Automated analysis of security-sensitive protocols

October 25 2005

The sheer number and variety of security protocols for Internet applications under development makes it difficult to be sure that any one protocol is 100 per cent secure from attack. Now an automated tool can systematically validate these security-sensitive protocols and applications.

“The AVISPA software tool enables a security protocol designer to input the protocol and the language he/she wishes to use, then feeds back information on this protocol including any known bugs or security weaknesses,” says Professor Alessandro Armando of the University of Genoa’s Artificial Intelligence Laboratory (DIST) and coordinator of the IST programme-backed Future and Emerging Technologies project AVISPA. “Previously such protocol designers had no automated support to help them in their design role – that is the purpose of the AVISPA tool."

Secure protocols are a vital element in carrying out safe online interactions between a user’s Web browser and a company Web server, for example a bank’s Web server in an online banking application. Though such protocols might look simple, they can often be extremely difficult to get absolutely right, such as with no bugs or weaknesses in the protocol.

Armando quotes the classic example of the Needham-Schroeder public-key protocol, which was first published in 1978 as a means of mutual authentication between two parties using public-key cryptography. The protocol was eventually found to be vulnerable to simple attacks in 1996, eighteen years later!

AVISPA participants aimed to develop a push-button, industrial-strength technology for the analysis of such security-sensitive Internet protocols and applications. The project finished in July 2005 with the release of the AVISPA tool, which is a simple software application that runs on a PC or via a Web interface. It can be accessed online, and offers both a Basic and an Expert mode.

The consortium partners believe that this new tool will help speed the development of the next generation of security protocols, and improve their security in the process.

Project partner Siemens has already discovered a weakness in one of its own protocols using the tool, and has revised the protocol and issued a new patent accordingly. The partners have started collaborating with SAP for continuing the analysis of more complex security-sensitive applications under future research projects.

Source: IST Results

Citation: Automated analysis of security-sensitive protocols (2005, October 25) retrieved 26 April 2024 from
https://phys.org/news/2005-10-automated-analysis-security-sensitive-protocols.html