Formalizing and proving a typing result for security protocols in Isabelle/HOL

There are several works on the formalization of security protocols and proofs of their security in Isabelle/HOL; there have also been tools for automatically generating such proofs. This is attractive since a proof in Isabelle gives a higher assurance of the correctness than a pen-and-paper proof or the positive output of a verification tool. However several of these works have used a typed model, where the intruder is restricted to "well-typed" attacks. There also have been several works that show that this is actually not a restriction for a large class of protocols, but all these results so far are again pen-and-paper proofs. In this work we present a formalization of such a typing result in Isabelle/HOL. We formalize a constraint-based approach that is used in the proof argument of such typing results, and prove its soundness, completeness and termination. We then formalize and prove the typing result itself in Isabelle. Finally, to illustrate the real-world feasibility, we prove that the standard Transport Layer Security (TLS) handshake satisfies the main condition of the typing result.

Meta-Logical Reasoning in Higher-Order Logic

The semantics of first-order logic (FOL) can be described in the meta-language of higher-order logic (HOL). Using HOL one can prove key properties of FOL such as soundness and completeness. Furthermore, one can prove sentences in FOL valid using the formalized FOL semantics. To aid in the construction of the proof an interactive proof assistant like Isabelle can be used. The proof assistant can even automate simple proofs using the formalized FOL semantics.
Projects:

**Composec: Secure Composition of Distributed Systems**

Technical University of Denmark

Period: 01/10/2015 → 30/09/2018

Number of participants: 3

PhD Student:

**Hess, Andreas Viktor (Intern)**

Supervisor:

**Villadsen, Jørgen (Intern)**

Main Supervisor:

**Mödersheim, Sebastian Alexander (Intern)**

**Financing sources**

Source: Internal funding (public)

Name of research programme: Forskningsrådsfinansiering

Project: PhD