HINZ Primary Care and Beyond: Building the e-Bridge to Integrated Care
Eds: Christopher Peck & Jim Warren
Publisher: Health Informatics New Zealand (HINZ) & Health Informatics Society of Australia Ltd (HISA)
ISBN 0 9751013 7 4

A Survey-Based Analysis of HIPAA Security Requirements

Jinho Lee
The University of Auckland
Secure Systems Group
jlee141@ec.auckland.ac.nz

Clark Thomborson
The University of Auckland
Secure Systems Group
cthombor@cs.auckland.ac.nz

Gary Guest
The University of Texas
Health Science Center at San Antonio
guest@uthscsa.edu

Abstract

This paper reports on the results of a survey-based investigation into the perceived security requirements held by the U.S. dental schools for their enterprise dental information systems. The U.S. dental schools are faced with the legal requirement to comply with HIPAA which contains provisions that are intended to protect electronic patient information. However it is proving to be a challenge to comply with HIPPA because of the lack of detail in its provisions. Consequently the perceived security requirements held by the dental schools vary. We used a survey-based misuse case analysis to engineer a more detailed set of security requirements. Due to low response rate of the survey the results of this study are not conclusive yet. However we have successfully obtained some promising security requirements that warrant further work in similar direction.

1. Introduction

Security of electronic patient health information (e-PHI) is emerging as a critical issue. However the lack of detail in existing security requirements for health information systems challenges designing of such systems. We present the results of a U.S. based pilot study so we can define the security requirements as perceived by the U.S. dental schools.

In the U.S. the Health Insurance Portability Accountability Act (HIPAA) contains provisions for ensuring the security of e-PHI. It was passed to make adequate protection a legal requirement for the covered entities, the U.S. dental schools in this case. Other works relating to HIPAA security requirements are generally concern legal analysis and organisational processes rather than technical requirements [1-4]. To our knowledge there has been no previous attempt to investigate the perception of the covered entities regarding HIPAA's technical security requirements.

This work was inspired by the difficulty experienced in satisfying consumers' varied requirements for security by a N.Z. based software vendor called Software of Excellence Ltd. This business exports dental information systems to the U.S. and U.K. dental schools market. Satisfying the security requirements imposed by the new legislation is a challenge because they neither prescribe implementation nor specify specific threats to defend against [3, 5-7]. So each dental school has to interpret the legal requirements and devise more detailed security requirements that can readily map to implementation.

ISBN 0 9751013 7 4

We used misuse case analysis to elicit and analyse the detailed security requirements held by the dental schools themselves for enterprise dental information systems. The enterprise dental information system is a computer system that supports and is used by an entire dental school across every department, i.e. the whole enterprise. This paper is a pilot study into defining and engineering dental security requirements, with suggested areas for more research based on our results. The next section contains the particular methodology we used.

2. Methodology

Three broad classes of requirement engineering methodologies were identified - goal-based, scenario-based and viewpoint-based. Each approach drives the requirement engineering process by eliciting goals, scenarios and viewpoints respectively. The scenario-based approach was preferred to the goal-based one because the stakeholders are often better at articulating scenarios than their goals [8]. As for the viewpoint-based approach, considering multiple viewpoints was impossible given our time/resource constraints. So we opted for the scenario-based approach over the others.

Misuse case analysis, which is a scenario-based methodology, was chosen for our investigation. It reverses the famous use case analysis and models security requirements by eliciting misuse cases which are negative scenarios that should not be allowed by a system [9]. Thus the detailed requirements referred to in the previous section will be elicited in the form of misuse cases that the dental schools are concerned about.

In order to elicit misuse cases from the dental schools and to shed light on the overall perception about the technical provisions of HIPAA, we designed an online survey and sent invitation letters through the American Dental Education Association (ADEA) listserv. The survey was organised according to the

Technical Safeguards of the HIPAA which consists of the following five standards:

S1 Access Control
S2 Transmission Security
S3 Audit Control
S4 Integrity
S5 Entity Authentication

There were two types of questions for each of the above standards and a set of general questions that were not limited to any particular standard:

Type–1 ”Are you satisfied with your current information system with respect to S1? If not, please describe why”

Type–2 ”Please describe a scenario of system use that you perceive as non-HIPAA compliant with regard to S1”

General These were aimed at discovering the overall perception of the respondents about the Technical Safeguards provisions; e.g., “Do you consider insider attacks as a significant part of the threats? If yes, please describe a scenario of a likely insider attack that you are concerned about.”

Most of the survey questions required narrative responses. In particular, the usage scenarios from the respondents were used to develop misuse cases. For example if a respondent gave a scenario, “A student sharing his password with his peers,” the corresponding misuse case would consist of ‘Student’ as the actor and ‘sharing his password’ as the action of misuse.

We hypothesised that our survey-based misuse case analysis would be capable of engineering more detailed security requirements than what is available in the legal provisions. In the next section we will summarise the results and provide discussion.

ISBN 0 9751013 7 4

3. Results

Most of the questions in our survey required narrative responses which may have affected the response rate. Out of the sixty potential respondents, only seven responded. This makes the data difficult to analyse statistically. However the narrative responses allowed for some interesting qualitative analysis. As this is only a pilot study, the results and lessons learnt here can be used to improve future attempts in similar investigations.

Responses to the general questions yielded the following findings:

F-1 Among the five standards of the HIPAA Security Rule, the respondents were most concerned about 'Audit Control'.

F-2 Insider attacks were considered as a significant part of the attacks.

As for the detailed security requirements held by the dental schools, we developed four different misuse cases from the survey responses. Each misuse case was analysed in terms of use case/misuse case interaction. The relationship semantics proposed in [9] were used to identify potential mitigating use cases. Following is a short summary of the misuse cases we identified.

Password sharing by legitimate users occurs when an authorised user shares his/her password with others allowing them to potentially misuse e-PHI.

Covering up for dental malpractice is when a dentist tries to cover up an omission that led to an adverse outcome by unauthorised modification.

Email used to communicate e-PHI happens when a staff member of a school carelessly sends an email containing e-PHI to an external party.

Workstation unattended is where a staff member leaves his/her workstation unattended with confidential information in accessible form.

4. Discussion

Goedert wrote in 2005 that dentists were most concerned about audit control as we discovered in F-1 [2]. Goedert argued that the provisions for Audit Control are the most ambiguous and therefore the covered entities will have difficulty implementing them.

Other research shows that insiders are often the weakest link of a system security [1, 10]. This supports our finding in F-2.

It is interesting to see that all the misuse cases identified by the dental schools concerned authorised insiders misusing e-PHI either accidentally or intentionally. None of the responses contained any misuse case that involved a skilled hacker attacking the system externally.

Our experimental hypothesis was that our survey-based misuse case analysis would result in more detailed security requirements than the existing legal provisions. Because of the low response rate of the survey, it is difficult to generalise about these results and confirm the hypothesis yet. Our survey-based methodology was successful in eliciting some specific threats, i.e. the misuse cases that the dental schools perceived to be important for complying with the technical safeguards of HIPAA. Despite the low response rate of the survey, the results are promising enough to warrant further work in security requirements for computerised record keeping in the medical field.

5. References

[1] Huston T. Security issues for implementation of e-medical records. Commun.ACM 2001; 44(9): 89-94.

[2] Goedert J. HIPAA security: The home stretch. Health Data Management 2005; 13(2):88.

ISBN 0 9751013 7 4

[3] Walker R. A HIPAA strategy for dental schools. Journal of Dental Education 2003; 66(5): 624-33.

[4] Andis R. Noncompliant and unconcerned. Modern Healthcare 2005; 35(32): 33.

[5] Northcutt S, editor. *HIPAA Security Implementation*. SANS PRESS, 3rd edition, Dec 2004.

[6] Walker R, Ao M. Cios' view of HIPAA security rule implementation – an application of q-methodology. Journal of Healthcare Information Management 2005; 19(2): 73-80.

[7] Sfikas PM. HIPAA security regulations: protecting patients' electronic health information. The Journal of the American Dental Association 2003; 134(5): 640-3.

[8] Nuseibeh B, Easterbrook SM. Requirements engineering: a roadmap. Proceedings of the International Conference on Software Engineering (ICSE 2000), Limerick, Ireland, ACM Press, 2000.

[9] Alexander I. Misuse cases: use cases with hostile intent. IEEE Software 2003; 20(1):58-66.

[10] Cushman R. Information and medical ethics: Protecting patient privacy. IEEE Technology and Society Magazine 1996; 15(3): 32-39.