CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

On the Soundness of Infrastructure Adversaries

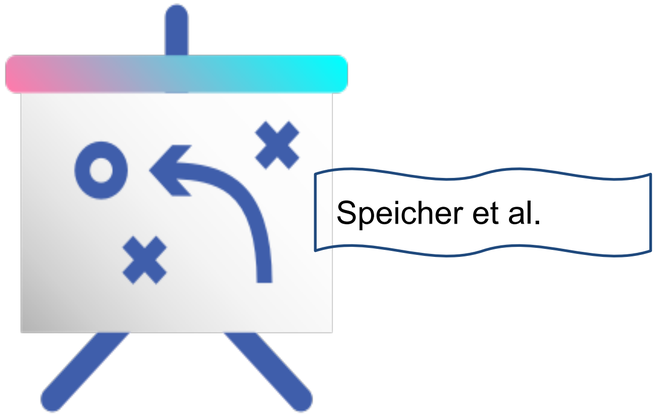
Robert Künnemann[1]

Alexander Dax[1]

[1]CISPA Helmholtz Center for Information Security, Saarbrücken, Germany

Motivation

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

Infrastructure Model

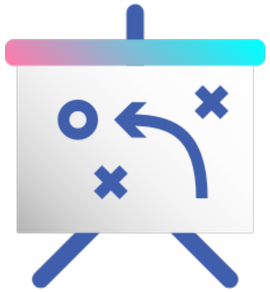
Infrastructure Model

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

Established

ProVerif

DEEPSEC

Outline

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

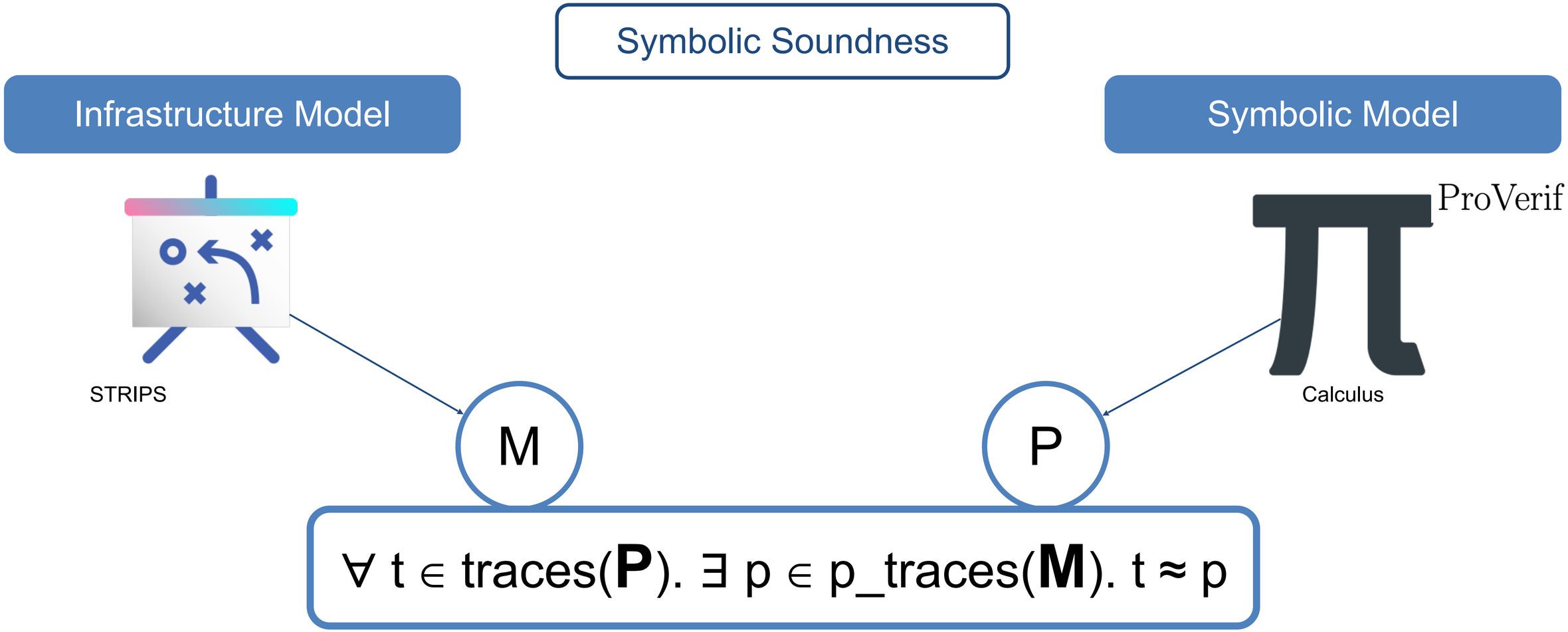
Symbolic Soundness - Definition

Symbolic Soundness - Proof Concept

Symbolic Model - Construction

Summary and Results

Symbolic Soundness



Symbolic Soundness - Conditions

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

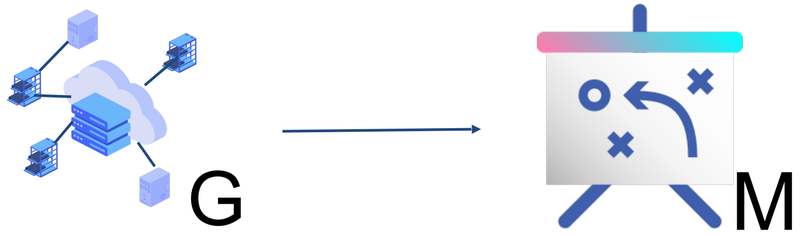
C 1	C 2	C 3	C 4	C 5
Depended on Formalism	Syntactic check on IA	Depended on Formalism	Syntactic check on IA	Prove in the symbolic model

Conditions for

Symbolic Soundness

π

Symbolic Model - Construction



$$F(G) = P$$

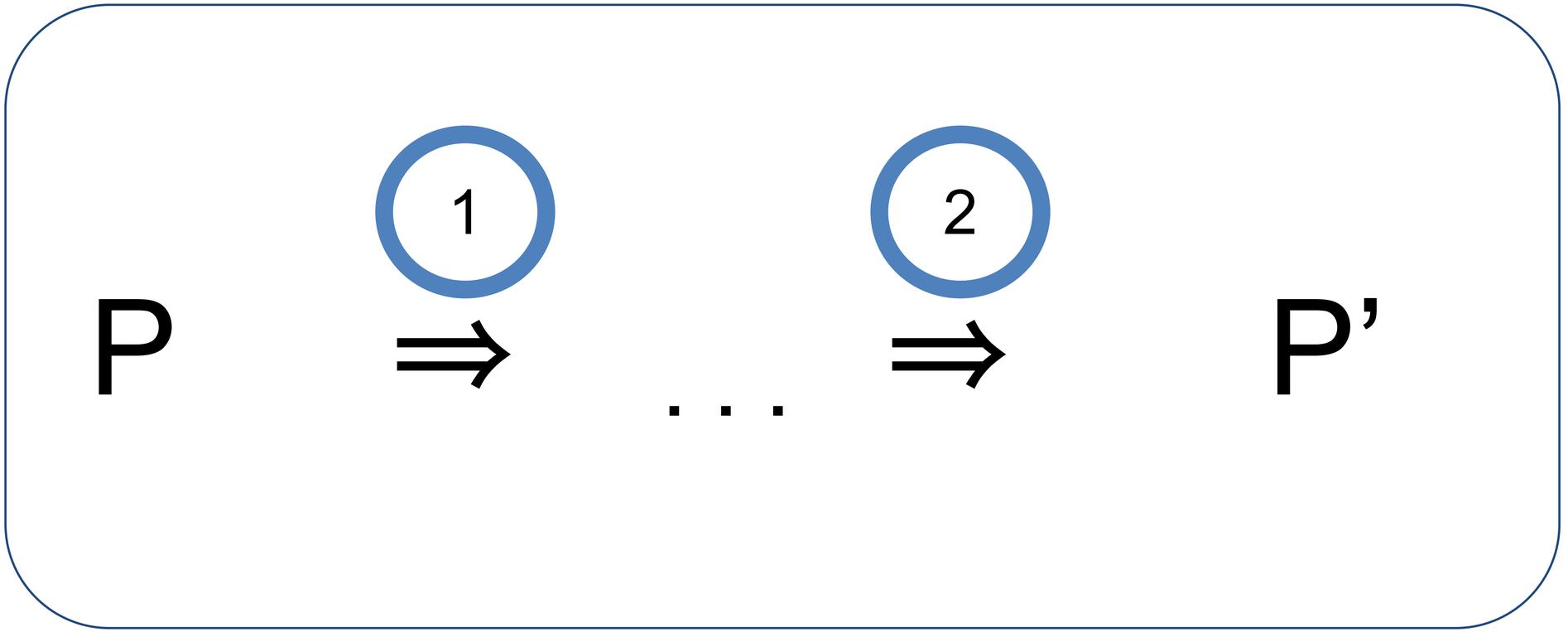
G
=
Graph presentation
of analysed infrastructure

F
=
Mapping from infrastructure
graph to pi calculus process

G is hardcoded ⇒ Changes in analysed infrastructure invalidate assessment

G can have millions of nodes ⇒ Verifiers do not scale well with model size

Process transformations



1 Allow adversary to choose concrete infrastructure.

$Q(s_1) \mid \ldots \mid Q(s_n) \Rightarrow !in(s).Q(s)$

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

Results

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

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

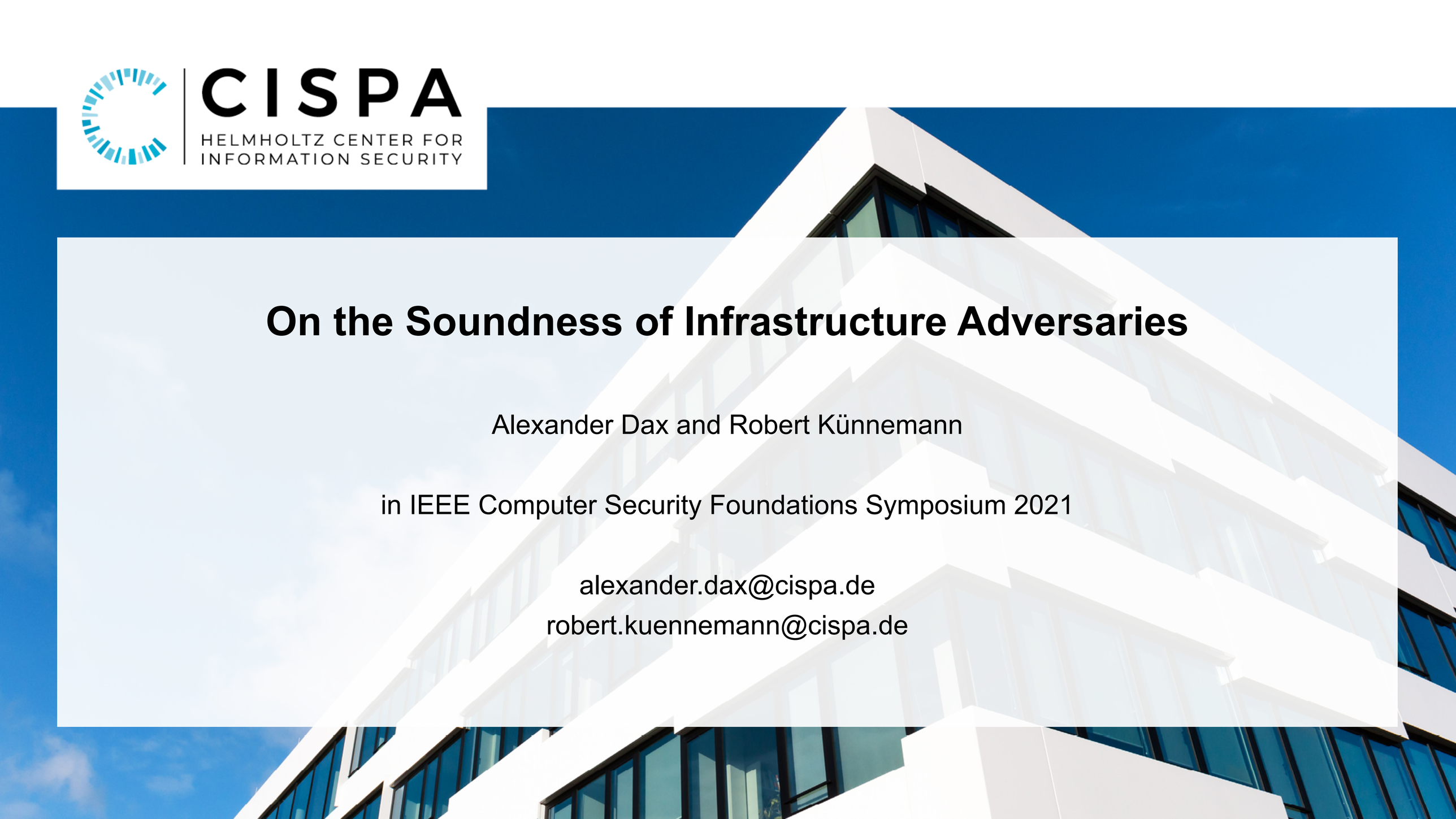
Includes PKI,SMTP, DNS, DNSSEC and inter-AS routing

(Github repository)

Symbolic Completeness

Corresponding notion to soundness

Conditions contain liveness properties



CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

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