Proposal for a master’s thesis

**Verified Translation of Symbolic Security Protocols to a Computational Model**

Supervisors: Dr. Andreas Lochbihler  
Professor: Prof. David Basin  
Issue date:

**Prerequisites**

- Strong background in security protocol verification  
- Good knowledge of functional programming and logic (e.g., from the FMFP course)  
- Knowledge of the Isabelle theorem prover or other interactive proof assistants (e.g., from the Computer-Aided Modelling and Reasoning course) or willingness to learn the basics before the start

**Introduction**

New security protocols are nowadays analysed during their design phase by automated formal-methods tools. Examples include the TLS protocol in version 1.3 and fifth generation mobile networks. Two such tools, Scyther(-proof) and Tamarin, have been (co-)developed in the Information Security group at ETH. To achieve good automation, they represent network messages symbolically as expressions, e.g., \( \text{enc}_k(A, B, N) \), rather than actual bitstrings. In particular, they assume that cryptography is perfect. For example, the adversary cannot infer anything about an encryption unless he knows the key.

This idealised view works great for finding design errors, but when no bugs are found, the security guarantees are not clear (in the sense of provable security). The research area of computational soundness tries to provide computational guarantees for symbolic analyses such as: a computationally bounded adversary has only a negligible chance of breaking the protocol if the cryptographic primitives can be broken only with negligible probability. In the FCSPI project, we develop such soundness results and formalise them in the proof assistant Isabelle/HOL. These results are based on the intermediate language CoSP [1], into which various execution models can be embedded. For example, there are translations from the applied \( \pi \)-calculus of the security protocol analysis tool ProVerif [1] and from the Java crypto API for Dalvik bytecode [2], but none of the translations themselves has been formally checked by a tool.
Objectives

The goal of this thesis is to develop a *machine-checked* embedding from scyther-proofs’s execution model ESPL [3] to our formalisation of CoSP in Isabelle/HOL. The embedding can be expressed as a compiler from ESPL protocols to CoSP protocols, possibly with multiple stages. The embedding is correct if every trace of the compiled protocol can be reflected in the source protocol. This way, this thesis closes the gap between the protocol verifier scyther-proof and the computational soundness result. Thus, protocols verified with scyther-proof come with mechanically-checked computational guarantees, because (i) scyther-proof generates a transcript of its security proof which Isabelle/HOL can check, and (ii) every trace property of the scyther-proof protocol also holds on the compiled protocol, (iii) to which the formalised computational soundness result for CoSP applies.

Tasks

This project can be subdivided into the following tasks:

0. (before the start) Brush up your formalisation skills in Isabelle/HOL or acquire them (e.g., by working through the first chapters of [4]).

1. Familiarise yourself with the execution models of scyther-proof [3] and CoSP [1].

2. Define a translation from the ESPL execution model to CoSP in Isabelle/HOL, possibly in multiple stages.

3. Prove in Isabelle/HOL that every (symbolic) trace in the translated CoSP semantics corresponds to a trace in ESPL.

4. (optional) Define a translation for ESPL trace properties to CoSP trace properties and prove it correct.

5. (optional) Identify conditions on ESPL protocols for the translated protocol satisfying the CoSP protocol conditions of the computational soundness result. Prove that the conditions are sufficient.

6. Write the final report and prepare the presentation.

Deliverables

The following deliverables are due at the end of the project:

**Final report** The final report should consist of an introduction; a theoretical background section; one or more sections describing the modelling, the ideas of the formalisation and the proof; and a conclusion. The report may be written in English or German. Two copies of the report must be delivered to the supervisor.
**Isabelle/HOL theories** Complete Isabelle/HOL development that runs with the latest release or a recent developer’s version.

**Presentation** At the end of the project, a presentation of 30 minutes must be given during an InfSec group seminar. It should give an overview and discuss the most important highlights of the work.

**References**


