Crafting Requirements for Mobile and Pervasive Emergency Response based on Privacy and Security by Design Principles

Stefan G. Weber, UBIN AG, Berlin, Germany

Prima Gustiené, Karlstad Business School, Karlstad University, Karlstad, Sweden

ABSTRACT

According to fundamental principles of the Privacy by Design approach, the consultation of privacy issues should be embedded into analysis and design of information systems, from the early stages of system planning to implementation. In this article, the authors extend this perspective towards Privacy and Security by Design. Exemplary focusing on mobile and pervasive emergency response, as a specific area of the emergency management domain, this article conveys how the early requirements elicitation can be supported by a semantically integrated conceptual modeling method. Presenting the results of the exemplary executed elicitation processes, it contributes a concrete set of security and privacy requirements for mobile and pervasive emergency response settings. By also taking into account conflicting security goals, this article provides a substantial grounding for the development and deployment of multilaterally secure pervasive ICT that effectively supports emergency management during and in the aftermath of critical response missions.

Keywords: *Conceptual Modeling, Emergency Response, Information Security, Information Systems, Pervasive Computing, Privacy by Design*

1. INTRODUCTION

Mobile and pervasive computing refers to the paradigm that information and communication technologies (ICT) become seamlessly embedded into everyday's life and work activities and processes in manifold aspects (Satyanarayanan, 2001). ICT research communities have recognized the huge potential of applying such post-desktop computing approaches to emergency response settings in order to improve crucial processes (Jiang et al., 2004; Flentge et al., 2008; Fischer et al., 2010; Smirnov et al., 2011). While representing a new area of technological development that brings new opportunities, at the same time mobile and pervasive computing is associated to new risks. In particular, the interwoven security and privacy issues are often

DOI: 10.4018/jiscrm.2013040101

mentioned as major obstacles towards the real world deployment of pervasive systems (Cas, 2005; Dritsas, 2006).

In order to become acceptable and trustworthy, mobile and pervasive ICT should be integrated into application scenarios in a systematic manner. In particular, it is most important that all actors and stakeholders who are involved in ICT-supported processes are able to clearly perceive the vision and rationale for the introduction of new technologies. Especially with regards to privacy, every new technology increases complexity problems. Moreover, since privacy protection is also in conflict with the protection goal of accountability, it requires a particularly thorough assessment.

The approach presented in this paper reflects that, in order to be successful, also the involved organizations need to have an accurate understanding of how new technologies may fit into the application context and how they can be integrated into a broader framework, which is driven both by organizational goals and by end users. Privacy and security requirements are always embedded in an organization; therefore they should be analyzed and elicited as thoroughly as other system requirements during the development of information systems. Also, organizational and technical design issues are interrelated. In particular, an information system cannot function in isolation from the whole enterprise system in which it is embedded in (Nuseibeh & Easterbrook, 2000). Therefore, all the aspects of the system including static aspects (related to data and information), dynamic aspects (related to process and interaction) as well as security and privacy aspects should be maintained and controlled throughout the system development life cycle, from early stages of system planning activities up to design and implementation stage. As security and privacy concerns much about *what kind, to which extent and for which purpose* certain data and digital information should be collected, stored and shared among different actors, it is very important that the analysis of the actual usage of data takes place at the very early stage of requirement determination. In turn, an appropriate analysis method can also contribute to data minimization, which is one of the most important design goals concerning security and privacy.

In this article, we consider emergency response as a particular challenging application scenario, which benefits form a thorough elicitation of privacy and security requirements. In particular, we analyze:

1. How mobile and pervasive ICT may enhance the cooperation between emergency workers in a control center and the entities in the field respectively at the incident site;
2. To which extent security and privacy protection goals have to be considered to achieve multilateral security, i.e. security that fairly balances conflicting security requirements.

This perspective is what we consider as *Privacy and Security by Design*. W.r.t. requirement elicitation, the presented considerations are based on a three-level framework for systematic and integrated way of modeling (Gustiené, 2010; Gustas & Gustiené, 2011), which is necessary for integration of all the necessary aspects of system specifications, including security and privacy issues. Thus, we also introduce grounding principles such as data minimization, data life cycle management, privacy assurance and negotiations, which represent areas that are important to the development of privacy-enhancing technologies.

W.r.t. the application scenario, the findings presented in this article result from discussions and experiences with German emergency workers, ranging from executive levels over trainers to volunteers, build upon technical standards (Murgatroyd, 2003; Linde, 2008), benefit from an exchange with the scientific research communities (Weber, 2009; Brucker et al., 2010; Weber et al., 2011) as well as from extensive literature studies (Turoff et al., 2004; Committee, 2007).

The remainder of this article is structured as follows: in the following parts, we introduce the multilevel approach towards the elicitation

Collaborative Command and Control Practice: Adaptation, Self-Regulation and Supporting Behavior

Jiri Trnkaand Björn Johansson (2009). *International Journal of Information Systems for Crisis Response and Management (pp. 47-67).*
www.irma-international.org/article/collaborative-command-control-practice/4012