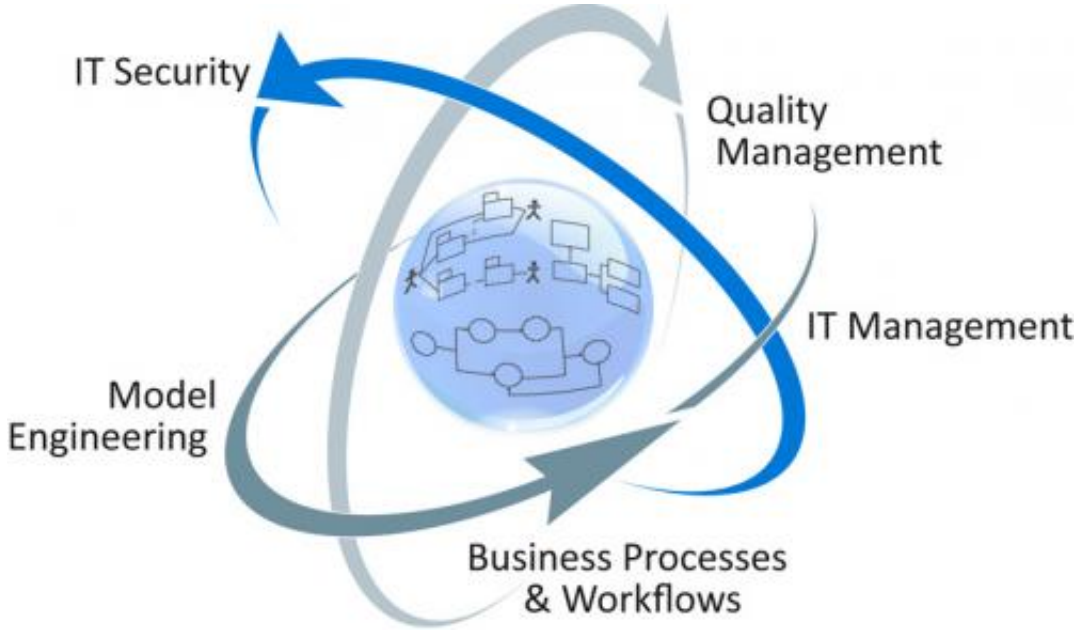
Better non-functional security tests for software

September 15 2014



An increasingly connected world requires better and better non-functional security tests for software. A project of the FWF provides basic know-how. Credit: Quality Engineering

The integration of digital expert knowledge and automation of risk analyses can greatly improve software test procedures and make cloud computing more secure. This is shown by the latest results of a project by the Austrian Science Fund FWF on the quality assurance of security critical systems which has just been published. The results provide a platform for what are known as non-functional security tests. These

attempt to identify weaknesses in software which do not arise directly from the execution of the program – and play an increasingly important role for cloud computing. The recently developed platform allows such tests to be automated further and made more user-friendly.

Software developers frequently experience nasty surprises: Even after long and successful use of cloud programs, unexpected weaknesses can suddenly emerge. In fact, cloud programs are particularly susceptible to this. Not because they are badly written, but because they have many interfaces which are continually adapted. These require functionalities that go well beyond the actual running of the program and are dependent on third-party systems. Non-functional security tests, as they are called, may be able to test these aspects, but the conventional methods of quality assurance are often defeated by the complexity of the requirements. Researchers at the University of Innsbruck have now presented a platform which can significantly improve non-functional tests.

To Test is The Best

The main success criteria of this platform, which was developed by a team led by Prof. Ruth Breu, Head of the Institute of Computer Science, are the integration of expert knowledge as well as automation of the processes for risk analysis. The importance of the integration of formalised expert knowledge about weak points in software is strikingly expressed by Prof. Breu: "In the year 2012 alone, 9,762 previously unknown security vulnerabilities were registered in the Open Source Vulnerability Database, a globally accessible database for the administration of knowledge about security vulnerabilities in software. But in fact, the causes of many of these security vulnerabilities have been known for a long time. They could therefore have been avoided at the point when the software was developed. Thus optimised non-functional tests should make use of such existing knowledge. That is

exactly what our procedure does."

To this effect, the team headed by Prof. Breu, Dr. Michael Felderer and Philipp Zech formalise such knowledge to make it available for subsequent automatic risk analysis. These analyses then result in risk profiles for the systems to be tested, which are used for the production of executable security tests. This involves the application of modern programming languages such as Scala and ASP, as well as model-based techniques. "The problem with earlier non-functional security tests is the sheer endless number of possibilities for error. Previous attempts to master this situation involved human expert knowledge, e.g. for penetration tests. But the approach we selected now allows a structured and automated test procedure", explains Prof. Breu with reference to this automated risk analysis process.

Practical Test

Prof. Breu continues: "Our work initially tended to be guided by theory. But we also wanted to demonstrate the practical relevance of our deliberations. So we performed real-life tests which checked reactions to common problem situations such as SQL injection attacks." Within the framework of the currently published work, programs written by the researchers were initially relied upon to do this. However, for some time now, Prof. Breu's team has also been using publicly available test systems. With impressive results: Up to 90 per cent of all weak points can currently be identified reliably.

Overall, the results of this FWF project represent significant progress for the future quality assurance of security critical systems – a result which once more confirms the significance of basic research work for the smooth functioning of our daily life.

More information: P. Zech, M. Felderer, B. Katt and R. Breu:

"Security Test Generation by Answer Set Programming." The Eighth International Conference on Software Security and Reliability (SERE 2014), IEEE, 2014

Provided by Austrian Science Fund (FWF)