Innovation Reports

DIAMONDS
(ITEA 2 ~ 09018)

Security-testing regime for interconnected software-based systems and networks.

ISN
(ITEA 2 ~ 09034)

Accelerating the use of standardised wireless technologies for systems monitoring and management.

DIAMONDS
(ITEA 2 09018)

Ina Schieferdecker, Fraunhofer FOKUS, Germany

Security-testing regime for interconnected software-based systems and networks

Current security testing is based mainly on audits of processes, systems and networks but this still lacks generic security models and systematic testing approaches that allow risk-oriented semi-automated analysis. The basic aim of the ITEA 2 DIAMONDS project was to produce an effective methodology capable of strengthening the practices of security testing commonly used in computer science and various industrial areas.

Nowadays open networks are taken for granted yet this continuous interconnection and data-sharing are vulnerable to a growing number of security threats from both internal and external sources. In sectors such as transport with train control systems, medical patient care, automotive with car-to-infrastructure communications and mobile telecommunications, there are safety-critical implications. Failures can endanger human lives and the environment, implying serious damage to industrial and social infrastructures, jeopardising confidentiality and privacy, or undermine the viability of whole business sectors. It is common knowledge that the security of most systems is directly related to the quality of the underlying software – software defects lie at the root of over 90% of software security incidents.

MODEL-BASED TESTING FOR SECURITY WEAKNESSES

Against this background, DIAMONDS developed a series of systematic, model-based risk analysis, test and monitoring approaches for the security testing of software systems with advanced model-based security-testing methods enabling the early identification of design vulnerabilities and underpinning a focus on the efficient testing of security aspects.

The consortium focused on the particular issue of testing networked systems for susceptibility to malice, error or mischance, helping to build trust in such systems by enabling them to demonstrate their robustness and fault-tolerance in the face of such attacks. Security issues with industrial-scale networked systems, as in banking, smart cards, information technology, software-defined radio and defence electronics, are a high priority. By deriving common principles and methods, efficient security testing methods relevant to a swathe of industries can be derived. The DIAMONDS security-test methodology is adaptable to different domain security standards, enables risk-analysis oriented test generation and underpins risk assessments by evaluation of test results. This industrial-scale European security-test methodology has been demonstrated on security-critical systems in a variety of application domains.

INNOVATIONS FOR FORMAL SECURITY TESTING

The four main security-testing method innovations

developed are focused on building a 'pre-standard' for model-based security testing to represent the enabling technology necessary for the introduction of formal security testing in industry:

- Advanced model-based security testing methods which combine different techniques to obtain improved results applicable to multi-domain security
- Development of autonomous testing techniques based on automatic monitoring to improve the resilience of dynamically evolving systems
- Pre-standardisation work on multi-domain security test methodologies and test patterns, allowing DIAMONDS to offer interoperable security test techniques and tools
- An open-source platform for security-test tool integration to provide a common platform and single user interface for various test tools, as well as a single tracing and reporting interface.

Through these innovations DIAMONDS will strengthen the practices of security testing, stimulate a wider range of use of security testing in projects in different domains and help improve the quality, with respect to security, of the systems developed, reducing the security risks and the risk-related costs during operation. Losses incurred are due not only to the consequences of a security breach but also to the effort needed to repair the deployed systems and the loss of confidence in the systems concerned (e.g. drop in vendor stock values). Productivity will also be improved by accelerating the testing process, increasing the confidence in a system when it is modified and eliminating the repetitive tasks needed when manually testing the resilience of a system.

CASE STUDIES

Key to quantifying the success of the DIAMONDS innovations and steering the project came in the shape of use cases through questionnaires and interviews with the persons involved. The criteria included estimation of cost savings, productivity gains, trust improvement and overall impact of the methods introduced. The information gathered was analysed and conclusions were drawn to evaluate the work and provide feedback on the technical work packages. Iterating this process throughout the project helped the methods and tools developed for the case study needs to be constantly improved and adapted. In order to guarantee that the project remained innovative with respect to other advances in the security testing area, the partners maintained a state-of-the-art, addressing and changing objectives as necessary. In addition, DIAMONDS developed the Security Testing Improvement Profile (STIP) approach, that is dedicated to assess security testing processes. The STIP approach has been used to evaluate all of the DIAMONDS case studies. It demonstrated substantial improvements in all case studies due to the innovations of the project.

Among the case studies in such domains as banking, radio protocol, automotive, telecom and industrial automation were risk-based security testing, advanced fuzz testing, model-based behavioural fuzzing active testing, integration of model-based test generation and monitoring, autonomous testing methods, and open-source tools for security testing. Furthermore, by developing an open-source platform for security test tool integration, DIAMONDS provides a common platform, giving the user a single-user interface towards various test tools as well as a single tracing and reporting interface to have concise report from the various tools. This platform will support the integration of testing modules from various vendors and the open-source community developed specifically for the platform as well as integration of existing tools. The platform is available for all security testing vendors and open-source community members as integration point for their tools.

As a result of this ITEA 2 project, developers will benefit by being able to test software for vulnerabilities and thus prevent their introduction to the software cycle in the first place; systems integrators, testers, software quality assurers and software buyers will be able to evaluate the quality of software before using it, process owners will be able to improve their security testing analysis and testing processes, and researchers will be able to investigate and establish new knowledge in systems testing.

SUCCESSFUL EXPLOITATION

The success of the DIAMONDS project, underlined by two successive achievement awards at the ITEA 2 & ARTEMIS Co-summits in 2011 and 2012, is evident in the exploitation of new commercial products including Codenomicon (new platform release, several fuzzing test suites), Montimage (Montimage Monitoring Core), Smartesting (security-requirements driven test generation), Testing Technologies (TTCN-3 Fuzz Testing Extensions) and Dornier Consulting (Atoms Security Testing Module). Furthermore, DIAMONDS generated open-source products and product updates, and FOKUS (Fuzzino, Tracebility Platform for RBST) as enabled the adoption of methods in the production environment (Giesecke & Devrient – CORAS, METSO – Network Hoover and Thales – combination of active & passive testing) along with new research projects such as FOKUS, SINTEF and Smartesting.

A EUROPEAN GUARANTEE

A formal security-testing regime for European software will benefit software designers, developers and vendors of all kinds. Rather than providing timely patches to 'buggy' software, developers will be able to find vulnerabilities before hackers exploit them. Above all, there is a growing need to evaluate software coming from unknown or little-known European sources for vulnerabilities, especially those which could allow malicious entities to penetrate systems or their connected networks. A European solution designed by European actors will present a certain standard and a certain guarantee to market actors and administrations around the world that wish to preserve their systems, their data privacy and their sovereignty.

FOR MORE INFORMATION

www.itea2-diamonds.org