ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

Project Results

DIAMONDS

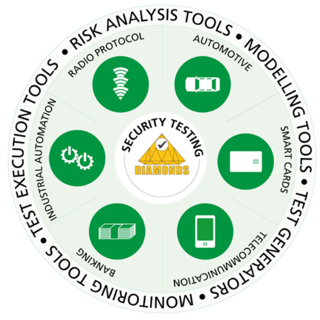
Effective security-testing for interconnected software-based systems and networks

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 security-critical implications. 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.

Against this background, the ITEA 2 project DIAMONDS developed a series of systematic, model-based risk analysis, test and monitoring approaches for the security testing of software-based 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. 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 risk analysis and security testing methods relevant to a swathe of industries can be derived.

DEVELOPING A PRE-STANDARD

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. 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; the 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 traceing and reporting interface.



Test methods and tools and application domains

Through these innovations DIAMONDS strengthens the practices of security testing, stimulates 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.

STEERED BY PRACTICE

Key to quantifying the success of the DIAMONDS innovations and steering the project came in the shape of use cases with the criteria including estimation of cost savings, productivity gains, trust improvement and overall impact of the methods introduced. Among the case studies in the 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, DIAMONDS has developed an assessment scheme called Security Testing Improvement Profile (STIP), that is dedicated to assess security testing processes. It can be used stand alone or in addition to established test process assessment approaches. STIP defines a set of key areas relevant for security

DIAMONDS
(ITEA 2 ~ 09018)

Partners

Codenomicon
Conformiq Software Ltd.
Dornier Consulting GmbH
Ericsson
Fraunhofer FOKUS
FSCOM
Gemalto SA
Giesecke & Devrient GmbH
Graz University of Technology
Institut Polytechnique de Grenoble
Institut Télécom SudParis
ITRUST
Metso Automation Inc.
Montimage EURL
Norse Solutions AS
Secure Business Austria
SINTEF Stilftelsen
Smartesting
Testing Technologies IST GmbH
Thales Communications and Security
Trusted Labs
University of Oulu
VTT Technical Research Centre of Finland

Countries involved

Austria
Finland
France
Germany
Luxembourg
Norway

Project start

October 2010

Project end

May 2013

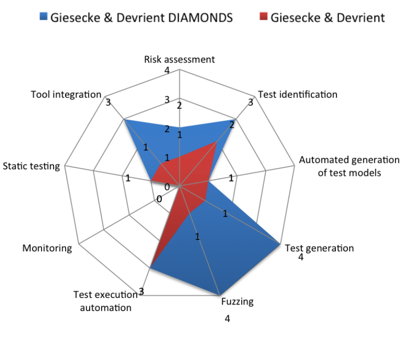
Contact

Project Leader :
Ina Kathrin Schieferdecker,
Fraunhofer FOKUS

Email :
ina.schieferdecker@fokus.fraunhofer.de

Website :
www.itea2-diamonds.org/index.html

testing. The key areas describe major aspects or activities in a security testing process and are chosen in a way, that they are aligned with the DIAMONDS methodology for model-based security testing (MBST) and that they address the most relevant DIAMONDS innovations [2]. The key areas are defined to be self-contained and distinct so that each of the areas represents a relevant aspect of an MBST process.



Security Testing Improvement Profile (STIP)

For each of the key areas, four performance levels that are hierarchically organised and built on each other are defined. The levels can be used to evaluate and subsequently improve concrete security testing processes with respect to their performance in the belonging key area. Each level with a higher number represents an improvement for the underlying security testing process. The STIP approach has been used to evaluate all of the DIAMONDS case studies.

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. The success of this approach is evident in the exploitation of new commercial products like Codenomicon (new platform release, several fuzzing test suites), Montimage (Security & Performance Testing Modules) and Smartesting (security-requirements driven test generation) as well as open-source products and product updates, and the adoption of methods in the production environment along with new research projects.

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.

Major project outcomes

DISSEMINATION

- 102 publications e.g. at ICTSS'11, ICMT'11, ICSSEA'11, SERE'12, PASSAT'12, QSIC'12, ASQT'13, INFOTECH'13
- 90 presentations at industrial conferences/fairs
- academic and industrial workshops e.g. Sectest'11, Sectest'12, STV'12, SASSI'13, Risk'13
- DIAMONDS Tutorial at the ICST'13

EXPLOITATION

- new commercial products e.g. Codenomicon Traffic Capture Test Suite, Web Application Fuzzing, Bluetooth LE Fuzzing
- new open source products e.g. Montimage Monitoring Tool (core), FhG FOKUS Fuzzino (Fuzz Testing Library), FhG FOKUS RiskTest (Traceability Tool)
- new services e.g. FhG FOKUS Security Improvement Profile (STIP), Security Testing for Automotive Applications, Security Testing for Industrial Automation
- commercial product updates e.g. new versions of Montimage Performance Analysis and Security Analysis Modules, TTworkbench TTCN-3 Fuzzing Support, Smartesting CertifyIt Model-based Security Test Generation Support, Dornier Consulting's do.ATOMS Security Testing Framework
- R2GS Germany (Industrial Operational Security Management Thought and Research Club)

STANDARDISATION

- ETSI TR 101582 Security Testing Case Study Experiences
- ETSI TR 101583 Security Testing Terminology and Concepts
- ETSI ES 201837-1 TTCN-3 Core Language Change Request (Security Testing)
- ETSI GS ISI 005 Information Security Indicators (ISI) Event Testing

ITEA 2 Office
High Tech Campus 69 - 3
5656 AG Eindhoven
The Netherlands
Tel : +31 88 003 6136
Fax : +31 88 003 6130
Email : info@itea2.org
Web : www.itea2.org

ITEA 2 – Information Technology for European Advancement – is Europe's premier co-operative R&D programme driving pre-competitive research on embedded and distributed software-intensive systems and services. As a EUREKA strategic Cluster, we support co-ordinated national funding submissions and provide the link between those who provide finance, technology and software engineering. Our aim is to mobilise a total of 20,000 person-years over the full eight-year period of our programme from 2006 to 2013.

ITEA 2-labelled projects are industry-driven initiatives building vital middleware and preparing standards to lay the foundations for the next generation of products, systems, appliances and services. Our programme results in real product innovation that boosts European competitiveness in a wide range of industries. Specifically, we play a key role in crucial application domains where software dominates, such as aerospace, automotive, consumer electronics, healthcare/medical systems and telecommunications.

ITEA 2 projects involve complementary R&D from at least two companies in two countries. We issue annual Calls for Projects, evaluate projects and help bring research partners together. Our projects are open to partners from large industrial companies and small and medium-sized enterprises (SMEs) as well as public research institutes and universities.

EUREKA