Jalon 1B : Sapic+: protocol verifiers of the world, unite!

SVP

Date: 01/03/2024
Doc. Version: <1>

Ce travail a bénéficié d’une aide de l’État gérée par l’Agence Nationale de la Recherche au titre du Plan France 2030 portant la référence ANR-22-PECY-0006

Document Control Information

Settings	Value
Document Title:	Sapic+: protocol verifiers of the world, unite!
Project Title:	SVP
Document Author:	<Veronique Cortier>
Scientific Coordinator:	<Stéphanie Delaune>
Project Manager (PM):	<Benoît Josset (PM)>
Doc. Version:	<1>
Sensitivity:	<Public >
Date:	01/07/2023

Sapic+: protocol verifiers of the world, unite!

Symbolic security protocol verifiers have reached a high degree of automation and maturity. Today, experts can model real-world protocols, but this often requirqes model-specific encodings and deep insight into the strengths and weaknesses of each of those tools. Sapic+ is a protocol verification platform, designed by Cheval, Jacomme, Kremer and Künnemann, that lifts this burden and permits choosing the right tool for the job, at any development stage. It provides automated translations from Sapic+ to Tamarin, ProVerif and DeepSec. We prove each part of these translations sound. A user can thus, with a single Sapic+ file, verify reachability and equivalence properties on the specified protocol, either using ProVerif, Tamarin or DeepSec. Moreover, the soundness of the translation allows to directly assume results proven by another tool which allows to exploit the respective strengths of each tool. We demonstrate our approach by analyzing various existing models. This includes, among others, a large case study of the 5G authentication protocols, previously analyzed in Tamarin. Encoding this model in Sapic+ we demonstrate the effectiveness of our approach. The Sapic+ platform is completely integrated in, and distributed with the open source Tamarin prover

[https://tamarin-prover.github.io/].