Model Based Process to Support Security and Privacy Requirements Engineering

Shareeful Islam, University of East London, UK

Haralambos Mouratidis, University of East London, UK

Christos Kalloniatis, University of the Aegean, Greece

Aleksandar Hudic, SBA Research gGmbH, Austria

Lorenz Zechner, SBA Research gGmbH, Austria

ABSTRACT

Software systems are becoming more complex, interconnected and liable to adopt continuous change and evolution. It's necessary to develop appropriate methods and techniques to ensure security and privacy of such systems. Research efforts that aim to ensure security and privacy of software systems are distinguished through two main categories: (1) the development of requirements engineering methods, and (2) implementation techniques. Approaches that fall in the first category usually aim to address either security or privacy in an implicit way, with emphasis on the security aspects by developing methods to elicit and analyse security (and privacy) requirements. Works that fall in the latter categories focus specifically on the later stages of the development process irrespective of the organisational context in which the system will be incorporated. This work introduces a model-based process for security and privacy requirements engineering. In particular, the authors' work includes activities which support to identify and analyse security and privacy requirements for the software system. Their purpose process combines concepts from two well-known requirements engineering methods, Secure Tropos and PriS. A real case study from the EU project E-vote, i.e., an Internet based voting system, is employed to demonstrate the applicability of the approach.

Keywords: *PriS, Privacy, Requirements Engineering, Secure Tropos, Security, Security Modelling*

1. INTRODUCTION

Recent advancement of software systems have changed the way that humans work, interact, learn and socialise. For instance, software platforms have been working without physically being at the same location as e-learning tools enable learning from distance and social networking services allow communication between people who might be thousand miles apart from each other. Large amount of sensitive and private information, i.e., customer bank

DOI: 10.4018/jsse.2012070101

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

account information and health care records, usually store on such geologically distributed systems. Users and stakeholders realise that without appropriate storage systems for such information, those systems cannot operate as required. Survey results (Green & Yang, 1998; Gritzalis, 2004; PricewaterhouseCoopers, 2001) have shown that users are concerned about their personal data privacy is at risk and they are worried about security vulnerabilities of software systems that might endanger their personal data.

Therefore, it has become increasingly important for software system developers to ensure that systems are developed with security and privacy in mind (Liu, Yu, & Mylopoulos, 2003; Massey, Otto, Hayward, & Antón, 2009; Haley, Moffett, Laney, & Nuseibeh, 2003). In fact recent research (Mouratidis & Giorgini, 2006; Islam, Mouratidis, & Jürjens, 2011) emphasise the need to consider security and privacy from the early stages of the development process. Several works in the literature (Fischer-Hübner, 2001; Islam, 2010a) focus on the development of methodologies, modelling languages and tools for the integration of security or privacy during the development lifecycle of software systems. These works either consider security and privacy as two independent concepts or they consider privacy as a subset of security. However latest research efforts (Gritzalis, 2004; Korrn, 2004; Kalloniatis, Kavakli, & Gritzalis, 2008) identify that privacy should be treated as a separate requirement criterion, since privacy itself is a multifaceted concept, but not independent from security and vice-versa. Thus, the need to analyse security and privacy separately but under a unified framework is of vital importance.

Our work fulfills this gap in the literature in such manner by proposing a structure approach to model and analyse security and privacy concepts under a unified framework. The work is based on the integration of two software engineering methodologies: one from the security requirements domain, and other from the privacy domain, i.e., Secure Tropos (Mouratidis & Giorgini, 2006b) and PriS (Kavakli, Gritzalis, & Kalloniatis, 2007; Kalloniatis, Kavakli, & Gritzalis, 2008) respectively. Secure Tropos focuses on the elicitation and analysis of security requirements while PriS focuses specifically on the incorporation of privacy requirements in the system design process. We decided to use these two approaches for the following reasons: Firstly, the applicability and usefulness of both these approaches has been widely presented in the literature (Islam, 2010; Islam, Mouratidis, & Jürjens, 2011; Kalloniatis, Kavakli, & Gritzalis, 2008); Secondly, both approaches share similar concepts, therefore a combination of these two results in a comprehensive analysis of security and privacy concepts; Thirdly, Secure Tropos is mainly focus on the requirements engineering and early design stages, while PriS is mainly focused on the later design and implementation stage. As such, the integration of these approaches results as a framework that covers the development process from early stages, such as the requirement gathering process, all the way to implementation.

To support such integration, we consider Secure Tropos as the main underlying methodology, which we have extended, both its modelling language and its process aspects, with concepts (such as privacy goal, process pattern and implementation technique) and processes from the PriS methodology. The result of our work enables identification and analysis of security and privacy requirements from an organisational context and the translation of these requirements into system components.

This paper is structured as follows. The next section presents a summary of Secure Tropos and PriS concepts, furthermore it also explains in depth the integration of PriS to Secure Tropos. The following section presents the concepts of the metamodel, which is a result from the integration of the PriS language to Secure Tropos language, while the section after presents the unified process for modelling the aforementioned concepts. A detailed application of our work is evaluated through a real case study, presented in the following section, while the section after presents relevant related

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/model-based-process-support-security/69391

Related Content

An Outlook Architecture: Protocols and Challenges in IoT and Future Trends
Kajal Pateland Mihir Mehta (2023). *International Journal of Software Innovation (pp. 1-20).*
www.irma-international.org/article/an-outlook-architecture/315744

RESCUE: An Integrated Method for Specifying Requirements for Complex Sociotechnical Systems
Sara Jonesand Neil Maiden (2005). *Requirements Engineering for Sociotechnical Systems (pp. 245-265).*
www.irma-international.org/chapter/rescue-integrated-method-specifying-requirements/28413

Association Rule Mining and Audio Signal Processing for Music Discovery and Recommendation
Md. Mahfuzur Rahman Siddiquee, Md. Saifur Rahman, Shahnewaz Ul Islam Chowdhuryand Rashedur M. Rahman (2016). *International Journal of Software Innovation (pp. 71-87).*
www.irma-international.org/article/association-rule-mining-and-audio-signal-processing-for-music-discovery-and-recommendation/149140

From Business Process Model to Information Systems Model: Integrating DEMO and UML
Peter Rittgen (2009). *Handbook of Research on Modern Systems Analysis and Design Technologies and Applications (pp. 179-188).*
www.irma-international.org/chapter/business-process-model-information-systems/21071

Credit Risk Assessment of Internet Financial Platforms Based on BP Neural Network
Yu Yuanand Yue Yang (2020). *International Journal of Cyber-Physical Systems (pp. 29-45).*
www.irma-international.org/article/credit-risk-assessment-of-internet-financial-platforms-based-on-bp-neural-network/280468