

Why should Alice trust Bob?



Motivation

Cryptographic protocols are often described in an “Alice sends message m to Bob” fashion, which is easy to write but hard to proof secure.

Modern tools, based on formal methods, can **automatically** find attacks in protocols. Unfortunately, those tools do not support the notion of “trust” as offered by the TPM.

We will add this feature to enable the analysis of Trusted Computing Protocols.

Project description

- Protocols from the Trusted Computing literature will be studied.
- Protocols will be modeled in the input languages of the AVISPA tool.
- A new predicate for “trust” will be included in the intermediate format model attacks.
- Different protocols will be compared.

Literature

- Sebastian Mödersheim and Luca Viganò, The Open-Source Fixed-Point Model Checker for Symbolic Analysis of Security Protocols, LNCS 5705, Springer Verlag 2009
<http://www.springerlink.com/content/1284277217522544>
- Müller, Thomas: Trusted Computing Systeme : Konzepte und Anforderungen, Springer, 2008
<http://ftubhan.tugraz.at/han/ZDB-2-STI/www.springerlink.com/content/h671v3/>

Deliverables

- Term paper
- Source files
- Presentation

Project schedule

- Start: immediately
- Schedule will be defined with candidate at project start

Curriculum

Studies: INF SEW TEL MAT Master Thesis
Working scope and awarded credits are scalable.

Prerequisites

- Basics in IT-Security, Crypto or Trusted Computing
- Basics in logic or verification

Advisor / contact

Ronald.Toegl@iaik.tugraz.at