Informationsmanagement und Computer Aided Team
Hrsg.: Helmut Krcmar

Ali Sunyaev

Health-Care Telematics in Germany

Design and Application of a Security Analysis Method

GABLER

RESEARCH

Ali Sunyaev

Health-Care Telematics in Germany

GABLER RESEARCH

Informationsmanagement
und Computer Aided Team

Herausgegeben von Professor Dr. Helmut Krcmar

Die Schriftenreihe präsentiert Ergebnisse der betriebswirtschaftlichen Forschung im Themenfeld der Wirtschaftsinformatik. Das Zusammenwirken von Informations- und Kommunikationstechnologien mit Wettbewerb, Organisation und Menschen wird von umfassenden Änderungen gekennzeichnet. Die Schriftenreihe greift diese Fragen auf und stellt neue Erkenntnisse aus Theorie und Praxis sowie anwendungsorientierte Konzepte und Modelle zur Diskussion.

Ali Sunyaev

Health-Care Telematics in Germany

Design and Application of a Security Analysis Method

GABLER

RESEARCH

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Dissertation Technische Universität München, 2010

1st Edition 2011

Editorial Office: Stefanie Brich | Anita Wilke

Gabler Verlag is a brand of Springer Fachmedien.
Springer Fachmedien is part of Springer Science+Business Media.
www.gabler.de

Coverdesign: KünkelLopka Medienentwicklung, Heidelberg
Printed on acid-free paper
Printed in Germany

ISBN 978-3-8349-2442-1

Foreword

The importance of security management in the development and operation of information systems (IS) has been growing with the ubiquity of information system use. Along with this growth and technological advances IS security has changed tremendously over the past decades and so have its scope, complexity, and the variety of analyzed security aspects. To meet these challenges IS security methodologies should become more industry specific and at the same time integrate organizational and technical aspects.

Securing the privacy of health information on systems is a major challenge to the widespread adoption of new healthcare information systems like the forthcoming German electronic health information infrastructure. Encouraged by the lack of healthcare IS research with respect to security, this work presents the design and development of an IS security methodology for the organizational and technical analysis of security issues in health care. Grounded on the research literature on IS security and healthcare IS, and a variety of current theories in the fields of information systems, business administration, and computer science, it develops a security analysis method for healthcare information systems. This security analysis method builds the foundation to practically examine the current status of the German healthcare telematics, its constitutive elements, and process management in order to identify possible vulnerabilities. Based on these insights, the work proposes appropriate solution mechanisms for the security management of the German healthcare telematics including recommendations for future IS developments in the health care sector.

Ali Sunyaev‘s work shows that IS security should be linked to the needs of an application area, both on the organizational and technical side. He clearly depicts the current security situation of German health information infrastructure and so facilitates a broader understanding of analyzing healthcare IS security. This work is an important contribution to the research field of managing information systems. In a methodological way it gives valuable impulses for combining different security approaches and research methods depending on the context of a security arrangement. The work appeals by its broad scope of theory, method engineering background, and its comprehensive argumentation. Researchers of information systems will gain new insights on which practical security analysis methods and theories are applicable given for healthcare information systems. For practitioners, it provides recommendations for orchestrating the development of secure healthcare IS and presents the identification of security problems in the current concept of German healthcare telematics.

I recommend this book as a valuable reading and resource. It provides new and promising insights into an IS security research field and inspires different kinds of readers to adopt a new perspective on healthcare information systems.

I hope this work will find the broad dissemination and attention it deserves.

Prof. Dr. Helmut Krcmar

Abstract

Purpose: The objective of this thesis is to develop a method for the organizational and technical analysis of security issues in health care (using tools, methods and processes in a structured and traceable way). Using this method the current security status of health care telematics in Germany is evaluated and recommendations for future developments in the health care sector are derived.

Methodology: This work is based on the methodological foundation of design-oriented artifact construction in Information Systems (IS) research, in particular method engineering. This research project creates a method to analyze healthcare telematics and also demonstrates the practical application of the designed artifact, based on the integral parts of the design science research framework.

Findings: During the planning stage of designing a healthcare specific IS security analysis method, it is advisable to base the design procedure on established standards and best practice approaches. The resulting method therefore relies heavily on previously approved frameworks. Based on the PDCA (Plan/Do/Check/Act) model the HealthcAre Telematics SECurity-HatSec-analysis method is constructed in a compositional manner. Hence, the HatSec method was designed from existing IS security analysis approaches (like ISO 27001 and IT-Grundschutzhandbuch), which were previously selected according to their suitability for healthcare and subdivided into method fragments. Applying the concept of method engineering, these method fragments were used to design the HatSec security analysis method. The identified method fragments of the selected IS security analysis approaches were methodically composed into seven steps: (1) scope identification, (2) asset identification, (3) basic security check, (4) threat identification, (5) vulnerability identification, (6) security assessment and (7) security measures. The application of the HatSec method identified 24 deficiencies in the current state of German health care telematics (including weaknesses, inconsistent and conflicting development documents and violation of security demands). Solutions for the uncovered vulnerabilities were also provided during the practical application of the method.

Practical Implications: The outcome of this research project facilitates a broader understanding of analyzing healthcare IS security. The HatSec method is designed for chief information security officers (CISO) to analyze healthcare information systems currently in use or under development. A further contribution to practice is the identification of security problems in the current concept of German healthcare telematics.

Contents

List of Figures

List of Tables

1 Introduction

Since the beginnings of time, human beings have displayed a strong need for safety and security. As a matter of course, this need has been oriented towards the specific situations of the time. In the 19th and 20th centuries, the so-called "industrial age", this safety and security need was displayed in physical security measures, including measures and equipment to protect factory workers. Helmet and gloves remain essential parts of workers clothing on every building site. With the development of electronic data processing and the internet our society is moving rapidly into the "information age". Modern information and communication technology allows data to be collected, saved, transmitted, and used in numerous ways. This development has led to an outstanding growth of processed information and produces new central resource - raw material *information*. Some of this information is freely accessible, some not. Information systems (IS) security demands that information is kept confidential and that the dependability of processing information systems is guaranteed.

Healthcare is in the center of this global networking. The use of networked information technology across the boundaries of institutions and various sectors is a potential opportunity for increased efficiency and improved delivery of healthcare services (Haux/Ammenwerth/-Buchauer 2001). It creates numerous possibilities such as improved communication between healthcare providers and patients (Michel-Verkerke/Schuring/Spil 2004), smoother transfer of information across electronic boundaries (Sunyaev et al. 2008b), lower costs (gematik 2006q), increased access transparency, and improved treatment quality and safety (Kuhn et al. 2006). An essential step towards the implementation of a networked information system in healthcare is the introduction of an electronic health card (eHC) for patients (Avison/Young 2007) and its counterpart health professional card (HPC) for healthcare providers in Germany. These cards will form an essential part of a comprehensive national telematics infrastructure currently being developed. The eHCs will be mandatory for every German citizen. Furthermore, each healthcare provider will be required to have an HPC. Both cards will have a clearly defined structure and set of functions.

In accordance with the most recent German healthcare reform plan, the introduction of the electronic health card will be followed by the introduction of an electronic patient record (Tang et al. 2006). For this reason, a health telematics platform will be implemented in Germany as a communication platform for all parties, involved in the healthcare industry. Furthermore, there is a worldwide movement to develop global healthcare telematics infrastructures in order to improve the quality of care and empower patients (AbouZahr/Boerma 2005). Some of the national and regional healthcare telematics initiatives are (Sittig 2001):

A. Sunyaev, *Health-Care Telematics in Germany,* DOI 10.1007/978-3-8349-6519-6_1,

- United States of America (National Health Information Infrastructure (NHII) (Yasnoff et al. 2004; Mandl et al. 2007; Simons/Mandl/Kohane 2005)).

- United Kingdom (Connecting for Health (CfH) (NHS 2007)).

- Denmark (National IT Strategy (Danish Health Service) (Lippert/Kverneland 2003; Bernstein et al. 2005; Nohr et al. 2005)).

- Netherlands (National Healthcare Information System).

- Australia (HealthConnect – National Health Information Network (Rowlands 2005)).

- New Zealand (Health Information Strategy for New Zealand (HIS-NZ) (Health Information Strategy Steering Committee 2005)).

- Hong Kong (China, Health Information Infrastructure (Sek et al. 2007; Holliday/Tam 2004)).

- Bangladesh (Integrated Rural Health Information System (IRHIS) (IRHIS)), Malaysia (Telehealth Platform (Hashim et al. 2001)).

- Europe (European Health Insurance Card – eEurope 2005 Action Plan (Commission of the European Communities 2002; Kontaxakis et al. 2006; Pattichis/Schizas/-Andreou 2002)).

Because of telematics, healthcare is currently undergoing a revolutionary process of qualitative improvement. The vision of a locally-independent and continuously accessible electronic patient record is becoming a reality as a result (Richardson 2005). The cooperating partners are no longer bound by place or time and can be located to any nation or jurisdiction (Haux/-Ammenwerth/Buchauer 2001).

The German healthcare system is experiencing crucial changes as well. Due to medical and technical progress, hospitals will be able to provide better quality medical treatment at reduced costs compared to the current situation. Restructuring internal processes in an economically sustainable and effective way while complying with legal and ethicals requirements is the main aim of future developments in German healthcare.

The information systems (IS) penetration rate and the use of affordable IS applications to increase productivity are insufficient throughout the German healthcare system. The Roland

Berger study – “Quality and Innovation in a Hospital” (Roland Berger & Partner GmbH – International Management Consultants 2003) reveals that one in six German hospitals have not implemented even the most basic elements of a medical information system. Only the largest and most significant institutions have adopted comprehensive IS solutions. Apart from the problem of medical documentation and billing processes being manual in many cases, the automatization of internal and external data transfer from one system to another is often missing.

Expenses for healthcare in Germany are rising steadily, with a total increase of 43% between the years 1992 and 2002 (Alex&Gross 2004; Gericke/Rohner/Winter 2006). Regulations require, however, that the maximum fees for compulsory public health insurance remain stable. This situation leads to a necessity of significant cost reductions that affect not only the funding agencies (insurance companies) but also service providers (especially hospitals). Information technology can play an especially role in this situation; in much the same way it has done in other industries before. On the one hand in combination with appropriate changes in the structural and process organization in healthcare IS can make the provision of service more effective, thereby reducing costs (Babulak 2006), while on the other the quality of medical service provision in different areas (not only in imaging systems, but also for example in value-added services for patients, etc.) can be increased significantly through the correct application of IS (Ammon 2002).

In such an information system (telematics platform) of communication and co-operation, the requirements for data security, data safety, and data integrity are of the highest priority when dealing with sensitive data such as personal medical information or administrative operational data (Anderson 2001; Beynon-Davies/Lloyd-Williams 1999; Krause/Brown 1996; Serour 2006; Wen/Tarn 2001). The future of this kind of integrated treatment is made possible by solutions that comprise health services and information delivered or enhanced through secure information systems. This requires the development and use of an adequate process-oriented security analysis on information systems in healthcare (Tettero et al. 1997). Guaranteeing the protection of patient-related information and the healthcare information systems is becoming increasingly important (Anderson 1996a). Modern data security services in order to protect such sensitive information are even required by law (Hildebrand et al. 2006). This new technology must not, under any circumstances, endanger the privacy of patients and risk its large-scale acceptance by the general population (Choi et al. 2006).

1.1 Motivation

Dependable clinical information systems form the basis for the social and economic development of healthcare in the 21st century, particularly with regard to the quality of medical care.

Undependable systems would result in not only economic losses but also and more critically threats to the safety of patients. Because of their ethical, judicial and social implications, medical information requires extremely sensitive handling. This demands specific security solutions and guidelines for the appropriate use of information and communication technology (ICT) in public health systems on both technical and organizational level (Adams/Blandford 2005).

At present, it is generally assumed that pervasive changes, resulting from technological progress in the future, will be especially significant from an organizational perspective (Schneier 2004a). Forthcoming healthcare developments, particularly in Germany, suggest the vision of an integrated healthcare system providing seamless healthcare (Schweiger et al. 2006). This vision lays out that data is provided according to the principle of information logistics (Sunyaev et al. 2006). But the combination of different systems and infrastructure elements creates a very complex and almost unmanageable complete solution (Ash/Bates 2005). In order to deliver continuous and secure information flows along all medical treatment processes within the distributed healthcare information systems, specific security requirements for the medical sector are to be defined and implemented. From this it can be assumed that there are various possible security problems with different danger potentials (Gillon 1991). According to (Heeks 2006) such threats not only endanger IT systems but, more importantly, pose an indirect threat to the health of human beings. This implies a bridging between technology and human security requirements and assumes specific facts and their pendency according to the framing of the healthcare structures (Churches 2003). This leads to the question of whether German healthcare telematics is secure enough to satisfy requirements in areas such as privacy, safety, security and availability (Aljareh/Rossiter 2002).

It is generally agreed that security issues should be considered very early on in developing an IS process such as German healthcare telematics in order to avoid risks and to facilitate the success of the overall system. Addressing these special information security needs of the health sector, a security approach should accordingly take the unique operating environment in healthcare into consideration (ISO/FDIS 27799:2007(E) 2007). By their nature, health organizations operate in an environment where visitors and the public at large can never be totally excluded (LeRouge/Mantzana/Wilson 2007). In large health organizations, the number of people moving through operational areas is significant (ISO/FDIS 27799:2007(E) 2007). These factors increase the vulnerability of the information systems not only to physical threats but also to threats from personnel and administrative issues. The other unique healthcare characteristic is the array of factors to be considered when assessing these threats and vulnearbilities (ISO/FDIS 27799:2007(E) 2007).

Furthermore, the forthcoming health telematics infrastructure in Germany is the biggest telematics solution in the world, with an overall budget exceeding one and a half billion euros (gematik 2006q).

These factors exacerbate the need for a security analysis method that analyzes both the technical and social aspects of information security in a health environment (Bakker 2004; Bates/Gawande 2003; France 2004; Neame/Olson 2004; Smith/Eloff 1999; van der Bijl 2005; Win/Susilo 2006). “At present there are no guaranteed methods for securing the privacy of health information on systems and the resulting lack of trust presents a major challenge to widespread voluntary adoption of these systems for health-and-security critical information” (Kuhn et al. 2008).

On account of this and because of the current application concerns[1] about the reliability of healthcare telematics in Germany, this thesis explores a security analysis method for healthcare telematics and offers practical information to give valuable hints for future developments in the healthcare sector. This thesis also analyzes both the technical and social aspects of information and communication security in the healthcare sector by using the constructed security analysis method. On the basis of this method the current security status of healthcare telematics in Germany is analyzed and valuable suggestions for future developments in the healthcare sector are derived.

[1] 73 % of German citizens have serious reservations regarding the confidentiality of their personal health data because of the introduction of forthcoming and mandatory healthcare telematics infrastructure in Germany (Forsa, 2008).

1.2 Objectives of the Thesis

The purpose of this research is to develop a method for analyzing security issues in healthcare telematics. The application of the developed security analysis method is demonstrated on a security analysis of the German healthcare telematics. The HatSec (HealthcAre Telematics SECurity) method is used to identify possible security problems in German healthcare telematics and to evaluate the imposed trade-offs of the current security solution.

In order to pursue the main objective of this research, the following research questions are addressed:

1. *What are the characteristics of healthcare telematics with respect to security?*

Creating a security analysis method for information systems in a health environment requires an examination of general conditions in the healthcare sector and corresponding problems. In the next step the security requirements have to be collected. The analysis results will be consolidated within a catalogue of IS healthcare security characteristics. For this reason the first research question can be subdivided into the following questions:

1.1. What are the unique characteristics of the German healthcare system?

1.2. Which standardized communications mechanisms are healthcare information systems based on?

1.3. What are the common healthcare IS architecture types?

1.4. What are the key elements of healthcare telematics in Germany?

1.5. What are common risk and security issues of healthcare information systems like German healthcare telematics?

1.6. What are specific security requirements for healthcare telematics?

1.7. What are the characteristics of IS security approaches with respect to healthcare?

First, a description of German healthcare system is introduced in detail, including the concept, special characteristics, and key elements of the forthcoming German healthcare telematics infrastructure. Second, the specific security requirements for healthcare telematics are described in detail and summarized in a catalogue of IS healthcare security characteristics.

The third outcome of this question is an identification of relevant organizational and technical aspects affecting the specific healthcare security analysis. These characteristics demand specific security requirements for the appropriate use of information and communication technology (ICT) in public health systems on both technical and organizational level.

2. *What different types of security analysis methods can be identified in research and practice?*

This thesis incorporates parts of currently established security analysis methods into the design of a HatSec method. For this reason the IS security analysis approaches which are currently the most examined, discussed, and applied in both literature and practice have to identified. In a next step, the identified IS security analysis methods have to categorized and reviewed according to their suitability for the healthcare sector. Research question 2 can be subdivided into following questions:

2.1. What is the state of the art in IS security analysis approaches?

2.2. What are the different foci of the examined IS security analysis approaches?

2.3. What are the insufficiencies of existing IS security analysis approaches especially regarding their applicability in healthcare?

The study of the second research question describes state of the art of IS security analysis methods that are currently receiving attention both in scientific literature and practice. The aim of the literature review is to provide a structured overview of IS security analysis approaches and to structure the IS security research around a classification scheme that can be used in future research and practice. Such an aggregation and systematization of IS security analysis methods could not be identified during the literature research.

Moreover, the literature review and the examination of IS security approaches with respect to healthcare show insufficiencies with current IS security analysis approaches that lack techniques to analyze the technical and social aspects of information security in a healthcare environment. This fact again emphasizes the need for a security analysis method specific to healthcare telematics.

3. *What are the design elements and constructs of a security analysis method for healthcare telematics in Germany?*

The concept of method engineering methodology has to be applied and implemented in order to design a security analysis method for healthcare telematics. It has to be shown, which method elements are used to design the HatSec method. Furthermore, the design of the HatSec method has to be traceable and transparent. Research question 3 can be subdivided into following questions:

3.1. What are the principles of method construction?

3.2. What are the fundamental parts and elements of the methods?

3.3. What are the rules of assembling method fragments into a meaningful method?

3.4. What are the steps of the HatSec method?

3.5. What are the advantages of the HatSec method compared to existing IS security analysis methods?

The development of a security analysis method, its concept and its incorporation into the discipline method engineering are described as an answer to research question 3. Furthermore, the specific building blocks needed for the construction of the method are explained and analyzed. As a result an example of a security analysis method for healthcare telematics in Germany is expected. This example has been named HatSec.

The answer to this research question also provides a detailed overview of IS method engineering approaches in order to describe the concept of method engineering (ME). Through a literature review a formal description of methods is derived that can be used to describe methods in a basic way and transfer them to other fields of application. With the formal description of methods the process of understanding method engineering is facilitated both for the method user and its engineer. In this thesis the derived formal description of method engineering is used as a representation technique for the development and presentation of security analysis method for healthcare telematics. The described formal representation allows the HatSec method to be precisely understood regarding the usage of it as a model artifact and a re-interpretation of its syntactical elements (e.g., method elements, method chains and alliances, method fragments, method chunks and method components).

Furthermore, the last part of the answer on the research question three has to identify the advantages of the HatSec method in comparison to existing IS security analysis methods.

4. *What are the implications found when applying the method and which recommendations can be given for future healthcare telematics security trade-offs?*

To demonstrate the application of the constructed HatSec method the current security status of the German healthcare telematics has to be analyzed. It has to be shown, which security shortcomings of the German healthcare telematics can be discovered and resolved. Furthermore, it has to be shown, whether the developed HatSec method is practically applicable. Research question 4 can be subdivided into following questions:

4.1. How does the practical application of the HatSec method look like?

4.2. What are the current open security issues of the German healthcare telematics?

4.3. What practical implications can be derived for the further development of the German healthcare telematics from the security point of view based on the results of the practical application of the HatSec method?

The security analysis of the German healthcare telematics based on the constructed HatSec method is the answer on the last research question. The conducted practical application of the HatSec security analysis method has to show the suitability of the HatSec method to healthcare IS security issues. Furthermore, the current status of the security concept of the German healthcare telematics has to be analyzed and where necessary solutions for open security issues have to be provided.

The second part of this question identifies design proposals for the healthcare telematics security trade-offs in future.

1.3 Research Methodology

This section describes the research methodology used in this thesis. First, the theory of the design science approach is explained. Then the design science methodology is strictly applied during the construction and the practical application of the HatSec method, which is presented in the derived research design of this thesis. To conclude this section, the design theory of the developed artifact and its potential use in IS research is illustrated.

1.3.1 Design Science

Theories in information systems research always concern *artificial phenomena* (March/Smith 1995). Such theories are about artificially created organization systems and thereby used information systems. In IS research there are two different ways to deal with *artificial phenolmena*. On the one hand theories can be observed and analyzed and on the other theories can be created and designed (March/Smith 1995). The goal of IS theories is to understand and describe a reality (March/Smith 1995; Hevner et al. 2004). According to (Kaplan 1964), the process of understanding and describing a reality consists of two parts: *Discovery* and *Justification*[2]. At first a scientist develops a scientific predication (e.g., a theory or a model). In order to describe the predicted theory, the theory has to be conceptualized (e.g., via a specifically developed language). In the next step of the process the scientist tries to justify the predication (Frank 2000).

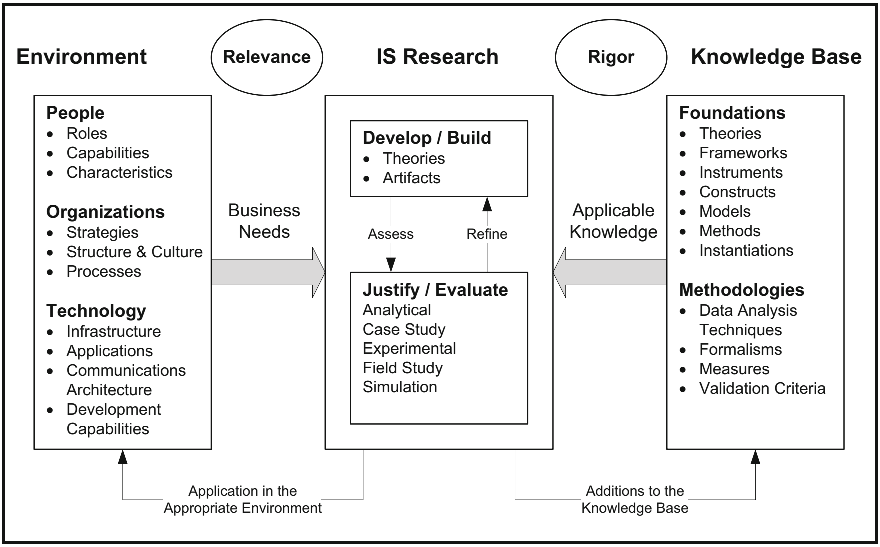

Figure 1: IS Research Framework for Design Science *(Source: (Hevner et al. 2004))*

(Hevner et al. 2004) designed a conceptual research framework for design science in the information systems field (Figure 1). Accordingly IS research is influenced by an *environment* and a *knowledge base* as direct research constraints. The research environment consists of three components: people, organizations, and technology. These three components have goals and tasks, define problems or explore new possibilities.

[2] (Hevner et al. 2004) use the terms *build* and *evaluate*.