DIAMONDS

Strengthening software security for a connected world

Published December 2017

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, healthcare with medical patient care, automotive with car-to-infrastructure communications and mobile telecommunications, there are safety-critical implications. The ITEA project DIAMONDS set out to examine how to secure these safety and security-critical systems. The project, which brought together 22 industrial and scientific players from six countries to develop a new security testing paradigm and methodology, known as model-based security testing, successfully demonstrated and evaluated it in eight industrial settings from four different industrial domains.

Impact highlights

- As a result of the DIAMONDS project, Fraunhofer FOKUS gained recognition as an expert in the field of security testing in industry as well as in the academic realm. RACOMAT, the outcome of DIAMONDS, is currently the main tool for risk-based security testing within Fraunhofer FOKUS.
- Thanks to the business impact coming from the results of the project, Montimage's workforce was increased from five to twelve people.
- Using the results from DIAMONDS, Codenomicon was able to identify the OpenSSL Heartbleed vulnerability, which had gone unidentified for over two years and impacted over 500,000 websites.
- Multiple standardisation documents reflecting the project's case studies have been adopted by the European Telecommunications Standards Institute (ETSI) and have been forwarded to international standardisation bodies.
- Techniques like fuzz-testing and risk-based testing have been recognised by international and national certification bodies like the German BSI. They will become part of supplemental guidelines to support guidelines such as e.g. the Common Criteria Certification.

Project results

DIAMONDS developed a series of systematic, model-based risk analysis, test and monitoring approaches for security testing of software systems. This included advanced model-based security testing methods that enable the early identification of design vulnerabilities, underpinning a focus on 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 were a high priority. The DIAMONDS security-test methodology is adaptable to different domain security standards through the derivation of common principles and methods. Furthermore, it integrates security risk assessment and security testing over the whole software life cycle, encompassing early testing, risk assessment, and automatic testing and monitoring.

Exploitation

Montimage has improved and integrated the security analysis functionality of their Monitoring Tool, and it is now being used and evaluated by the Thales TCS business division, the French DGA, and academic research (Institute Mines Télécom, Université de ParisSud). Two public tenders have been won and six licenses have been sold. It will also be evaluated by setting up a Proof-of-Concept with Orange beginning of 2018.
Smartesting developed, prototyped and validated a new approach to security testing based on security test patterns. This has been implemented in the Smartesting CertifyIt MBT tool and is under deployment in the context of security components and ePayment systems.

In DIAMONDS, Codenomicon extended its main product Defensics. Defensics and Codenomicon have both gained a widely acknowledged reputation. Codenomicon has been acquired by Synopsys, one of the leaders in Application Security Testing according to Gartner in 2017.

The System Quality Centre at Fraunhofer FOKUS provides methods, processes and tools for the development and quality assurance of software-intense systems that often perform business-critical or security- and safety-relevant functions in urban infrastructures, cars, trains, planes or factories. In order for such systems to work in a fault-tolerant, fail-safe and IT-secure way, even in unexpected situations, the system quality has to be ensured throughout the entire development process, from the requirements analysis to the certification. DIAMONDS results such as FUZZINO and RACOMAT have become essential products that complement and support Fraunhofer FOKUS' security testing services and research.

Testing Technologies extended the capabilities of its TTCN-3 test development and execution platform TTworkbench towards security testing and successfully initiated standardisation work on security testing at ETSI MTS. Testing Technologies has been acquired by Spirent and the TTworkbench has become a central building block of Spirent's Automotive Testing Products, an emerging part of Spirent's business and therefore with significant growth potential.

DIAMONDS

09018

PROJECT LEADER

Ina Schieferdecker, Fraunhofer FOKUS

PROJECT START

October 2010

PROJECT END

May 2013

PROJECT WEBSITE

https://www.itea2-diamonds.org

PARTNERS

Austria
- Graz University of Technology ◉
- Secure Business Austria ○

Finland
- Codenomicon ⊙
- Conformiq Software Ltd ⊙
- Ericsson ●
- Metso Automation Inc ●
- University of Oulu ◉
- VTT Technical Research Centre of Finland ○

France
- FSCOM ⊙
- Gemalto SA ●
- Institut Polytechnique de Grenoble ◉
- Institut Télécom SudParis ◉
- Montimage EURL ⊙
- Smartesting ⊙
- Thales Communications and Security ●
- Trusted Labs ⊙

Germany
- Dornier Consulting GmbH ⊙
- Giesecke & Devrient GmbH ●
- Fraunhofer FOKUS ○
- Testing Technologies IST GmbH ⊙

Luxembourg
- ITRUST ⊙

Norway
- Norse Solutions AS ⊙
- SINTEF Stilftelsen ○

● (Large) Industry ○ Research institute ⊙ SME ◉ University ● Government