Automated Verification of Infinite State Systems

Wyniki w skrócie

Paving the way for faster and more secure Internet transactions

On the basis of automated deduction, a newly developed prototype tool for protocol analysis offers users advanced capabilities for fast and reliable identification of flaws in protocols. Thereby, it may lead to great reductions in time-to-market and increased security in the fields of eCommerce, telecommunications, multimedia and other security-sensitive applications.

GOSPODARKA CYFROWA

© PhotoDisc

A key area of computer science research is the automatic verification of large practical systems, and towards this goal, several different formal methods have been developed and applied. As such, model checking normally used in industry may automatically establish the correctness of finite-state systems, including descriptions of hardware and protocols.

Nevertheless, most practical system descriptions involve large or infinite state spaces whose flaws may not be easily identified by finite-state verification methods. In this case, theorem proving constitutes an alternative solution; however, it requires a lot of manual effort from the user and sophisticated mathematics to employ.

To address all these problems, an innovative protocol analysis tool for the automated verification of infinite state systems (AVISS) has been designed, implemented and tested. This push-button technology effectively combines three techniques namely the on-the-fly model checking using lazy data types, constrained theorem-proving and model checking via propositional satisfiability checking.

Each of these emerging techniques is working independently while the system allows their systematic and quantitative comparison as well as their effective interaction. Moreover, the easy-of-use model checkers and the power of the theorem proving method are integrated in a fully automated way leading to a robust, flexible, reliable, fast and cost-effective system.

Applying this breakthrough development to the Clark/Jakob library that includes 51 protocol verification problems, the AVISS tool has shown a better coverage and/or performance than potentially any other analysis tool. For instance, unlike most other tools, this novelty could detect various subtle attacks such as typing ambiguities.

The AVISS tool may be used for validation of security-sensitive protocols in various fields including telecommunications, multimedia and other applications. Furthermore, it may significantly contribute to the acceleration of the next generation of network protocols development and to the standardisation and regulation processes in eCommerce, eGovernment, and other Internet applications. For more info, click: http://www.informatik.uni-freiburg.de/~softech/research/projects/aviss/

Znajdź inne artykuły w tej samej dziedzinie zastosowania

Giving a voice to voice privacy

8 Kwietnia 2022

An easy-to-use, automatic means for making online video campaigns

4 Października 2019

Digitising brick-and-mortar retail stores

3 Stycznia 2020

Blockchain technology makes secure, low-cost and simple payments a reality for all

26 Czerwca 2020

Informacje na temat projektu

AVISS

Identyfikator umowy o grant: IST-2000-26410

Strona internetowa projektu

Projekt został zamknięty

Data rozpoczęcia	Data zakończenia
1 Maja 2001	30 Kwietnia 2002

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

Koszt całkowity
€ 205 434,00

Wkład UE
€ 100 000,00

Koordynowany przez
ALBERT-LUDWIGS-UNIVERSITAET FREIBURG
🇩🇪 Germany

Ostatnia aktualizacja: 18 Września 2005

Permalink: https://cordis.europa.eu/article/id/81451-paving-the-way-for-faster-and-more-secure-internet-transactions