EUREKA CLUSTER PROJECT

09018 ITEA DIAMONDS

© Fraunhofer FOKUS

BOOSTING SOFTWARE SECURITY FOR A CONNECTED WORLD

Our increasingly connected world is more and more at risk from software vulnerabilities and security flaws. The new security testing paradigm developed in the DIAMONDS project resulted in several European SMEs bringing new products and services into this fast-growing market, and continues to influence international standards.

Software," as online pioneer and entrepreneur Marc Andreessen noted in 2011, "is eating the world", with everything from entire governments and cities through to individual cars and smartphones increasingly connected and in continuous communication with each other - and us.

This brings huge benefits, but also challenges and risks: these complex systems are vulnerable to attack, potentially endangering human lives and undermining entire business sectors.

"Nine software security failures in ten are caused by software defects – generally, a hacker exploits a vulnerability which should have been spotted during software testing as early as possible in the development process," explains Dr Ina Schieferdecker of Germany's Fraunhofer FOKUS institute. "The problem is that these systems' complexity, openness and dynamic nature makes it hard to test them – it's extremely difficult to assess what a new system's security risks will be, or test the security of a system when it's ready to deploy."

As a result, the market for security testing – particularly security test automation - is expected to reach €4.5bn by 2019, doubling in size in just five years.

This market, however, is dominated by large US companies. The DIAMONDS project has placed software security testing on a more solid footing and helped several European SMEs develop new products and services.

Setting the software security standard

The project brought together 22 industrial and scientific players from six countries to develop a new security testing paradigm and methodology, and successfully demonstrated and evaluated it in eight industrial settings.

"Software security is not a problem with a single fix – it's too complex a field," says Dr Schieferdecker. "Instead, we developed a new paradigm, known as model-based security testing, along with a diverse array of test automation methods. We then tested those innovations through the case studies brought by our project partners from banking, telecommunication, automotive and other sectors."

The DIAMONDS methodology integrates security risk assessment and security testing over the whole software life cycle, encompassing early testing, risk assessment, and automatic testing and monitoring. The systematic integration means that each component reinforces the others: risk assessment improves testing procedures, for example, while testing systematically improves risk assessments.

Industry-tested enabling technology

With the DIAMONDS methodology representing a unique enabling technology for testing the security of critical software systems, the project continues to deliver results years after it ended.

Several standardisation documents have been adopted by the European Telecommunications Standards Institute, for example, and have been forwarded to international standardisation bodies. These documents reflect the project's case studies, where the partners fine-tuned the methodology for several different industrial domains.

"The case studies also accelerated the project's results to market," Schieferdecker points out. "This was particularly beneficial for the small companies in the project - overall, DIAMONDS enabled five new products, three new services and ten product updates."

> ***"The case studies transferred the DIAMONDS results to market quickly, accelerating its impact***

For French SME Montimage, for example, the project created new partnerships, enlarged their skills base, added new features to their flagship software tool and directly led to their involvement in more European projects.

Similarly, Smartesting - another French SME partner - developed, prototyped and validated a new approach to testing Web application security, upgraded their CertifyIt product and forged new relationships with major European industrial clients.

MAIN PARTNER

Fraunhofer FOKUS, Germany
www.fokus.fraunhofer.de
ina.schieferdecker@fokus.fraunhofer.de
www.itea2-diamonds.org

OTHER PARTNERS

Codenmicon Oy, Conformiq Software Oy, Dornier Consulting GMBH, FSCOM SARL, Gemalto, Giesecke & Devrient, Graz University of Technology, Grenoble INP – Laboratoire d'Informatique de Grenoble, Institute Telecom, itrust consulting s.à r.l., Metso Automation Inc., Montimage, Norse Solutions, Oulu University Secure Programming Group, Oy L M Ericsson Ab, Secure Business, Verein zur Förderung der IT-Sicherheit in Österreich, SINTEF ICT, Smartesting, Testing Technologies IST GmbH, Thales

TOTAL R&D INVESTMENT

€ 13.47 million

DURATION

October 2010 to October 2013

COUNTRIES INVOLVED

EUREKA is a European network for market-oriented R&D.

www.eurekanetwork.org