For Secure Software: X-rays instead of Passport Control

JOANA Software Analysis Tool Checks Source Text of a Program to Discover Security Gaps

Trust is good, control is better. This also applies to the security of computer programs. Instead of trusting "identification documents" in the form of certificates, JOANA, the new software analysis tool, examines the source text (code) of a program. In this way, it detects leaks, via which secret information may get out or strangers may enter the system from outside. At the same time, JOANA reduces the number of false alarms to a minimum. The analysis tool developed by Karlsruhe Institute of Technology (KIT) has already proved to work successfully in realistic test scenarios. In a next step, an industrial case study is planned.

Monika Landgraf
Chief Press Officer

Kaiserstraße 12
76131 Karlsruhe, Germany
Phone: +49 721 608-47414
Fax: +49 721 608-43658
E-mail: presse@kit.edu

For further information, please contact:

Lilith C. Paul
Public Relations and Marketing
Phone: +49 721 608-48120
Fax: +49 721 608-43658
E-mail: l.c.paul@kit.edu

"Established software certificates certify the manufacturer to be trustworthy. With JOANA, we can also check the real behavior of a program," says Gregor Snelting, who developed the analysis tool with his research group at the Chair of Programming Paradigms of KIT. In his opinion, this is important, because most weaknesses result from unintended programming errors. The scientists currently focus on mobile applications for Android smartphones. In principle, however, they can test any program written in JAVA, C or C++. First, software companies are to test their products before commercialization. As experts are required to set up and operate JOANA, it is less suited for private users.

JOANA checks all data channels of a software, through which information flows. In this way, it detects security gaps. "We distinguish between publicly visible channels that e.g. map the user interface and protected channels that cannot be accessed by users," Snelting explains. "To protect secret information, such as passwords or account numbers, these data have to be transmitted in protected channels exclusively. Where secret and public data flows cross, however, information may be exchanged in principle. Here, there is a risk of sensitive information being transmitted.

Scientists distinguish several types of security gaps: Directly readable copies of sensitive data may get out (explicit leak) or the patterns of their encryption only (implicit leak). Secret passwords may affect the

probable order of visible information flows (probabilistic leak) from which they could be reconstructed. An example: The command to print a “red L” reaches the printer at the same time as the secret password for access authorization. If the password is AB, the information “L” mostly arrives shortly before the information “red”. If the password is BA, it is just the opposite. JOANA reliably detects such security gaps, although they are more difficult to identify.

“Minimizing false alarms is at least as important as finding all security gaps,” Snelting says. Many false alarms lead to a massively increased inspection effort or to the alarms being ignored. JOANA reduces the number of false alarms for all security gaps, even for probabilistic leaks. For this purpose, the KIT scientists developed a new computation method (Relaxed Low-Security Observational Determinism) that requires a fixed order of observable process steps at safety-critical points only. For the example above, this would mean that the information “red” has to reach the printer always before the information “L” irrespective of the password. ”The challenge was to exclude safety-irrelevant processes from such strict requirements,” Snelting emphasizes. Otherwise, the number of false alarms would increase, because any deviation would be classified as dangerous or executions of the program would have to be restricted considerably, such that it would hardly be usable anymore.

So far, JOANA is the only software analysis tool worldwide that does not only find all security gaps but also minimizes the number of false alarms without affecting the functioning of programs. With funds granted by the German Research Foundation, the KIT scientists have conducted research in this area for about 20 years now. “In the longer term, software inspected by JOANA might be given a new certificate that confirms security of the program code,” Snelting says.

Interested experts may download JOANA as an open source software: http://pp.idp.kit.edu/projects/joana

Digital Press Kit Relating to the Science Year 2014

Communication, energy supply, mobility, industry, health care, leisure time: Digital technologies have long been part of our everyday life, they open up new opportunities and offer solutions for problems of society. At the same time, they pose challenges. Opportunities and risks will be in the focus of the Science Year 2014 – The Digital Society. At the KIT, researchers of all disciplines study various – technical and societal – aspects of digitization. The digital press kit of KIT relating to the Science Year 2014 contains short portraits, press releases, and videos:

http://www.pkm.kit.edu/digitalegesellschaft

Karlsruhe Institute of Technology (KIT) is a public corporation according to the legislation of the state of Baden-Württemberg. It fulfills the mission of a university and the mission of a national research center of the Helmholtz Association. Research activities focus on energy, the natural and built environment as well as on society and technology and cover the whole range extending from fundamental aspects to application. With about 9.400 employees, including more than 6.000 staff members in the science and education sector, and 24.500 students, KIT is one of the biggest research and education institutions in Europe. Work of KIT is based on the knowledge triangle of research, teaching, and innovation.

This press release is available on the internet at www.kit.edu.