

 Content archived on 2024-05-24



# Automated Validation of Internet Security Protocols and Applications

## Results in Brief

### Analysing cryptographic protocols with AVISPA

Within the AVISPA project, new tools that support an automatic, but rigorous validation of Internet security protocols have been designed. With a high level specification language as input format, they can provide the level of assurance required by both developers and users in developing the next generation of security protocols.



DIGITAL ECONOMY




© PhotoDisc

In many network applications and services, where data integrity, confidentiality and other security related properties are crucial, cryptographic protocols play a major role. They allow for the secure authentication of entities and the establishment of a secure communication channel between agents for sharing information while protecting the privacy of their inputs.

With the wide spread of the Internet and network-based services, new security protocols under development are out-pacing the current ability to rigorously analyse and validate them. To speed up their development and moreover improve their reliability, it is crucial to have robust automated tools for finding flaws in a security-sensitive protocol or for establishing their absence.

The AVISPA tool rise to this challenge in a systematic way by providing a modular and highly expressive formal language for modelling security protocols and specifying their intended properties. The security protocols specifications written in the AVISPA's High-Level Protocol Specification Language (HLP SL) are translated into rewrite-base formalism, the Intermediate Format (IF), before given as input to four different back-ends. A security protocol, written in IF, is executed over a finite number of iterations, or entirely if no loop is involved. Eventually, either an attack is identified, or the protocol is considered safe.

Implementing a variety of analysis techniques, ranging from falsification to bounded and unbounded verification, the back-ends perform the analysis and produce the results in precisely defined output format. The AVISPA tool is equipped with a graphical user interface that supports the editing of protocol specifications and allows the user to select and configure the back-ends integrated into the tool. Upon termination, if an attack on a protocol is found, the tool displays it as a message-sequence chart or postscript files.

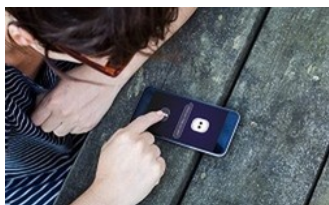
The AVISPA tool can be freely accessed either through its Web-based interface or by downloading and installing the software distribution. For more details, please refer to the AVISPA Web site: <http://www.avispa-project.org/> 

## Discover other articles in the same domain of application



[Algorithms to improve traffic conditions on busy motorways](#)

6 September 2019



[A 'social' virtual assistant for migrants](#)

26 June 2018





## Multitasking is redefined thanks to new app

16 January 2018



## Using behavioural models to upgrade User Interface design

15 September 2020



### Project Information

#### AVISPA

Grant agreement ID: IST-2001-39252

[Project website](#) 

Project closed

#### Start date

1 January 2003

#### End date

30 June 2005

#### Funded under

Programme for research, technological development and demonstration on a "User-friendly information society, 1998-2002"

#### Total cost

€ 2 047 586,00

#### EU contribution

€ 808 000,00

#### Coordinated by

UNIVERSITA DEGLI STUDI DI  
GENOVA



Italy

**Last update:** 22 January 2007

**Permalink:** <https://cordis.europa.eu/article/id/83181-analysing-cryptographic-protocols-with-avispa>

European Union, 2025

