Tools and Techniques for Symbolic Protocol Verification

Muhammad Usama Sardar, Thomas Fossati, and Simon Frost
Ack: Nikolaus Thümmel, Ante Derek, Shale Xiong
Funding: CPEC, EuroProofNet WG3

Chair of Systems Engineering
Technische Universität Dresden

EuroProofNet WG3 meeting
Timisoara, Romania

February 8, 2023

Outline

Relevance for PV community

- Program $\rightarrow$ Product/service

Relevance for PV community

- Program $\rightarrow$ Product/service
- Infrastructure management issues $\rightarrow$ Deployed in cloud

Relevance for PV community

- Program $\rightarrow$ Product/service
- Infrastructure management issues $\rightarrow$ Deployed in cloud
- Safety and security interplay

Relevance for PV community

- Program $\rightarrow$ Product/service
- Infrastructure management issues $\rightarrow$ Deployed in cloud
- Safety and security interplay
- Additional challenges, e.g.,

Relevance for PV community

- Program $\rightarrow$ Product/service
- Infrastructure management issues $\rightarrow$ Deployed in cloud
- Safety and security interplay
- Additional challenges, e.g.,
  - Identity of code?

Relevance for PV community

- Program $\rightarrow$ Product/service
- Infrastructure management issues $\rightarrow$ Deployed in cloud
- Safety and security interplay
- Additional challenges, e.g.,
  - Identity of code?
  - Unspecified/not well-understood mechanisms

Relevance for PV community

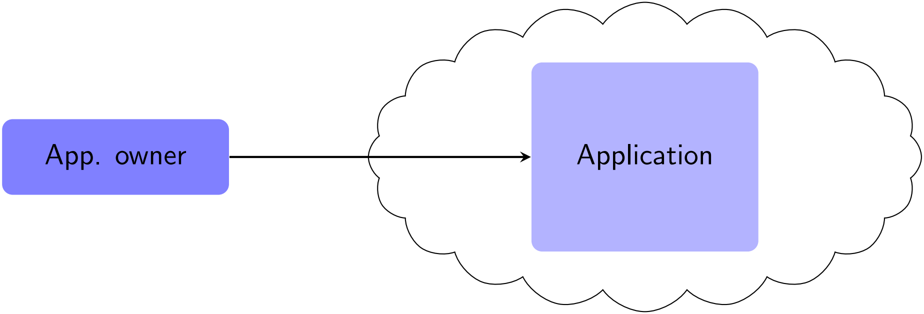
- Program $\rightarrow$ Product/service
- Infrastructure management issues $\rightarrow$ Deployed in cloud
- Safety and security interplay
- Additional challenges, e.g.,
  - Identity of code?
  - Unspecified/not well-understood mechanisms
  - Closed-source nature of SCONE

Confidential Computing

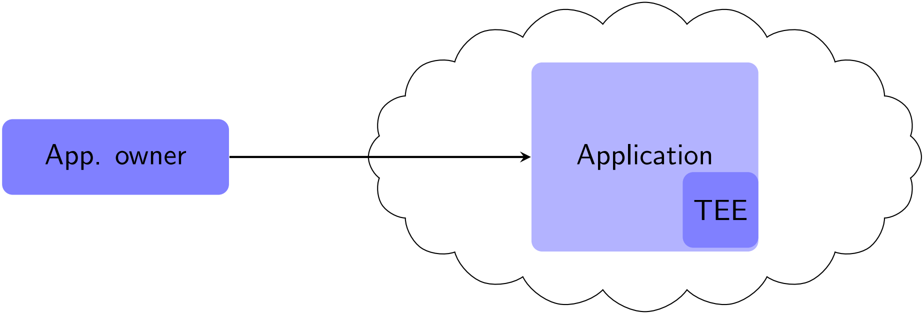
Confidential Computing

App. owner

Confidential Computing

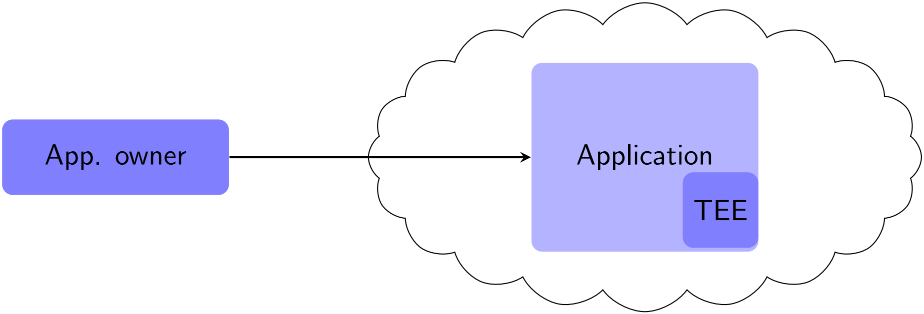


Confidential Computing



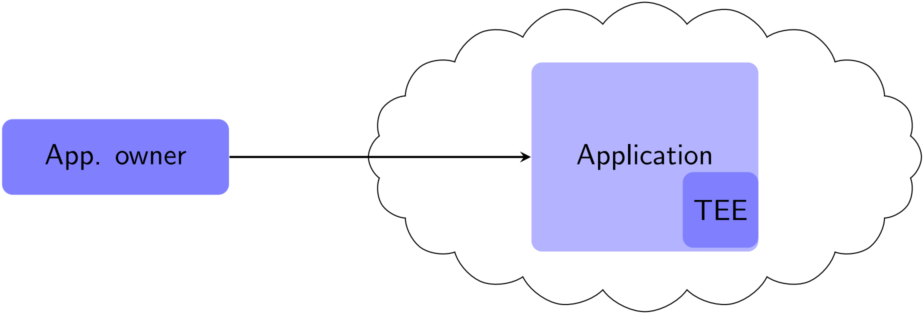
- Protection of data in use

Confidential Computing



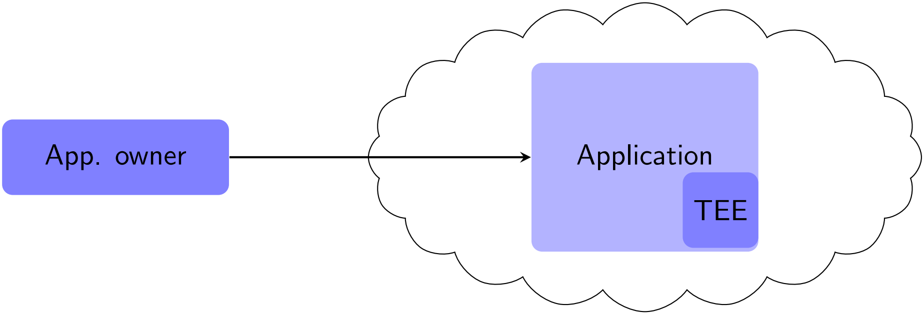
- Protection of data in use
- Adversary: root access

Confidential Computing



- Protection of data in use
- Adversary: root access
- Isolation and attestability

Confidential Computing



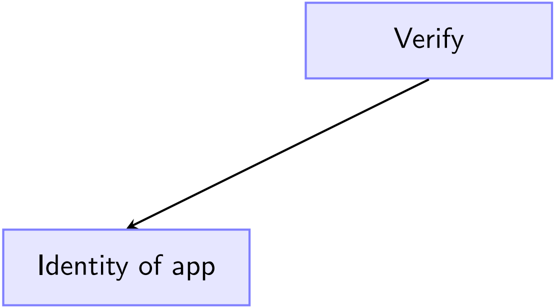
- Protection of data in use
- Adversary: root access
- Isolation and attestability
- Attestation: arguably the most critical but most misunderstood concept in CC

Attestation

- Trust to app owner: right app in right platform

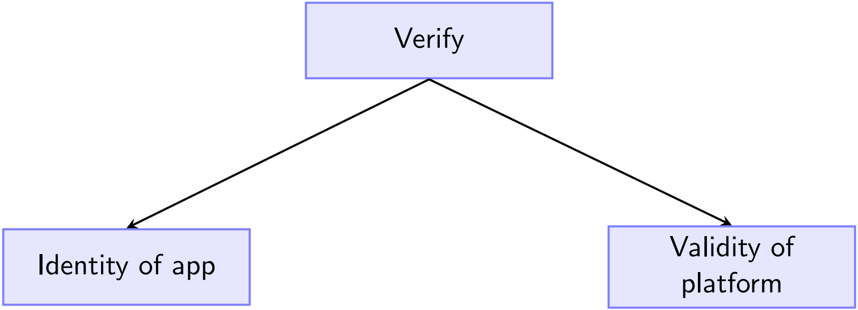
Attestation

- Trust to app owner: right app in right platform



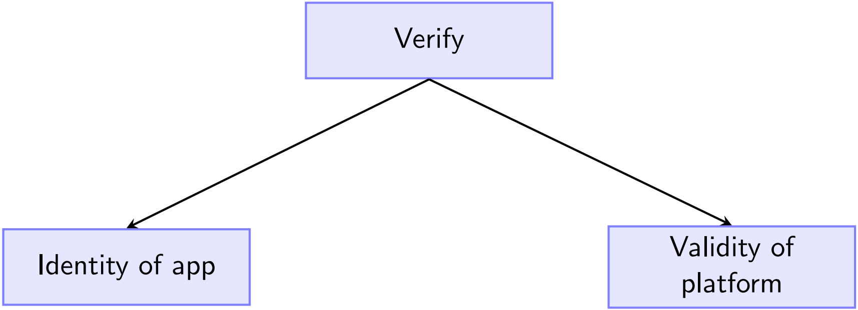
Attestation

- Trust to app owner: right app in right platform



Attestation

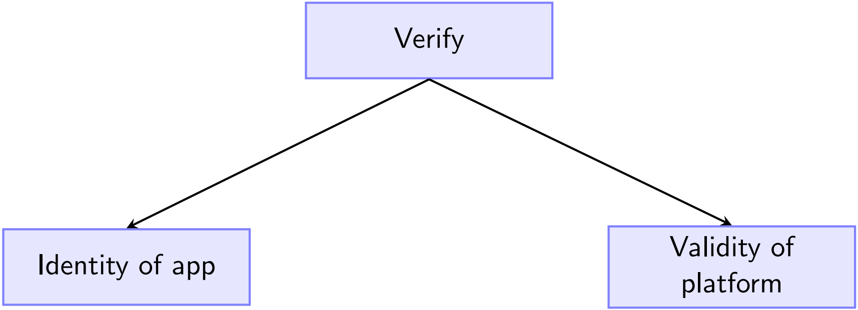
- Trust to app owner: right app in right platform



- Secure channel creation

Attestation

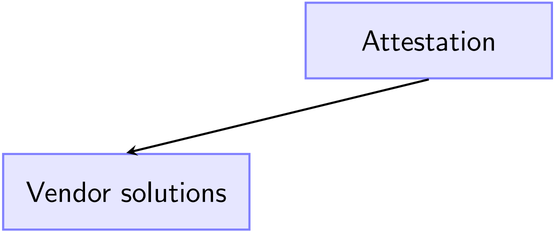
- Trust to app owner: right app in right platform



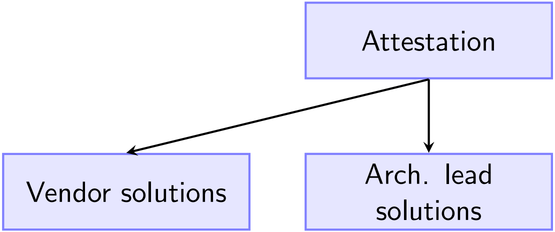
- Secure channel creation
- Provisioning of secrets and config.

Outline

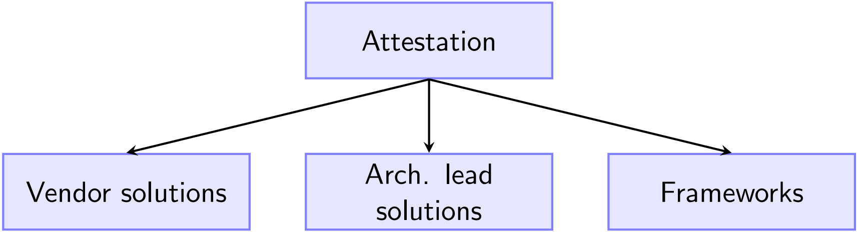
Systemization for Attestation Mechanisms



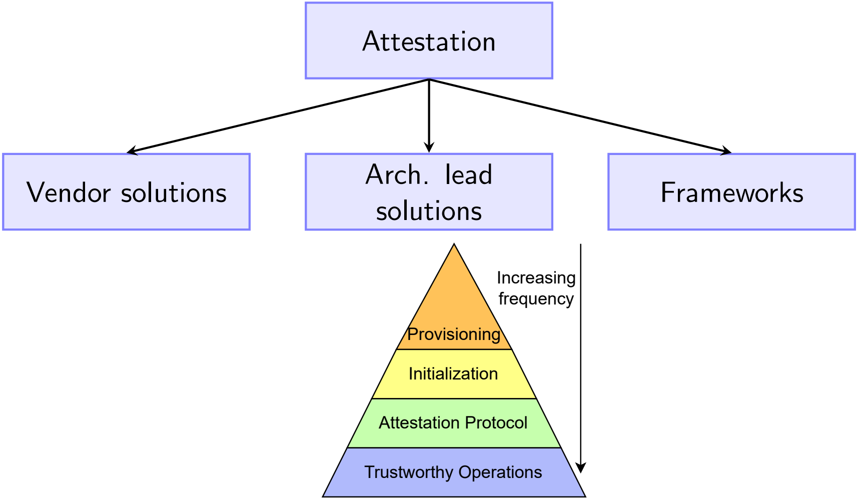
Systemization for Attestation Mechanisms



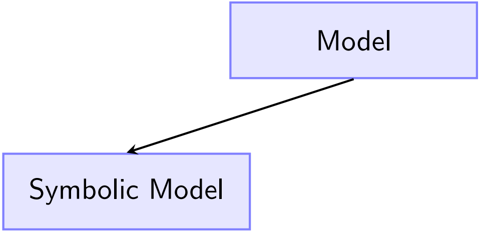
Systemization for Attestation Mechanisms



Systemization for Attestation Mechanisms



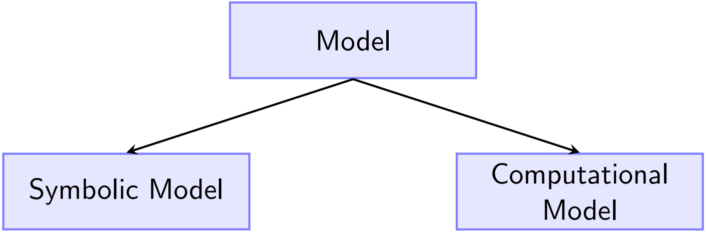
Model for Security Analysis[1]



- Formal model
- Messages represented by “Terms”
- What attacker can do

[1] Barbosa et al., “SoK : Computer-Aided Cryptography”, 2021

Model for Security Analysis[1]



- Used by cryptographers
- What attacker cannot do

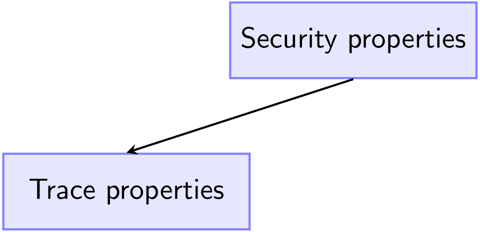
[1] Barbosa et al., "SoK : Computer-Aided Cryptography", 2021

Threat Model for Symbolic Analysis

- "Dolev-Yao"[2] (symbolic) attacker
- Full control of communication network
- Unbounded number of sessions and messages
- Attacker behavior: Non-deterministic
- Assume cryptographic primitives are perfect

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

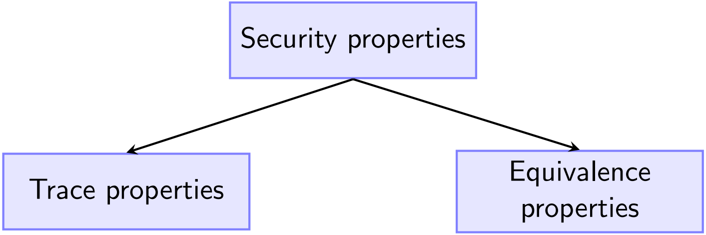
Security properties[3]



- Defined on each run of the protocol
  - Confidentiality/Secrecy
  - Authentication

[3] Blanchet, "Modeling and verifying security protocols with the applied pi calculus and ProVerif", 2016

Security properties[3]



- Adversary cannot distinguish 2 processes
- e.g., observational equivalence
- Tools: ProVerif, DeepSec (almost the same semantics)

[3] Blanchet, "Modeling and verifying security protocols with the applied pi calculus and ProVerif", 2016

ProVerif[4] vs. Tamarin prover[5]

- More automation vs. user interaction

[4]Blanchet, "Modeling and verifying security protocols with the applied pi calculus and ProVerif", 2016

[5]Basin et al., "Symbolically analyzing security protocols using Tamarin", 2017

ProVerif[5] vs. Tamarin prover[6]

- More automation vs. user interaction
- Computational security analysis on *same* model (CryptoVerif[4])

[4] Blanchet, *CryptoVerif: A computationally-sound security protocol verifier*, 2017

[5] Blanchet, "Modeling and verifying security protocols with the applied pi calculus and ProVerif", 2016

[6] Basin et al., "Symbolically analyzing security protocols using Tamarin", 2017

ProVerif[6] vs. Tamarin prover[7]

- More automation vs. user interaction
- Computational security analysis on *same* model (CryptoVerif[4])
- Faster[5]

[4] Blanchet, *CryptoVerif: A computationally-sound security protocol verifier*, 2017

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

[6] Blanchet, "Modeling and verifying security protocols with the applied pi calculus and ProVerif", 2016

[7] Basin et al., "Symbolically analyzing security protocols using Tamarin", 2017

ProVerif[7] vs. Tamarin prover[8]

- More automation vs. user interaction
- Computational security analysis on *same* model (CryptoVerif[4])
- Faster[5]
  - esp. recent improvements[6]

---

[4] Blanchet, *CryptoVerif: A computationally-sound security protocol verifier*, 2017

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

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

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

[8] Basin et al., "Symbolically analyzing security protocols using Tamarin", 2017

ProVerif[7] vs. Tamarin prover[8]

- More automation vs. user interaction
- Computational security analysis on *same* model (CryptoVerif[4])
- Faster[5]
  - esp. recent improvements[6]
- Supports equivalence properties

[4] Blanchet, *CryptoVerif: A computationally-sound security protocol verifier*, 2017

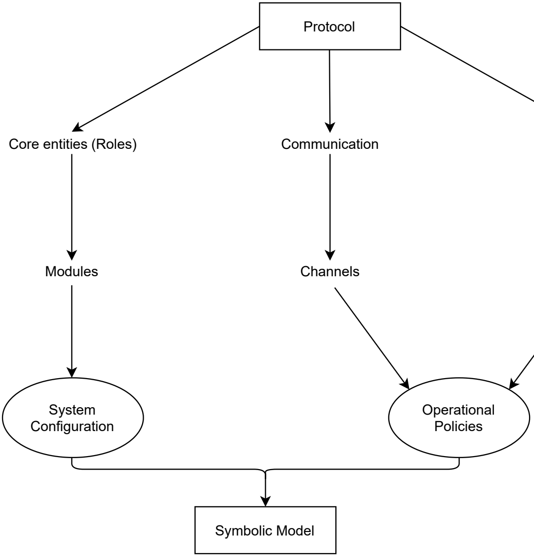
[5] Lafourcade and Puys, "Performance Evaluations of Cryptographic Protocols Verification Tools Dealing with Algebraic Properties", 2016

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

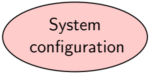
[7] Blanchet, "Modeling and verifying security protocols with the applied pi calculus and ProVerif", 2016

[8] Basin et al., "Symbolically analyzing security protocols using Tamarin", 2017

Overview of Approach

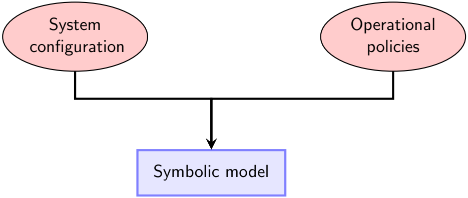


Workflow of the Analysis Approach

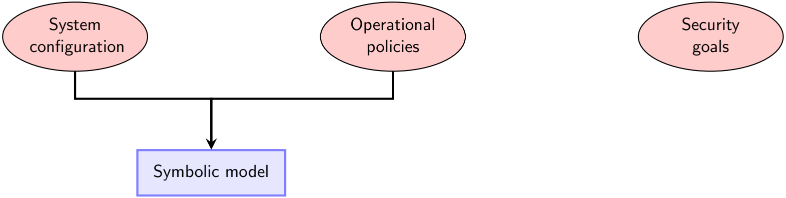


Workflow of the Analysis Approach

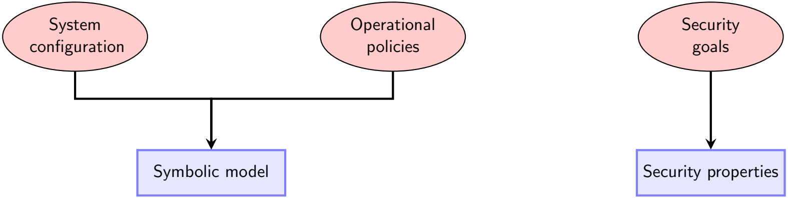
Workflow of the Analysis Approach



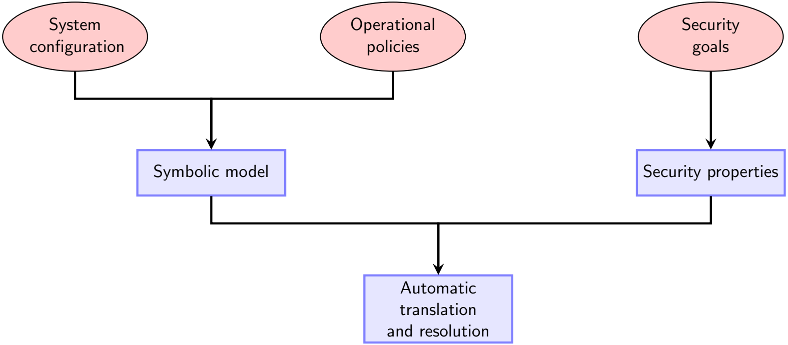
Workflow of the Analysis Approach



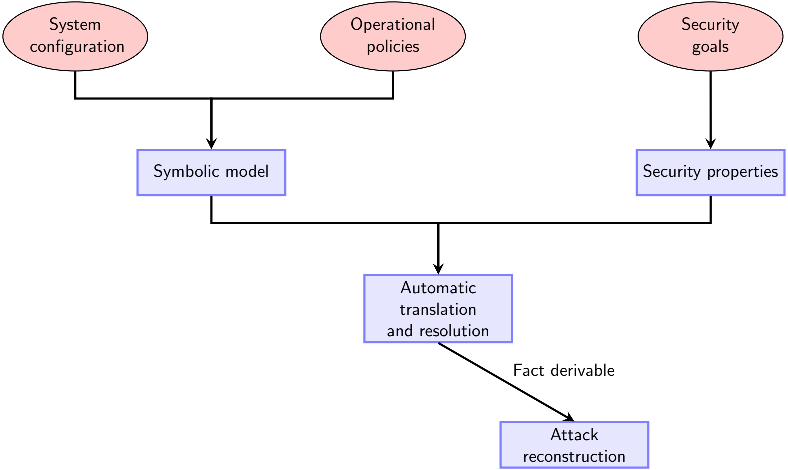
Workflow of the Analysis Approach



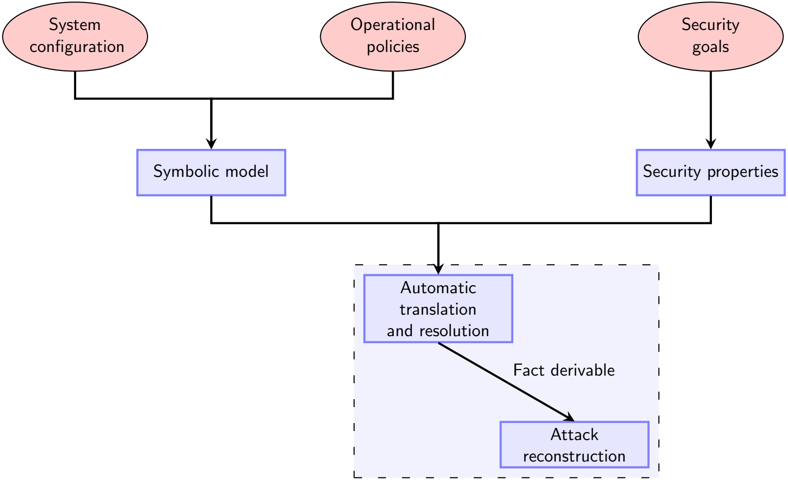
Workflow of the Analysis Approach



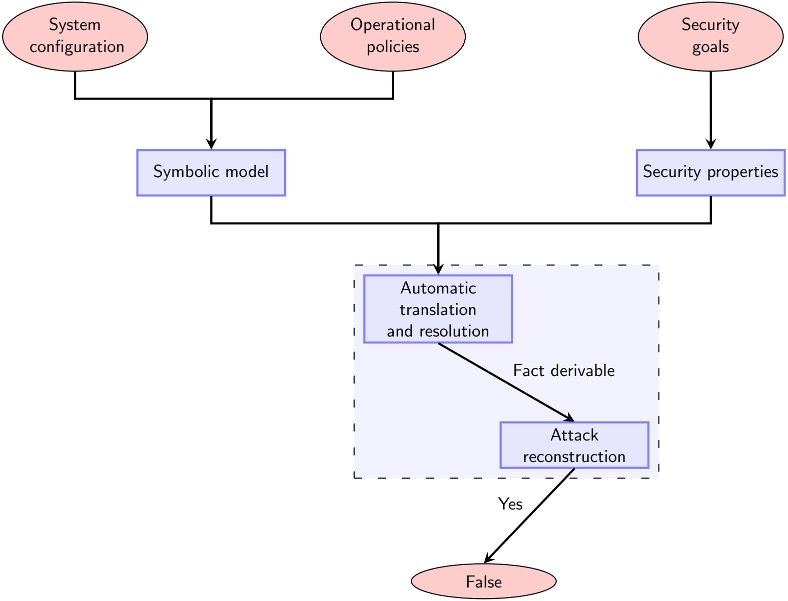
Workflow of the Analysis Approach



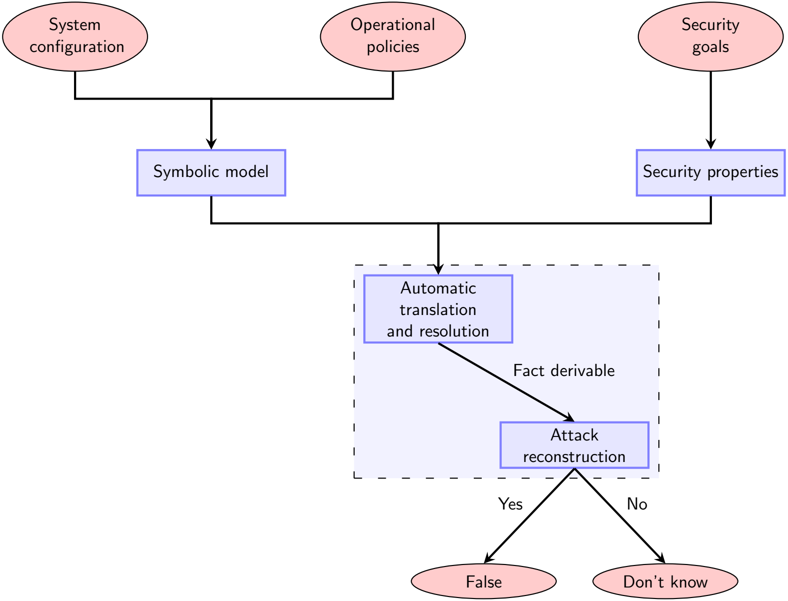
Workflow of the Analysis Approach



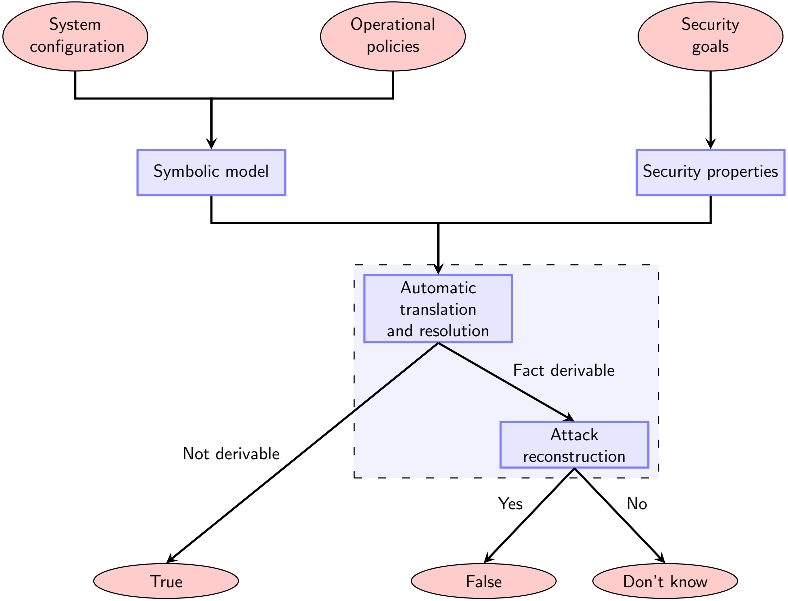
Workflow of the Analysis Approach



Workflow of the Analysis Approach

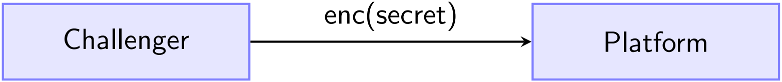


Workflow of the Analysis Approach



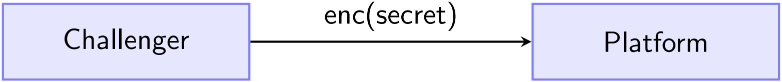
Specification of Security Goals

- Confidentiality



Specification of Security Goals

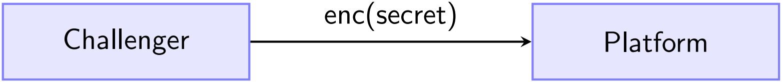
- Confidentiality



  - Formalized as a reachability property

Specification of Security Goals

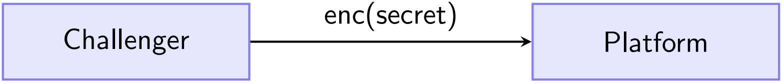
- Confidentiality



  - Formalized as a reachability property
- Authentication

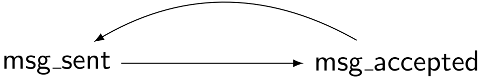
Specification of Security Goals

- Confidentiality



  - Formalized as a reachability property

- Authentication



Specification of Security Goals

- Confidentiality

$$\boxed{\text{Challenger}} \xrightarrow{\text{enc(secret)}} \boxed{\text{Platform}}$$

  - Formalized as a reachability property
- Authentication

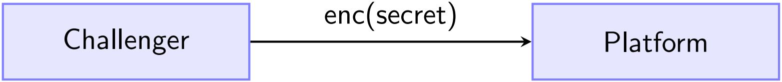
$$\begin{tikzcd} \text{msg\_sent} \arrow[r] & \text{msg\_accepted} \arrow[l, bend right] \end{tikzcd}$$

  - Correspondence assertions

$$\texttt{query } x_1 : t_1, \ldots, x_n : t_n \, ;$$
$$\texttt{event } (\mathit{msg\_accepted}(M_1, \ldots, M_j)) \texttt{ ==> } \texttt{event } (\mathit{msg\_sent}(N_1, \ldots, N_k)). \tag{1}$$

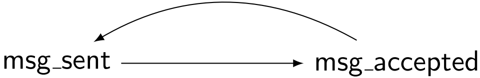
Specification of Security Goals

- Confidentiality



  - Formalized as a reachability property

- Authentication

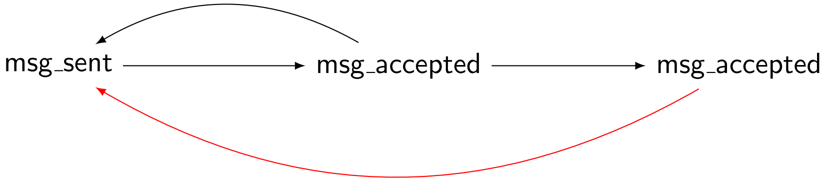


  - Correspondence assertions

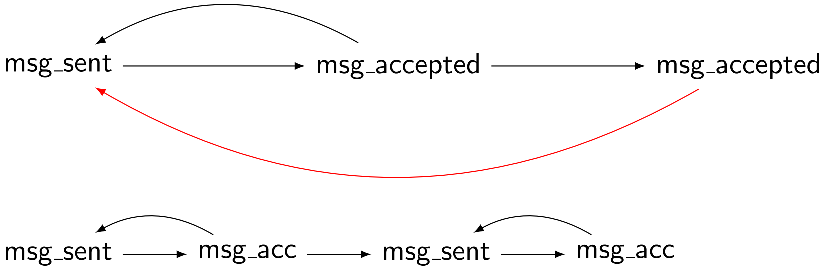
$$\texttt{query } x_1 : t_1, \ldots, x_n : t_n ;$$
$$\texttt{event } (msg\_accepted(M_1, \ldots, M_j)) \texttt{ ==> event } (msg\_sent(N_1, \ldots, N_k)). \quad (1)$$

  - Additional check: Reachability of `msg_accepted`

Authentication



Authentication



Authentication

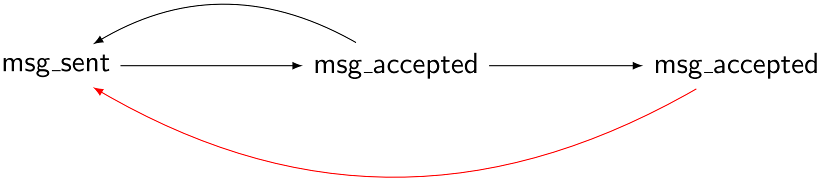
$$\begin{tikzcd}
\text{msg_sent} \arrow[r] & \text{msg_accepted} \arrow[l, bend right] \arrow[r] & \text{msg_accepted} \arrow[ll, bend left, red]
\end{tikzcd}$$

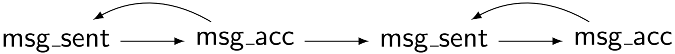
$$\begin{tikzcd}
\text{msg_sent} \arrow[r] & \text{msg_acc} \arrow[l, bend right] \arrow[r] & \text{msg_sent} \arrow[r] & \text{msg_acc} \arrow[l, bend right]
\end{tikzcd}$$

- Injective correspondence assertions

$$\texttt{query}\ x_1 : t_1, \ldots, x_n : t_n\,;$$
$$\texttt{event}\ (\mathit{msg\_acc}(M_1, \ldots, M_j))\ \texttt{==>}\ \texttt{inj-event}\ (\mathit{msg\_sent}(N_1, \ldots, N_k)). \tag{2}$$

Authentication





- Injective correspondence assertions

$$\texttt{query}\ x_1 : t_1, \ldots, x_n : t_n\texttt{;}$$
$$\texttt{event}\ (\mathit{msg\_acc}(M_1, \ldots, M_j))\ \texttt{==>}\ \texttt{inj-event}\ (\mathit{msg\_sent}(N_1, \ldots, N_k)). \tag{2}$$

- Additional check: Reachability of `msg_accepted`

Outline

Analysis

- Intel TDX: how do we precisely express trust boundaries?

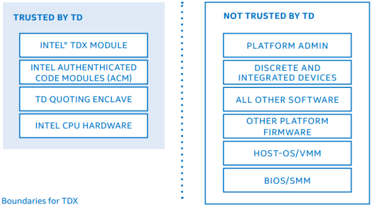


Figure 5.1. Trust Boundaries for TDX

Analysis

- Intel TDX: how do we precisely express trust boundaries?

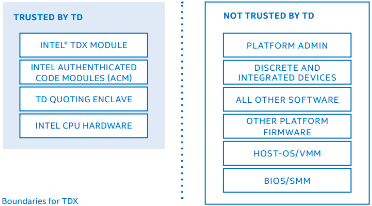


Figure 5.1. Trust Boundaries for TDX

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

Analysis

- Intel TDX: how do we precisely express trust boundaries?

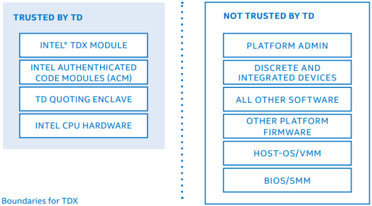


Figure 5.1. Trust Boundaries for TDX

- SCONE: when do we say that something is attested?
- Arm CCA: authentication properties

$$\begin{aligned}&\texttt{query}\ \ data : bitstring\,;\\ &\texttt{event}\ \ (accepted(data))\ \texttt{==>}\ \texttt{inj-event}\ \ (sent(data)).\end{aligned} \tag{3}$$

Outline

Take-home

- Towards TEE-agnostic verification infrastructure for transparency and interoperability

Take-home

- Towards TEE-agnostic verification infrastructure for transparency and interoperability

- Lots of work required for precise specification and standardization

Take-home

- Towards TEE-agnostic verification infrastructure for transparency and interoperability

- Lots of work required for precise specification and standardization
  - Formal definitions and semantics associated with the attestation mechanisms

Take-home

- Towards TEE-agnostic verification infrastructure for transparency and interoperability
- Lots of work required for precise specification and standardization
  - Formal definitions and semantics associated with the attestation mechanisms
  - Provisioning protocols not well-understood

Take-home

- Towards TEE-agnostic verification infrastructure for transparency and interoperability
- Lots of work required for precise specification and standardization
  - Formal definitions and semantics associated with the attestation mechanisms
  - Provisioning protocols not well-understood
  - Analysis and categorization of Claims

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.

Basin, David et al. "Symbolically analyzing security protocols using Tamarin". In: *ACM SIGLOG News* 4.4 (Nov. 2017), pp. 19–30. ISSN: 2372-3491. DOI: 10.1145/3157831.3157835.

Blanchet, Bruno. *CryptoVerif: A computationally-sound security protocol verifier*. Tech. rep. 2017.

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

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.

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.

Contributions/collaborations welcome

link here