Information and Software Technology 56 (2014) 273–293

Contents lists available at ScienceDirect

Information and Software Technology

journal homepage: www.elsevier.com/locate/infsof

A systematic review on security in Process-Aware Information Systems – Constitution, challenges, and future directions ☆

Maria Leitner *, Stefanie Rinderle-Ma

University of Vienna, Faculty of Computer Science, Research Group Workflow Systems and Technology, Waehringerstrasse 29, 1090 Vienna, Austria

ARTICLE INFO

Article history:
Received 28 January 2013
Received in revised form 21 November 2013
Accepted 5 December 2013
Available online 16 December 2013

Keywords:
Business Process Management
Business process security
Process-Aware Information Systems
Security
Systematic literature review
Workflow security

ABSTRACT

Context: Security in Process-Aware Information Systems (PAIS) has gained increased attention in current research and practice. However, a common understanding and agreement on security is still missing. In addition, the proliferation of literature makes it cumbersome to overlook and determine state of the art and further to identify research challenges and gaps. In summary, a comprehensive and systematic overview of state of the art in research and practice in the area of security in PAIS is missing.
Objective: This paper investigates research on security in PAIS and aims at establishing a common understanding of terminology in this context. Further it investigates which security controls are currently applied in PAIS.
Method: A systematic literature review is conducted in order to classify and define security and security controls in PAIS. From initially 424 papers, we selected in total 275 publications that related to security and PAIS between 1993 and 2012. Furthermore, we analyzed and categorized the papers using a systematic mapping approach which resulted into 5 categories and 12 security controls.
Results: In literature, security in PAIS often centers on specific (security) aspects such as security policies, security requirements, authorization and access control mechanisms, or inter-organizational scenarios. In addition, we identified 12 security controls in the area of security concepts, authorization and access control, applications, verification, and failure handling in PAIS. Based on the results, open research challenges and gaps are identified and discussed with respect to possible solutions.
Conclusion: This survey provides a comprehensive review of current security practice in PAIS and shows that security in PAIS is a challenging interdisciplinary research field that assembles research methods and principles from security and PAIS. We show that state of the art provides a rich set of methods such as access control models but still several open research challenges remain.

Contents

* Corresponding author. Tel.: +43 1 4277 79124; fax: +43 1 4277 8 79124.
E-mail addresses: maria.leitner@univie.ac.at (M. Leitner), stefanie.rinderle-ma@univie.ac.at (S. Rinderle-Ma).

0950-5849/$ - see front matter © 2013 The Authors. Published by Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.infsof.2013.12.004

1. Introduction

The adequate support of business processes constitutes a crucial challenge for enterprises through all application domains. Hence, Business Process Management (BPM) and the support of Process-Aware Information Systems (PAIS) has become a major research area nowadays.

1.1. Process-Aware Information Systems and Security

Process-Aware Information Systems (PAIS) support the automated enactment and execution of business processes [1]. Often, these systems involve a multitude of participants and manage large data sets. Imagine, for example, a hospital with hundreds of employees managing the (information) flow of daily processes such as patient admission, examination, release, or surgeries. Such processes involve many participants (e.g., doctors, patients, and administrative staff), employ resources (e.g., X-ray machines and databases) and manage public and private information (e.g., patient records, lab results, and medical images). Furthermore, process choreographies and inter-organizational business processes fulfill business operations over one or more domains. Often, these processes are enacted over the web or in a cloud. In these infrastructures, security can be an issue (cf. [2]).

It is a PAIS characteristics to offer support for task automation as well as for human interaction. Both aspects are of importance when it comes to security. Reasoning about automatic processes and their correctness in regard to certain requirements is as crucial as to consider security from a human perspective. Examples for the latter are as attackers with malicious actions or insiders with unintentional, security threatening actions.

The level of abstraction a PAIS application exhibits can be characterized by using an enterprise architecture model (e.g., [3,4]). This paper provides a extensive literature review that investigates security controls across all layers, as security architectures are an example for cross-layer views (cf. [3]).

Furthermore, most enterprises and organizations have to fulfill legal requirements. For example, the Health Insurance Portability and Accountability Act (HIPAA) §1173(d)(2)(AB) states that each person who maintains or transmits health information has to *(A) ensure the integrity and confidentiality of the information; (B) to protect against any reasonably anticipated (i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information*. This federal law does not only affect hospitals but also anyone who handles health information e.g., general practitioners, specialists, medical labs, and paramedics. In fact, many of these legal or regulatory restrictions refer to legal requirements to enforce security (e.g., to prevent unauthorized access) and can be found in regulations and law worldwide such as U.S. Code (U.S.C.) 44 Section 3542 (2012) or EU Directive 95/46/EC of 24 October 1995. Adherence to legal requirements, employment of different process participants, handling possibly sensitive data, and distributed process scenarios are only some of the reasons that require security to become a key concern in PAIS.

1.2. State of the art

Although research has started to investigate the topic of security in PAIS, current state of research and practice on security in PAIS is unbalanced. First of all, an agreement on a common terminology or requirements on security in PAIS as well as widely accepted guidelines or models are missing, although, there is a general understanding that security in PAIS is a key challenge. One reason could be that since the proposition of security considerations by the Workflow Management Coalition (WfMC) as global organization for process related standards in 1998 [5], the maturing of the PAIS research as a discipline [6] has not been accompanied with further standardization efforts and developments with respect to security. Another reason is that PAIS research has centered on the design and development of core PAIS-relevant features when addressing security-related questions so far. In fact, security in PAIS should constitute a rather interdisciplinary research field, bringing together different disciplines such as PAIS/BPM and security (in particular, information security). This provides new challenges such as defining security in PAIS or applying methods from both disciplines. Finally, certain process scenarios such as processes that are executed in a collaborative manner among different partners have not been considered with respect to security, although such scenarios pose high demands on security and confidentiality (e.g., a partner should not be able to access details of the other partner's process). Altogether, a review of terminology and concepts as currently used in PAIS security, the analysis of questions and existing approaches addressing PAIS security as an interdisciplinary research area, and the investigation of challenges and existing solutions for security in advanced process scenarios could significantly contribute to a common and deeper understanding within the PAIS discipline, but also within the different related disciplines such as information security.