Combining Privacy and Security Risk Assessment in Security Quality 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

Security risk assessment identifies the threats to systems, while privacy risk assessment identifies data sensitivities in systems. The Security Quality Requirements Engineering (SQUARE) method is used to identify software security issues in the early stages of the development lifecycle. We propose combining the existing security risk assessment techniques in SQAURE with the Privacy Impact Assessment (PIA) technique and the Health Insurance Portability and Accountability Act (HIPAA) to address the full spectrum of security and privacy risks. Our ultimate goal is to introduce a privacy requirements engineering method that uses steps of SQUARE for privacy instead of or in addition to security.

Introduction

Requirements elicitation in software development concentrates on functional and nonfunctional requirements. Functional or end user requirements are the tasks that the system under development is expected to perform. However, nonfunctional requirements are the qualities that the system is to adhere to. Functional requirements are not as difficult to tackle, as it is easier to test their implementation in the system under development. Security and privacy requirements are considered nonfunctional requirements, although in many instances they do have functionality. To identify privacy risks early in the design process, privacy requirements engineering is used (Chiasera et al. 2008). However, unlike security requirements engineering, little attention is paid to privacy requirements engineering, thus it is less mature (Pfleeger and Pfleeger 2009).

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 privacy policies and procedures. The procedures in privacy impact assessment vs. the procedures in security risk assessment can be summarized as follows (Abu-Nimeh, Miyazaki, and Mead 2009).

1. Security risk assessment
   - Threat identification
   - Vulnerability identification
   - Control analysis
   - Likelihood determination
   - Impact analysis
   - Risk determination
2. Privacy impact assessment
   - Data description
   - Data sources
   - Data collection process, data accuracy, data completeness, and data currentness
   - Data comprehensiveness and documentation
   - Data access description, access procedures, access controls, and access responsibilities
   - Access levels and restrictions
   - Authorized access misuse
   - Shared data restrictions and controls
   - Data relevancy and necessity
   - Possibility of data derivation and aggregation
   - Protection and control of consolidated data
   - Data retrieval
   - Equitable treatment of users
   - Data retention and disposal
   - User monitoring and protection against unauthorized monitoring

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) (Flaherty 2000) is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal information.

The present study discusses the combination of PIA and HIPAA with security risk assessment techniques that are used in the Security Quality Requirements Engineering (SQUARE) methodology. Initially, a classification of PIA and HIPAA following the methodology in (Campbell and Stamp 2004) is discussed, after which we propose the addition of privacy impact and risk assessment techniques to the current SQUARE model. In the next section we discuss SQUARE in further detail.

Security Quality Requirements Engineering

SQUARE is a structured methodology used to address software security issues in the early stages of the development lifecycle (see Figure 1). The technique consists of nine steps and generates categorized and prioritized security requirements (Mead, Hough, and Stehney 2005).

1. Technical definitions are agreed upon by the requirements engineering team and project stakeholders.
2. Assets, business and security goals are identified.
3. In order to facilitate full understanding of the studied system, artifacts and documentation are created.
4. A security risk assessment is applied to determine the likelihood and impact of possible threats to the system.
5. The best method for eliciting security requirements is determined by the requirements engineering team and the stakeholders.
6. Security requirements are elicited.
7. Security requirements are categorized.
8. Security requirements are prioritized.
9. The security requirements are inspected to ensure consistency and accuracy.

SQUARE uses security risk assessment techniques that are unsuitable to assess privacy risks. In the following sections we discuss the limitations in the current security risk assessment techniques in SQUARE, then we present combing privacy impact assessment techniques with security risk assessment techniques to address privacy requirements in software.

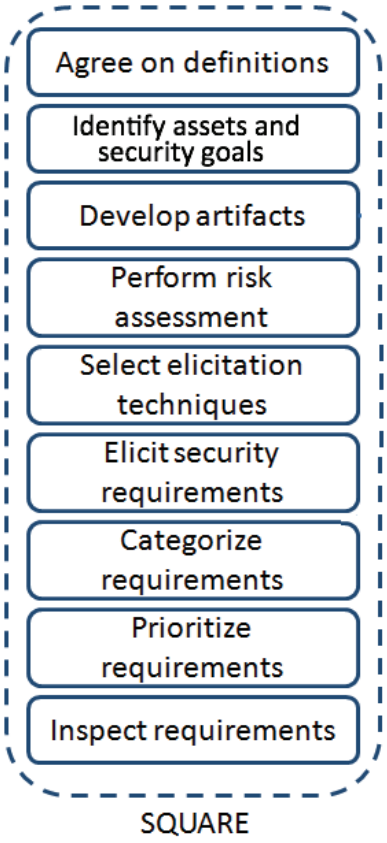

Figure 1: SQUARE Steps

Privacy Risk Assessment Techniques

In this section we discuss PIA and HIPAA in detail.

Privacy Impact Assessment

According to (Statistics Canada 2008), the PIA process is used to determine the privacy, confidentiality and security risks associated with the collection, use, and disclosure of personal information. In addition, it defines how to mitigate and eliminate the identified risks. The PIA process should be considered in any new program or service delivery initiative, and should communicate to the public the privacy and confidentiality of their information.

According to US-CERT (United States Computer Emergency Readiness Team 2008), the following should be addressed when conducting a PIA on systems.

1. Characterization of the information: what information is collected and maintained in the system.
2. Uses of the information: use of information and tools to analyze data.
3. Information retention: how long is information retained.
4. Internal sharing and disclosure: which internal organizations share the information.
5. External sharing and disclosure: which external organizations share the information.
6. Notice of collection of information: notifying individuals prior to collection of information.
7. Individual access, redress and correction: how can individuals access their information.
8. Technical access and security: who can access the information or the system.
9. Technology: what development process was used to develop the system.

HIPAA Privacy Risk Assessment

HIPAA addresses privacy concerns of health information systems by enforcing data exchange standards. The act also provides a guideline to analyze risks. The overall objective of a HIPAA risk analysis is to document the potential risks and vulnerabilities of confidentiality, integrity, or availability of electronic protected health information (ePHI) and to determine the appropriate safeguards to bring the degree of risk to an acceptable and manageable level. Risks found by the analysis fall into three categories: access, storage, and transmission.

The entities of interest in HIPAA are called the Covered Entities (CEs) that must comply with the HIPAA Security Rule. These are health plans (HMOs, group health plans, etc.), health care clearinghouses (billing and repricing companies, etc.), and health care providers (doctors, dentists,

hospitals, etc.) who transmit any ePHI. There are 7 steps involving in HIPAA risk assessment.

1. Inventory and classify assets
2. Document likely threats to each asset
3. Vulnerability assessment
4. Evaluate current safeguards (administrative, physical or technical)
5. Document risks
6. Recommend appropriate safeguards
7. Create report of results

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 methodology and require the same expertise, we apply the classification scheme presented in (Campbell and Stamp 2004). The proposed privacy risk assessment techniques must conform to the methodology used by the risk assessment techniques in SQUARE; however, they need to address privacy rather than security. In (Campbell and Stamp 2004), the authors 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. They summarize the strengths and weaknesses of assessment methods in a nine cell matrix as shown in Table 1. This comparative matrix helps the user to understand the following information: what to expect from an assessment method, what the relationship is among different assessment methods, and what the best way is to use an 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.

As shown in Table 2, 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.

Table 3 shows the three different approaches that can be followed by risk assessment methods. An assessment method can be *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.

The nine numbered cells (i.e, engagement (1) through audit (9)) show what needs to be done by the driver of the method. They can be summarized as follows:

1. Engagement: Experts try to compromise a system without the owner's help.
2. Exercise: Owner collaborates with experts to compromise a system.
3. Compliance Testing: Similar to door rattling performed by the owner of the system.
4. Sequence: Series of questions or flow chart answered by the user.
5. Assistance: Similar to an assistant, a track of the system details is kept.
6. Matrix: A table lookup is used by the user.
7. Principles: This is a list of all comparative types. Principles have to be applied to the system by the user.
8. Best Practice: A more specific list than the principle's list.
9. Audit: A list based on an explicit standard, but more specific than the best practice's list.

The interested reader can refer to (Campbell and Stamp 2004) for further details on the description of these types.

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) (National Institute of Standards and Technology 2002) and Yacov Haimes's Risk Filtering, Ranking, and Management Framework (RFRM) (Haimes 2004). The RFRM approach contains eight phases, some of which were found to be out of scope. Only two relevant phases of RFRM are included in SQUARE: phase III, Bicriteria filtering and ranking, and phase IV, multicriteria filtering and ranking.

NIST's model for risk assessment is broken into nine steps, each with an output that serves as the input to the next step. SQUARE excludes steps 1, 8, and 9 in NIST, as they are irrelevant or redundant. Therefore, the steps included in SQUARE are threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, and risk determination. Apparently, the risk assessment in SQUARE corresponds to the system under analysis. Most importantly, the risk assessment should categorize the likelihood and impact of the major threats to the system (Mead, Hough, and Stehney 2005).

According to (Campbell and Stamp 2004), NIST SP 800-30 is considered among the "Assistant" methods. This risk assessment approach is performed by an expert and is a functional approach (see Table 3). However, RFRM is not listed as one of the risk assessment methods in (Campbell and Stamp 2004). NIST and RFRM are both concerned with hardware failure or destruction; however, they rank the importance differently. Also, the outputs of both methods concentrate on different aspects. In NIST, the output concentrates on what the attacker can do once inside the system, e.g., destroying data or disclosing information. In RFRM the output concentrates on the attacker's ability to break the frontline of a defense system (Mead, Hough, and Stehney 2005). Due to the similarity of the NIST model and RFRM, we consider RFRM an "Assistant" method as well.

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

Table 1: Classification matrix

Level		Approach		
		Temporal	Functional	Comparative
Abstract	Expert	Engagement (1)	Sequence (4)	Principles (7)
Mid-level	Collaborative	Exercise (2)	Assistant (5)	Best Practice (8)
Concrete	Owner	Compliance Testing (3)	Matrix (6)	Audit (9)

Table 2: Approach level

	Abstract	Mid-level	Concrete
Level	High level (3)	Mid level (2)	Low level (1)
Expertise	Requires expert's knowledge	Requires both expert's and owner's knowledge	Requires user's knowledge
Description	How an expert performs an assessment	How both (an expert and an owner) perform an assessment	How a system owner performs an assessment
Application	Broad	Middle	Narrow
Driver	Expert	Collaborative (both expert and owner)	Owner

Table 3: Approach classification

	Temporal	Functional	Comparative
Procedure	Stresses a system and actual tests are applied in real time	It is a blend of the other two approaches. It performs threat analysis, which focuses on how a system functions without testing	A comparison against an explicit standard. The system model and the threat lists are only implicitly present in a generic form
Outcome	The performance of the system as a consequence of the application of those tests	Threat analysis	Comparing the system with an explicit standard
Advantages	Testing the system clears misconceptions	Considers specific threats, vulnerabilities, assets and countermeasures	Simple and focused
Disadvantages	Impractical to test the system, so a model of the system is tested. Similarly, cannot perform all attacks on the system and a subset of attacks is performed	No testing involved	No testing or examination of function and no explicit system model involved

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 as shown in the previous subsections.

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 methodology, and require the same level of expertise used by the security risk assessment techniques in SQUARE.

Combining Privacy Risk Assessment with Security Risk Assessment

According to (Mitrano, Kirby, and Maltz 2005), 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 (Abu-Nimeh and Mead 2009).

Related Work

In (Heckle and Holden 2006), the authors show that classic risk assessment approaches do not address the privacy considerations in vote verification systems. They also demonstrate that security risk assessment does not provide guidelines on how to classify data in accordance to their privacy sensitivity. Instead, they suggest applying privacy impact assessments (PIA) to address concerns related to privacy.

Privacy requirements elicitation technique (PRET) is a tool that helps software engineers and stakeholders elicit privacy requirements early in the design process using a computer-aided approach (Miyazaki, Mead, and Zhan 2008). PRET is based on SQUARE. After the initial SQUARE steps, PRET is integrated into the SQUARE tool to elicit the privacy requirements of the system. To elicit information, PRET relies on both requirements engineers and stakeholders to complete a questionnaire. A database of privacy requirements is searched to utilize the input from the questionnaire and provides results.

In (Abu-Nimeh, Miyazaki, and Mead 2009), the authors 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 PRET with a privacy impact assessment model, such as the IRS PIA.

Conclusions and Future Work

The present study showed that 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. Thus SQUARE will target both privacy and security risks in software.

Acknowledgements

This research was supported in part by CyLab at Carnegie Mellon under grant DAAD19-02-1-0389 from the Army Research Office.

References

Abu-Nimeh, S., and Mead, N. R. 2009. Privacy risk assessment in privacy requirements engineering. In *RELAW: The Second International Workshop on Requirements Engineering and Law*.

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

Campbell, P. L., and Stamp, J. E. 2004. A classification scheme for risk assessment methods. Technical Report SAND2004-4233, Sandia National Laboratories.

Chiasera, A.; Casati, F.; Daniel, F.; and Velegrakis, Y. 2008. Engineering privacy requirements in business intelligence applications. In *SDM '08: Proceedings of the 5th VLDB workshop on Secure Data Management*, 219–228. Berlin, Heidelberg: Springer-Verlag.

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

Haimes, Y. Y. 2004. *Risk Modeling, Assessment, and Management*. Wiley-Interscience, 2nd edition edition.

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

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

Mitrano, T.; Kirby, D. R.; and Maltz, L. 2005. What does privacy have to do with it? privacy risk assessment. In *Security Professionals Conference*. presentation.

Miyazaki, S.; Mead, N.; and Zhan, J. 2008. Computer-aided privacy requirements elicitation technique. *Asia-Pacific Conference on Services Computing*. 0:367–372.

National Institute of Standards and Technology. 2002. Risk management guide for information technology systems. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Pfleeger, S. L., and Pfleeger, C. P. 2009. Harmonizing privacy with security principles and practices. *IBM Journal for research and development* 53(2).

Statistics Canada. 2008. Privacy impact assessment. http://www.statcan.gc.ca/about-apercu/pia-efrvp/gloss-eng.htm.

United States Computer Emergency Readiness Team. 2008. Privacy impact assessment for EINSTEIN 2. Technical report, Department of Homeland Security.