Privacy Risk Assessment in Privacy Requirements Engineering

Saeed Abu-Nimeh
Websense Security Labs
San Diego, CA 92121
sabu-nimeh@websense.com

Nancy R. Mead
Carnegie Mellon University
Pittsburgh, PA 15213
nrm@sei.cmu.edu

***Abstract*—In spite of the overlap between privacy requirements engineering and security requirements engineering, each addresses a different set of problems. As a result, security risk assessment techniques used in security requirements engineering may be unsuitable to assess privacy risks. This paper proposes considering security risk assessment along with privacy impact and risk assessment approaches using the Security Quality Requirements Engineering (SQUARE) method. The study focuses on PIA and HIPAA as privacy risk assessment techniques.**

***Keywords*-HIPAA, PIA, Privacy, Requirements Engineering, SQUARE**

I. Introduction

Several laws and regulations provide a set of guidelines that can be used to assess privacy risks. For example, the Health Insurance Portability and Accountability Act (HIPAA) addresses privacy concerns of health information systems by enforcing data exchange standards. In addition, Privacy Impact Assessment (PIA) [1] is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal information. Despite their overlap, the goals of security and privacy risk assessments differ. The goals of a security risk assessment include the implementation of authentication and authorization systems; however, the goals of a privacy risk assessment relate to policies and procedures that focus on data collection and protection.

Security Quality Requirements Engineering (SQUARE) is a structured method used to address software security issues in the early stages of the development lifecycle. The technique consists of nine steps and generates categorized and prioritized security requirements [2]. This paper discusses the combination of PIA and HIPAA with security risk assessment techniques that are used in SQUARE. Initially, a classication of PIA and HIPAA following the methodology by Campbell and Stamp [3] is discussed, after which we propose the addition of privacy impact and risk assessment techniques to the current SQUARE model.

II. Related Work

Heckle and Holden [4] show that classic risk assessment approaches do not address the privacy considerations in vote verification systems. They demonstrate that security risk assessment does not provide guidelines on how to classify data in accordance to their privacy sensitivity, and suggest applying PIA to address concerns related to privacy.

Abu-Nimeh et al. [5] recommend alternatives to the existing security risk assessment techniques in SQUARE to make it applicable to privacy. They suggest replacing, or combining, current risk assessment techniques in the Privacy Requirements Elicitation Technique (PRET) with a privacy impact assessment model, such as the IRS PIA [6].

III. Classification of Risk Assessment Techniques

In order to make sure that both the existing security and the proposed privacy risk assessment techniques follow the same method and require the same expertise, we apply the classification scheme presented by Campbell and Stamp [3]. The proposed privacy risk assessment techniques must conform to the method used by the risk assessment techniques in SQUARE; however, they need to address privacy rather than security.

Campbell and Stamp [3] propose a classification scheme for risk assessment methods based on the level of detail of the assessment method and the approach used in that assessment method. Note that this classification scheme does not help us determine which methods are appropriate for addressing security risks and which are appropriate for addressing privacy risks, yet it helps us analyze the methods suitable for privacy and those suitable for security relative to their detail and the assessment approach they follow.

An assessment method can be one of three levels: abstract, mid-level, and concrete. An *abstract* method requires an expert to drive the method. However, a *concrete* method requires someone who knows the details of the system to drive the method that is, the owner of the system. A *mid-level* method requires a collaborative effort to drive the method therefore, both an expert and the owner of the system are needed. Further, an assessment method follow one of three approaches; *temporal*, which is a method that stress-tests a system in real-time, *functional*, which performs threat analysis on the system without testing, or *comparative*, which compares the system against an explicit standard.

2009 Second International Workshop on Requirements Engineering and Law (relaw'09)
978-0-7695-4102-0/10 $26.00 © 2010

A. Classification of Security Risk Assessment Methods in SQUARE

SQUARE relies on two risk assessment techniques in step 4, namely the Risk Management Guide for Information Technology Systems (NIST SP 800-30) and Yacov Haimes's Risk Filtering, Ranking, and Management Framework (RFRM). According to Campbell and Stamp [3], NIST SP 800-30 is considered among the *assistant* methods. This risk assessment approach is performed by an expert and is a functional approach. RFRM is not listed as one of the risk assessment methods in Campbell and Stamp [3]. However, due to the similarity of the NIST model and RFRM, we consider RFRM an *assistant* method as well.

B. Classification of Privacy Risk Assessment Methods

PIA and HIPAA are driven by experts. They require someone other than the owner of the system to perform the risk assessment. Further, they perform threat analysis on the system without testing it. Actually, they consist of a series of questions that are answered by the users of the system. Both techniques require the same level of expertise, i.e., expert, used in NIST SP 800-30 and RFRM. In addition, both methods follow the same methodology, i.e., functional, used in NIST SP 800-30 and RFRM. Consequently, PIA and HIPAA are regarded as *assistant* methods.

Based on the previous discussion, our goal is met. We introduced risk assessment techniques that address privacy rather than security, follow the same assessment method, and require the same level of expertise used by the security risk assessment techniques in SQUARE.

IV. Combining Privacy Risk Assessment with Security Risk Assessment

According to Mitrano et al. [7], the goals of a security risk assessment include the implementation of authentication and authorization systems, which can be done by building firewalls, enforcing levels of authority, and generating audit trails and logs. In addition, security risk assessments ensure the protection of network security, physical security, and system security.

However, the goals of a privacy risk assessment relate to policies and procedures. The focus is on the nature of data collected, the purpose of data collection, and the procedures for obtaining an individual's consent. Further, the privacy risk assessment takes into account the necessity and accuracy of data, and compliance to regulations. The assessment ensures that standards exist for development projects and auditing compliance. The assessment checks authorization and authentication requirements, risks of theft, modification, or disclosure and mitigation procedures, third party vulnerabilities, and disclosure incident procedures.

Since security and privacy risks overlap, we use both security and privacy risk assessment techniques in SQUARE. PIA and HIPAA help to identify the data sensitivities in systems, while NIST and RFRM help to identify the full spectrum of threats to systems.

V. Conclusions and Future Work

Security risk assessment methods cannot be used as an alternative to privacy risk assessment ones. We presented the addition of privacy risk and impact assessment techniques to a security requirements engineering technique, SQUARE.

To make sure that both the existing security and the proposed privacy risk assessment techniques follow the same methodology and require the same expertise, a classification scheme of risk assessment methods was applied. Then, we combined the existing security risk assessment methods in SQUARE, namely Risk Management Guide for Information Technology Systems (NIST SP 800-30) and Yacov Haimes's Risk Filtering, Ranking, and Management Framework (RFRM), with the privacy risk assessment techniques in Privacy Impact Assessment (PIA) and Health Insurance Portability and Accountability Act (HIPAA). Our extensions to SQUARE took us further down the path of privacy requirements engineering.

Future work will explore building a privacy requirements engineering method called P-SQUARE that covers all the 9 steps of SQUARE. However, it will target both privacy and security risks in software.

References

[1] D. H. Flaherty, "Privacy impact assessments: an essential tool for data protection," in *22nd Annual Meeting of Privacy and Data Protection Officials*, 2000.

[2] N. R. Mead, E. Hough, and T. Stehney, "Security quality requirements engineering (SQUARE) methodology," Software Engineering Institute, Carnegie Mellon University, CMU/SEI-2005-TR-009, 2005.

[3] P. L. Campbell and J. E. Stamp, "A classification scheme for risk assessment methods," Sandia National Laboratories, Tech. Rep. SAND2004-4233, 2004.

[4] R. R. Heckle and S. H. Holden, "Analytical tools for privacy risks: Assessing efficacy on vote verification technologies," in *Symposium On Usable Privacy and Security*, 2006, poster.

[5] S. Abu-Nimeh, S. Miyazaki, and N. R. Mead, "Integrating privacy requirements into security requirements engineering," in *Proceedings of the 21st International Conference on Software and Knowledge Engineering*, 2009, pp. 542–547.

[6] Internal Revenuse Service, "Model information technology privacy impact assessment," 1996. [Online]. Available: http://www.cio.gov/Documents/pia_for_it_irs_model.pdf

[7] T. Mitrano, D. R. Kirby, and L. Maltz, "What does privacy have to do with it? privacy risk assessment," in *Security Professionals Conference*, 2005, presentation.

2009 Second International Workshop on Requirements Engineering and Law (relaw'09)
978-0-7695-4102-0/10 $26.00 © 2010