2-SQUARE: A Web-Based Enhancement of SQUARE Privacy and Security Requirements Engineering

Alan Lai, College of Agricultural and Environmental Science, University of California, Davis, CA, USA
Cui Zhang, Department of Computer Science, California State University, Sacramento, CA, USA
Senad Busovaca, Department of Computer Science, California State University, Sacramento, CA, USA

ABSTRACT

This paper presents a highly flexible and expandable tool called 2-SQUARE in support of the SQUARE methodology for security and privacy requirements engineering developed by the Software Engineering Institute at Carnegie Mellon University. Security and privacy requirements engineering can be a daunting task even with the proper expertise. 2-SQUARE aims at making it straightforward to perform requirements engineering regardless of expertise by providing flexible workflows and process guidance. 2-SQUARE also facilitates communication between requirements engineers and stakeholders throughout the requirements engineering process.

Keywords: Privacy, Requirements Engineering, Security, Security Quality Requirements Engineering (SQUARE), Web-Based Enhancement

INTRODUCTION

The latest web-based applications encourage the sharing of information through social networks and ad networks, allowing companies to provide free services. These free services can provide the convenience to access an individual’s own personal data from anywhere. However because these applications are available over the internet, they have a significantly larger exposure to attacks and thus should be able to defend the user’s data from security and privacy breaches.

Because of the sensitivity of information stored within databases it is essential to ensure that information is not shared without the approval of the owner.

Security Quality Requirements Engineering (SQUARE) is a methodology developed by the Software Engineering Institute (SEI)’s Network Systems Survivability (NSS) Program at Carnegie Mellon University. It is designed to foster communication between software engineers and stakeholders to effectively elicit security requirements (Mead, Hough, & Stehney

DOI: 10.4018/ijsi.2013010104
II, Security Quality Requirements Engineering, 2005). The SQUARE process has been further adapted to provide privacy requirements engineering with a proven structured method of producing a set of verifiable requirements (Bijwe & Mead, 2010). While some general purpose requirements engineering process can be used, it can be beneficial to have a process designed specifically for eliciting privacy requirements.

This paper presents 2-SQUARE, an integration and automation system aimed at security and privacy requirements engineering using the SQUARE methodology. The 2-SQUARE system was developed utilizing the Microsoft .NET Model-View-Controller (MVC) Framework and Entity Framework. It is a web-based system that allows for multi-location collaboration through one system and provides guided help for each role involved with the security and privacy requirements engineering process.

First we describe all background and related work leading to the development of 2-SQUARE. Then we discuss the design of the 2-SQUARE system. The section afterwards covers the implementation of each of the layers for the tool. Followed by a section that shows a case study demonstrating the improvements achieved by 2-SQUARE over existing methods. And finally we provide a brief summary and potential future work to enhance the abilities of 2-SQUARE.

BACKGROUND AND RELATED WORK

SQUARE Methodology

The SQUARE process was designed as a method to elicit, categorize and prioritize security requirements. Its goal was to integrate security into the early stages of software development, but it has also proved useful for evaluating security of existing systems (Mead, Hough, & Stehney II, Security Quality Requirements Engineering, 2005). SQUARE guides teams through a series of nine steps in order to determine a project’s security requirements in a structured manner. Tasks include agreeing on definitions, developing artifacts, assessing risks, eliciting and validating requirements.

This process has been proved useful for security requirements engineering and been recently adapted for usage with privacy requirements engineering (Bijwe & Mead, 2010). Privacy requirements engineering poses a range of different challenges compared to security requirements engineering. Privacy policies of an application are not dictated solely by the stakeholders, but they can be mandated by laws and regulations. Laws and regulations can be difficult to understand; a fair amount of knowledge can be required to properly interpret and comply with all applicable laws. Goal-Based Requirements Analysis Method (Antón, Carter, Dagnino, Dempster, & Siege, 2001), Pattern-Based Approach (Schumacher, 2003) and E-Commerce Personalization Approach (Cranor, 2003) have all been used in privacy requirements engineering; however, these methods are generic in nature and require a detailed understanding of privacy laws, standards and policies (Bijwe & Mead, 2010).

mySQUARE

mySQUARE (Yip & Zhang, 2009) was the first tool to provide semi-automation for SQUARE for security requirements engineering. It is a desktop application and can only be used by one person at a time. mySQUARE provides guidance information as a user works through the steps and at the end of the process the tool is able to generate reports that would be a fairly labor-intensive job to perform manually. mySQUARE also has the capability to export all the data into an xml formatted file, which can be used with other tools.

This application was able to reduce the workload and expertise required to use the process but it was limited to how many users could use it and did not have a built in risk assessment tool. SQUARE requires a certain amount of communication between requirements engineers and stakeholders, an application restricted to one user means collaboration is performed outside of the tool.
Related Content

The Effect of Online Service Retailers' Quality Gaps on Customer Satisfaction
Asem Majed Othman, Vincent Omachonu and Emad Hashiem Abualsauod (2017). International Journal of Systems and Service-Oriented Engineering (pp. 21-44). www.igi-global.com/article/the-effect-of-online-service-retailers-quality-gaps-on-customer-satisfaction/188593?camid=4v1a

What Practitioners Think of Inter-Organizational ERP Requirements Engineering Practices: Focus Group Results
TEA: A Generic Framework for Decision Making in Web Services
Zhaohao Sun, Grant Meredith and Andrew Stranieri (2012). *International Journal of Systems and Service-Oriented Engineering* (pp. 41-63).
www.igi-global.com/article/tea/79238?camid=4v1a

Automated Evaluation of Interest Point Detectors
www.igi-global.com/article/automated-evaluation-of-interest-point-detectors/111452?camid=4v1a