SAPIC+: protocol verifiers of the world, unite!

Vincent Cheval, *Inria Paris;* Charlie Jacomme, *CISPA Helmholtz Center for Information Security;* Steve Kremer, *Université de Lorraine LORIA & Inria Nancy;* Robert Künnemann, *CISPA Helmholtz Center for Information Security*

https://www.usenix.org/conference/usenixsecurity22/presentation/cheval

This artifact appendix is included in the Artifact Appendices to the Proceedings of the 31st USENIX Security Symposium and appends to the paper of the same name that appears in the Proceedings of the 31st USENIX Security Symposium.

August 10–12, 2022 • Boston, MA, USA

978-1-939133-31-1

Open access to the Artifact Appendices to the Proceedings of the 31st USENIX Security Symposium is sponsored by USENIX.

A Artifact Appendix

A.1 Abstract

Our artifact is a docker image that provides the fully pre-installed SAPIC$^+$ platform. The SAPIC$^+$ platform for automated protocol security analysis allows to use multiple backends (TAMARIN, PROVERIF and DEEPSEC) from a single model.

We carried out a set of case-studies, described in Figure 7 of the paper, that are included in the docker and can be verified using the pre-installed platform.

A.2 Artifact check-list (meta-information)

- **Run-time environment:** Our artifact is a Docker Image.
- **Metrics:** Execution time, verification results (security proofs or attacks).
- **Output:** A csv file summarizing results.
- **Experiments:** Verification scripts.
- **How much disk space required (approximately)?:** 250MB for the docker image.
- **How much time is needed to prepare workflow (approximately)?:** A few minutes.
- **How much time is needed to complete experiments (approximately)?:** 2—3 hours.
- **Publicly available (explicitly provide evolving version reference)?:** Docker link.
- **Code licenses (if publicly available)?:** GNU GPL v3.
- **Archived (explicitly provide DOI or stable reference)?:** link to docker image or, alternatively, link to github repository.

A.3 Description

A.3.1 How to access

If docker is installed the artifact can be obtained by the following command:

```
docker pull robertkuennemann/sapicplusplatform
```

As SAPIC$^+$ is an extension of the TAMARIN prover is has been merged in the official develop branch of the repo and can be directly obtained from https://github.com/tamarin-prover/tamarin-prover. SAPIC$^+$ can then be installed by first installing Tamarin, and then Proverif v2.04 and DeepSec v2.0.0.

A.3.2 Hardware dependencies

N/A

A.3.3 Software dependencies

Docker.

A.3.4 Data sets

N/A

A.3.5 Models

N/A

A.3.6 Security, privacy, and ethical concerns

N/A

A.4 Installation

Installation instruction for Docker are provided at https://docs.docker.com/engine/install/.

The image is obtained with

```
docker pull robertkuennemann/sapicplusplatform
```

and can then be browsed by running

```
docker run -it robertkuennemann/sapicplusplatform bash
```

A.5 Experiment workflow

Once inside the Docker, our case-studies can be reproduced by running two scripts in the `example` directory

- `./run-proverif-CS.sh`
- `./run-tamarin-CS.sh`

A.6 Evaluation and expected results

The scripts above execute all the case studies discussed in the paper (Figure 7), and store the results of either using Tamarin or Proverif to verify a given protocol. After completion, they should have created respectively a "examples/res-pro.csv" (PROVERIF results) and "examples/res-tam.csv" (TAMARIN results) files. Each line corresponds to one verification, using the format "protocol name; verification result; run time".

Note that the case studies need approximately 2–3 hours and 12GB to run. On OS X, Docker runs on a virtual machine with a builtin memory limit of 2GB, which must thus be increased to at least 12GB in the configuration pane located at 'Preferences/Resources/Advanced settings'.

Outside of a Docker, the PROVERIF script should complete in a few minutes on a standard laptop, while the TAMARIN script may take longer, but no more than one hour on a laptop. This may vary inside the docker depending on allocated resources.

We provide an additional docker image that is built from the previous one and by running the two scripts. It can be used to see the expected results by browsing the csv files:

```
docker pull robertkuennemann/sapicplusplatformbench
```

A.7 Experiment customization

Users familiar with protocol verification can use the docker image to verify new protocols. The image can be used to run SAPIC$^+$ with TAMARIN, PROVERIF or DEEPSEC on new examples. See the "README-platform" file in the docker image for more information.

A.8 Notes

N/A

A.9 Version

Based on the LaTeX template for Artifact Evaluation V20220119.