GUEST EDITORIAL PREFACE

Special Issue on Evolving Security and Privacy Requirements Engineering (ESPRE'14) 2014, Sweden

Kristian Beckers, University Duisburg-Essen, Duisburg, Germany

Shamal Faily, Bournemouth University, Poole, UK

Seok-Won Lee, Ajou University, Suwon, Republic of Korea

Nancy Mead, CERT Division, SEI, Carnegie Mellon University, Pittsburgh, PA, USA

When security and privacy are addressed, we discover how difficult it really is to specify security and privacy. We lack clarity about what it means to secure a system, test to prove that a system is secure, and the means to establish a firm a grasp of all possible solutions for satisfying a specified security problem. Without a clear outline of the related security functionality or expectations, we cannot make claims about a system's security. The Requirements Engineering (RE) community is starting to make traction in addressing these problems, but the scope of security and privacy requirements is widening. In addition to specifying software systems, requirements are now helping shape security education and training, privacy audits, and certification; this means that the distinction between requirements and related security and privacy concepts is becoming blurred.

Most people agree that when specifying a system, security and privacy needs to be addressed as early as possible. Yet, security is never the main motivation when building any system, especially when engaging in innovation; many teams remove or deprioritize security requirements as projects rush to meet deadlines, and they do so without understanding the impact their actions might have. Similarly, many people fail to appreciate how privacy expectations are shaped by contextual information flows and norms, and they treat privacy merely as a private-public dichotomy. As the public outcry over the Snowden leaks has demonstrated, misjudging privacy implications influences not only a system under construction, but the wider world within which it is situated.

At the Evolving Security and Privacy Requirements Engineering (ESPRE) workshop, practitioners and researchers interested in security and privacy requirements gather to discuss significant issues in the field. In particular, ESPRE participants probe the interfaces between requirements engineering and security and privacy. At ESPRE workshops, participants also take the first step in evolving security and privacy requirements engineering to meet the needs of stakeholders ranging from business analysts and security engineers to technology entrepreneurs and privacy advocates. The most recent ESPRE workshop was held in Karlskrona, Sweden in August 2014, and was co-located with the RE 2014 conference (IEEE Proceedings of the ESPRE 2014, Karlskrona, Sweden. IEEE 2014, ISBN 978-1-4799-6340-9).

Based on this background and understanding, the ESPRE Call for Papers invited general submissions addressing a wide range of issues such as identifying and managing all stakeholders (including attackers), modeling domain knowledge for security and privacy requirements, considering legal compliance during security and privacy requirements engineering, and discussing positive (and especially negative) lessons learned in applying security and requirements engineering in practice.

The selection of the best papers among the eight research papers presented in the workshop was based on the re-submission of a revised and extended version suitable for a journal publication. The selection process included an additional cycle of review of each submission. We thank the following reviewers for their guidance.

REVIEWERS

- Aida Omerovic, SINTEF ICT, Norway
- Aljosa Pasic, ATOS, Spain
- Andrea Atzeni, University Torino, Italy
- Denis Hatebur, ITESYS, Germany
- Federica Paci, University Trento, Italy
- Holger Schmidt, TÜV Informationstechnik GmbH, Germany
- Huseyin Dogan, Bournemouth University, UK
- Isabelle Cote, ITESYS, Germany
- Jorge Cuellar, SIEMENS, Germany
- Martin Gilje Jaatun, SINTEF ICT, Norway
- Meiko Jensen, Syddansk Universitet, Denmark
- Raian Ali, Bournemouth University, UK
- Seda Gürses, New York University, US

Based on the reviews and the respective improvements of the submissions, we accepted three papers.

The first paper proposes and demonstrates an approach for eliciting security requirements using misuse cases derived from malware analysis. Moreover, the authors present a method for including existing practical experiences from known software exploits into future software development efforts (e.g. as part of a security development lifecycle). By following the proposed method, developers can create future systems that are more secure, from inception, by including use cases that address previous attacks. In support of this, a case study is presented. Ideally the approach will allow us to reduce software vulnerabilities in related systems.

The second paper addresses an important issue in the ISO 27001 certification scheme. The authors present a structured method that resolves ambiguities in the standard. Their method empowers small and medium enterprises (SMEs) to conduct a security analysis and comply with the documentation demands of ISO 27001—specifically for the cloud computing domain. In this method, risk analysis—including typical information security demands such as asset identification, threat and vulnerability analysis—is supported by graphical and textual patterns. The paper provides step-by-step instructions for using the method and illustrates its execution using an example of a cloud logistics application. A support tool that contains all the patterns helps SMEs apply the method to any kind of cloud computing scenario.

The third paper touches on an important subject of security assurance, which is defined as the means of reducing certification time for evolving software products. The paper discusses how to use an agile, model-based approach for security certification related to the Common Criteria (CC). The authors discuss two results: (1) traceability links from CC security objectives to functional security requirements and the subsequent documentation of design, implementation, and testing, and (2) an analysis that can detect the affected parts of the security evaluation and related documentation when the certified system changes. These results are valuable to the security standardization effort because currently, a changed target of evaluation requires a complete re-evaluation of it. This re-evaluation is expensive and prevents security certification efforts to be conducted by small- and medium-sized companies. A less expensive approach may change this practice over time.

We would like to thank each of the reviewers for their careful consideration of the papers. Special thanks to the following attendants to the ESPRE workshop, and the researchers and practitioners who have helped us improve the quality of the workshop.

Kristian Beckers
Shamal Faily
Seok-Won Lee, Ajou
Nancy Mead
Guest Editors, IJSSE

Kristian Beckers is a security requirements engineering researcher at the University of Duisburg-Essen. He investigates how security requirements engineering methods can be used to support the development and documentation of security standards. Kristian has been a PC member of the CD-ARES conference, and a guest reviewer for the International Journal of Information Security.

Shamal Faily is a Lecturer in Systems Security Engineering at Bournemouth University. His research explores `security-by-design', and how the design of usable and secure systems can be better supported with design techniques and software tools, particularly those from Requirements Engineering. Shamal organised the inaugural workshop on Designing Interactive Secure Systems at British HCI 2012, and ran a special interest group on this topic at CHI 2013. Shamal has also been a PC member and external reviewer for several security and usability conferences, including ARES, Trust, CHI, EICS, and British HCI.

Seok-Won Lee is the Dean of the Graduate School of Software and Associate Professor of Information and Computer Engineering at Ajou University since 2012. He has published more than 100 scientific papers in software engineering with specific expertise in ontological requirements engineering and domain modelling, knowledge engineering with specific expertise in knowledge acquisition and machine learning, and security requirements engineering. Seok-Won has been a PC member of several security and software engineering conferences (including RE), and has organised the SESS workshop series at ICSE for several years.

Nancy Mead is a Fellow and Principal Researcher at the Software Engineering Institute (SEI), a faculty member in the Master of Software Engineering program at Carnegie Mellon University, a Fellow of the Institute of Electrical and Electronic Engineers (IEEE) and a Distinguished Member of the Association for Computing Machinery (ACM). She is currently involved in the study of security requirements engineering and the development of software assurance curricula. Nancy has organised several security engineering events, including the SPREE Workshop in 2011, and the RHAS workshops.