CSP FORUM

Security Assessment for Systems, Services and Infrastructures (SASSI) Workshop – Report

CSP Forum (www.cspforum.eu)
Funded by SecCord CSA (www.seccord.eu)
Unit H4, European commission, DG CONNECT
Consortium Partners: WIT, UNITN, HP, SAP ATOS

SecCord

Table of contents

Table of figures

1. Introduction

Mobile devices, industrial equipment and facilities, smart grids, and even vehicles are connected via the Internet and becoming accessible and thus vulnerable to security breaches and hacker attacks. Software that runs this kind of system is exposed to a large number of different threats that pose special requirements on the quality and robustness of the software. These requirements can only be identified and met if security and privacy risks and their impact are systematically considered already during the early phases of the software development and quality assurance processes. A systematic and capable security risk and quality assessment program and its tight integration within the software development life cycle are keys to building and maintaining secure and dependable software-based infrastructures.

The SASSI workshop, co-organized by the CSP Forum, took place on September 15-16 in Berlin. It provided a forum to discuss innovative approaches to security assessment, security testing and security certification for software-based systems. Experts from industry and academia presented and discussed their solutions to key issues like legal-risk analysis, security risk analysis, risk-based engineering, vulnerability testing, model based security testing, standardization, and certification. The workshop also focused on the interaction between innovations and industrial requirements, especially when security meets the demands of cost efficiency and scalability. The contributions originated from industrial practice and were complemented by industry grade research results from national and international research projects (e.g., EU Rasen[1], EU Trespass[2], BMBF Mosaik[3], BMBF Prevent[4]).

After a welcome speech by the organizers, the CSP Forum and Seccord project were introduced. The workshop continued then with a keynote that set the scenes for the three main focus areas:

- Security risk & compliance assessment;
- Secure Software Development; and
- Security Testing and Validation.

Two tutorials were also presented. Post-proceedings will be published about the SASSI workshop. Around 30 people attended the workshop, most of them from industry and research institutions.

[1] http://www.rasenproject.eu/
[2] http://www.trespass-project.eu/
[3] http://www.mosaikprojekt.info/
[4] http://www.prevent-project.org/

2. Agenda

Figure 1 and Figure 2 show the agenda of the SASSI workshop. Via the online version https://www.fokus.fraunhofer.de/en/sassi15/programoverview abstract details can be retrieved.

10:30 – 12:00		WELCOME	14:00 – 14:30		The attack navigator – Finding and defending against socio-technical attacks Christian W. Probst Technical University of Denmark
10:45 – 11:00		CSP Forum Introduction			
11:00 – 12:00	1st Keynote	Living risk-based security at SAP, the solved challenges and the open ones Paul El-Khoury CISSP, SAP SE	14:30 – 15:00		COFFEE BREAK
12:00 – 13:00		LUNCH	15:00 – 16:00	Session 1	SECURITY RISK & COMPLIANCE ASSESSMENT
13:00 – 14:30	Session 1	SECURITY RISK & COMPLIANCE ASSESSMENT	15:00 – 15:30		Threat modelling using attack trees Jan Willemsen Cybernetica AS
13:00 – 13:30		Security issues in financial cloud environments Volker Krummel Wincor Nixdorf AG	15:30 – 16:00		Security Management as a Service Marian Margraf Freie Universität Berlin
13:30 – 14:00		Risk monitoring of an pseudonymisation service based on TRICK Service Ben Fetler itrust AG	16:00 – 17:00		TUTORIAL 1
			16:00 – 17:00		Tool-supported cyber-risk assessment Bjørnar Solhaug SINTEF ICT

Figure 1- Agenda Day 1

9.00 – 9.45		TUTORIAL 2	12:00 – 12:30		Selecting and deploying risk assessment methods for the development life cycle Jörn Eichler Fraunhofer AISEC
9.00 – 9.45		RACOMAT – Risk-based Security testing for networked systems Johannes Viehmann Fraunhofer-Institut Fokus SQC	12.30 – 13.30		LUNCH
10:00 – 12.30	Session 2	SECURE SOFTWARE DEVELOPMENT	13:30 – 15:00	Session 3	SECURITY TESTING AND VALIDATION
10:00 – 10:30		Risk Management in the Development Process Armin Lunkeit OpenLimit SignCubes GmbH	13:30 – 14:00		Security testing and validation research at SAP Luca Compagna SAP Product Security Research
10:30 – 11:00		Fast & Furious – A media style of software development Axel Allerkamp Axel Springer SE	14:00 – 14:30		The many faces of fuzzing Radek Domanski Huawei
11:00 – 11:30		Developing security software – The case for risk assessment Roman Maczkowski m-privacy GmbH	14:30 – 15:00		Systematically combine security risk assessment and testing based on standardsP Jürgen Großmann Fraunhofer-Institut Fokus SQC
11:30 – 12:00		Integration of risk assessment and vulnerability discovery into software development process Heiko Weber Software AG	15:00 – 15:45		WRAP UP, PANEL & GOODBYE

Figure 2- Agenda Day 2

3. Outcomes

This section presents only the main outcomes of the SASSI workshop. The slides and summary of each presentation will be published as Fraunhofer publica[5] post-proceedings.

- ***Living risk-based security at SAP, the solved challenges and the open ones***, Paul El-Khoury (SAP SE). Paul presented the SAP Secure Software Development Lifecycle, a risk-based process used to ensure SAP software is free of known vulnerabilities and guaranteeing the appropriate level of security for shipped products. The presentation focused in particular on the security risk assessment parts of this process, namely SECURIM and Threat Modeling, used per product to identify and manage product-specific security risks, define the targeted

[5] http://www.cse.fraunhofer.org/publica

level of trust and build a security test plan. Besides processes and tools, Paul made clear the criticality of the human factor: developers are the ultimate *owners* of the security of their products; friendly processes and tool-sets should be there to enable developers to be better equipped toward the security of their products.

- ***Session 1: Security risk & compliance assessment***. The session focused much more on risks management than compliance. Various interesting works were presented ranging from the security challenges in transitioning financial sector scenarios into the cloud (e.g., the risk of sensitive data leaking is so high that cloud operator cannot be trusted), to preliminary results toward continuous risk assessment (i.e., risk is continuously re-evaluated at runtime), to the importance of socio-technical aspects in computing the risk.
- ***Tutorials.*** The workshop included two tutorials about "Tool-supported cyber-risk assessment" and "RACOMAT – Risk-based Security testing for networked systems". Both presented a tool developed in the context of the EU CORAS[6] and EU Rasen projects. The CORAS tool supports conducting security risk analysis by means of a customizable language for threat and risk modelling. The CORAS tool can be freely downloaded here[7]. RACOMAT combines risk assessment and security testing. At the core of RACOMAT a catalog of security test patterns implementing CAPEC attack patterns. RACOMAT will be soon made available for the community. Both the tools tackle key industrial relevant problems and have been already assessed on industrial use cases.
- ***Session 2: Secure Software Development*.** Risk-driven approaches for secure software development were presented together with interesting outcomes from return of experiences. It is pretty clear that all companies face similar challenges related to available budget, estimated effort, willingness/reluctance to integrate more rigorous techniques in the software lifecycle, how to convince people, etc. However it is likely that facts such as company size, criticality of the software application under development, etc. play a role against these challenges. For instance, the safety-critical nature of the application and/or the legal/compliance requirements applying to it could make the usage of these more rigorous techniques a necessity at the beginning and a profit on the long run. Dissemination of industrial success stories was proved to be very well received by the audience. So successfully applied approaches used in industry should be disseminated as they may convince other companies to repeat that experience. For instance, the outcomes by Software AG while they were introducing a security dashboard to transparently monitor the security status of their company: acceptance was not easy at the beginning, but it improved over the time and it is now common practice in the company.
- ***Session 3: Security Testing and Validation.*** The techniques presented in this session ranged from domain-agnostic techniques (e.g., Fuzzing) to domain specific ones (e.g., model-based testing for cross-domain web applications) including approaches combining risk assessment and testing. For the latter the RASEN methodology was disseminated, presenting both sides: risk-based testing and testing-based risk assessment.

The workshop ended with a wrap-up discussion where session chairs summarized the highlights from their sessions and participants were invited to share their thoughts. The discussion was very lively and constructive. Most of the participants shared their opinions showing engagement and interest. It emerged a common belief: risk-driven approaches will play a fundamental role in the forthcoming years.

[6] http://coras.sourceforge.net/
[7] http://coras.sourceforge.net/downloads.html

4. Summary

The workshop was really successful, showing once more the importance of such risk-driven approaches for security. In this respect, significant investment in research and innovation will be necessary in order to make these approaches easier to be consumed within industrial settings. Last, but not least, it emerged that sharing more about successful experiences from forerunners in these areas, as it happened at the SASSI workshop, is perceived as an important means to motivate others to pursue similar paths.