On the Soundness of Infrastructure Adversaries

Robert Künemann

Alexander Dax

CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
Motivation

Use TLS
Use SSL
Use SSH
Use IPSec
Infrastructure Model

Quantitative Security Risk Assessment

Examples:
- Do we need DNSSEC?
- Biggest security risk?
- Best deployment strategy?

Administrators
*Plan investments; secure infrastructure*

Standardization bodies & Policy Makers
*Focus efforts*
*Evaluate impact of policies; improve self-reliance*

Protocol designers
*Assess deployment issues with regard to status quo*

Speicher et al.
Infrastructure Model

Symbolic Soundess

Symbolic Model

- quantitative
  - analyse IT-infrastructures
    - building blocks: security protocols
    - rule-based, infrastructure adversary (IA)

- possibilistic
  - analyse security protocols
    - building blocks: cryptographic primitives
    - rule-based, Dolev-Yao threat model

ProVerif

Established
∀ t ∈ traces(P). ∃ p ∈ p_traces(M). t ≈ p
Symbolic Soundness - Conditions

- C 1: Depended on Formalism
- C 2: Syntactic check on IA
- C 3: Depended on Formalism
- C 4: Syntactic check on IA
- C 5: Prove in the symbolic model
Symbolic Model - Construction

\[ F(G) = P \]

- **G** is hardcoded \( \Rightarrow \) Changes in analysed infrastructure invalidate assessment
- **G** can have millions of nodes \( \Rightarrow \) Verifiers do not scale well with model size

**G**

- Graph presentation of analysed infrastructure

**F**

- Mapping from infrastructure graph to pi calculus process
Process transformations

1. Allow adversary to choose concrete infrastructure.
   \[ Q(s_1) \ | \ \cdots \ | \ Q(s_n) \Rightarrow !\text{in}(s).Q(s) \]

2. Technical transformation: move message inputs deeper into the process.
Results

Summary

Symbolic soundness: Definition and Conditions
Construction of Symbolic Model

Case Study

‘Formally Reasoning about the Cost and Efficacy of Securing the Email Infrastructure’ - EuroS&P, (Speicher et al. 2018)
Detection of flaws in their adversary model
Includes PKI, SMTP, DNS, DNSSEC and inter-AS routing
(Github repository)

Symbolic Completeness

Corresponding notion to soundness
Conditions contain liveness properties
On the Soundness of Infrastructure Adversaries

Alexander Dax and Robert Künnemann

in IEEE Computer Security Foundations Symposium 2021

alexander.dax@cispa.de
robert.kuennemann@cispa.de