aek \quad m}{aenc(aek, m)}$ $\quad att(aek) \bigwedge att(m) \rightarrow att(aenc(aek, m))$

Inference System and Horn Clauses (Simplified)

- Composition rules
  - pair $\frac{x \quad y}{\langle x,y \rangle}$ $\quad att(x) \bigwedge att(y) \rightarrow att(\langle x, y \rangle)$
  - hash $\frac{m}{h(m)}$ $\quad att(m) \rightarrow att(h(m))$
  - hmac $\frac{mk \quad m}{hmac(mk,m)}$ $\quad att(mk) \bigwedge att(m) \rightarrow att(hmac(mk, m))$
  - senc $\frac{sek \quad m}{senc(sek,m)}$ $\quad att(sek) \bigwedge att(m) \rightarrow att(senc(sek, m))$
  - aenc $\frac{aek \quad m}{aenc(aek,m)}$ $\quad att(aek) \bigwedge att(m) \rightarrow att(aenc(aek, m))$
  - sign $\frac{sk \quad m}{signAppDet(sk,m)}$ $\quad att(sk) \bigwedge att(m) \rightarrow att(signAppDet(sk, m))$

Inference System and Horn Clauses (Simplified)

- Composition rules
  - pair $\frac{x \quad y}{\langle x,y\rangle}$ $\quad att(x) \bigwedge att(y) \rightarrow att(\langle x, y\rangle)$
  - hash $\frac{m}{h(m)}$ $\quad att(m) \rightarrow att(h(m))$
  - hmac $\frac{mk \quad m}{hmac(mk,m)}$ $\quad att(mk) \bigwedge att(m) \rightarrow att(hmac(mk, m))$
  - senc $\frac{sek \quad m}{senc(sek,m)}$ $\quad att(sek) \bigwedge att(m) \rightarrow att(senc(sek, m))$
  - aenc $\frac{aek \quad m}{aenc(aek,m)}$ $\quad att(aek) \bigwedge att(m) \rightarrow att(aenc(aek, m))$
  - sign $\frac{sk \quad m}{signAppDet(sk,m)}$ $\quad att(sk) \bigwedge att(m) \rightarrow att(signAppDet(sk, m))$
- Decomposition rules

Inference System and Horn Clauses (Simplified)

- Composition rules
  - pair $\frac{x \quad y}{\langle x,y \rangle}$ $att(x) \bigwedge att(y) \rightarrow att(\langle x, y \rangle)$
  - hash $\frac{m}{h(m)}$ $att(m) \rightarrow att(h(m))$
  - hmac $\frac{mk \quad m}{hmac(mk,m)}$ $att(mk) \bigwedge att(m) \rightarrow att(hmac(mk, m))$
  - senc $\frac{sek \quad m}{senc(sek,m)}$ $att(sek) \bigwedge att(m) \rightarrow att(senc(sek, m))$
  - aenc $\frac{aek \quad m}{aenc(aek,m)}$ $att(aek) \bigwedge att(m) \rightarrow att(aenc(aek, m))$
  - sign $\frac{sk \quad m}{signAppDet(sk,m)}$ $att(sk) \bigwedge att(m) \rightarrow att(signAppDet(sk, m))$
- Decomposition rules
  - projection $\frac{\langle x,y \rangle}{x}$, $\frac{\langle x,y \rangle}{y}$ $att(\langle x, y \rangle) \rightarrow att(x),\ att(\langle x, y \rangle) \rightarrow att(y)$

Inference System and Horn Clauses (Simplified)

- Composition rules
  - pair $\frac{x \quad y}{\langle x,y \rangle}$ $\quad att(x) \bigwedge att(y) \rightarrow att(\langle x, y \rangle)$
  - hash $\frac{m}{h(m)}$ $\quad att(m) \rightarrow att(h(m))$
  - hmac $\frac{mk \quad m}{hmac(mk,m)}$ $\quad att(mk) \bigwedge att(m) \rightarrow att(hmac(mk, m))$
  - senc $\frac{sek \quad m}{senc(sek,m)}$ $\quad att(sek) \bigwedge att(m) \rightarrow att(senc(sek, m))$
  - aenc $\frac{aek \quad m}{aenc(aek,m)}$ $\quad att(aek) \bigwedge att(m) \rightarrow att(aenc(aek, m))$
  - sign $\frac{sk \quad m}{signAppDet(sk,m)}$ $\quad att(sk) \bigwedge att(m) \rightarrow att(signAppDet(sk, m))$
- Decomposition rules
  - projection $\frac{\langle x,y \rangle}{x}$, $\frac{\langle x,y \rangle}{y}$ $\quad att(\langle x, y \rangle) \rightarrow att(x),\ att(\langle x, y \rangle) \rightarrow att(y)$
  - sdec $\frac{sek \quad senc(sek,m)}{m}$ $\quad att(sek) \bigwedge att(senc(sek, m)) \rightarrow att(m)$

Inference System and Horn Clauses (Simplified)

- Composition rules
  - pair $\frac{x \quad y}{\langle x,y \rangle}$ $\quad att(x) \bigwedge att(y) \rightarrow att(\langle x,y \rangle)$
  - hash $\frac{m}{h(m)}$ $\quad att(m) \rightarrow att(h(m))$
  - hmac $\frac{mk \quad m}{hmac(mk,m)}$ $\quad att(mk) \bigwedge att(m) \rightarrow att(hmac(mk,m))$
  - senc $\frac{sek \quad m}{senc(sek,m)}$ $\quad att(sek) \bigwedge att(m) \rightarrow att(senc(sek,m))$
  - aenc $\frac{aek \quad m}{aenc(aek,m)}$ $\quad att(aek) \bigwedge att(m) \rightarrow att(aenc(aek,m))$
  - sign $\frac{sk \quad m}{signAppDet(sk,m)}$ $\quad att(sk) \bigwedge att(m) \rightarrow att(signAppDet(sk,m))$
- Decomposition rules
  - projection $\frac{\langle x,y \rangle}{x}$, $\frac{\langle x,y \rangle}{y}$ $\quad att(\langle x,y \rangle) \rightarrow att(x),\ att(\langle x,y \rangle) \rightarrow att(y)$
  - sdec $\frac{sek \quad senc(sek,m)}{m}$ $\quad att(sek) \bigwedge att(senc(sek,m)) \rightarrow att(m)$
  - adec $\frac{adk \quad aenc(pk(adk),m)}{m}$
    $att(adk) \bigwedge att(aenc(pk(adk),m)) \rightarrow att(m)$

Inference System and Horn Clauses (Simplified)

- Composition rules
  - pair $\frac{x \quad y}{\langle x,y \rangle}$ $\quad att(x) \bigwedge att(y) \rightarrow att(\langle x,y \rangle)$
  - hash $\frac{m}{h(m)}$ $\quad att(m) \rightarrow att(h(m))$
  - hmac $\frac{mk \quad m}{hmac(mk,m)}$ $\quad att(mk) \bigwedge att(m) \rightarrow att(hmac(mk,m))$
  - senc $\frac{sek \quad m}{senc(sek,m)}$ $\quad att(sek) \bigwedge att(m) \rightarrow att(senc(sek,m))$
  - aenc $\frac{aek \quad m}{aenc(aek,m)}$ $\quad att(aek) \bigwedge att(m) \rightarrow att(aenc(aek,m))$
  - sign $\frac{sk \quad m}{signAppDet(sk,m)}$ $\quad att(sk) \bigwedge att(m) \rightarrow att(signAppDet(sk,m))$
- Decomposition rules
  - projection $\frac{\langle x,y \rangle}{x}$, $\frac{\langle x,y \rangle}{y}$ $\quad att(\langle x,y \rangle) \rightarrow att(x),\ att(\langle x,y \rangle) \rightarrow att(y)$
  - sdec $\frac{sek \quad senc(sek,m)}{m}$ $\quad att(sek) \bigwedge att(senc(sek,m)) \rightarrow att(m)$
  - adec $\frac{adk \quad aenc(pk(adk),m)}{m}$
    $att(adk) \bigwedge att(aenc(pk(adk),m)) \rightarrow att(m)$
  - verifysign $\frac{vpk(sk) \quad m \quad signAppDet(sk,m)}{true}$

Outline

1. Introduction
2. Formal Security Analysis Approach
3. TDX
   - Discrepancies Identified
   - Formal Specification
   - Automated Verification
4. Summary

Contributions

- Identification of discrepancies including inconsistent information

[7] Blanchet et al., "Modeling and verifying security protocols with the applied pi calculus and ProVerif", 2016

Contributions

- Identification of discrepancies including inconsistent information
- Precise specification of TD attestation protocol in ProVerif[7]

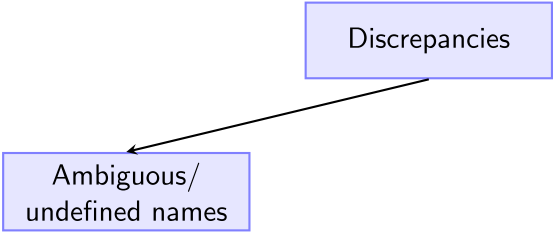
[7] Blanchet et al., "Modeling and verifying security protocols with the applied pi calculus and ProVerif", 2016

Contributions

- Identification of discrepancies including inconsistent information
- Precise specification of TD attestation protocol in ProVerif[7]
- Automated verification of confidentiality and authentication properties in ProVerif

[7] Blanchet et al., "Modeling and verifying security protocols with the applied pi calculus and ProVerif", 2016

Discrepancies Identified

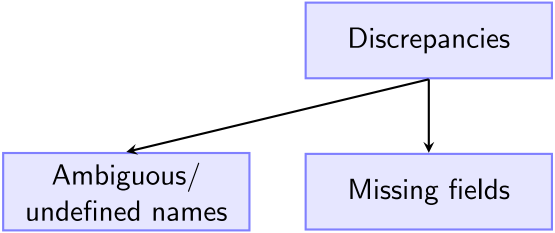


- SEAMINFO vs. TEE_TCB_INFO (e.g., p.2-8)[8]

[8]Intel, *Intel ® Trust Domain CPU Architectural Extensions*, 2020

[9]Intel, *Architecture Specification: Intel® Trust Domain Extensions (Intel® TDX) Module*, 2020

Discrepancies Identified

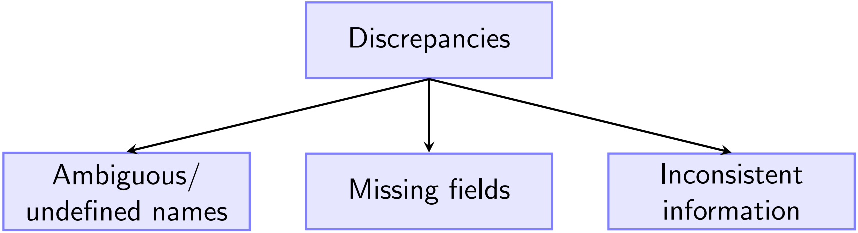


- MROWNERCONFIG missing in TDINFO (Fig. 10.1, p.85)[9]

[8] Intel, *Intel ® Trust Domain CPU Architectural Extensions*, 2020

[9] Intel, *Architecture Specification: Intel® Trust Domain Extensions (Intel® TDX) Module*, 2020

Discrepancies Identified



[8]Intel, *Intel ® Trust Domain CPU Architectural Extensions*, 2020

[9]Intel, *Architecture Specification: Intel® Trust Domain Extensions (Intel® TDX) Module*, 2020

Inconsistent Information: Example 1[10]

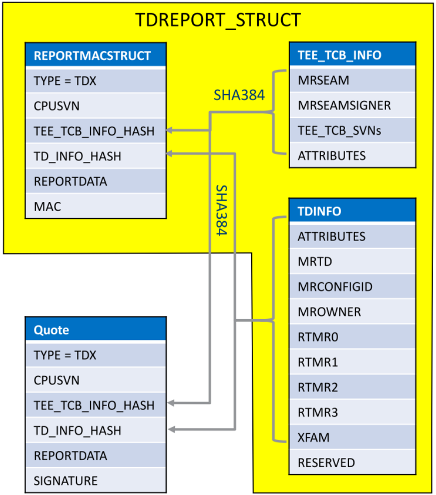


Figure 10.1: TDX Measurement Reporting

[10] Intel, *Architecture Specification: Intel® Trust Domain Extensions (Intel® TDX) Module*, 2020

Inconsistent Information: Example 1[11]

$$tmp\_seamreport.REPORTMACSTRUCT.TEE\_TCB\_INFO\_HASH = SHA384(tmp\_seamreport.TEE\_TCB\_INFO);$$

Table 2-3. TEE_TCB_INFO Structure

Name	Offset (Bytes)	Size (Bytes)	Description
VALID	0	8	Indicates TEE_TCB_INFO fields which are valid. ▪ 1 in the i-th significant bit reflects that the 8 bytes starting at offset (8 * i) are valid. ▪ 0 in the i-th significant bit reflects that either 8 bytes starting at offset (8 * i) is not populated or reserved, and is set to zero.
TEE_TCB_SVN	8	16	TEE_TCB_SVN array.
MRSEAM	24	48	Measurement of the Intel TDX module.
MRSIGNERSEAM	72	48	Measurement of TDX module signer if valid.
ATTRIBUTES	120	8	Additional configuration ATTRIBUTES if valid.
RESERVED	128	111	Must be zero.

[11] Intel, *Intel ® Trust Domain CPU Architectural Extensions*, 2020

Inconsistent Information: Example 2[12]

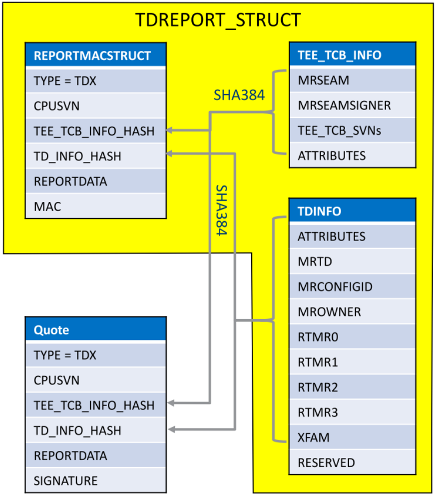


Figure 10.1: TDX Measurement Reporting

<u>RESERVED is not a part of hash!</u>

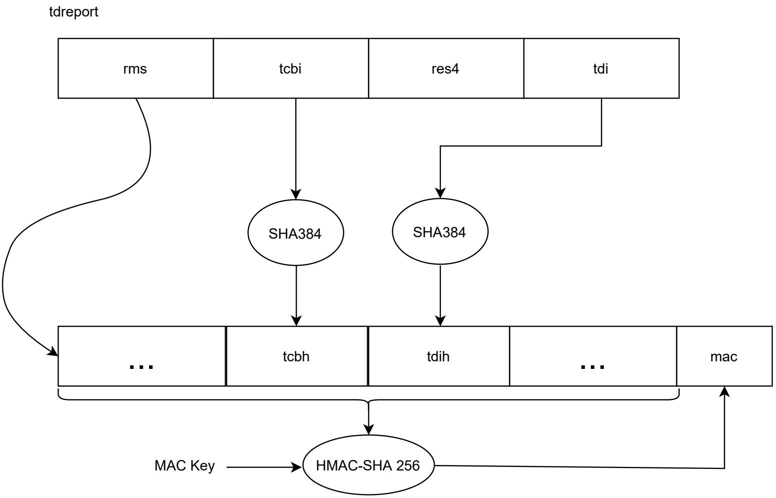
[12] Intel, *Architecture Specification: Intel® Trust Domain Extensions (Intel® TDX) Module*, 2020

Inconsistent Information: Example 2[13]

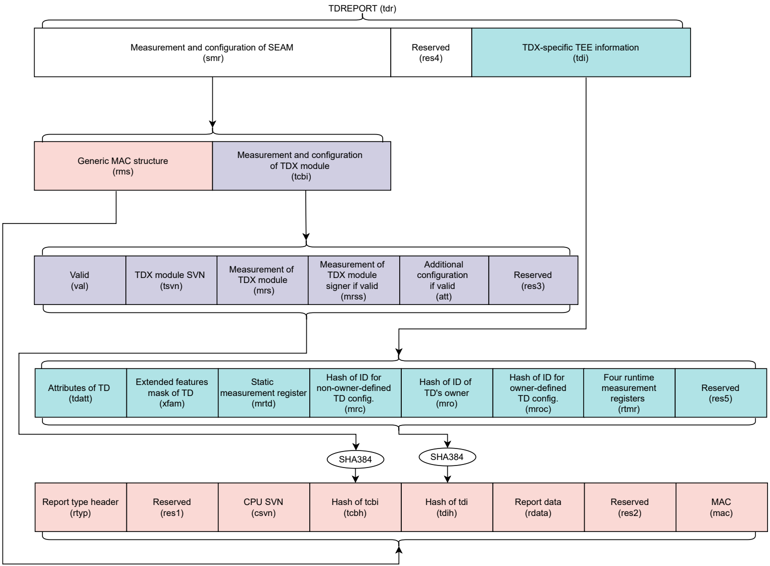
Software verifying a TEE report structure (for TDX, this includes TEE_TCB_INFO_STRUCT and TDINFO_STRUCT) should first confirm that its REPORTMACSTRUCT.TEE_TCB_INFO_HASH equals the hash of the TEE_TCB_INFO_STRUCT (if applicable) and that REPORTMACSTRUCT.TEE_INFO_HASH equals the hash of the TDINFO_STRUCT. Then, software uses

[13] Intel, *Architecture Specification: Intel® Trust Domain Extensions (Intel® TDX) Module*, 2020

TD Report Structures (Simplified view)



TD Report Structures[14]

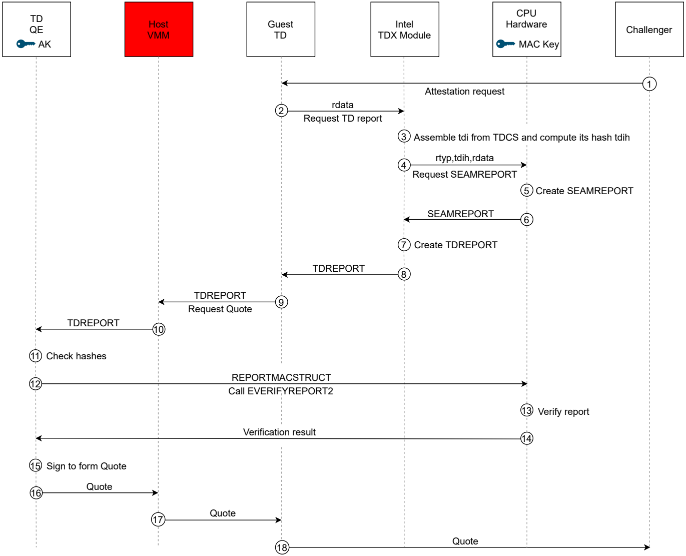


[14] Sardar, Musaev, and Fetzer, "Demystifying Attestation in Intel Trust Domain Extensions via Formal Verification", 2021

Simplified View of Protocol

- Local attestation → Symmetric crypto → MAC
- Remote attestation → Asymmetric crypto → Digital signatures

TDX Attestation Flow for Quote Generation[15]



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

Automated Verification

- Validation: reachability of all parts of code
- Confidentiality: reachability property
- Authentication properties, e.g.,
  $x \equiv \langle rtyp, res1, csvn, tcbh, tdih, rdata, res2 \rangle$

$$\forall\ x.$$
$$\exists\ mac, tcbi.$$
$$event(QuoteVerified(x)) \Rightarrow event(CPUsentSMR(x, mac, tcbi))$$

Outline

Take-home

- TDX specifications are inconsistent and poorly documented

Take-home

- TDX specifications are inconsistent and poorly documented
  - may lead to design and implementation flaws

Take-home

- TDX specifications are inconsistent and poorly documented
  - may lead to design and implementation flaws
- Reported to Intel and being updated by Intel

Take-home

- TDX specifications are inconsistent and poorly documented
  - may lead to design and implementation flaws
- Reported to Intel and being updated by Intel
- Works in progress (comments most welcome: also by email)

Take-home

- TDX specifications are inconsistent and poorly documented
  - may lead to design and implementation flaws
- Reported to Intel and being updated by Intel
- Works in progress (comments most welcome: also by email)
  - Model: PCE and cert chain, verifier end

Take-home

- TDX specifications are inconsistent and poorly documented
  - may lead to design and implementation flaws
- Reported to Intel and being updated by Intel
- Works in progress (comments most welcome: also by email)
  - Model: PCE and cert chain, verifier end
  - Properties:

Take-home

- TDX specifications are inconsistent and poorly documented
    - may lead to design and implementation flaws
- Reported to Intel and being updated by Intel
- Works in progress (comments most welcome: also by email)
    - Model: PCE and cert chain, verifier end
    - Properties:
        - Mutual authentication

Take-home

- TDX specifications are inconsistent and poorly documented
  - may lead to design and implementation flaws
- Reported to Intel and being updated by Intel
- Works in progress (comments most welcome: also by email)
  - Model: PCE and cert chain, verifier end
  - Properties:
    - Mutual authentication
    - Freshness

Take-home

- TDX specifications are inconsistent and poorly documented
  - may lead to design and implementation flaws
- Reported to Intel and being updated by Intel
- Works in progress (comments most welcome: also by email)
  - Model: PCE and cert chain, verifier end
  - Properties:
    - Mutual authentication
    - Freshness
    - Equivalence properties

Take-home

- TDX specifications are inconsistent and poorly documented
  - may lead to design and implementation flaws
- Reported to Intel and being updated by Intel
- Works in progress (comments most welcome: also by email)
  - Model: PCE and cert chain, verifier end
  - Properties:
    - Mutual authentication
    - Freshness
    - Equivalence properties
  - Tamarin for comparison

Take-home

- TDX specifications are inconsistent and poorly documented
  - may lead to design and implementation flaws
- Reported to Intel and being updated by Intel
- Works in progress (comments most welcome: also by email)
  - Model: PCE and cert chain, verifier end
  - Properties:
    - Mutual authentication
    - Freshness
    - Equivalence properties
  - Tamarin for comparison
- Shameless plug: we are hiring PhDs, post-docs ([muhammad_usama.sardar,christof.fetzer]@tu-dresden.de)

Key References I

Blanchet, Bruno. "CryptoVerif: A computationally-sound security protocol verifier". In: *Tech. Rep.* (2017).

Blanchet, Bruno et al. "Modeling and verifying security protocols with the applied pi calculus and ProVerif". In: *Foundations and Trends in Privacy and Security* 1.1-2 (2016), pp. 1–135.

Confidential Computing Consortium. *A Technical Analysis of Confidential Computing, v1.1*. Jan. 2021. URL: https://confidentialcomputing.io/wp-content/uploads/sites/85/2021/03/CCC-Tech-Analysis-Confidential-Computing-V1.pdf.

— .*Whitepaper feedback from Muhammad Usama Sardar, Issue #77*. 2020. URL: https://github.com/confidential-computing/governance/issues/77 (visited on 09/13/2021).

Intel. *Architecture Specification: Intel® Trust Domain Extensions (Intel® TDX) Module*. Sept. 2020. URL: https://software.intel.com/content/dam/develop/external/us/en/documents/intel-tdx-module-1eas.pdf.

— .*Intel ® Trust Domain CPU Architectural Extensions*. Sept. 2020. URL: https://software.intel.com/content/dam/develop/external/us/en/documents/intel-tdx-cpu-architectural-specification.pdf.

Lafourcade, Pascal and Maxime Puys. "Performance Evaluations of Cryptographic Protocols Verification Tools Dealing with Algebraic Properties". In: *Foundations and Practice of Security*. 2016, pp. 137–155. DOI: 10.1007/978-3-319-30303-1_9.

Sardar, Muhammad Usama and Christof Fetzer. *Confidential Computing and Related Technologies : A Review*. 2021. URL: https://www.researchgate.net/publication/356474602_Confidential_Computing_and_Related_Technologies_A_Review.

Key References II

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.