Comprehensive Specification and Formal Analysis of Attestation Mechanisms in Confidential Computing (Oral Communication)

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

[1]TU Dresden

[2]Arm Ltd.

June 19, 2023

Agenda

Motivation: memories from ICE 2022 (OC)

Take-home

- Need to design Intel TDX RA in a systematic way
- Most detailed formal model of RA
- Works in progress (participations welcome)
  - More detailed model and more properties
  - Comparison of specification and implementation
  - Frameworks

If you don't have good memory

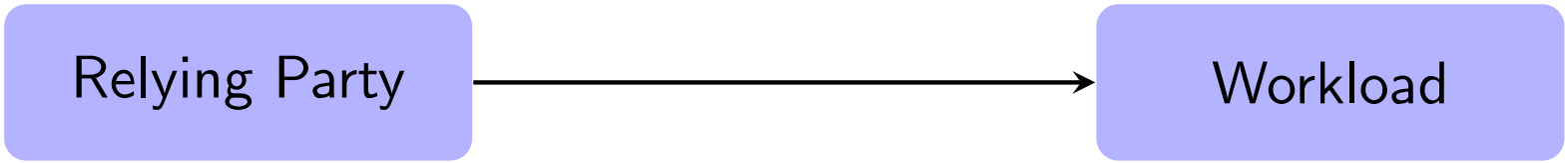
Just recall last question by Seyed Hossein Haeri before coffee

Confidential Computing[1]

Relying Party

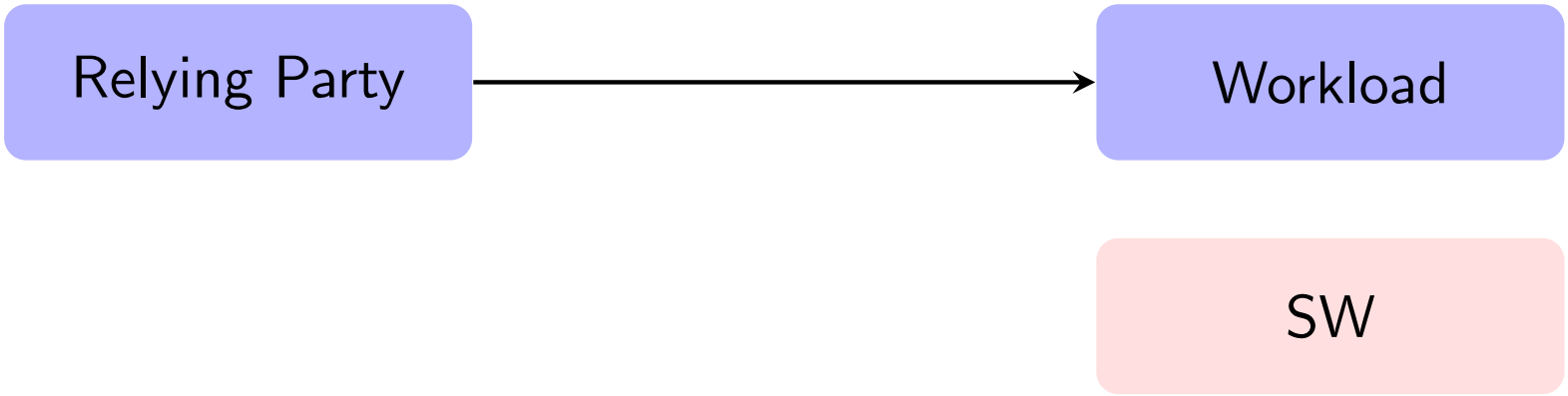
[1] Sardar and Fetzer, *Confidential Computing and Related Technologies : A Critical Review*, 2021.

Confidential Computing[1]



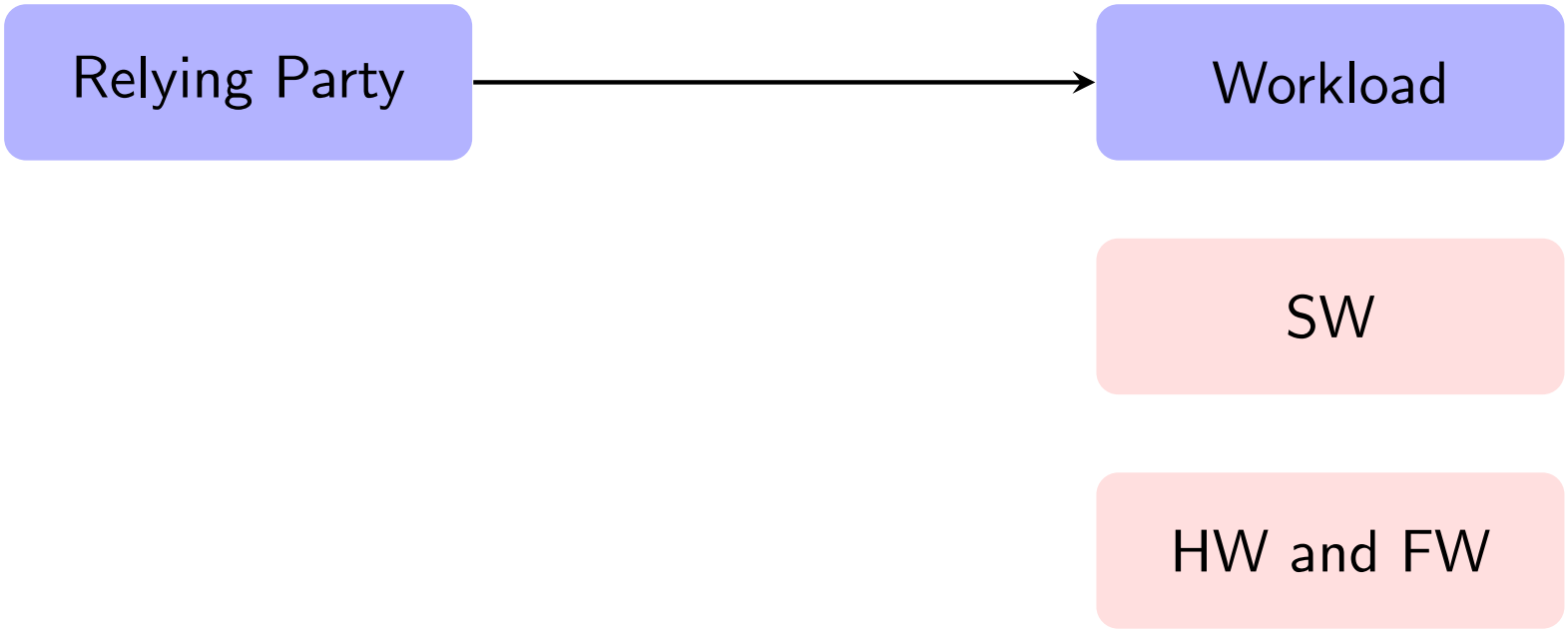
[1] Sardar and Fetzer, *Confidential Computing and Related Technologies : A Critical Review*, 2021.

Confidential Computing[1]



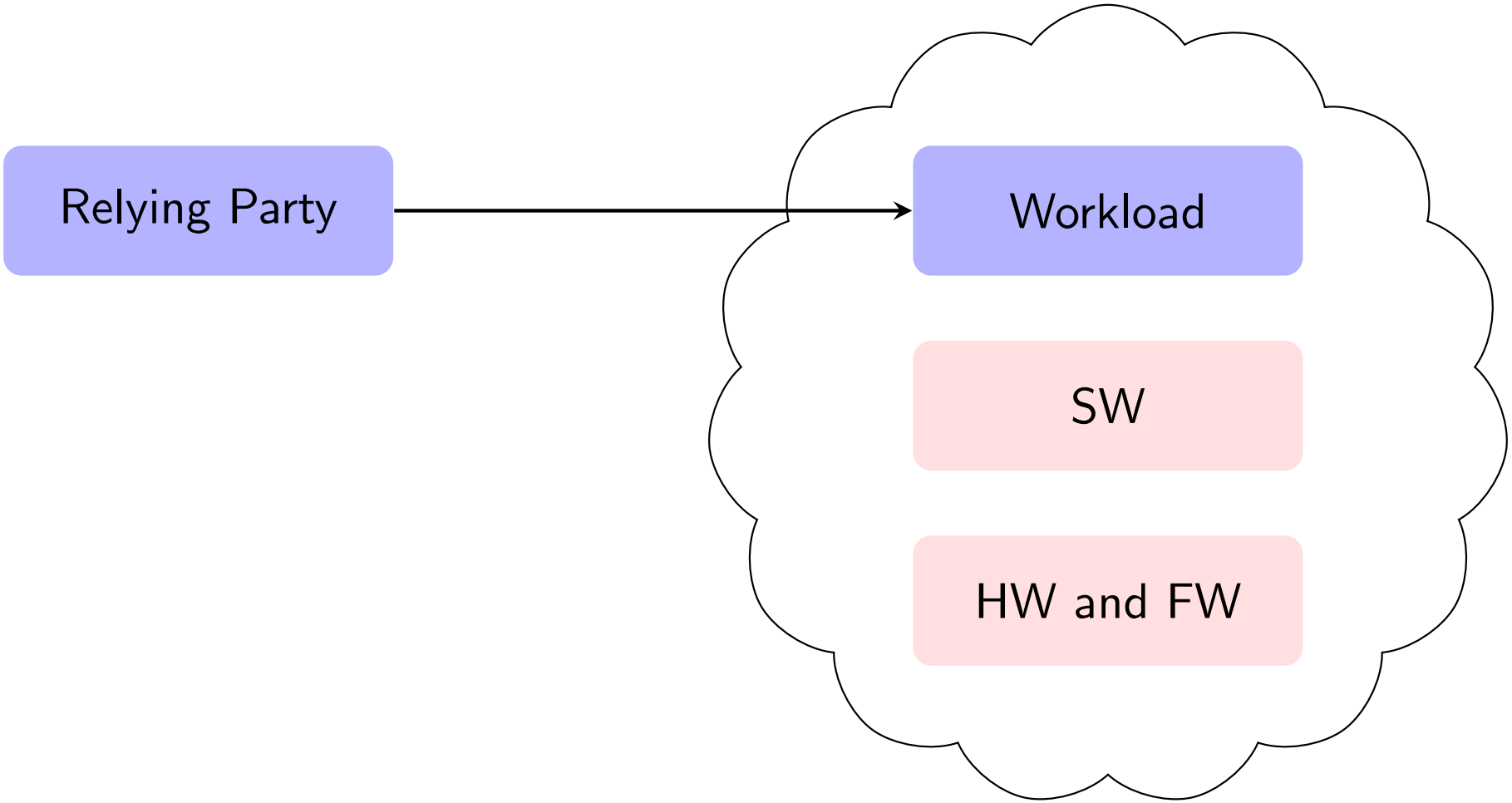
[1] Sardar and Fetzer, *Confidential Computing and Related Technologies : A Critical Review*, 2021.

Confidential Computing[1]



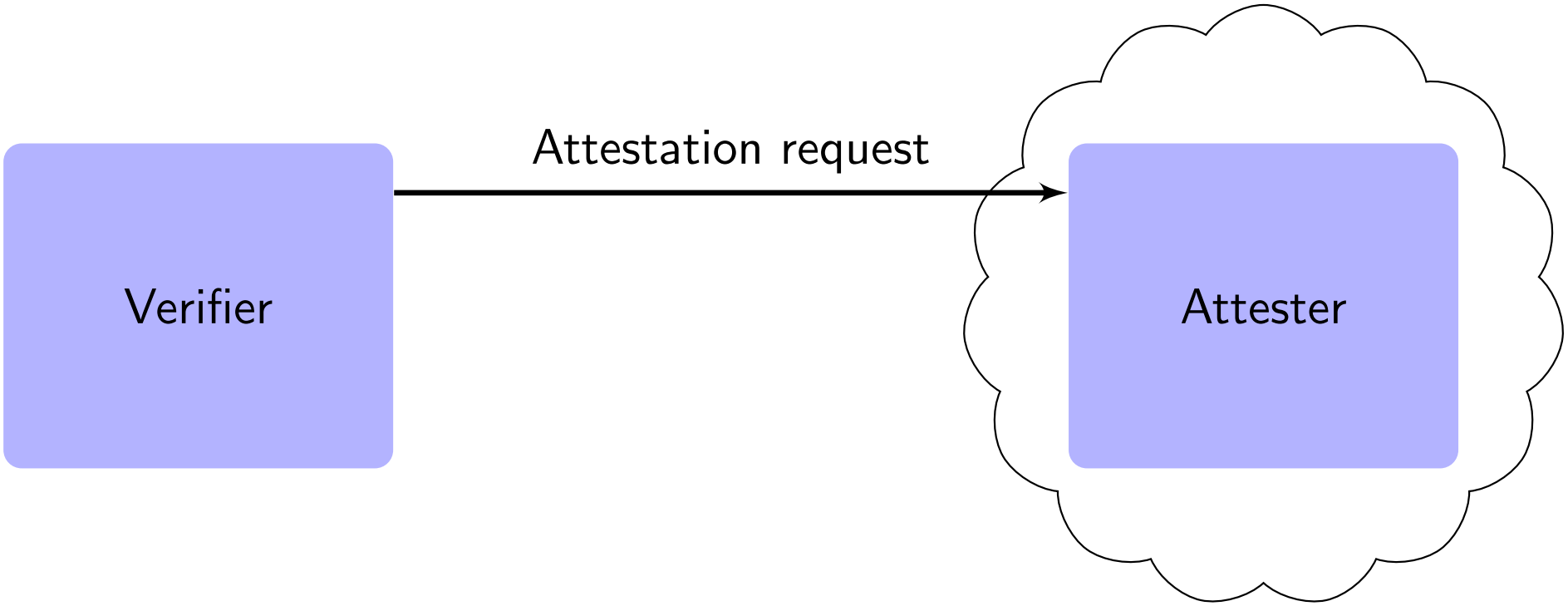
[1] Sardar and Fetzer, *Confidential Computing and Related Technologies : A Critical Review*, 2021.

Confidential Computing[1]

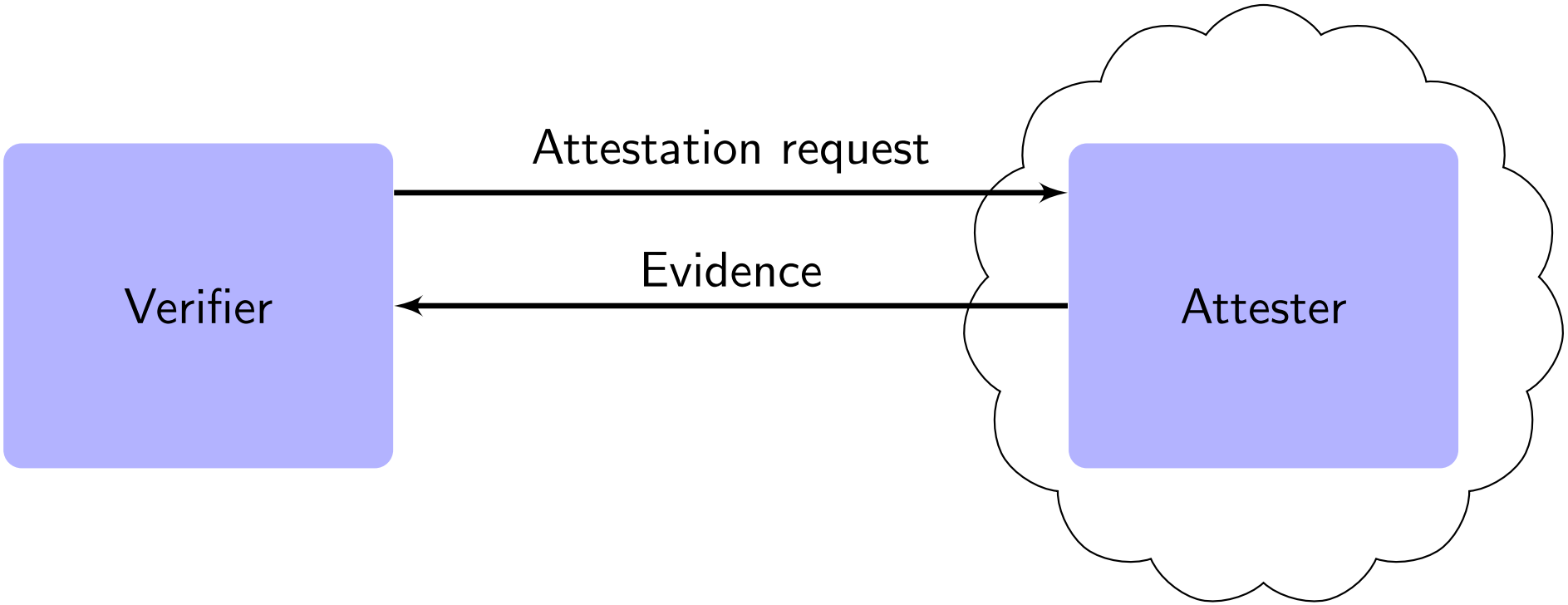


[1] Sardar and Fetzer, *Confidential Computing and Related Technologies : A Critical Review*, 2021.

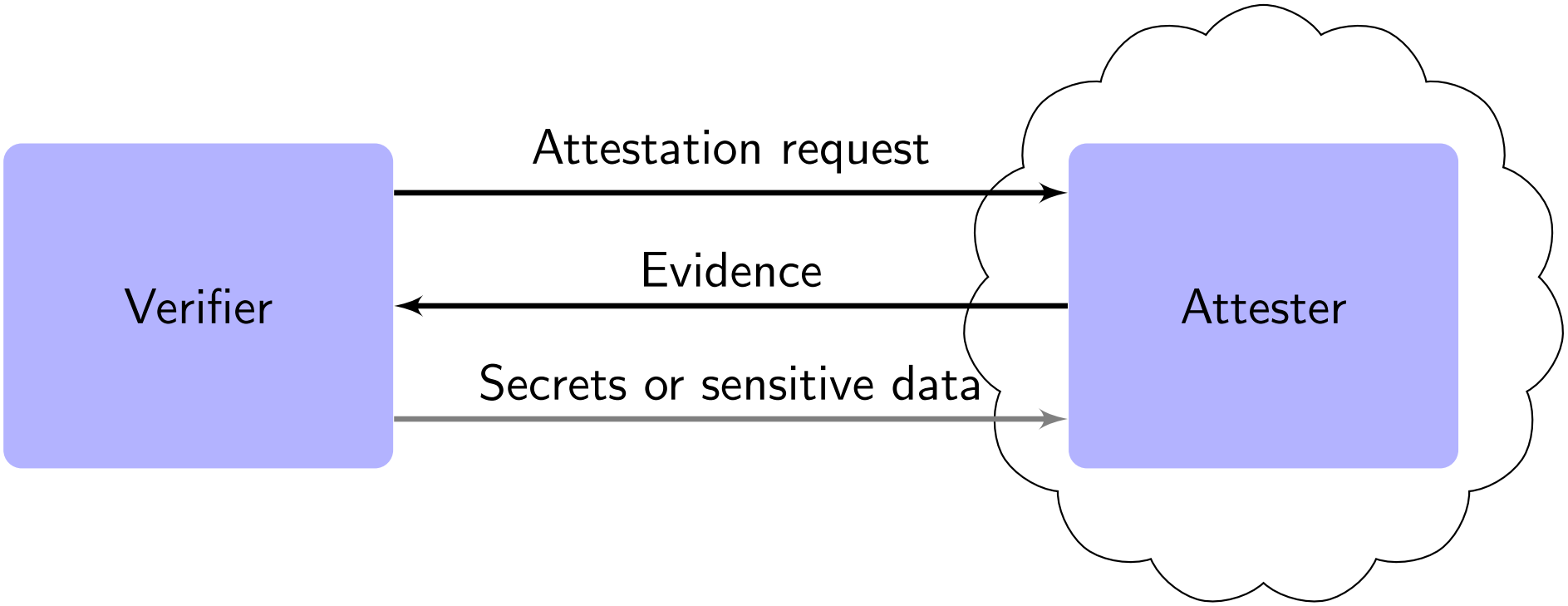
Attestation



Attestation

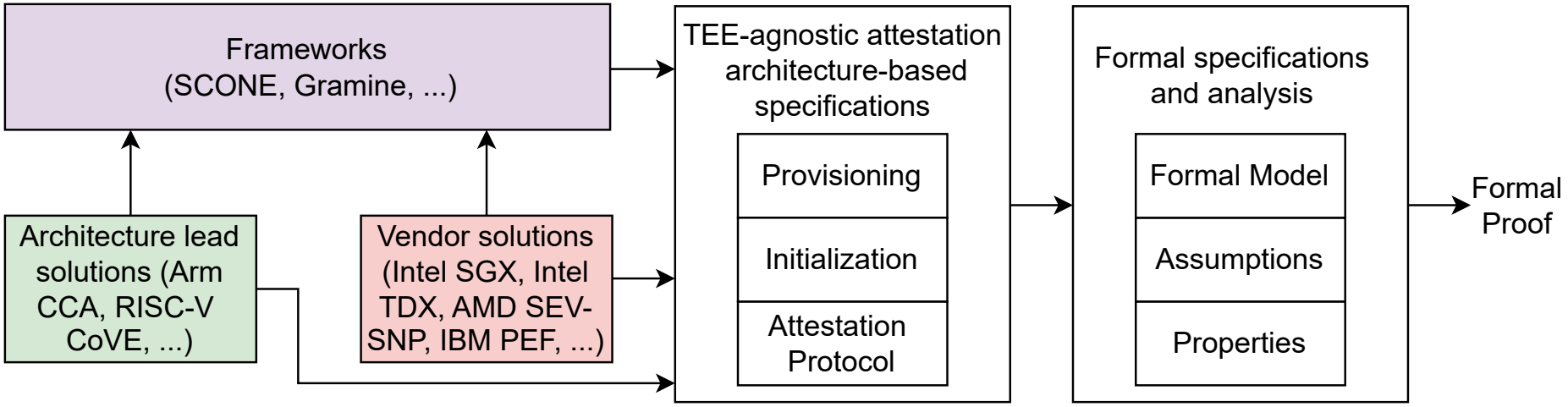


Attestation



Agenda

Overview of Approach



Formal Verification

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

Formal Verification

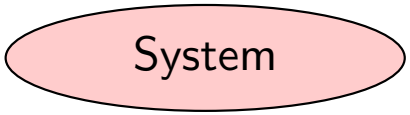
$$System \models Property \tag{1}$$

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

Formal Verification

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

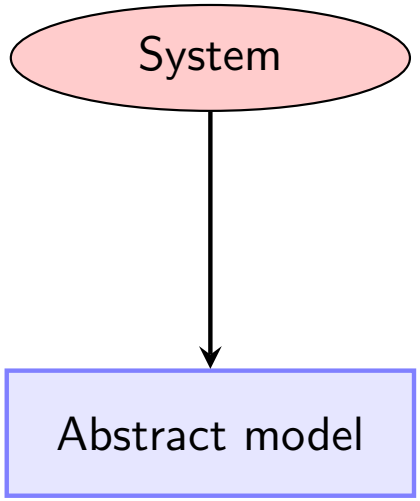
$$Protocol \parallel Adversary \models Property \tag{2}$$



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

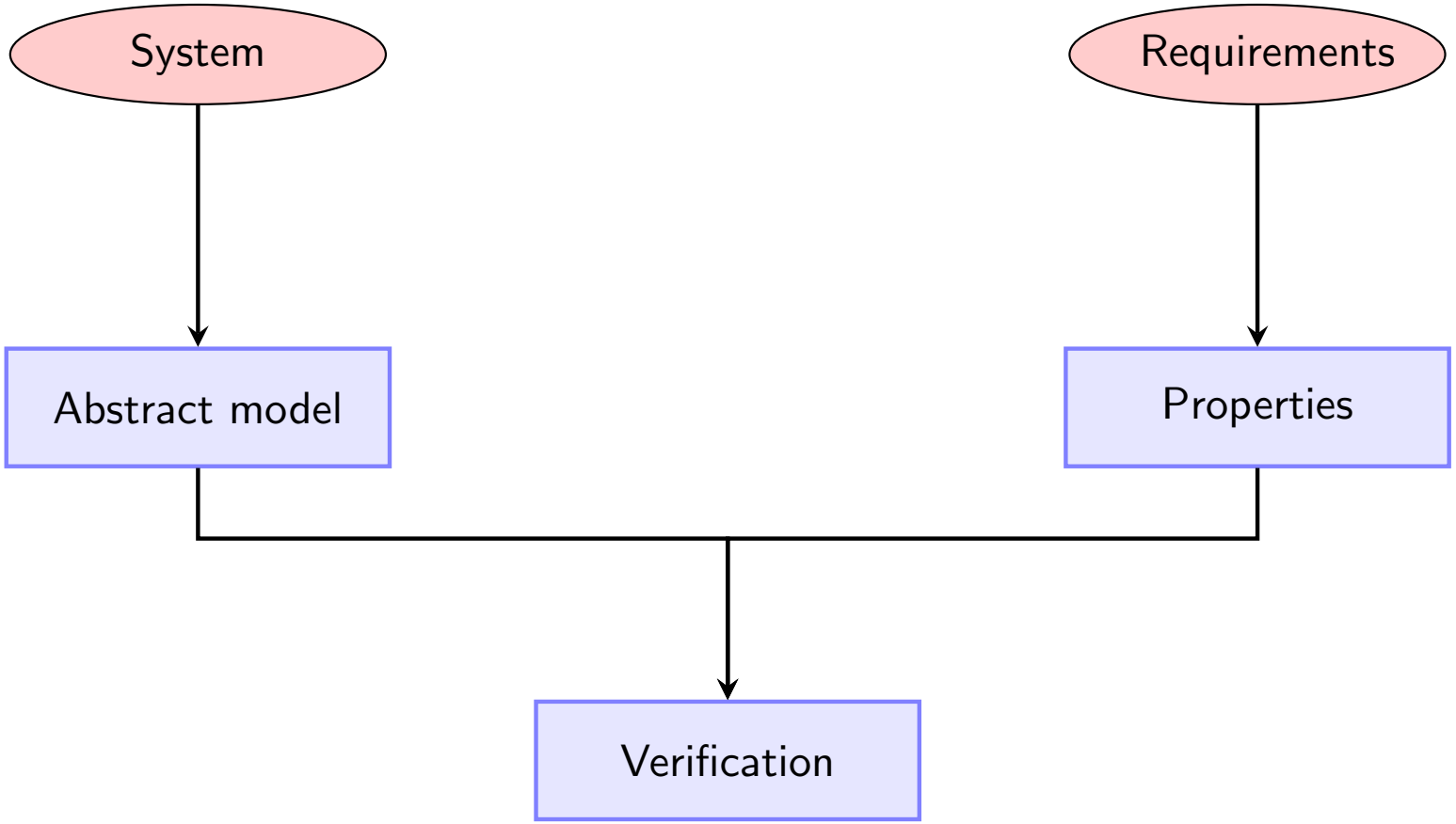
$$System \models Property \tag{1}$$

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

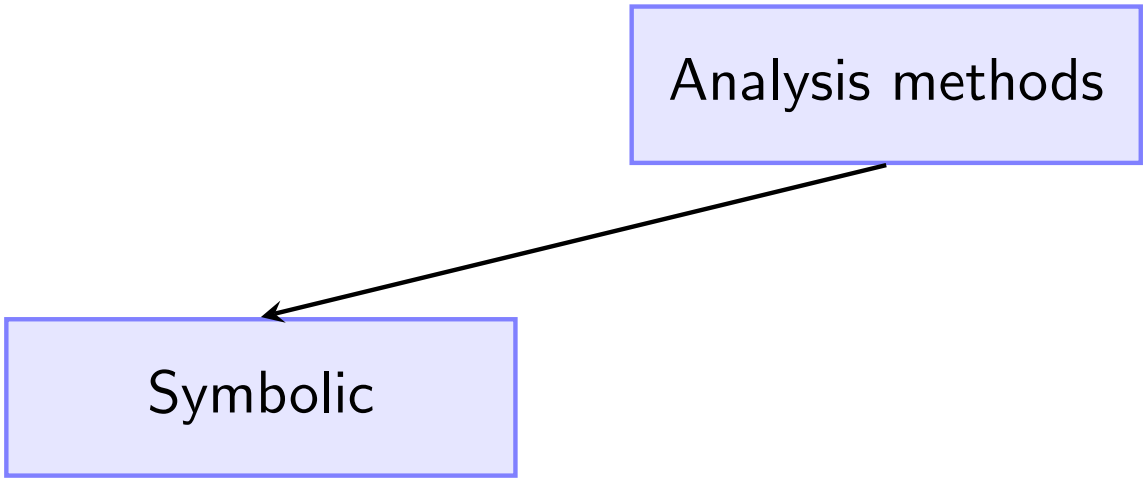
Formal Verification

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

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



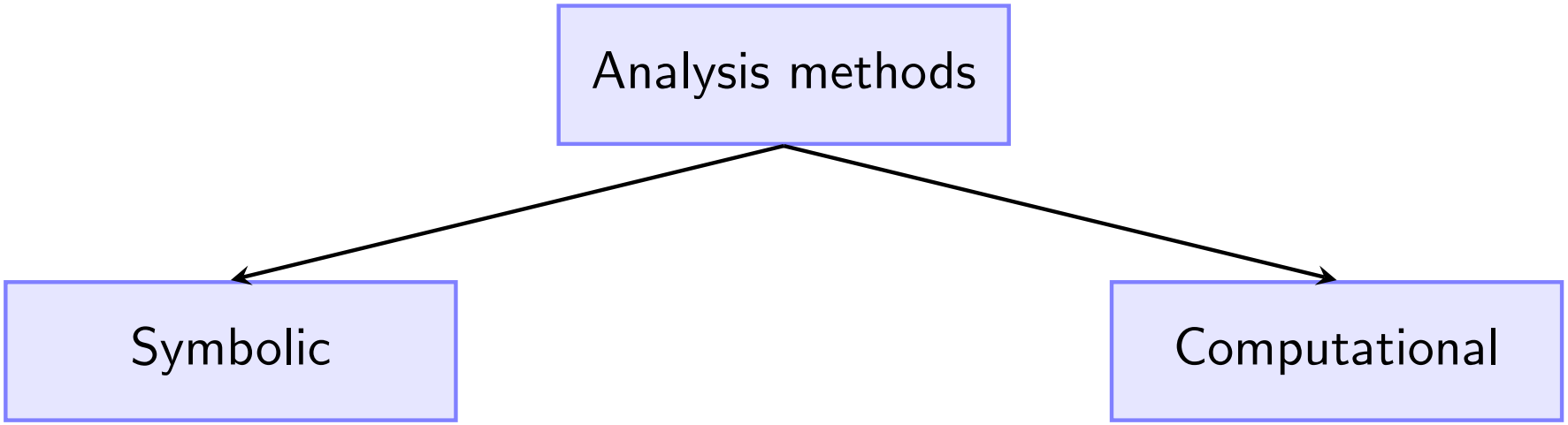
Analysis Approach[3] and Tool



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

[3] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021.

Analysis Approach[3] and Tool

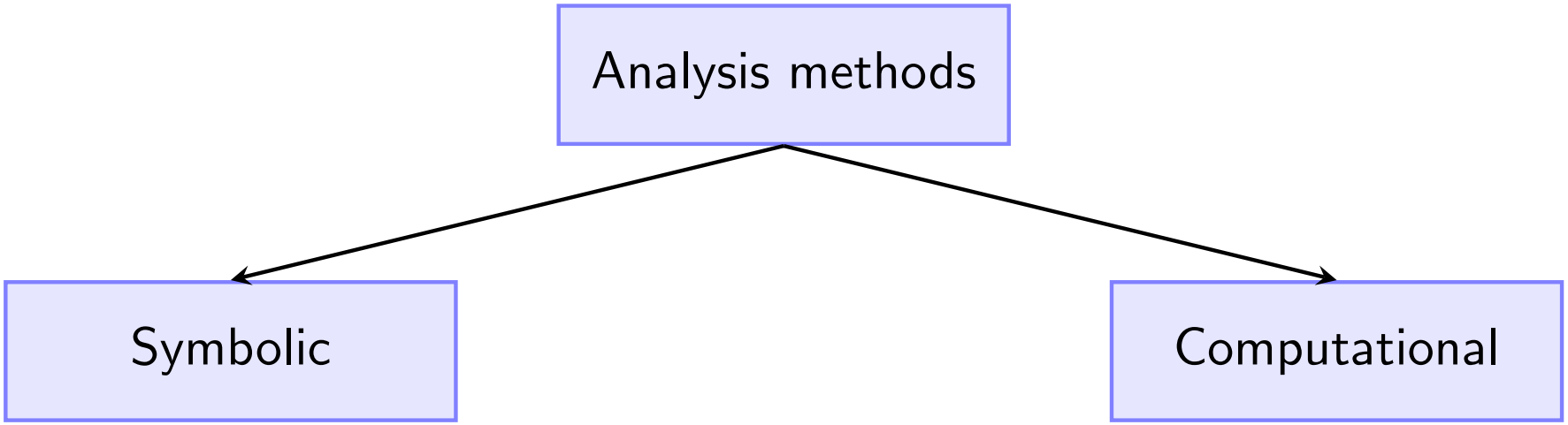


- Benefits of Symbolic

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

[3] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021.

Analysis Approach[3] and Tool

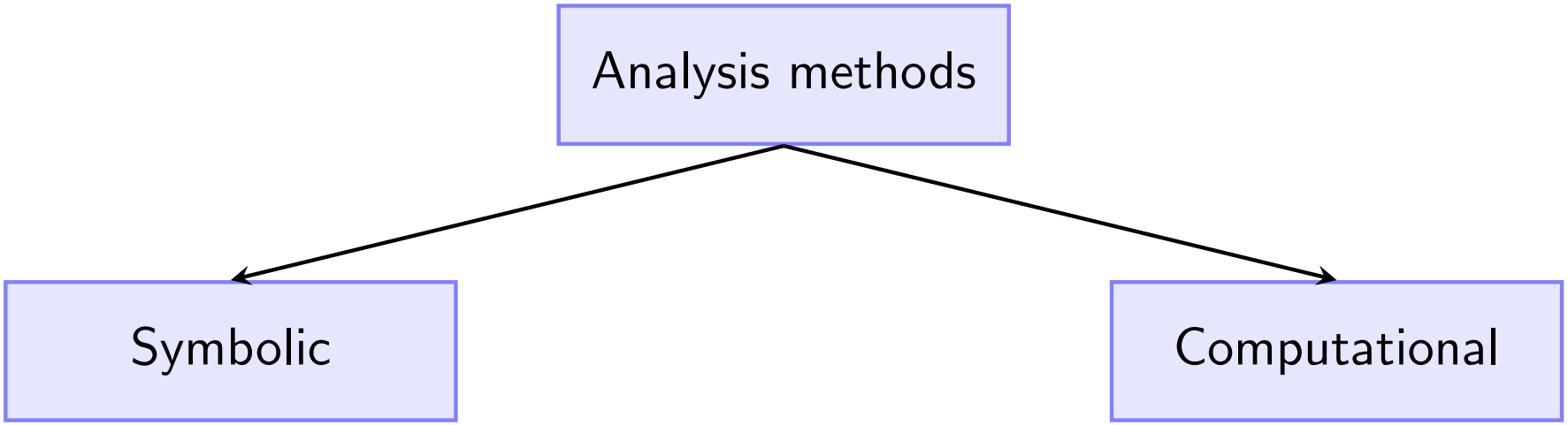


- Benefits of Symbolic
  - Reasonable level of abstraction

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

[3] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021.

Analysis Approach[3] and Tool

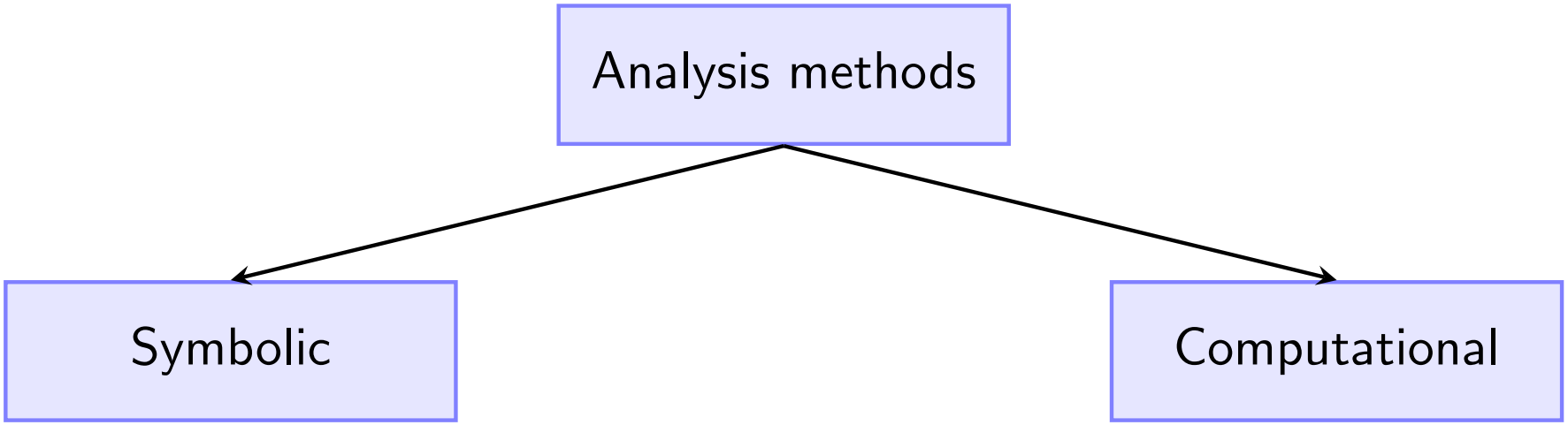


- Benefits of Symbolic
  - Reasonable level of abstraction
  - Unbounded number of sessions

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

[3] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021.

Analysis Approach[3] and Tool

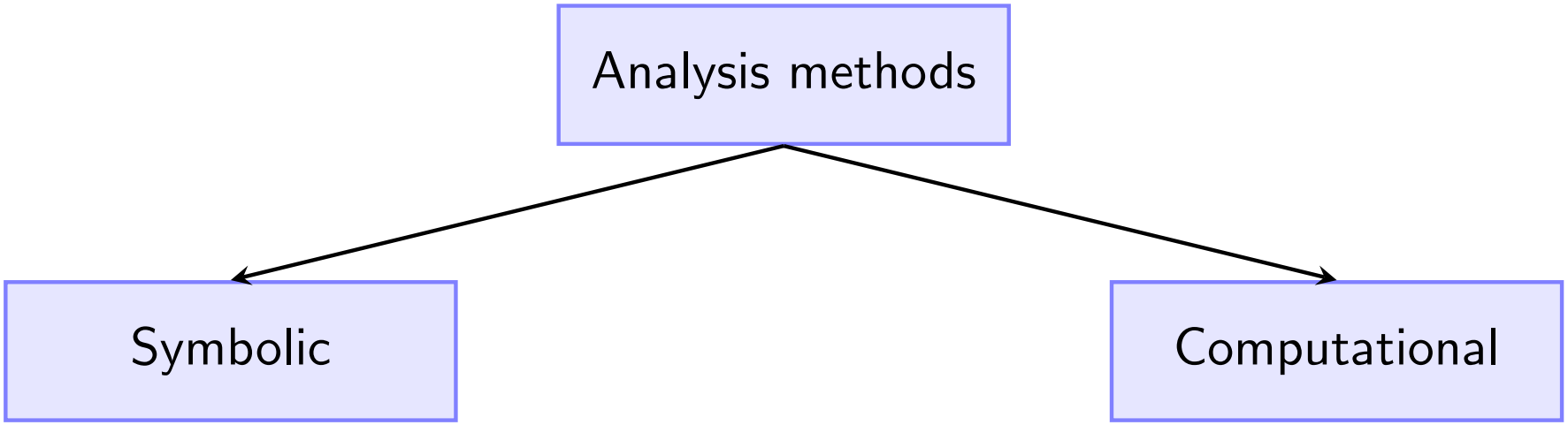


- Benefits of Symbolic
  - Reasonable level of abstraction
  - Unbounded number of sessions
- Limitation of Symbolic

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

[3] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021.

Analysis Approach[3] and Tool

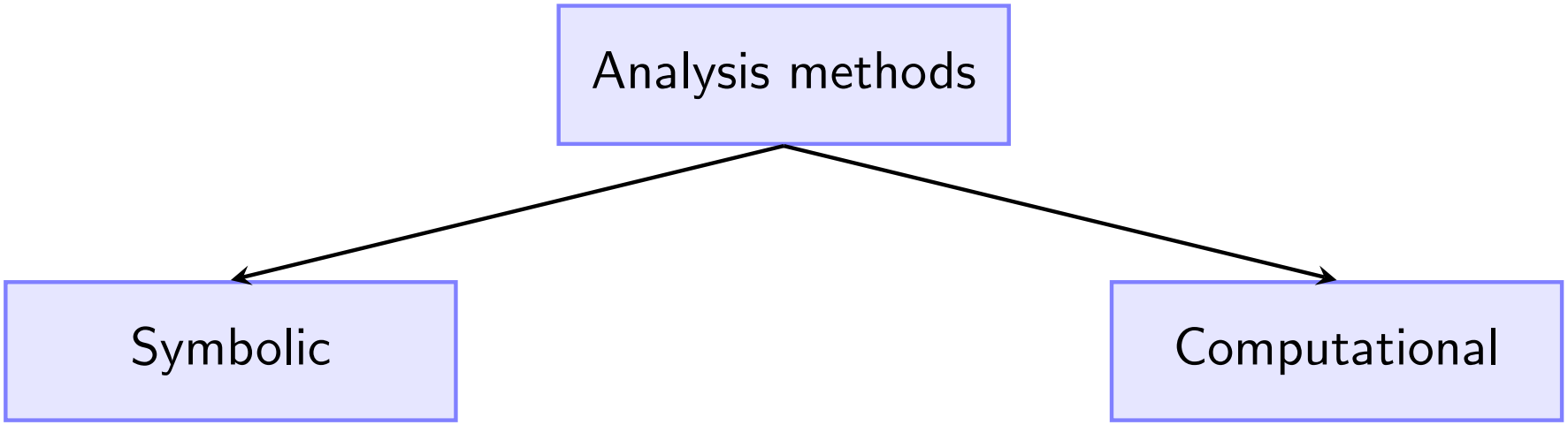


- Benefits of Symbolic
  - Reasonable level of abstraction
  - Unbounded number of sessions
- Limitation of Symbolic
  - Perfect cryptographic primitives

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

[3] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021.

Analysis Approach[3] and Tool

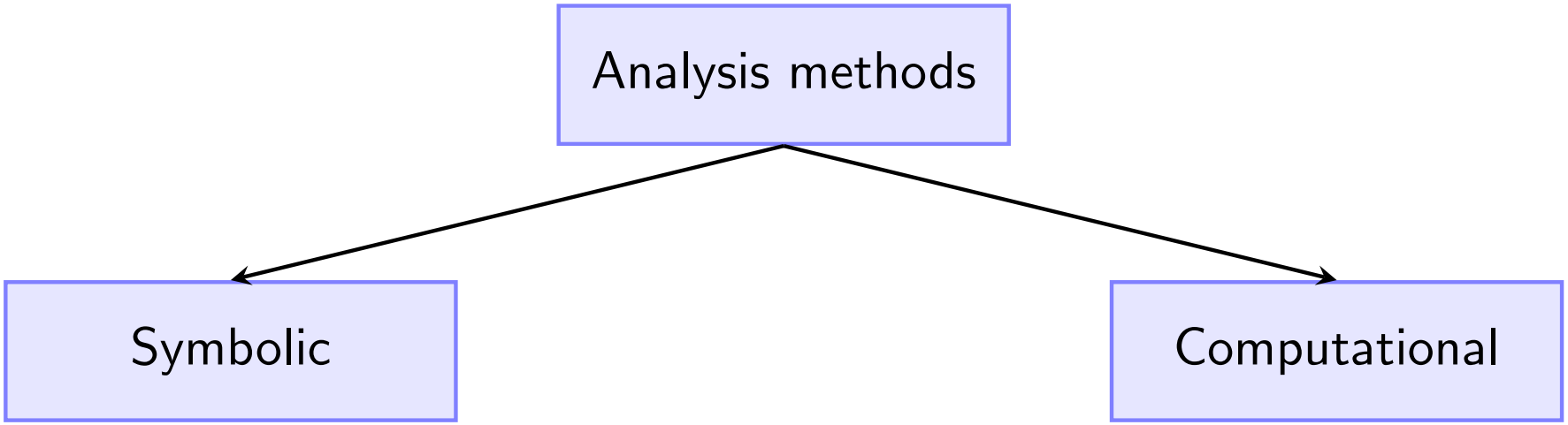


- Benefits of Symbolic
  - Reasonable level of abstraction
  - Unbounded number of sessions
- Limitation of Symbolic
  - Perfect cryptographic primitives
  - Side-channels out of scope

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

[3] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021.

Analysis Approach[3] and Tool

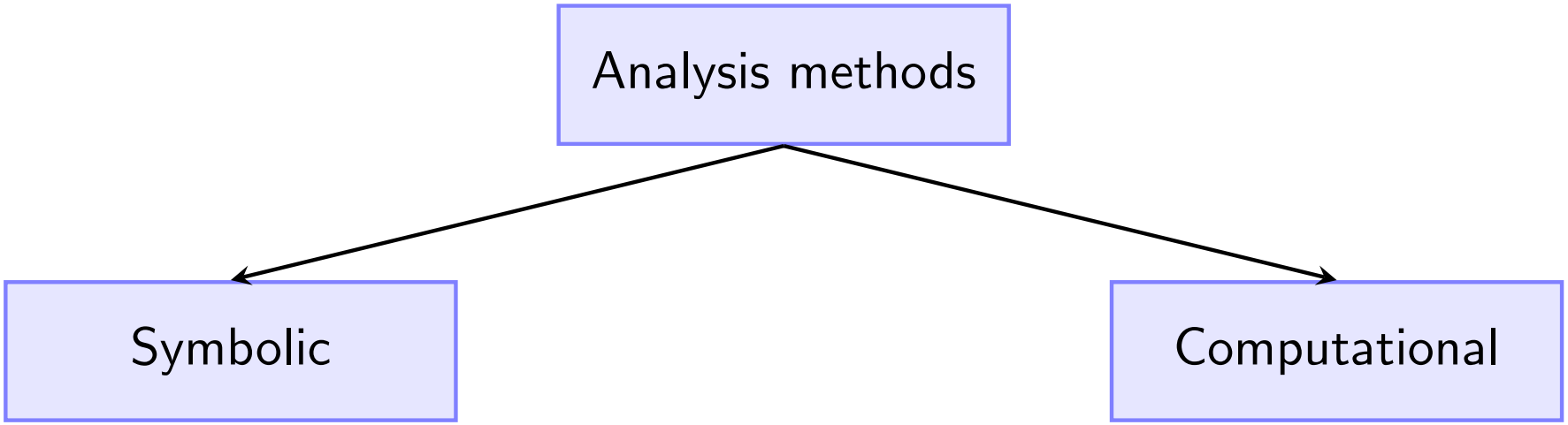


- Benefits of Symbolic
  - Reasonable level of abstraction
  - Unbounded number of sessions
- Limitation of Symbolic
  - Perfect cryptographic primitives
  - Side-channels out of scope
- Tool used: ProVerif[2]

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

[3] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021.

Analysis Approach[3] and Tool

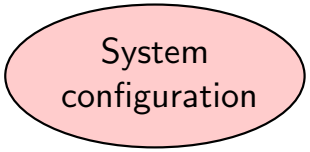


- Benefits of Symbolic
  - Reasonable level of abstraction
  - Unbounded number of sessions
- Limitation of Symbolic
  - Perfect cryptographic primitives
  - Side-channels out of scope
- Tool used: ProVerif[2]
  - Faster and extension to computational proofs (CryptoVerif)

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

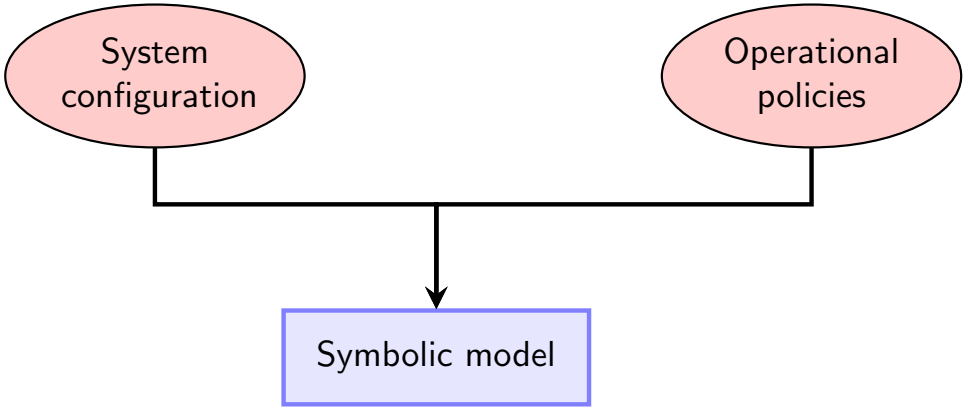
[3] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021.

Workflow of the Analysis Approach

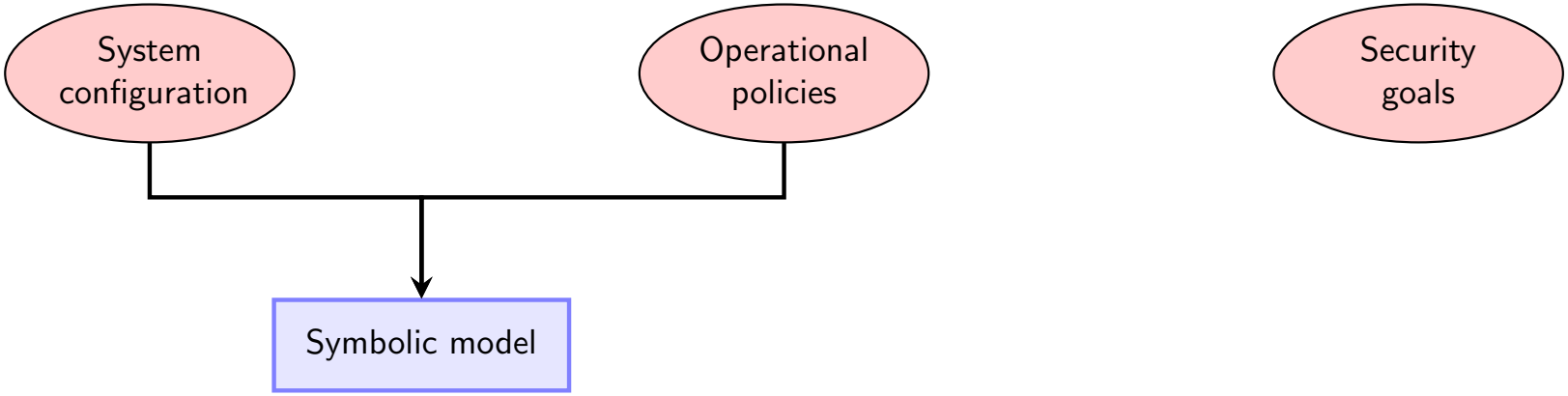


Workflow of the Analysis Approach

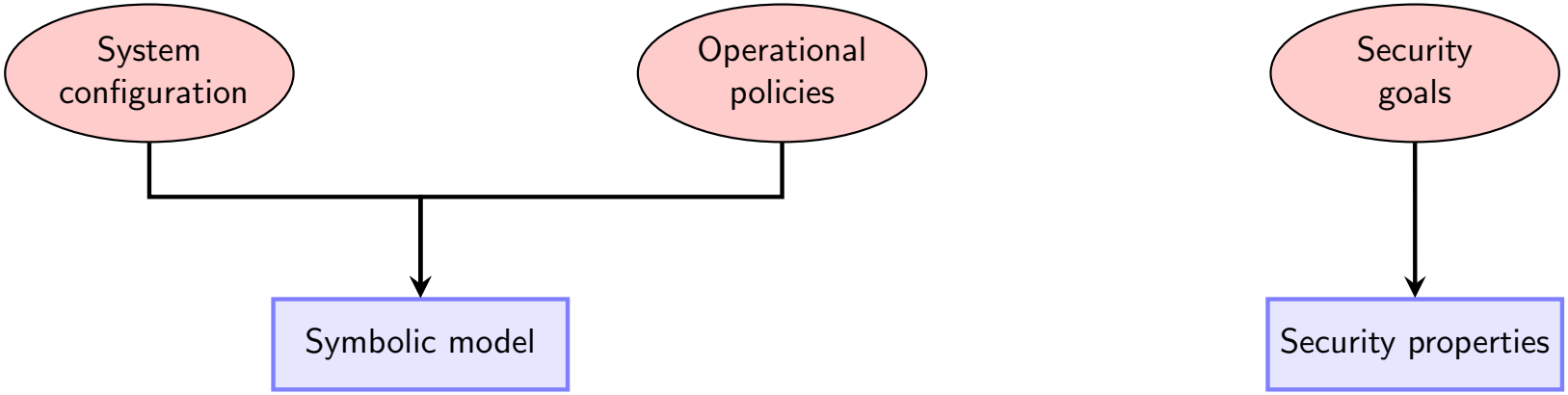
Workflow of the Analysis Approach



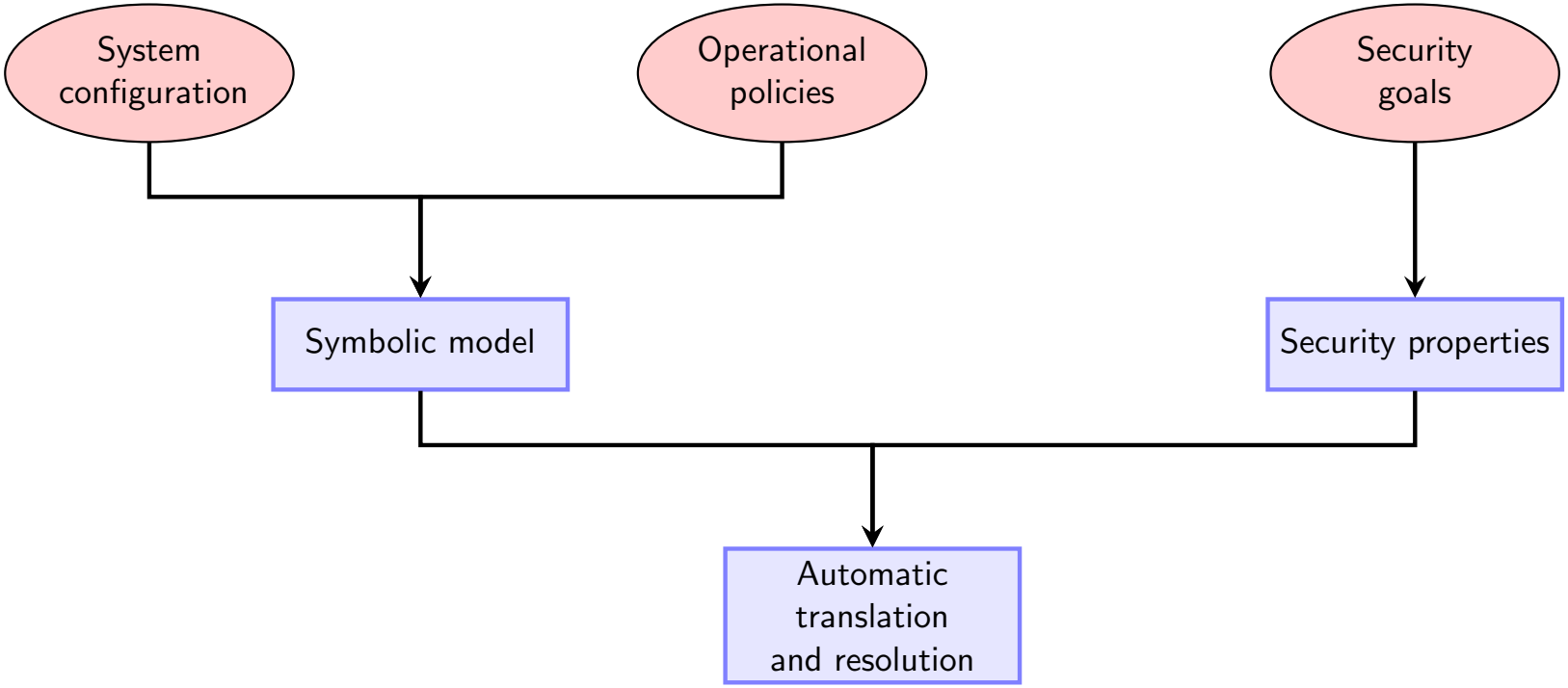
Workflow of the Analysis Approach



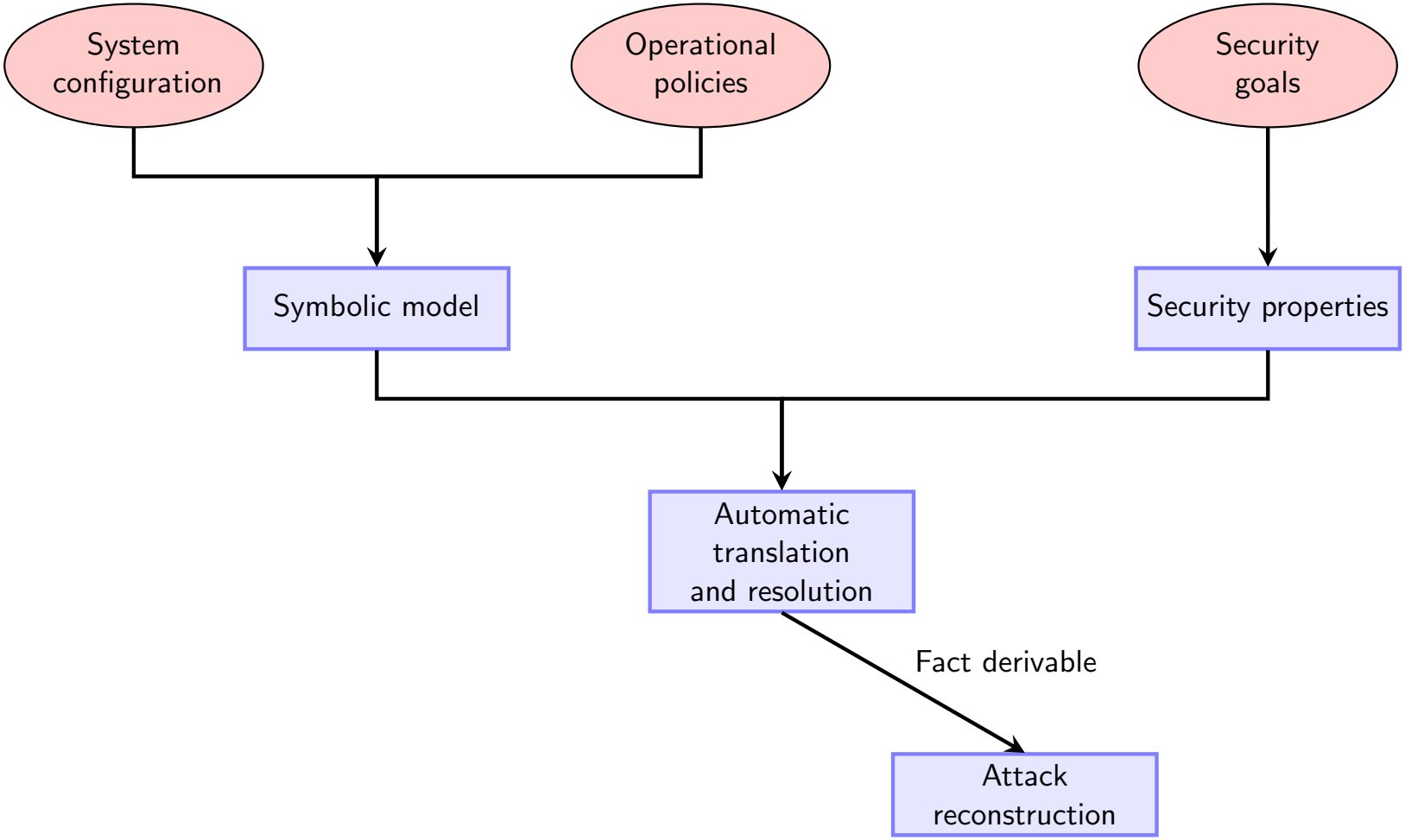
Workflow of the Analysis Approach



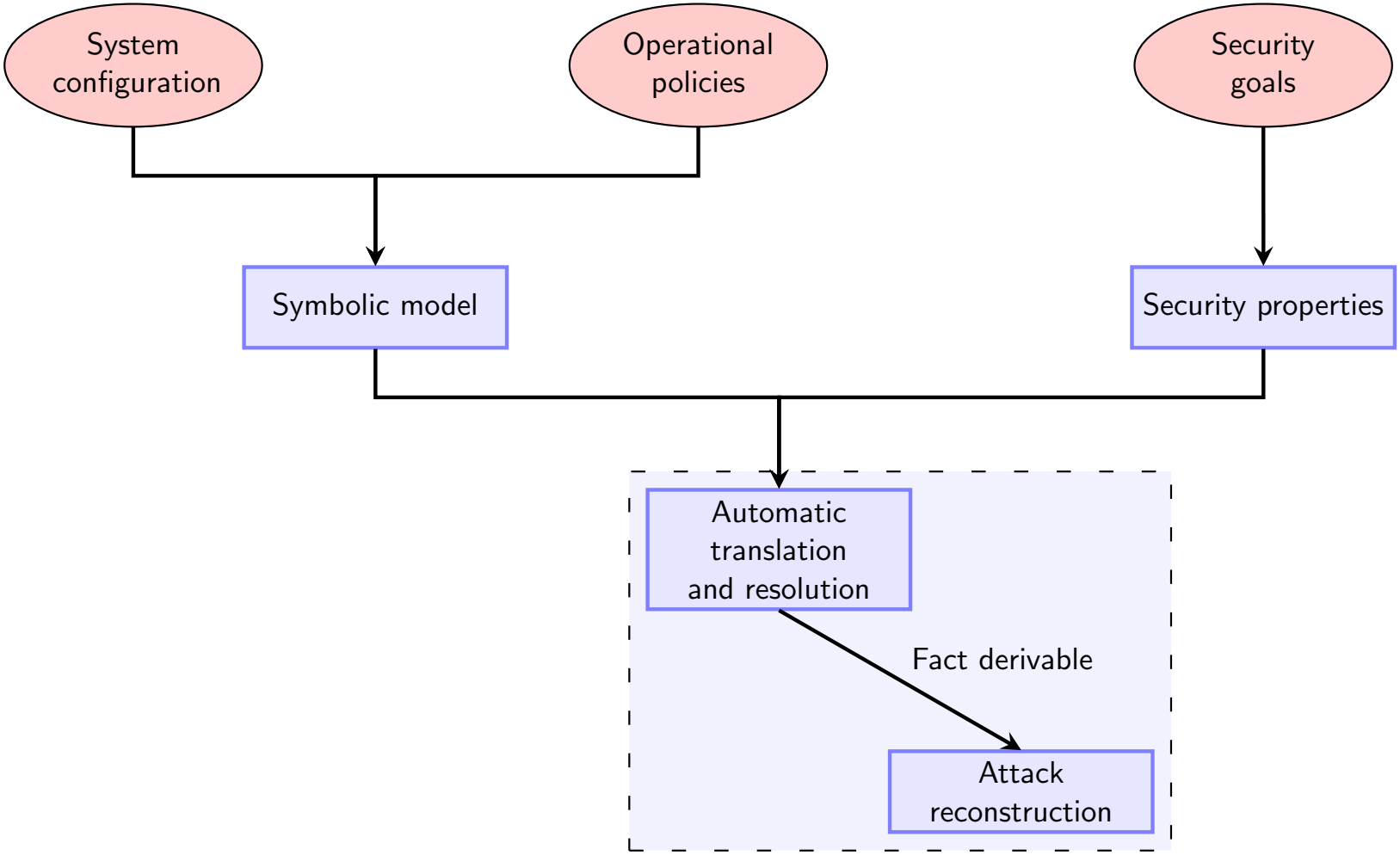
Workflow of the Analysis Approach



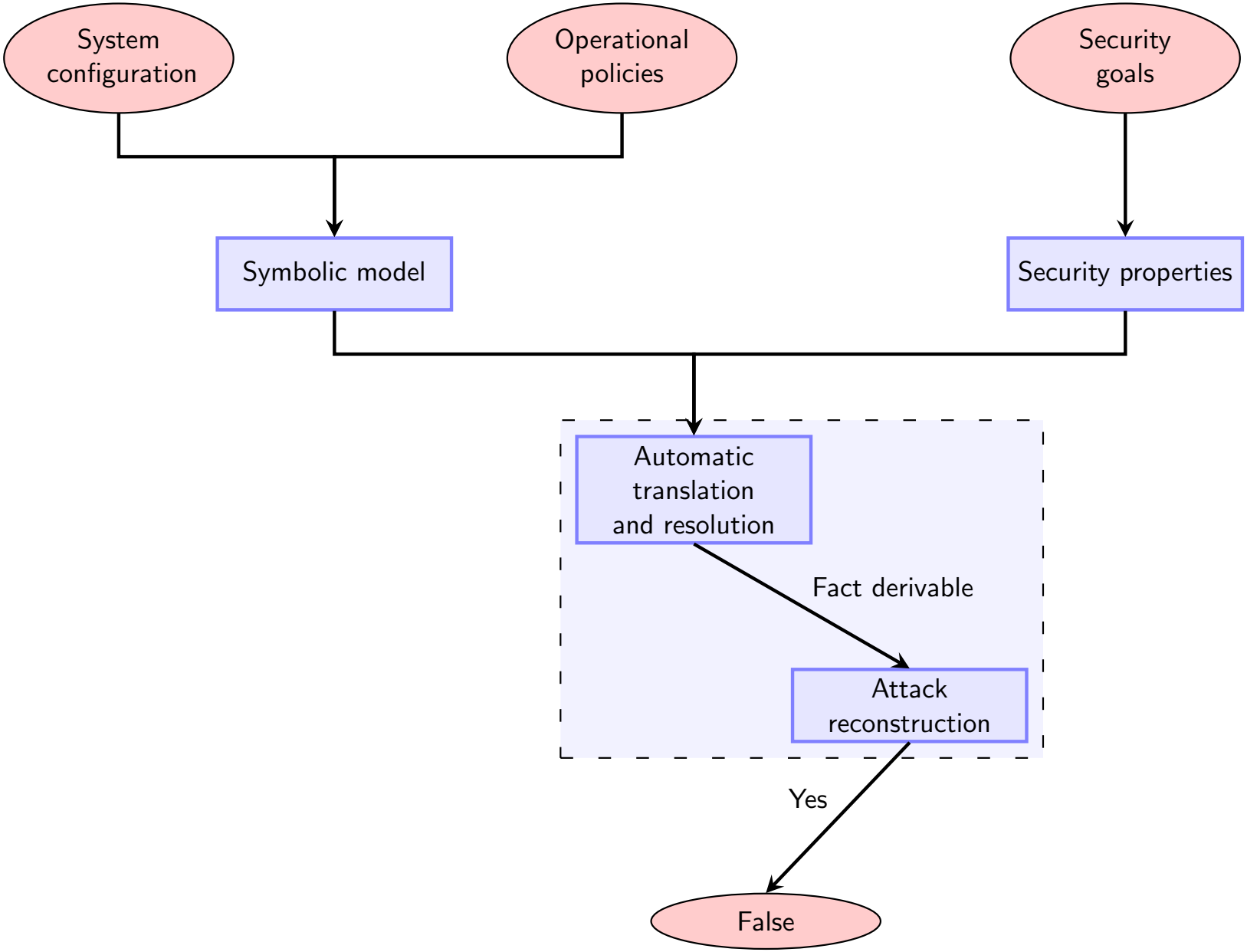
Workflow of the Analysis Approach



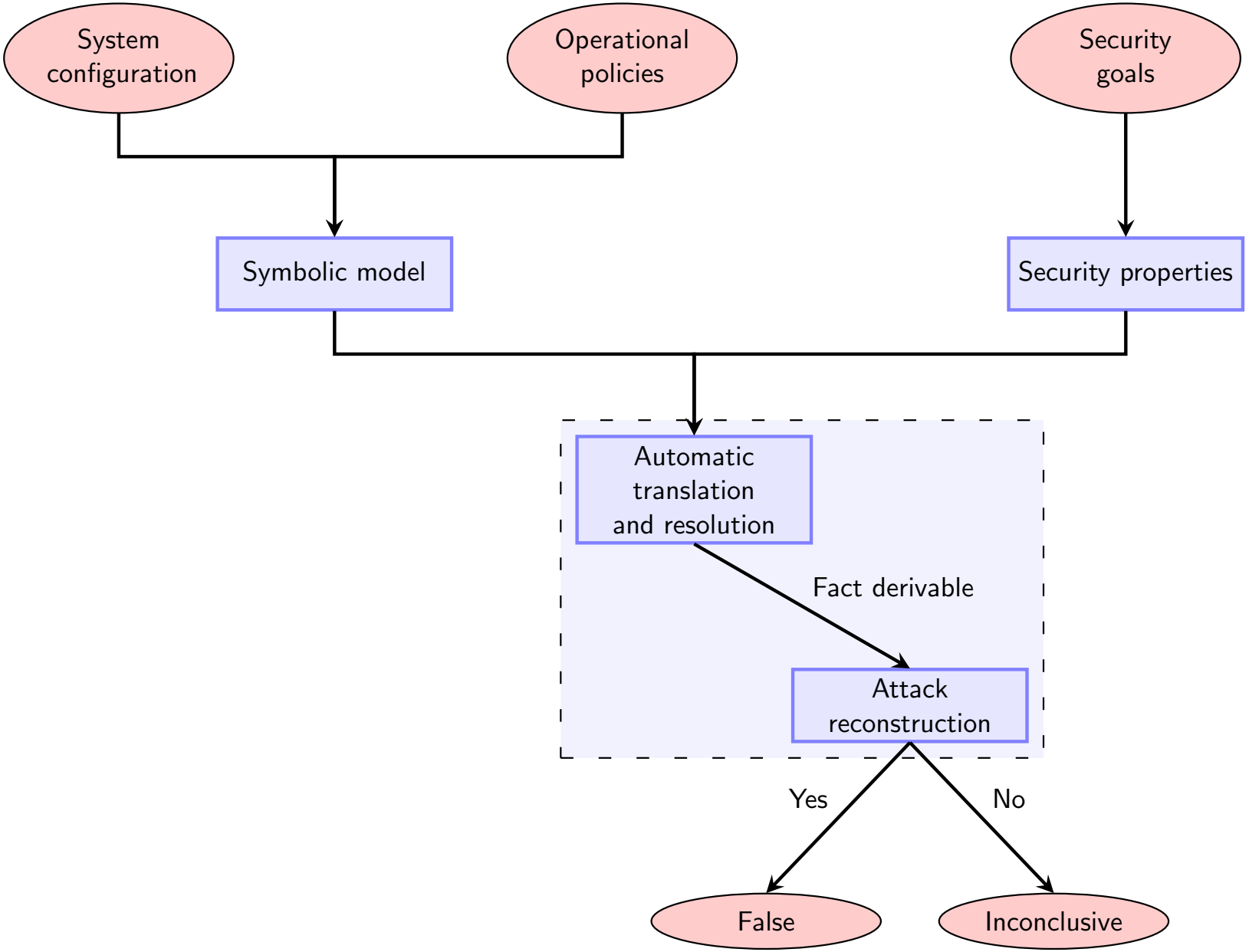
Workflow of the Analysis Approach



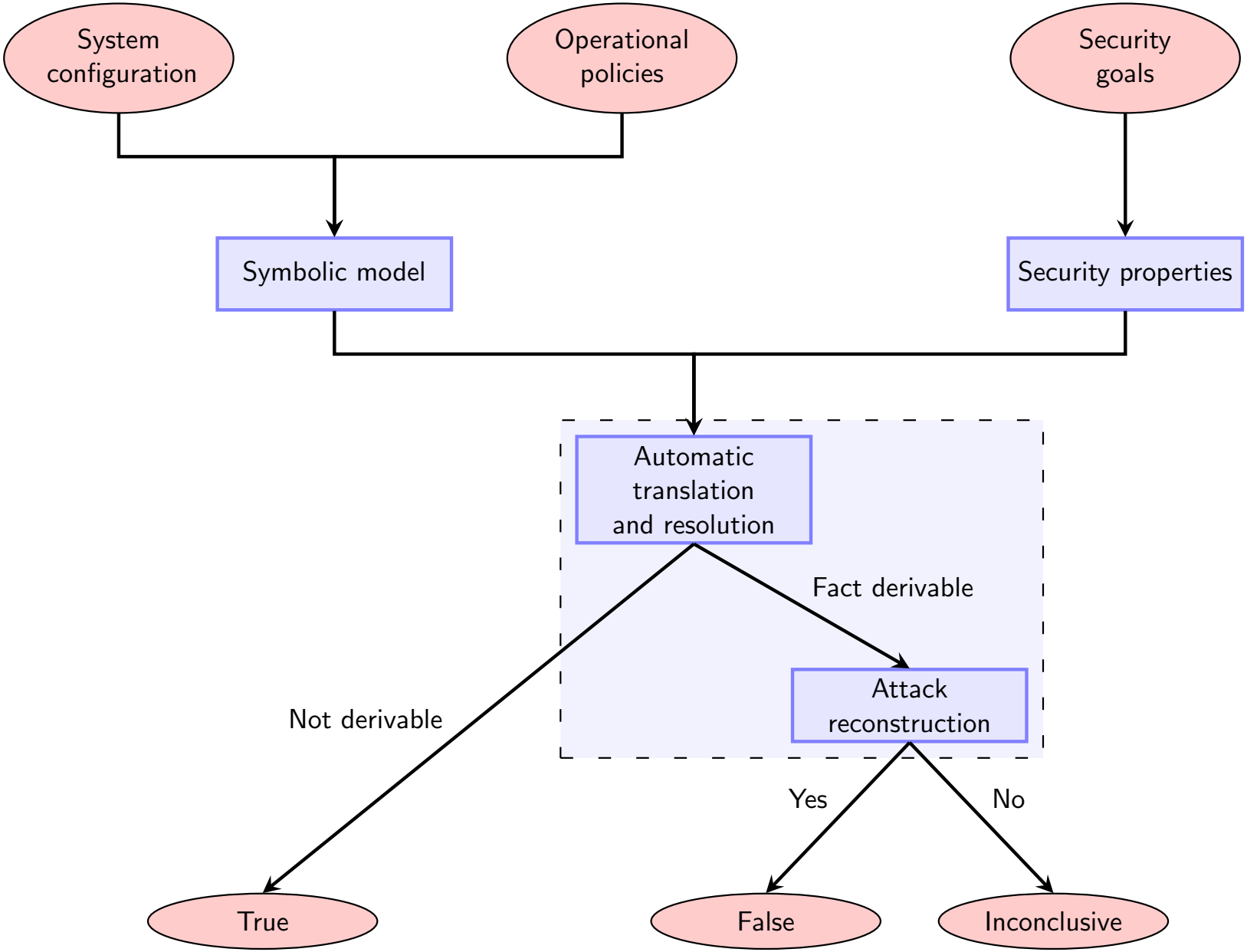
Workflow of the Analysis Approach



Workflow of the Analysis Approach



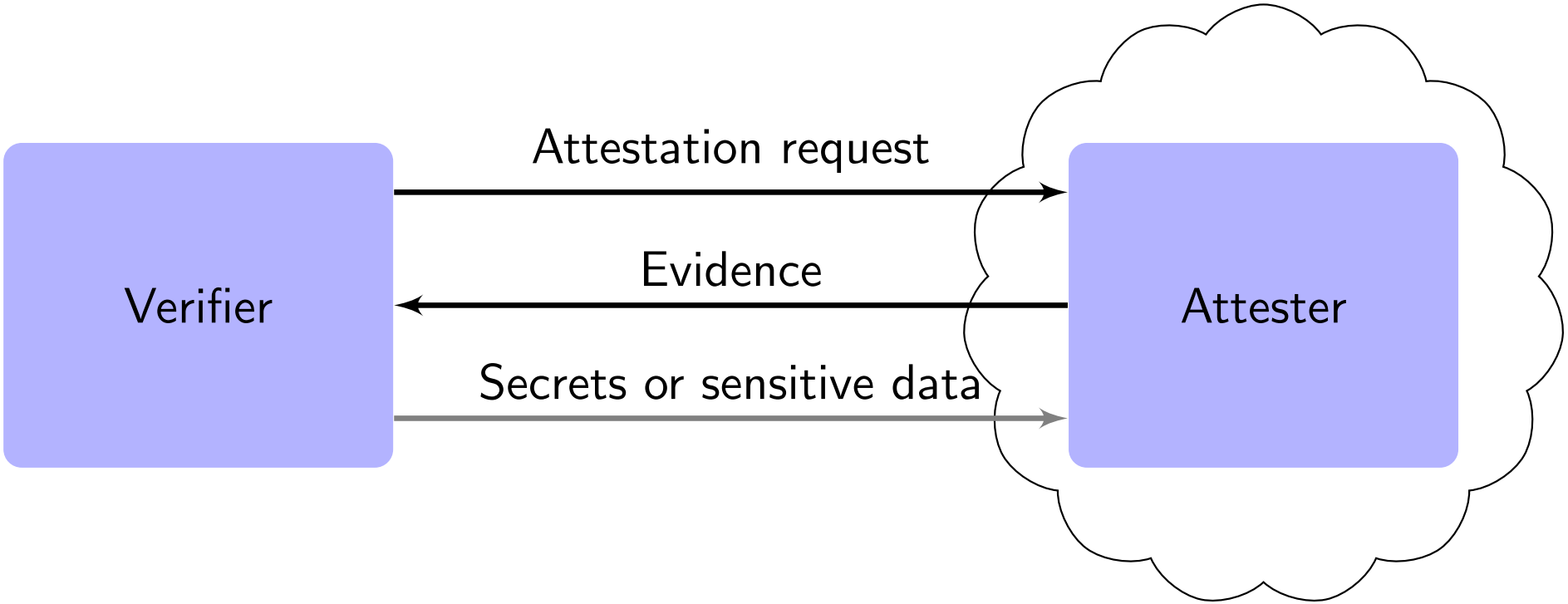
Workflow of the Analysis Approach



Agenda

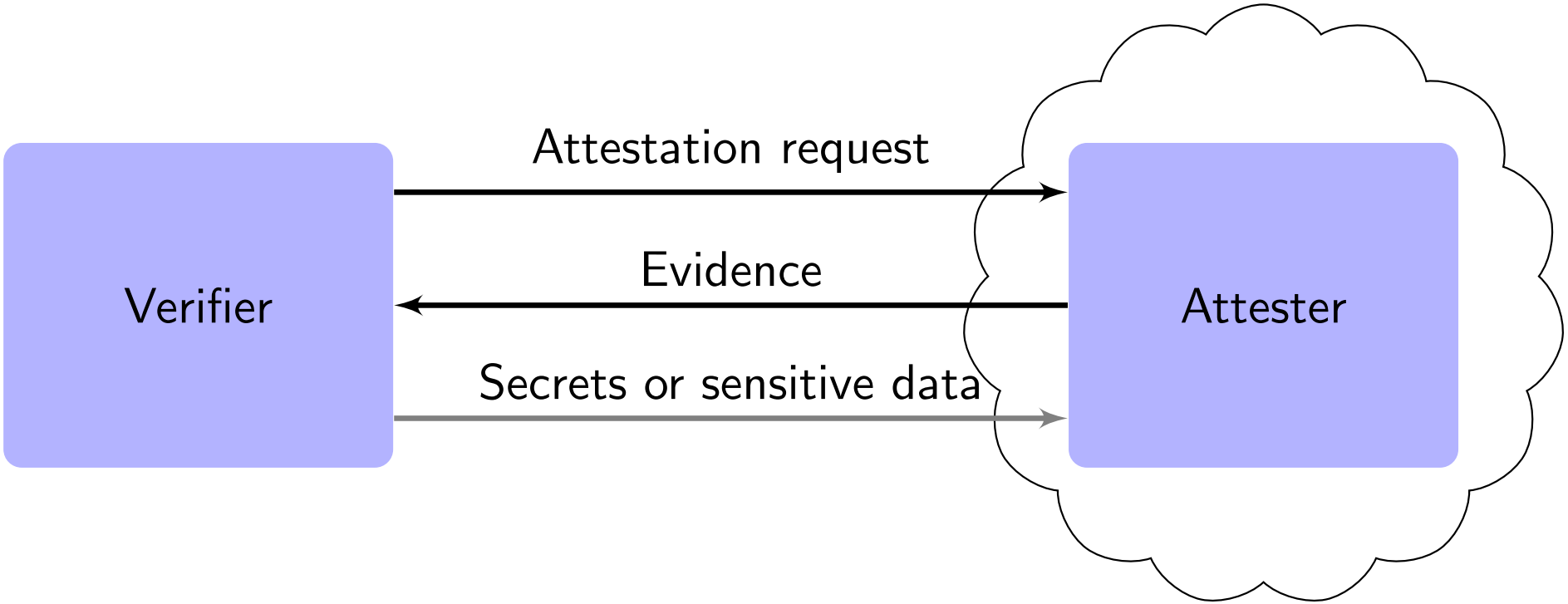
2. Approach
   - Properties
   - Model
   - Threat Model

Properties



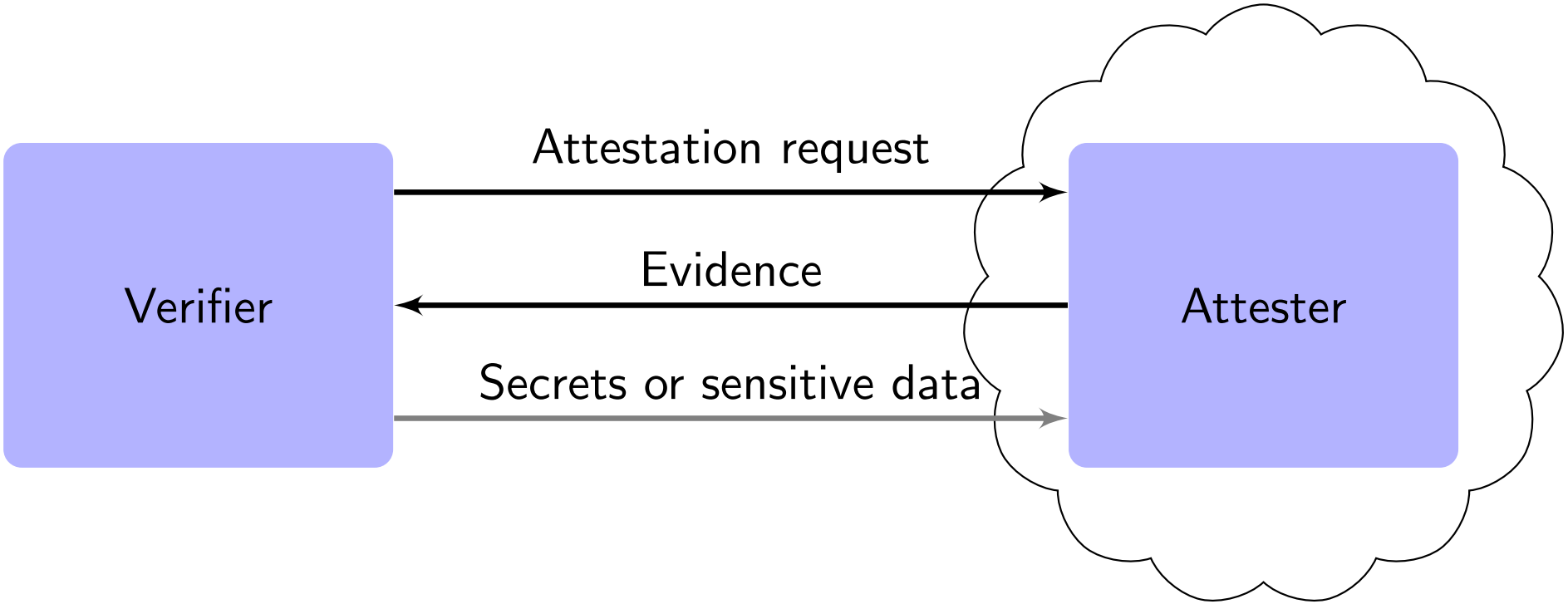
- Integrity (Data/Message) (motivation: identity fields)

Properties



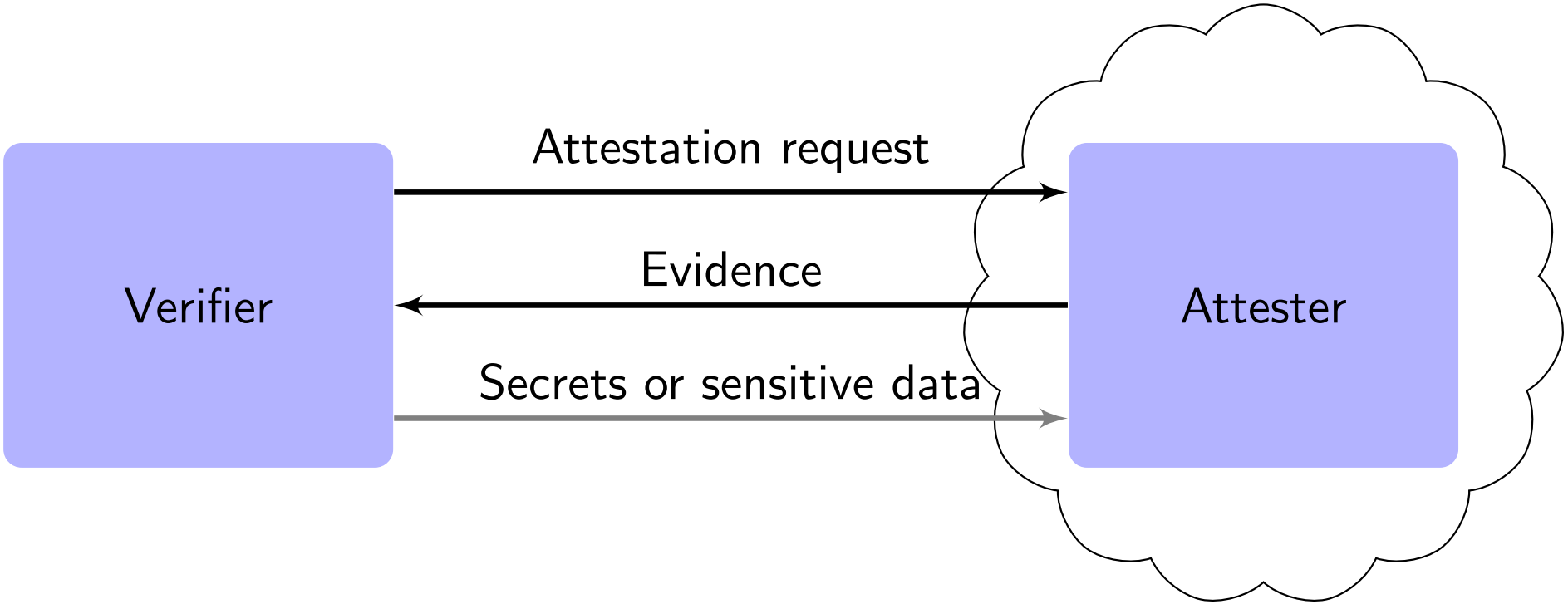
- Integrity (Data/Message) (motivation: identity fields)
- Authentication (Data origin/Sender)

Properties



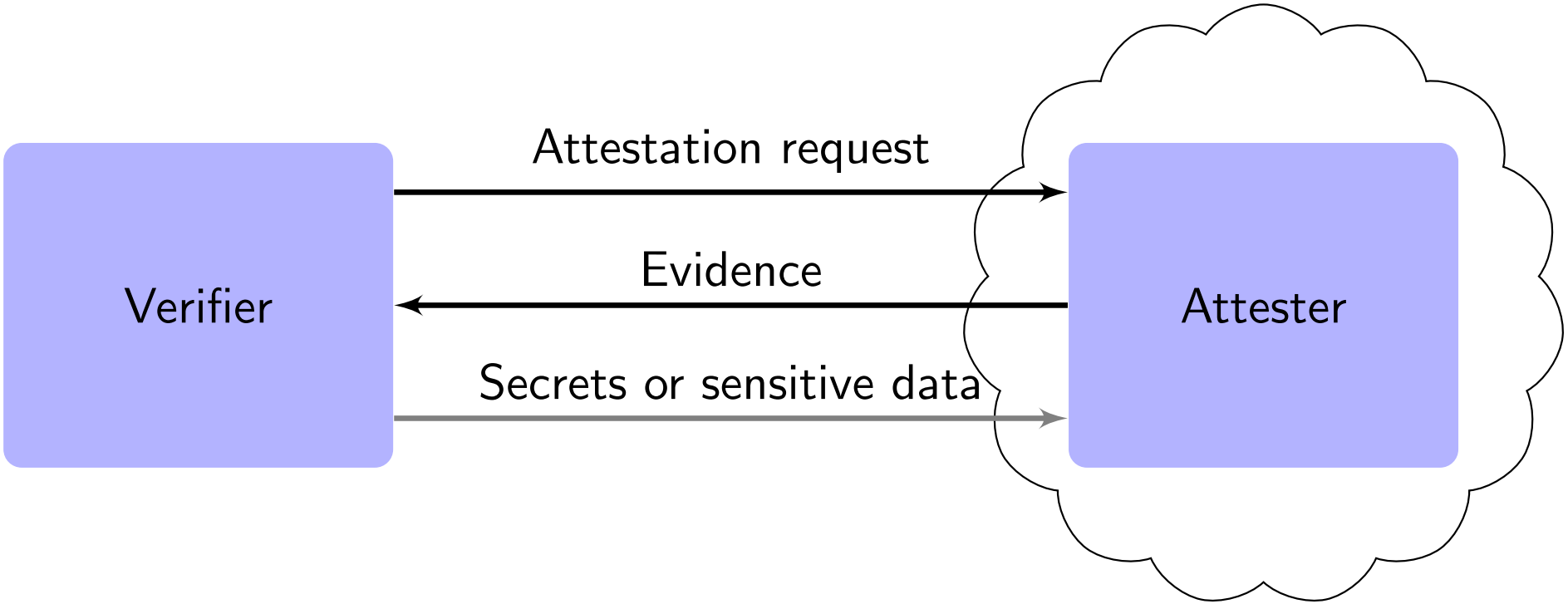
- Integrity (Data/Message) (motivation: identity fields)
- Authentication (Data origin/Sender)
- Freshness

Properties



- Integrity (Data/Message) (motivation: identity fields)
- Authentication (Data origin/Sender)
- Freshness
- Confidentiality/Secrecy

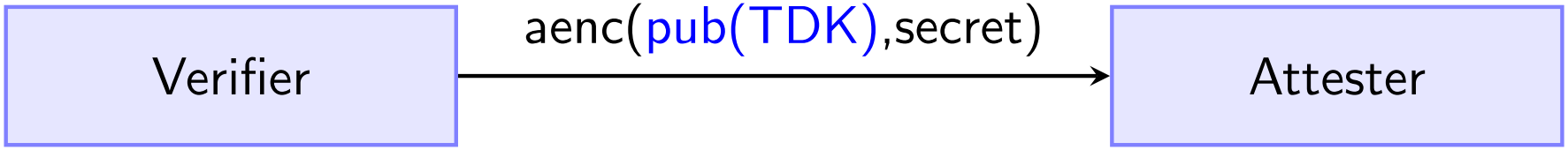
Properties



- Integrity (Data/Message) (motivation: identity fields)
- Authentication (Data origin/Sender)
- Freshness
- Confidentiality/Secrecy
- Sanity checks

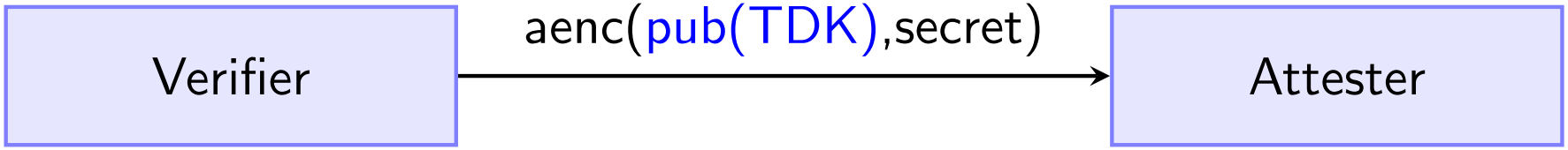
Specification of Security Goals

- Confidentiality of secret



Specification of Security Goals

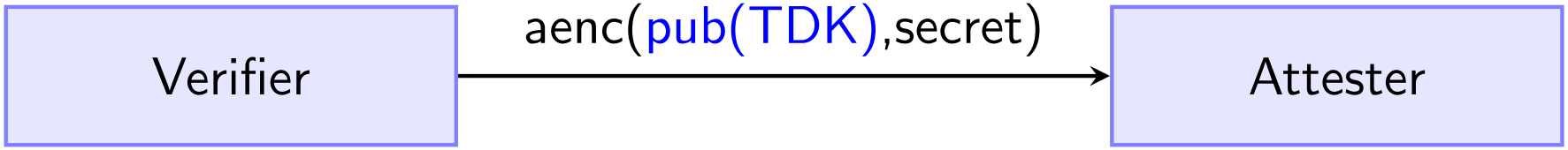
- Confidentiality of secret



  - Formalized as a reachability property

Specification of Security Goals

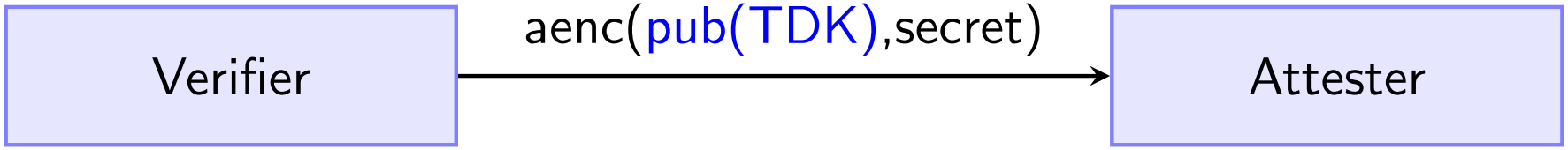
- Confidentiality of secret



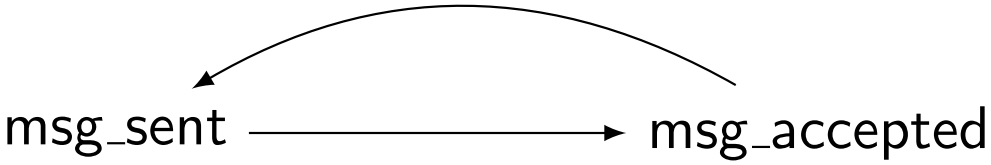
  - Formalized as a reachability property
- Integrity of Evidence

Specification of Security Goals

- Confidentiality of secret

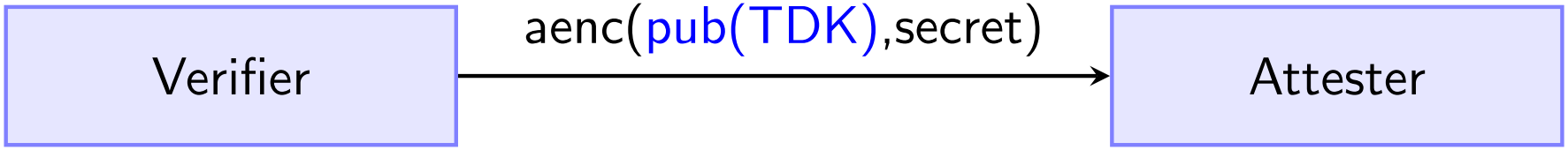


  - Formalized as a reachability property
- Integrity of Evidence

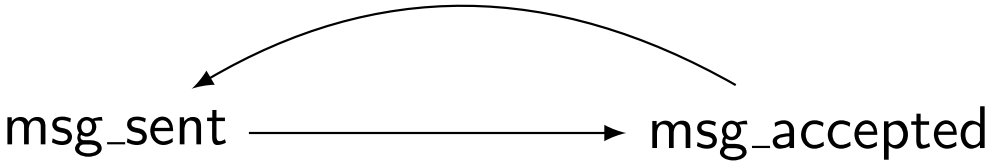


Specification of Security Goals

- Confidentiality of secret



  - Formalized as a reachability property
- Integrity of Evidence

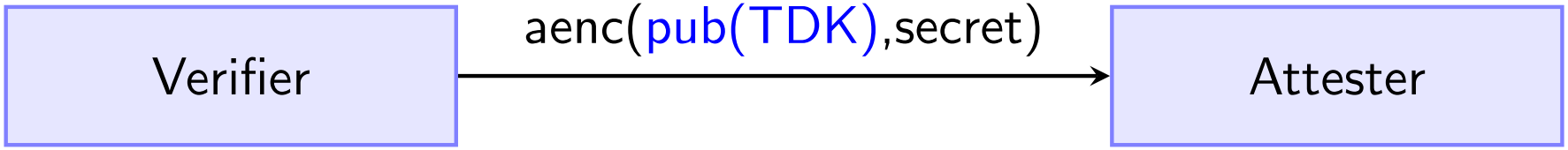


  - Correspondence assertions with $x_1, ..., x_n$ as variables of agreement

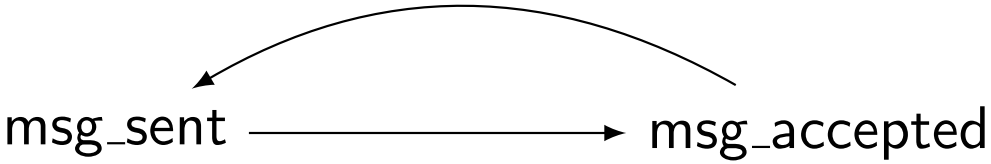
$$\texttt{query}\ x_1 : t_1, ..., x_n : t_n\texttt{;}$$
$$\texttt{event}\ (msg\_accepted(x_1, ..., x_n))\ \texttt{==>}\ \texttt{event}\ (msg\_sent(x_1, ..., x_n)). \tag{3}$$

Specification of Security Goals

- Confidentiality of secret



  - Formalized as a reachability property
- Integrity of Evidence

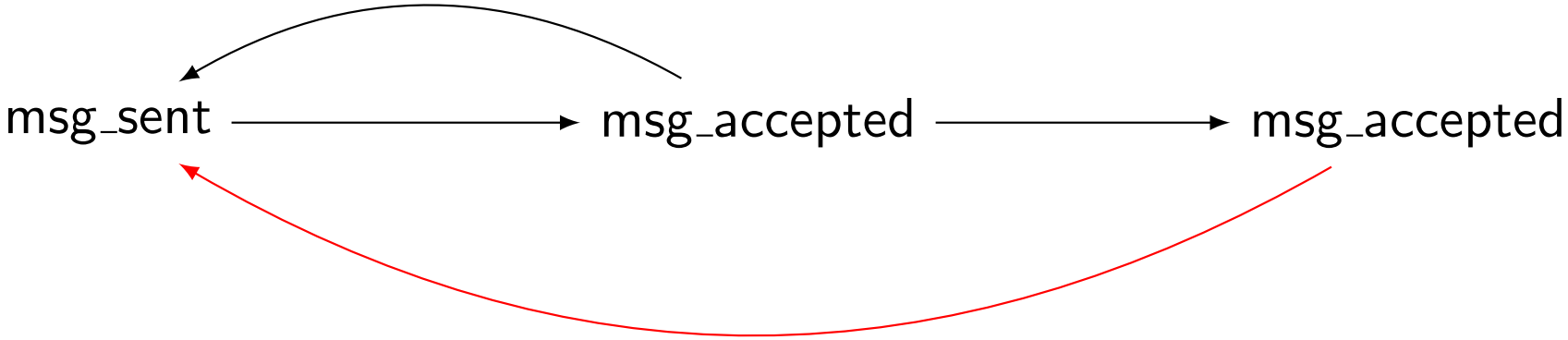


  - Correspondence assertions with $x_1, ..., x_n$ as variables of agreement

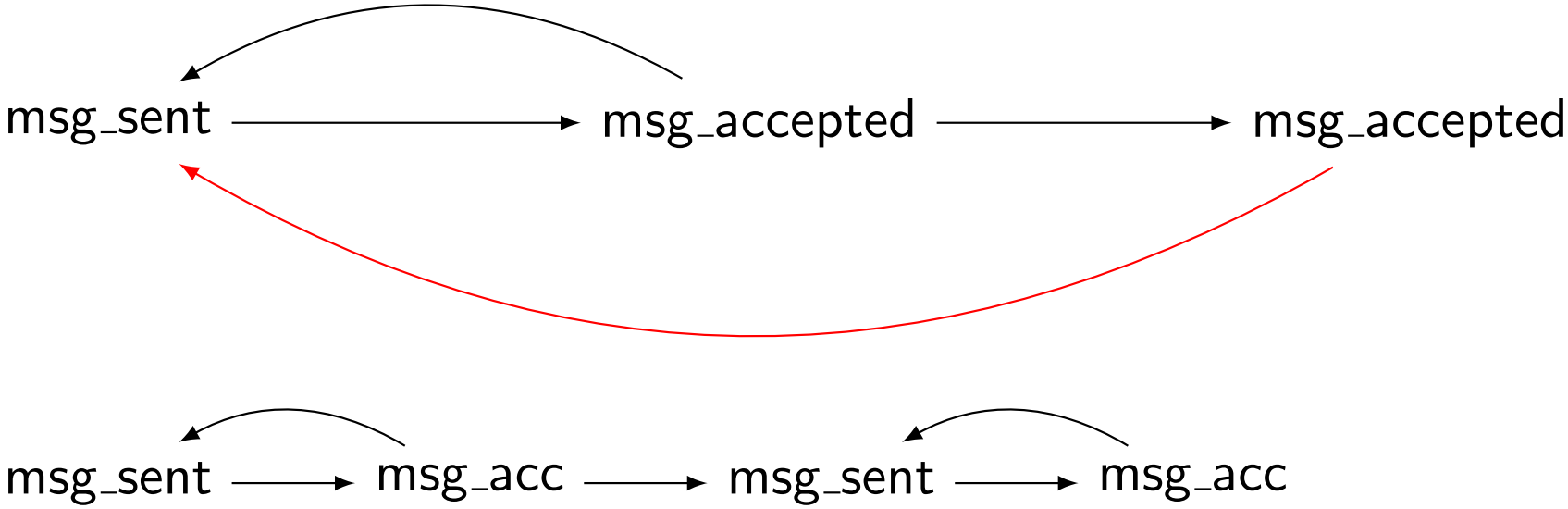
$$\texttt{query}\ x_1 : t_1, ..., x_n : t_n\texttt{;}$$
$$\texttt{event}\ (msg\_accepted(x_1, ..., x_n))\ \texttt{==>}\ \texttt{event}\ (msg\_sent(x_1, ..., x_n)). \tag{3}$$

  - Additional check: Reachability of `msg_accepted`

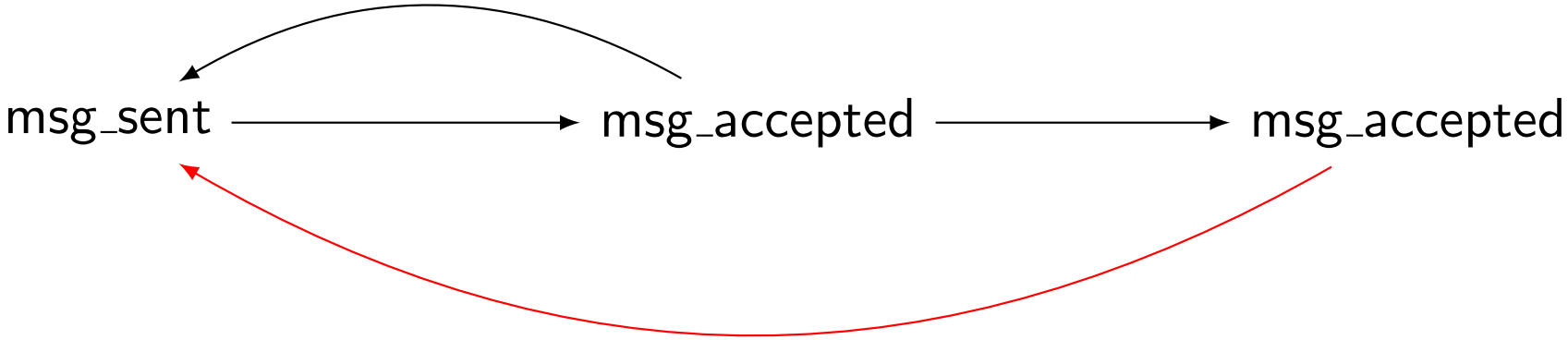
Freshness of Evidence

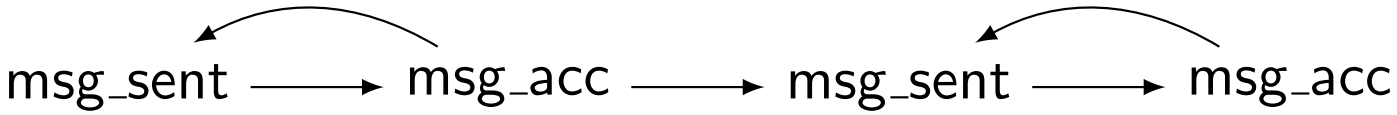


Freshness of Evidence



Freshness of Evidence

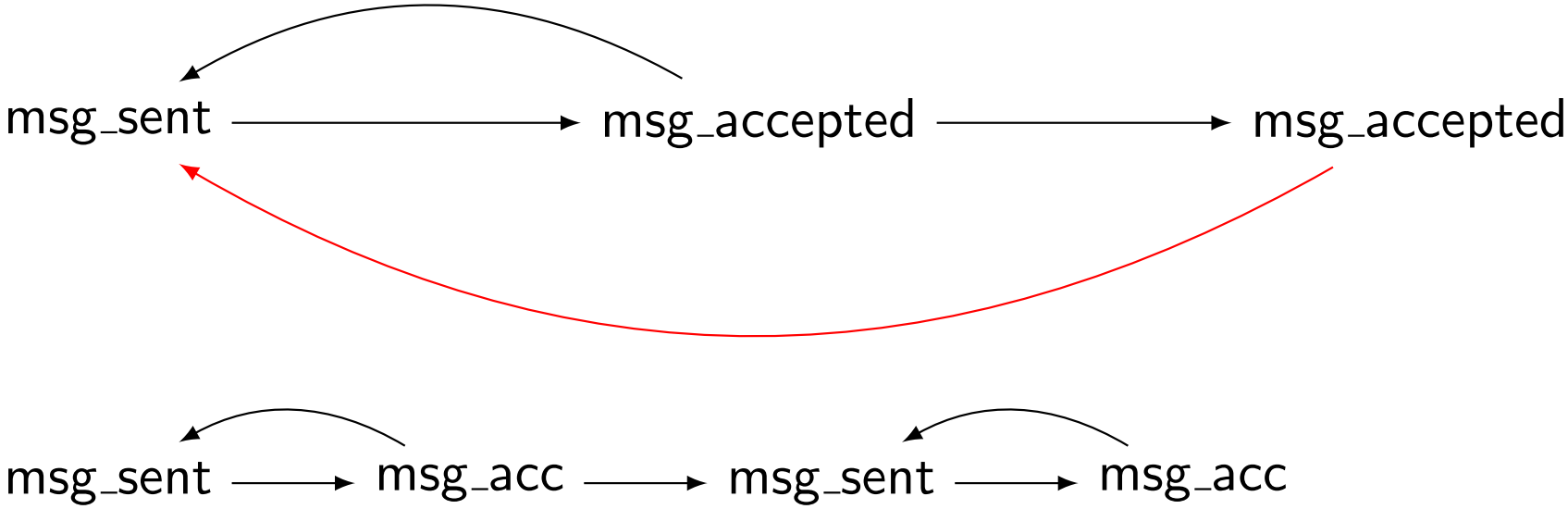




- Injective correspondence assertions

$$\texttt{query}\ x_1 : t_1, \ldots, x_n : t_n\texttt{;}$$
$$\texttt{event}\ (msg\_acc(x_1, \ldots, x_n))\ \texttt{==>}\ \texttt{inj-event}\ (msg\_sent(x_1, \ldots, x_n)). \tag{4}$$

Freshness of Evidence



- Injective correspondence assertions

$$\texttt{query}\ x_1 : t_1, \ldots, x_n : t_n\texttt{;}$$
$$\texttt{event}\ (msg\_acc(x_1, \ldots, x_n))\ \texttt{==>}\ \texttt{inj-event}\ (msg\_sent(x_1, \ldots, x_n)). \tag{4}$$

- Additional check: Reachability of `msg_accepted`

Agenda

2. Approach
   - Properties
   - Model
   - Threat Model

(Incomplete) Model

- Integrate FM asap[4]

[4] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021.

(Incomplete) Model

- Integrate FM asap[4]
- We filled in some details based on:

[4] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021.

(Incomplete) Model

- Integrate FM asap[4]
- We filled in some details based on:
  - our knowledge/experience/experiments with SGX and DCAP

[4] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021.

(Incomplete) Model

- Integrate FM asap[4]
- We filled in some details based on:
  - our knowledge/experience/experiments with SGX and DCAP
  - extensive discussions with Intel, Arm and Scontain

[4] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021.

(Incomplete) Model

- Integrate FM asap[4]
- We filled in some details based on:
  - our knowledge/experience/experiments with SGX and DCAP
  - extensive discussions with Intel, Arm and Scontain
- Rest are assumed to be secure and can be proved in future when more implementation details are available.

[4] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021.

Agenda

2. Approach
   - Properties
   - Model
   - Threat Model

Adversary Capabilities and Threat Model

- Dolev-Yao[5] (Full control of communication channel)

[5] Dolev and Yao, "On the security of public key protocols", 1983.

Adversary Capabilities and Threat Model

- Dolev-Yao[5] (Full control of communication channel)
- *Variable* measurements

[5] Dolev and Yao, "On the security of public key protocols", 1983.

Adversary Capabilities and Threat Model

- Dolev-Yao[5] (Full control of communication channel)
- *Variable* measurements
- Technology-specific capabilities: e.g., TDX: Adversary has full control to create fake TDs and get its Quote.

[5] Dolev and Yao, "On the security of public key protocols", 1983.

Adversary Capabilities and Threat Model

- Dolev-Yao[5] (Full control of communication channel)
- *Variable* measurements
- Technology-specific capabilities: e.g., TDX: Adversary has full control to create fake TDs and get its Quote.
- Secure channels explicitly mentioned (demo soon)

[5] Dolev and Yao, "On the security of public key protocols", 1983.

Agenda

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

Ambiguous, incomplete and contradicting specs

Challenges

ca. 1500 pages of specs of TDX

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

Specs in natural language

Ambiguous, incomplete and contradicting specs

Specs updated on same link!

Challenges

Code and comments in code inconsistent

Challenges

Code and comments in code inconsistent

Precise model of adversary

Challenges

Code and comments in code inconsistent

Precise model of adversary

Formal model as realistic as possible

Challenges

Code and comments in code inconsistent

Precise model of adversary

Formal model as realistic as possible

Variable (vs. constant) measurements

Challenges

Code and comments in code inconsistent

Precise model of adversary

Formal model as realistic as possible

Variable (vs. constant) measurements

User-defined inputs

Agenda

3. Challenges
   - Example of Security Issues: TDX

TCB Claimed by Intel[6]

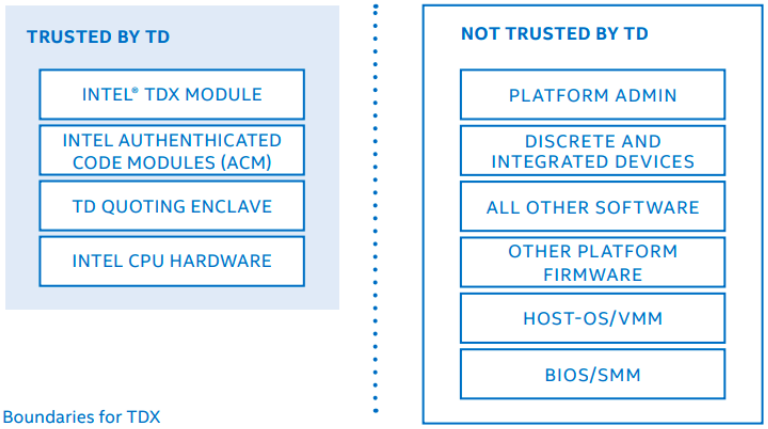
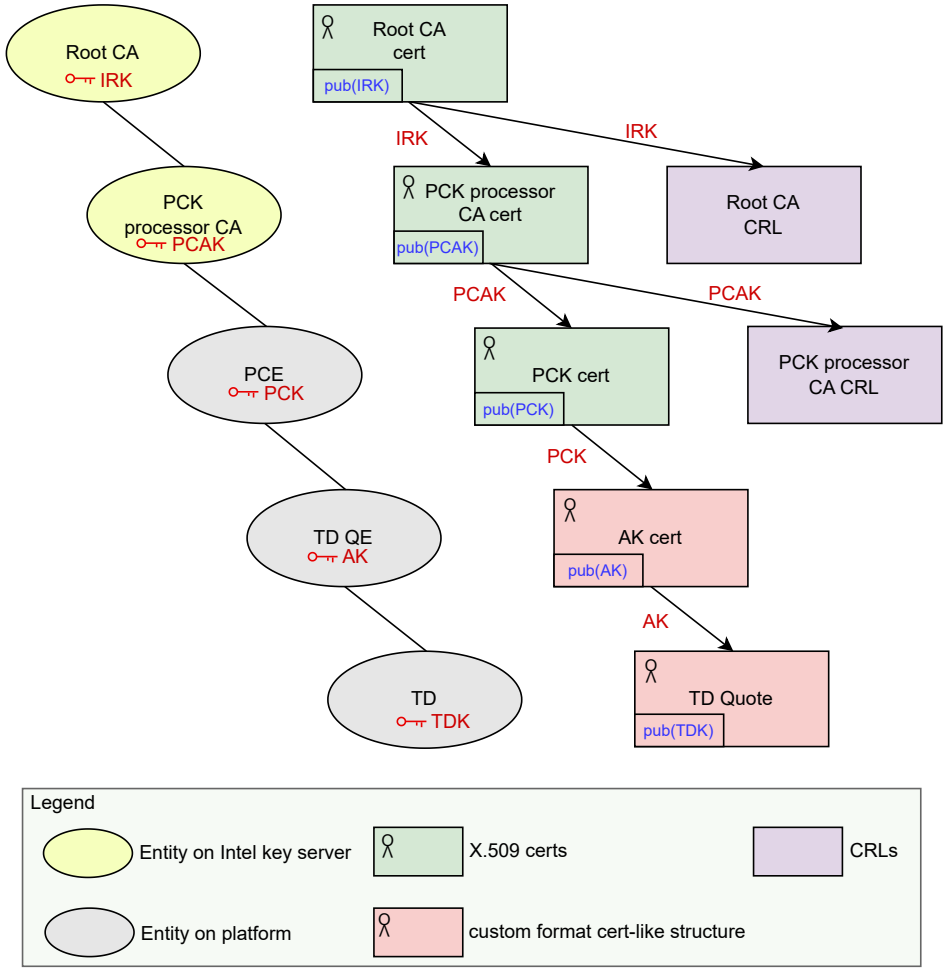


Figure 5.1. Trust Boundaries for TDX



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

Demo Time

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

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

Query not attacker(sec[]) is false.

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


real    7m34,151s
user    7m32,412s
sys     0m1,716s
```

- Code at https://github.com/CCC-Attestation/formal-spec-TEE under generous Apache License 2.0

Reported to Intel[8] and Fixed[9]

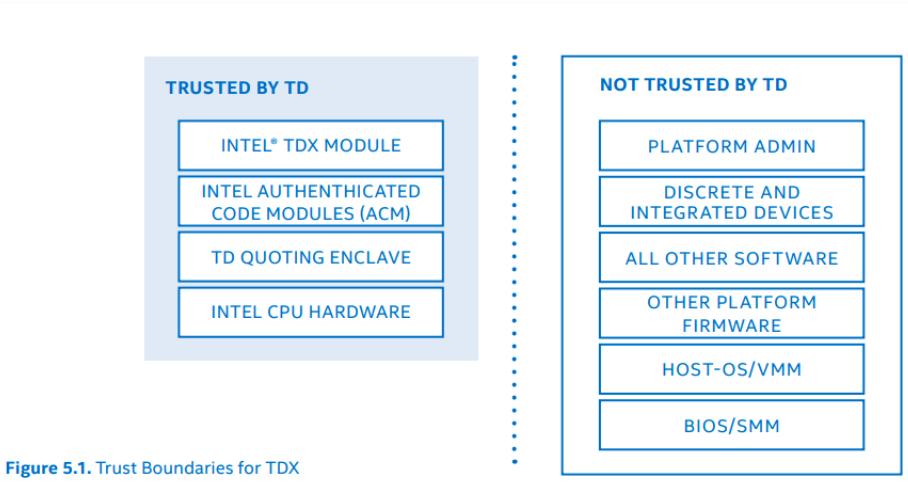


Figure: Old

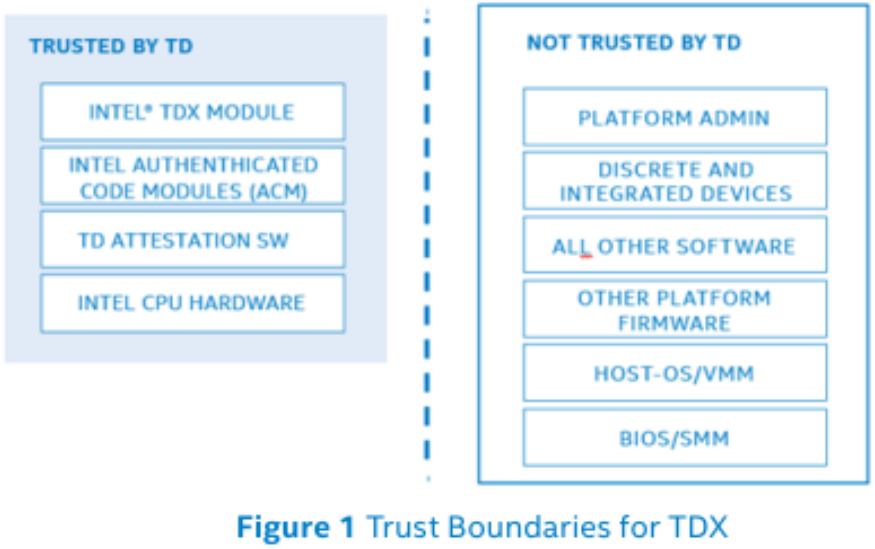


Figure: Updated

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

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

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

Reported to Intel[8] and Fixed[9]

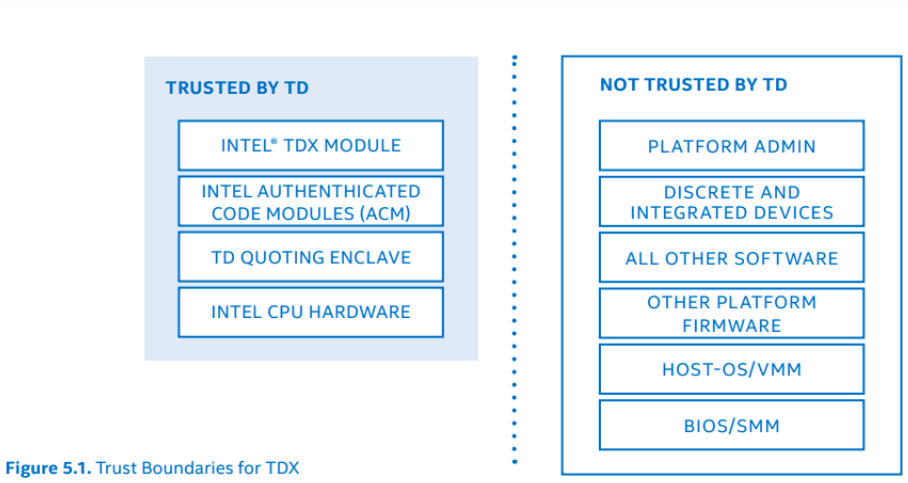


Figure: Old

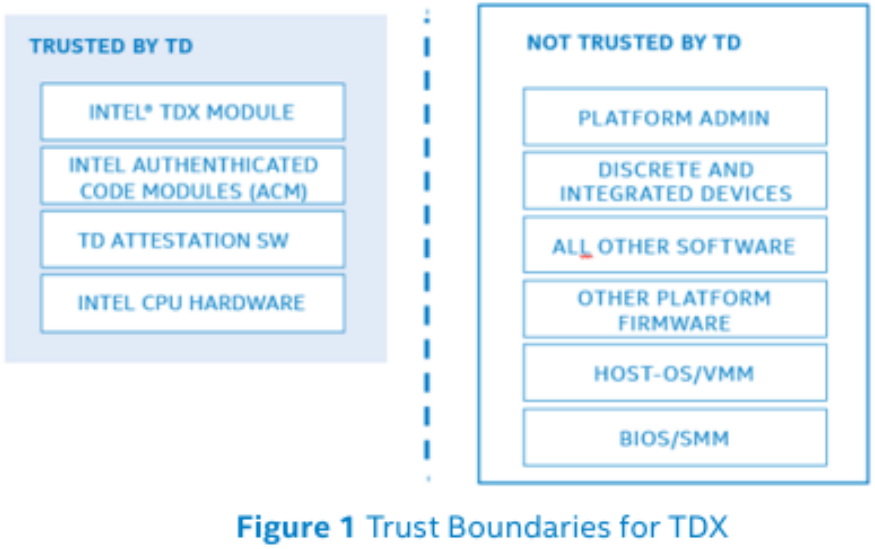


Figure: Updated

- Warning: on same link replacing the old white paper: Reported to Intel privately and publicly[7]

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

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

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

Agenda

Community response

Most read in the last month

SoK: Attestation in Confidential Computing

File available | Preprint | January 2023

Muhammad Usama Sardar · Thomas Fossati · Simon Frost

Source

1,815 Reads · 1 Recommendation

Most recommended in the last month

Confidential Computing and Related Technologies: A Review

File available | Preprint | November 2021

Muhammad Usama Sardar · Christof Fetzer

Source

2,735 Reads · 4 Recommendations

Demystifying Attestation in Intel Trust Domain Extensions via Formal Verification

File available | Preprint | May 2021

Muhammad Usama Sardar · Saidgani Musaev · Christof Fetzer

Source

3,564 Reads · 1 Recommendation

Formal Foundations for Intel SGX Data Center Attestation Primitives

File available | Preprint | July 2020

Muhammad Usama Sardar · Rasha Faqeh · Christof Fetzer

Source

4,086 Reads · 1 Recommendation

Towards Formalization of Enhanced Privacy ID (EPID)-based Remote Attestation in Intel SGX

File available | Preprint | April 2020

Muhammad Usama Sardar · Do Quoc Le · Christof Fetzer

Source

2,230 Reads

Vision

Open-source SW (Veraison)

Vision

Open-source SW (Veraison)

Open-source HW

Vision

Open-source SW (Veraison)

Open-source HW

Open-source Formal Verification

Take-home

- Ad-hoc attestation designs!

Take-home

- Ad-hoc attestation designs!
- CC is still in its infancy with very little science!

Take-home

- Ad-hoc attestation designs!
- CC is still in its infancy with very little science!
- No transparency of specs: on websites or non-persistent links

Take-home

- Ad-hoc attestation designs!
- CC is still in its infancy with very little science!
- No transparency of specs: on websites or non-persistent links
- Still huge gap between SE and FM communities

Take-home

- Ad-hoc attestation designs!
- CC is still in its infancy with very little science!
- No transparency of specs: on websites or non-persistent links
- Still huge gap between SE and FM communities
  - Many initiatives (e.g., teaching, workshops)

Take-home

- Ad-hoc attestation designs!
- CC is still in its infancy with very little science!
- No transparency of specs: on websites or non-persistent links
- Still huge gap between SE and FM communities
  - Many initiatives (e.g., teaching, workshops)
- Towards TEE-agnostic *verification* infrastructure

Take-home

- Ad-hoc attestation designs!
- CC is still in its infancy with very little science!
- No transparency of specs: on websites or non-persistent links
- Still huge gap between SE and FM communities
  - Many initiatives (e.g., teaching, workshops)
- Towards TEE-agnostic *verification* infrastructure
- Bring your expertise:
  https://github.com/CCC-Attestation/formal-spec-TEE

Take-home

- Ad-hoc attestation designs!
- CC is still in its infancy with very little science!
- No transparency of specs: on websites or non-persistent links
- Still huge gap between SE and FM communities
  - Many initiatives (e.g., teaching, workshops)
- Towards TEE-agnostic *verification* infrastructure
- Bring your expertise:
  https://github.com/CCC-Attestation/formal-spec-TEE
- Works in progress (contributions/collaborations welcome)

Take-home

- Ad-hoc attestation designs!
- CC is still in its infancy with very little science!
- No transparency of specs: on websites or non-persistent links
- Still huge gap between SE and FM communities
  - Many initiatives (e.g., teaching, workshops)
- Towards TEE-agnostic *verification* infrastructure
- Bring your expertise:
  https://github.com/CCC-Attestation/formal-spec-TEE
- Works in progress (contributions/collaborations welcome)
  - vTPM TD solution for Intel TDX (with Intel)

Take-home

- Ad-hoc attestation designs!
- CC is still in its infancy with very little science!
- No transparency of specs: on websites or non-persistent links
- Still huge gap between SE and FM communities
  - Many initiatives (e.g., teaching, workshops)
- Towards TEE-agnostic *verification* infrastructure
- Bring your expertise:
  https://github.com/CCC-Attestation/formal-spec-TEE
- Works in progress (contributions/collaborations welcome)
  - vTPM TD solution for Intel TDX (with Intel)
  - RA+TLS (with Arm, BI, Intuit)

Key References

Barbosa, Manuel et al. "SoK : Computer-Aided Cryptography". In: *42nd IEEE Symposium on Security and Privacy*. 2021. URL: https://eprint.iacr.org/2019/1393.pdf.

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.

Dolev, D. and A. Yao. "On the security of public key protocols". In: *IEEE Transactions on Information Theory* 29.2 (Mar. 1983), pp. 198–208. ISSN: 1557-9654.

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.

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