Security Issues in Health Care Process Integration – a Research-in-Progress Report

Rose-Mharie Åhlfeldt, Per Backlund, Benkt Wangler, Eva Söderström

University of Skövde, Sweden
{rose-mharie.ahlfeldt, per.backlund, benkt.wangler,
and eva.soderstrom}@ida.his.se

1. Introduction

The aim of this paper is to summarize our research and describe our current position in the areas of health care process integration and information security. Security is one of the important non functional aspect of interoperability within the INTEROP NoE. The paper will briefly introduce our work and some findings concerning security issues in process integration within the health care sector.

2. Information Security

The research area involves B2B[1] integration with a specific interest in information security in health care processes. Information security is a central concept, elaborated in SIS (2003) and Phleeger (2003). In this paper, we adhere to the definitions in SIS (2003) and SITHS (2000), summarized as follows: Information security is the collected effect of measures to minimize the risks addressed for the availability, confidentiality, integrity and accountability of information (Figure 1).

Availability concerns how to use resources to the expected extent and within the desired timeframe. *Secrecy* means that data must not be accessible or unveiled to unauthorized people. *Integrity* concerns protection against undesired changes. *Accountability* refers to the ability to distinctly derive performed operations to an individual. Technical and administrative security measures are both needed to reach these four characteristics. *Technical security* consist of physical security, e.g. alarm and fire protection; and IT-security, e.g. computer and network security. Computer security concerns specific computers and their applications. Network security concerns security measures for information distributed in networks. *Administrative security* concerns management of information security; strategies, policies etc. Planning and implementation in security work requires a structured way of working. We note that in a computerized environment, it is easy to focus more on technical measures and functions.

[1] Business-to-Business (B2B) is communication and transactions between at least two business partners via Internet technology (Wangler et al, 2001).

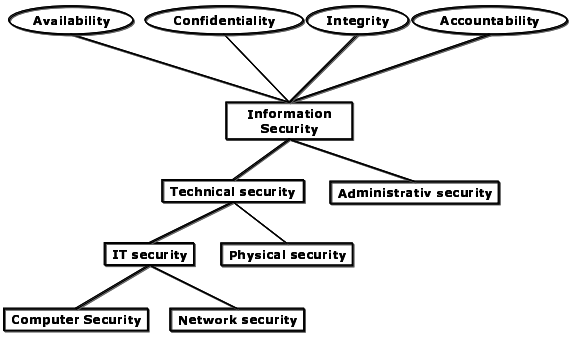

Figure 1: Information security model

3. Process integration in the health care sector

The health care sector is an example application area where numerous interoperability problems need to be resolved. The VITA Nova project (Wangler et al., 2003; Perjons et al., 2005) focuses on the patient process, and includes communication between healthcare providers and healthcare units. The project goals are to develop a methodology for and to investigate the potential of an IT architecture based on process manager technology.

In the context of information security in the healthcare sector it can be assumed that information is sensitive. Computerization of information handling gives access to information from databases in ways not previously possible. Healthcare sector information security has two important aims: a high level of patient security, i.e. to give patients opportunities to the best care with right information in right time; and a high level of patient privacy; i.e. to protect patients from that sensitive information is distributed to unauthorized persons. These aims are hard to reach together, since one aim is often reached at the expense of another. Hence, a balance between them is necessary (Teldok, 2004). Process integration herein entails that information transfer between units must be satisfactory from the perspective of the patient and the his/her relatives, as well as from the legal and security perspectives (Perjons et al., 2005).

In the following subsections, three case applications of information security will be presented in relation to the model in Figure 1.

3.1 IT Security

A case study from the VITA Nova project (Åhlfeldt and Nohlberg, 2005) shows that none of the involved systems had a function to log the use of user accounts automatically, and to alert when a user's account has not been used during a specific period of time. Furthermore, there is no verification technique for the identification of the users other than passwords. Sufficient control of authentication techniques for

access to sensitive information should be managed by a two-party solution (Protect Data, 2004): something you have and something you know.

The lack of a strong signing technique is a security risk. Earlier work (Åhlfeldt and Ask, 2004) has shown that users may utilize other users' login and password in order to avoid a new login procedure, since they believe it takes too long to do it.

3.2 Availability vs confidentiality

Authentication affects both availability and confidentiality. If we only have to reach availability it would be unnecessary to put so much effort into authentication and authorization. With the aim to reach both patient security and patient integrity, we need confidentiality as well. However, the balance between these two frequently mismatches (Åhlfeldt and Ask, 2004).

3.3 Administrative Security

A case study by Åhlfeldt and Nohlberg (2005) shows that non of the organizations studied has deliberate education in security. One of them shows some awareness, as they send out reminders on currently active viruses. Another organization has not undertaken any security education for their users for the past ten years.

The human element is another important aspect, since e.g. social engineering attacks are becoming more and more common (Nohlberg, 2005). Social engineering is defined as a hacker's manipulation of the human tendency to trust other people in order to obtain information that will allow unauthorized access to systems (Granger, 2001). Nohlberg (2005) shows that the human element is vulnerable to an extent that overshadows most other security measures. Such attacks are effective among technology-savvy users, and even more so among less skilled users (Nohlberg, 2005).

4. Conclusion

The information security model in Figure 1 is a major contribution from our research. It stresses the need to go beyond technical security, and highlights demands for maintaining availability, confidentiality, integrity, and accountability in an information security context. The model can be used as a means for analyzing security in a broader perspective. The following summarizes our major findings from our empirical material, based on the model:

- Technical security tends to be in focus, but major problems reside in administrative security as well, i.e. in the management of security issues. Security education is important in this context.
- There is a need for education in security matters, e.g. of higher awareness of why security issues are important.

- Problems in providing adequate technical security results in insufficient availability.
- Legitimacy control must be improved. Passwords are not sufficient for dealing with delicate information due to the risk of social engineering.

In future work, we intend to elaborate the information security model in order to make it useful as a tool for analysing security. We will also study and characterise standards within the healthcare sector, e.g. as a starting point for developing a core domain ontology for the healthcare sector. This ontology may be used for managing semantic interoperability issues in relation to security. Standards are essential for achieving interoperability between healthcare providers and healthcare units, in being a common language underpinning the communication. They enable applications to exchange messages and documents, and to automatically respond to actions by other applications.

5. References

Granger, S. (2001) Social Engineering Fundamentals [Online] Security Focus. Available from : http://www.securityfocus.com/printable/infocus/1527 [Accessed 2003-09-18]

Nohlberg, M. (2005) Social Engineering Audits Using Anonymous Surveys – Conning the Users in Order to Know if They Can Be Conned. In CD-ROM Proceedings of the 4th Security Conference 2005, Las Vegas, 30-31 March, 2005.

Perjons, E., Wangler, B., Wäyrynen, J. and Åhlfeldt, R. (2005) *Introducing a process manager in healthcare: an experience report*, Health Informatics Journal, 11(1).

Pfleeger, C (2003). *Security in Computing*, Prentice Hall. ISBN 0-13-035548-8.

ProtectData (2004). News from Pointsec Mobile Technologies June 2004. [on line] http://www.pointsec.com/news/download/PMT2_04_72dpi_klar.pdf [accessed November 2004]

SIS (2003). SIS Handbok 550. Terminologi för Informationssäkerhet. Stockholm 2003 (in Swedish).

SITHS-projekt, (2000). Infrastruktur för informationssäkerhet i hälso- och sjukvården. Stockholm: Säker IT i Hälso- och Sjukvården, ISBN 92- (in Swedish).

Teldok (2004). Patientdata - brist och överflöd i vården. Teldok rapport nr 154. ISSN 0281 - 8574 (in Swedish).

Wangler, B., Åhlfeldt, R. and Perjons, E. (2003) *Process Oriented Information Systems Architectures in Healthcare*, Health Informatics Journal, December 2003.

Wangler, B., Persson, A. and Söderström, E. (2001), Enterprise Modeling for B2B Integration, In Proceedings of the In International Conference on Advances in Infrastructure for Electronic Business, Science, and Education on the Internet, August 6-12, L'Aquila, Italy

Åhlfeldt, R-M. and Ask, L. (2004). Information Security in Electronic Medical Records: A case study with the user in focus. In Proceedings of the 2004 Information Resources Management Association International Conference. New Orleans, USA, May, pp. 345-347.

Åhlfeldt, R-M. and Nohlberg, M. (2005). System and Network Security in a Heterogeneous Healthcare Domain: A Case Study. In CD-ROM Proceedings of the 4th Security Conference, Las Vegas, USA, 30 – 31 March 2005.