CSP FORUM

Business Industry Challenges for (Cyber)Security – Report

Co-located with the Seminar on Road Mapping Cybersecurity Research and Innovation and the EU Proposers' day
Co-Organized with CAPITAL and European Commission NIS WG3

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

Table of contents

Table of figures

Executive Summary

The phase between research and successful innovation is often referred to as the *valley of death*, clearly indicating the extreme difficulties faced when converting an invention into a successful and concrete application. The security, privacy, and trust domains are not an exception. Increase the dialogue between industry and the research is one of the many best practices proposed to mitigate this challenge.

The CSP Forum event "Business Industry Challenges for (Cyber)Security" organized on October 8th 2014 in Florence targeted indeed this simple and fundamental best practice. Three industrial speakers from SAP, IBM, and Poste Italiane presented touchy business security challenges and prominent researchers presented solutions from EU-funded and national-funded projects that can contribute to answer some of those challenges. A panel with open floor discussion among the speakers and the attendees concluded the event.

The CSP Forum event was part of the "Seminar on Road Mapping Cybersecurity Research and Innovation" co-organized with the CAPITAL project and the European Commission NIS WG3 and co-located with the EU Proposers' day. Overall more than 120 participants attended the seminar with a good mixture of industry (large companies, but also SMEs), academy, and research institutions.

1. Introduction

The phase between research and successful innovation is often referred to as the *valley of death*, clearly indicating the extreme difficulties faced when converting an invention into a successful and concrete application. The security, privacy, and trust domains are not an exception. Increase the dialogue between industry and the research is one of the many best practices proposed to mitigate this challenge.

The CSP Forum event "Business Industry Challenges for (Cyber)Security" organized on October 8th 2014 in Florence targeted indeed this simple and fundamental best practice. The event has been run around the following game: industry raising real challenges and research try to answer. In particular, we run three sessions:

(1) *Industrial session*: Three industrial speakers from SAP, IBM, and Poste Italiane described touchy security challenges without neglecting ineradicable and orthogonal cost-benefit aspects;
(2) *Research session*: four prominent researchers presented solutions from EU-funded (SECONOMICS and TREsPASS) and national-funded (EC SPRIDE - Germany, TENACE – Italy, and DFG SPP "Reliably Secure Software Systems" – Germany) projects presented solutions that can contribute to answer some of those challenges, including cost-benefit considerations;
(3) *Panel* with open floor discussion: open discussion with the audience, larger Q&A, final statements, and wrap-up.

The CSP Forum event was part of the "Seminar on Road Mapping Cybersecurity Research and Innovation" co-organized with the CAPITAL project (http://www.capital-agenda.eu) and the European Commission NIS WG3 (https://resilience.enisa.europa.eu/nis-platform) and co-located with the EU Proposers' day. Overall more than 120 participants attended the seminar with a good mixture of industry (large companies, but also SMEs), academy, and research institutions.

2. Agenda

Figure 1 shows the agenda of the CSP Forum event "Business Industry Challenges for (Cyber)Security".

Industrial session	Industrial challenges of Secure Software Development	Achim Brucker (SAP)
	Industrial challenges toward Cyber-Security Trends and Risks	Domenico Raguseo (IBM)
	The Italian "Cyber Security District" and industrial challenges for malicious apps detection	Giantonio Chiarelli (Poste)
Research session	Developer-Centered Security Engineering Tools	Sven Türpe (Fraunhofer SIT)
	Efficient Vulnerability Management: Measuring Vulnerabilities and Exploits for Better Security Strategies	Luca Allodi (U. of Trento)
	The attack navigator - finding and defending against socio-technical attacks	Kai Rannenberg (Goethe University)
	Behavioural Malware detection with Quantitative Data-Flow Graphs	Martin Ochoa (TU München)
Panel	Open floor discussion	Luigi Rebuffi (EOS)

Figure 1- Agenda

3. Outcomes

This section presents an excerpt of the outcomes emerged from the CSP Forum event "Business Industry Challenges for (Cyber)Security". The slides of each presentation are available here.

1. Industrial session

Three industrial speakers from SAP, IBM, and Poste Italiane described touchy security challenges without neglecting ineradicable and orthogonal cost-benefit aspects. Hereafter more details:

- ***Industrial challenges of Secure Software Development***, Achim Brucker (SAP SE, Security Testing Strategy and Implementation at SAP): Developing secure software requires more than the definition of a process, i.e., a Secure Software Development Lifecycle. The successful implementation of a Secure Software Development Lifecycle relies on many factors among them providing the right tools to developers that support them in writing secure and reliable code. Based on SAP's experience in the large scale introduction of static code analysis tools as well as the use of dynamic (security) testing tools, Achim discusses several challenges of secure development approaches in industry such as finding the right balance between security requirements and development efforts or the between the precision of a security analysis and its scalability.
- ***Industrial challenges toward Cyber-Security Trends and Risks***, Domenico Raguseo (IBM, Europe Security Systems Technical Sales and Solutions Manager): The IBM X-Force Research and Development team continually analyses trends in attack behaviours across a range of industries. Besides presenting recent results from IBM X-Force, in this talk Domenico discussed which challenges industry faces to cope with these trends. This clearly indicated the importance of having in place, among others, runtime monitoring controls together with a well-established risk and governance approach. Not surprisingly this touched critical

subjects such as the accuracy of widely used scoring systems (e.g., CVSS) and inconsistencies that often occur across different organizations while using these systems.

- ***The Italian "Cyber Security District" and industrial challenges for malicious apps detection***, Giantonio Chiarelli (Cyber Security Analyst at Poste Italiane's CERT): Poste Italiane has a long history of innovation and it is currently one of the leading Italian companies in digital services provisioning. In this very line and believing in strong links between academia and industry, Poste Italiane coordinates the Italian "Cyber Security District" - a national project co-funded by the Italian Ministry of Education, Universities and Research - in partnership with scientific/academic partners and industrial ones in order to innovate on (i) end-users protection, (ii) protection of digital services and payment systems, and (iii) secure dematerialization. Giantonio provided an overview of the Italian "Cyber Security District", giving more emphasis to the approach ideated for monitoring app stores and take actions against malicious/unauthorized apps that are targeting customers posing them as related to Poste Italiane brand. In this monitoring process Giantonio emphasized some research challenges for malicious apps detection e.g., the need to devise behavioural-based techniques for malware detection.

2. Research session

Four prominent researchers presented solutions from EU-funded (SECONOMICS and TREsPASS) and national-funded (EC SPRIDE - Germany, TENACE – Italy, and DFG SPP "Reliably Secure Software Systems" – Germany) projects presented solutions that can contribute to answer some of the challenges raised by the industrial speakers, including cost-benefit considerations. Hereafter more details:

- ***Developer-Centered Security Engineering Tools***, Sven Türpe (Fraunhofer SIT - EC SPRIDE, German national project): To establish security engineering practices, a development organization needs to provide its developers and managers with suitable tools. To be effective, these tools must take into account human and organizational factors; they must guide and support developers without getting in the way of creative work. While automated security testing is an important feedback mechanism, further tools are required to address security issues proactively throughout the life cycle of a software product. Using examples from research and industry projects, Sven outlined how individuals and teams interact with security engineering tools and which factors to consider in their design. Empirical results show the complexity of threat modeling in a development team. Together with hands-on experience, these observations suggest that a development security toolbox needs to support boundary objects and negotiation, feedback tools, and date- and knowledge-based activities.
- ***Efficient Vulnerability Management: Measuring Vulnerabilities and Exploits for Better Security Strategies***, Luca Allodi (U. of Trento - TENACE Italian national project and EU SECONOMICS project): Vulnerability Management is of main importance in any security management plan. Many standards and best practices provide an aid to this purpose, but their cost effectiveness is unclear. In general, a central question to motivate security decisions remains open: What is the risk reduction entailed by the patching policy, and at what effort does it come? To answer this question Luca et al developed a methodology to measure policy effectiveness based on the notion of case-control study. Their results show that current (CVSS-based) best practices entail negligible risk reduction levels (4%) and may be indistinguishable from "randomly picking vulnerabilities to patch". Luca presented two additional example policies based on the existence of a Proof-of-Concept exploit and presence of an exploit in the cybercrime black markets, and showed that the risk reduction levels can increase dramatically (up to 80%) requiring only a fraction of the original patching effort.
- ***The attack navigator - finding and defending against socio-technical attacks***, Kai Rannenberg (Goethe University Frakfurt – TREsPASS EU project): Industry is under a

constant pressure to react to a myriad of both existing and unknown attacks on their intellectual property. These attacks today reveal a seemingly unbounded number of attacker behaviors, involving both physical and virtual components, and, rapidly increasing, also socio-technical components. To counter these attack behaviors, industry only has limited resources, be it work force or be it finances. The scoring systems developed to prioritize the use of defense resources often are limited in their applicability especially to socio-technical components. Kai presented the novel concepts that have been developed within TREsPASS project to guide risk assessment and use of resources. The concept of an attack navigator uses organisational maps and attacker profiles to identify attacks involving steps along all three dimensions, physical, virtual, and socio-technical. The attack navigation on the organisation maps is based on invalidation of organisational policies, resulting in weighted attack trees to guide risk assessment and governance using typical attacker profiles. The attacker profiles represent different types of attackers, with varying resources, skills, etc. The attack navigator and maps use novel visualisation techniques and serious play for map detection. The developed approaches are useful as metaphors beyond the scope of TREsPASS and can contribute to improvement also of existing approaches.

- ***Behavioural Malware detection with Quantitative Data-Flow Graphs***, Martin Ochoa (Technische Universität München - DFG SPP "Reliably Secure Software Systems", German national project): In his talk Martin presented recent experiences on detecting Malware by analysing its behaviour. Their approach is based on a generic system-wide quantitative data flow model. They base their data flow analysis on the incremental construction of aggregated quantitative data flow graphs. These graphs represent communication between different system entities such as processes, sockets, files or system registries. Martin demonstrated the feasibility of their approach through a prototypical instantiation and implementation for the Windows operating system. Initial experiments yield encouraging results in terms of efficiency and detection/false positives rates.

3. Panel and wrap-up session

Interesting discussions took already place during the various presentations and their Q&A slots. The panel, moderated by Luigi Rebuffi (EOS), encouraged further discussions among speakers and attendees including challenging questions such as: would liability be the means to improve state of affairs and software quality? Are the research subjects proposed in the EU calls in line with the industrial and research expectations? The second question received a quite positive answer from the speakers:

Risk-based security is generally perceived as the base for the development of future work. "Security versus usability" is another important perceived challenge and it should not only targeting the citizen, but all the actors of the security chain e.g., developers.

The first question triggered a more complex debate. Hereafter a short summary:

Liability would require software companies to make immediate use of cybersecurity insurance (a market that is more popular in US than in Europe) as the cost for the incident could be much higher of what a company can handle on its own. However cybersecurity insurance is well-known to have two main pain-points: it is not suited to cover intellectual property theft and it does not dispose of enough actuarial data to e.g., adjust premiums based on what security controls and products are most effective. Cybersecurity insurance would need further maturation and maybe rethinking the way is organized. Investing on cybersecurity insurance may be not convenient – why not investing on other areas, e.g. prosecution? Find the bad guys and ensure they pay for what they did so to discourage others. Also here several challenges, e.g., trial evidence of a cybercrime…

Figure 2 presents the mapping between the subjects discussed by each research presentation and the corresponding business challenge(s) raised by the industrial speakers.

Research	Industry	Challenges
Sven, Fraunhofer Developer-Centered Security Engineering Tools	Achim, SAP Industrial challenges of Secure Software Development	risk-based, cost-effective security techniques/controls/tools/... for development • automation vs interaction • "controllable unsound" security techniques: soundness is nice but what is its price? • composed software from multiple vendors
Luca, U. of Trento Efficient Vulnerability Management: Measuring Vulnerabilities and Exploits for Better Security Strategies	Domenico, IBM Industrial challenges toward Cyber-Security Trends and Risks	Vulnerability management (risk and governance): be sure you are prepared when an attack strikes Scoring system
	Achim, SAP Industrial challenges of Secure Software Development	As a developer what should I fix first? Can I wait for the next planned release or should we ship a patch immediately?
Kay, Goethe University Frakfurt The attack navigator - finding and defending against socio-technical attacks	Giantonio, Poste The Italian "Cyber Security District" and industrial challenges for malicious apps detection	Formalize security threats and risk scenarios in interactions between services and their users
	Achim, SAP Industrial challenges of Secure Software Development	Risk-based, cost-effective threat modeling ?
Martin, Technische Universität München Behavioral Malware detection with Quantitative Data-Flow Graphs	Giantonio, Poste The Italian "Cyber Security District" and industrial challenges for malicious apps detection	Malware detection via behavioral-based techniques
	Domenico, IBM Industrial challenges toward Cyber-Security Trends and Risks	Vulnerability detection

Figure 2- Mapping research contribution to raised industrial challenges

The promising discussions that took place during our CSP Forum event seem to indicate that both industry and research have strong willingness to dialogue each other. All the speakers state they found the event very interesting and helpful to identify potential opportunities.