SECURITY ANALYSIS OF THE HEALTH CARE TELEMATICS INFRASTRUCTURE IN GERMANY

Michael Huber, Ali Sunyaev and Helmut Krcmar
Chair for Information Systems, Technische Universität München, Germany

Keywords: Security analysis, Health Care Telematics, Electronic Health Card, Information Security Management Systems.

Abstract: Based on ISO 27001 for Information Security Management Systems, this paper introduces a newly developed security analysis approach, suitable for technical security analyses in general. This approach is used for a security analysis of several components and processes of the Health Care Telematics in Germany. Besides the results of the analysis, basics for further analysis and verification activities is given.

1 INTRODUCTION

In Germany, the *Electronic Health Card* (*eHC*) will replace the present health card as requested by law. By establishing the eHC, several improvements, such as cost savings, better ways of communication in the health care sector or the self-determination of the insured person concerning medical data, are supposed to be achieved (Schabetsberger et al., 2006).

The use of IT to administrate medical data of the insured, implicates the question, whether these systems are safe enough to satisfy requirements like privacy, safety, security and availability (Heeks, 2006). The data administrated by the eHC and its infrastructure is mosltly strictly confidential as it contains personal information about peoples state of health, course of disease and hereditary diseases (Lorence and Churchill, 2005). As for example insurance companies or employers would be highly interested in such information, the security measures of TI systems dealing with them have to be analysed in detail (Anderson, 2001).

Due to their ethical, judicial and social implications, medical information requires extremely sensitive handling. These aspects emphasise the need for a security method that evaluates the technical aspects of information security in a health environment. In this paper, we first introduce the health telematics infrastructure. After the introduction, an analysis approach based on ISO 27001 is introduced in chapter 3. The result of its application to several components of the health telematics infrastructure is presented in chapter 4. Chapter 5 concludes the paper and provides an outlook. The current security status of health care in Germany was evaluated and valuable hints for future developments in the health care sector could be derived.

The paper is based on a literature review (e.g. Computers & Security, Information Management & Computer Security, Information Systems Security, International Journal of Medical Informatics, Information Systems Journal, European Journal of Information Systems, International Journal of Information Security, security & privacy, Journal of computer security, ACM Transaction on Information and Systems Security und ACM Computing Surveys). The security analysis approach presented in this paper differs from other approaches due to the following aspects: Focus (health care sector; technical evaluation of security measures), being up-to-date (appliance of up-to-date techniques and standards) and regional distinctions (located in germany, regional and political conditions).

2 THE HEALTH TELEMATICS INFRASTRUCTURE

The present health card in Germany is a storage-only smart card, whereas the eHC will provide a microprocessor enabling services such as the ciphering or signing of information (Schweiger et al., 2007). This insurance card is actually used exclusively for administrative purposes such as identifying the insured person or accessing administrative data stored on the card

Huber M., Sunyaev A. and Krcmar H. (2008).
SECURITY ANALYSIS OF THE HEALTH CARE TELEMATICS INFRASTRUCTURE IN GERMANY.
In *Proceedings of the Tenth International Conference on Enterprise Information Systems - ISAS*, pages 144-153
DOI: 10.5220/0001684901440153

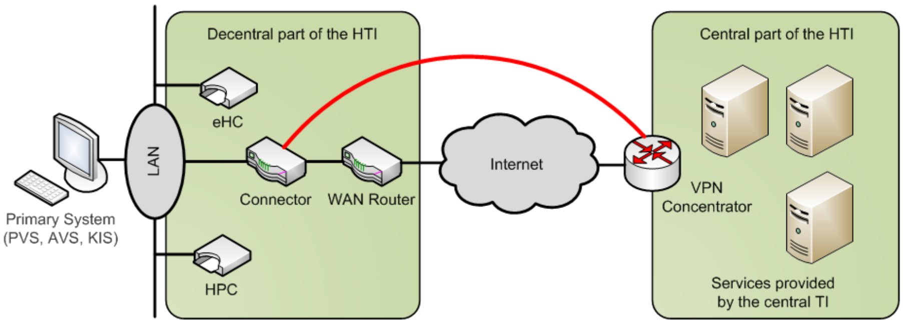

Figure 1: Schematic representation of the Health Telematics Infrastructure.

for accounting purposes.

Besides the eHC, there are also smart cards for health personnel, medics, chemists and various other professional categories, which need to interact with the eHC and its related infrastructure (these cards are called *Health Professional Cards*, shortened *HPC*).

The eHC as a smart card is only one part of the infrastructure required to implement the functionality demanded by law. The major part is represented by an IT system called *Health Telematics Infrastructure* (*HTI*) and its associated processes, both described in the following sections.

The given introduction has to be considered as a brief description of the major parts, functions and processes of the HTI. For a more detailed description, we refer to the public development documents by the Gematik mbH which can be found at the organisation's website[1]. Furthermore, a compact introduction to the eHC can be found in (Huber et al., 2008).

2.1 Functions and Stages of Expansion

The eHC and its associated infrastructure will be introduced in several steps with a growing amount of functionality and complexity. For the insured, the usage of some of the functionalities introduced by these steps is mandatory, the use of some other optional (Haux, 2005).

The first step of introduction will provide the eHC as a smart card with the ability to store the patients administrative data (for instance name, address, date of birth, insurance information, etc.). On its backside, the eHC provides a form, which enables the card to act as an europe-wide standardised health card. The acceptance of this step is mandatory for the insured.

The second step introduces the functionality to store prescriptions on the smart card, formally provided to the insured as a paper form. This step is mandatory for the insured as well.

Regarding the remaining steps three and four, the use of their functionality is optional. For these steps, it is planned to provide things like emergency-data, the documentation of the history of medication and an electronic dossier of the insured, partially stored on the smart card, partially provided by a centralised data processing center as part of the HTI.

2.2 Architecture

Figure 1 outlines the architecture of the HTI, which is divided into a central and a decentral part.

The central part consists of several services, which can be accessed by the insured and the service providers such as medics or hospitals. These services will be located and administrated in one or more central computing centres.

The decentral part of the HTI is located at the medical service providers. This part consists of the medical service provider's *LAN*, the *Connector*, *card readers* for eHC and HPC and the smart cards themselves. The connection between decentral and central part of the HTI is established by using a vpn connection over the internet, initialised by the medical service provider's Connector and accepted by a vpn concentrator located at the central part of the HTI.

Not part of either fraction of the HTI are the so called *Primary Systems*. These systems are software products, medical service providers use for storing their patients' records, for accounting purposes and various other tasks related to health care. Because of those components are being developed and maintained by third party companies, security aspects can not be supervised by governance and thus, they are by definition not part of the HTI. Nevertheless, these systems were considered in the security analysis from a general point of view, because they do store and administer sensitive medical data.

[1] http://www.gematik.de

3 A NEW SECURITY ANALYSIS APPROACH

According to (Gollmann, 2006), a technical security analysis is defined as a methodical, traceable analysis of an IT system concerning primarily its technical aspects.

Planning to perform a security analysis, it is advisable to base the used procedure on established standards and best practice approaches, so the analysis relies on a previously approved scaffold.

Regarding security analyses, there are many different solutions from activity catalogues to loose collections of analysis techniques and useful tools. Despite of each solution having its advantage in its dedicated domain, no appropriate standard or proceeding could be found to analyse the mentioned components in the way, the definition of (Gollmann, 2006) demands. Therefore, a new approach had to be developed, allowing to analyse the relating components from a technical point of view, using tools, methods and processes in a structured and traceable way.

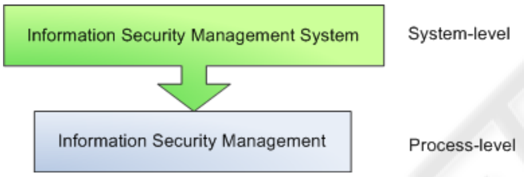
Information Security Management System
System-level
Information Security Management
Process-level

Figure 2: Levels of an Information Security Management System.

3.1 Information Security Management Systems

Although a new approach had to be developed, there are some standards which were used as its base. These standards apply to *Information Security Management Systems* (*ISMS*). These systems are used to implement and maintain IT security in organisations by coordinating various activities, processes and tools.

An ISMS contains two levels, a *System-level* and a *Process-level* as shown in figure 2. According to (BSI, Bundesamt für Sicherheit in der Informationstechnik, 2004), the Process-level contains several subprocesses such as development, planning, implementation, evaluation, and maintenance of IT security. The System-level in contrast is concerned with the orchestration of the Process-level's tasks. It contains matters like organisational structure, responsibilities, processes and resources.

3.2 ISO 2700x

Besides well known standards like the *BSI IT-Grundschutz*[2], *BS 7799-2* (BSI, British Standards Institution, 1999) or COBIT (ITGI, IT Governance Institute, 2007), there is a relatively new group of standards dealing with ISMS. This assembly of standards is called the *ISO/IEC 2700x* family and will contain at least seven standards. At the moment (november 2007), some standards of the 2700x family are already published, others are still under development.

ISO 2700x contains, respectively will contain standards for establishing and maintaining IT security. Therefore, it combines particular standards from simple vocabulary via ISMS requirements, risk management and management activities up to practical implementation guidelines. Thus, this family is or will be one of the most complete and comprehensive up-to-date compilations of standards regarding the ISMS issue.

3.3 The Plan-Do-Check-Act Approach of ISO 27001

One of the most important standards of the ISO 2700x family is the 27001 standard, which actually emerged from the British Standard 7799-2 (BSI, British Standards Institution, 1999). In this standard, fundamental processes to plan, establish, operate and maintain information security in organisations are described. The main scaffold to achieve these goals is represented by the *Plan-Do-Check-Act* approach (*PDCA*). This approach, as shown in figure 4, contains four steps, which are executed repeatedly.

In the first step of PDCA, an ISMS policy has to be established. Therefore, objectives, processes and procedures which are essential for managing risk and improving information security have to be set up in accordance with an organisation's objectives and policies.

[2] http://www.bsi.de/gshb/index.htm

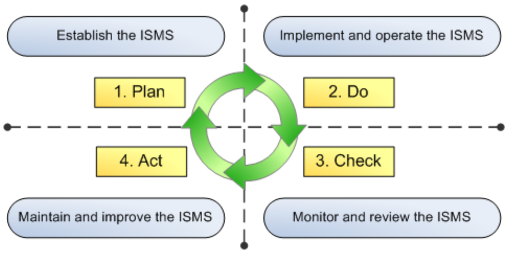
Establish the ISMS
Implement and operate the ISMS
1. Plan
2. Do
4. Act
3. Check
Maintain and improve the ISMS
Monitor and review the ISMS

Figure 4: The Plan-Do-Check-Act approach (PDCA).

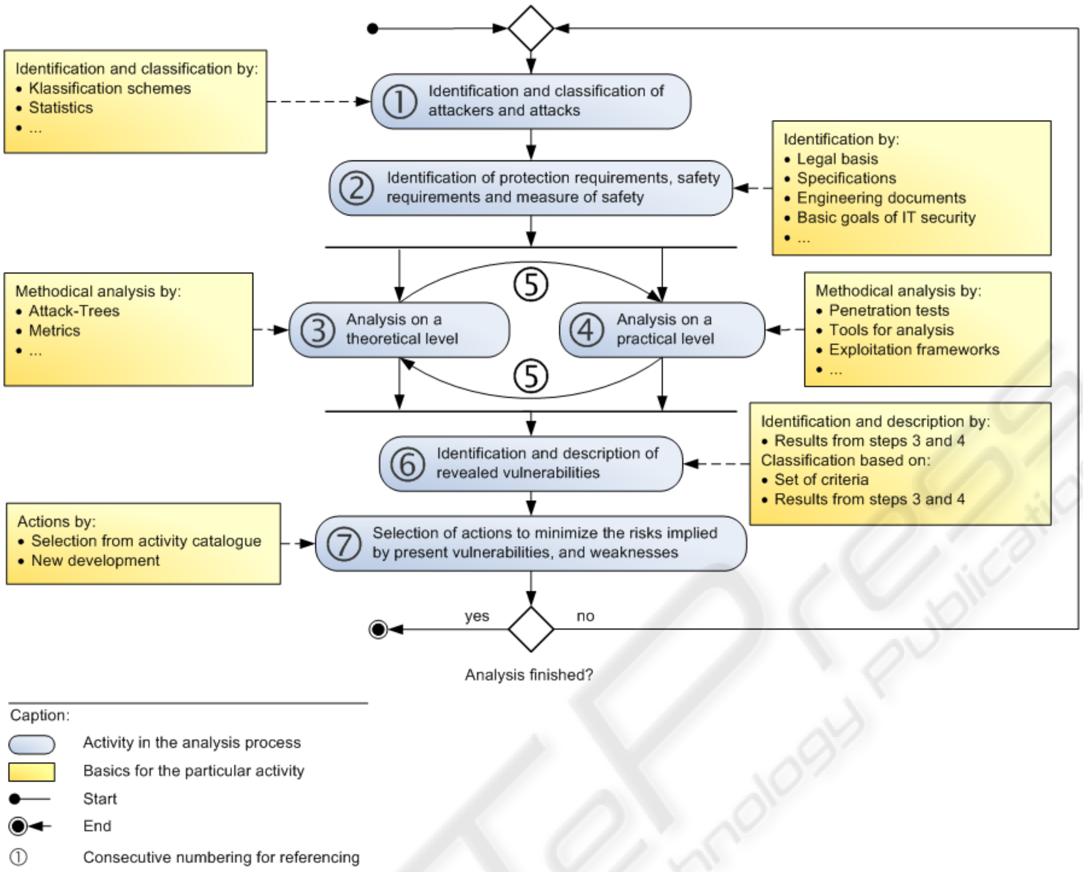
Identification and classification by:
• Klassification schemes
• Statistics
• ...
1 Identification and classification of attackers and attacks
Identification by:
• Legal basis
• Specifications
• Engineering documents
• Basic goals of IT security
• ...
2 Identification of protection requirements, safety requirements and measure of safety
Methodical analysis by:
• Attack-Trees
• Metrics
• ...
5
3 Analysis on a theoretical level
4 Analysis on a practical level
5
Methodical analysis by:
• Penetration tests
• Tools for analysis
• Exploitation frameworks
• ...
Identification and description by:
• Results from steps 3 and 4
Classification based on:
• Set of criteria
• Results from steps 3 and 4
6 Identification and description of revealed vulnerabilities
Actions by:
• Selection from activity catalogue
• New development
7 Selection of actions to minimize the risks implied by present vulnerabilities, and weaknesses
yes
no
Analysis finished?
Caption:
Activity in the analysis process
Basics for the particular activity
Start
End
① Consecutive numbering for referencing

Figure 3: The developed security analysis approach.

In a second step, the ISMS policy has to be implemented and operated. Therefore, the controls, processes and procedures set up in step one have to be implemented.

The third step measures the effectiveness and performance of the ISMS. The measurement results are reported to the management for review.

During the fourth step, corrective and preventive actions based on the results of step three and the review of further relevant information have to be taken.

3.4 From PDCA to Security Analysis

Based on the PDCA model, we developed a new approach for a technical security analysis. By building a new approach based on this model, various activities during a security analysis can be orchestrated in a reasonable manner. Furthermore, the repeated execution of the approach's steps provides a continuous feedback of the analysis results to accommodate the analysis activities. Figure 3 outlines the developed security approach.

The steps of the PDCA approach described in 3.3 are adopted as a scaffold to be filled with analysis tasks of the developed approach.

The first step of the approach contains the identification of possible attackers and attack types. The result of this step will be used later on to design possible attacks on the IT system. For achieving these results, statistics, common classification schemes and other resources can be used. Thus, the first step of the approach is quite analogue to the first step of PDCA where an analysis of possible threats takes place.

In the second step of the approach, the assets of the IT system, security and also legal requirements and finally security measures are being identified. This step goes par with actions of the *plan* and *do* steps of the PDCA approach. There, assets, requirements and measures are identified as well. The sources for the accomplishment of step two can be documents of the IT system's legal basis, results from a former risk analysis or just basic objectives of IT security in general.

The third and fourth step are both the central steps, where analysis activities actually take place. Step four contains activities of a theoretical character. This could be for example an Attack-Tree Analysis (cp. 4.4.5) or the application of proper metrics to measure security. The fourth step in contrast contains analysis activities in a practical way. This could include for example penetration tests, the use of one or more exploitation frameworks or the use of individual tools like port scanners, dedicated exploits, brute forcing tools, etc. These two steps are thus similar to the *check* step of the PDCA approach where the ISMS is being reviewed and tested.

The fifth step implements a synchronisation of the steps three and four. The results of each step are used to improve and complete the activities of the complementary step. The synchronisation of these steps results in a more complete and accurate analysis, as both, theoretical and practical activities are used and improve each other. This step has no analogy in the PDCA approach as it is a combination of two steps, which have no counterpart in the PDCA approach.

Step six is more or less optional as it just contains a recapitulation of the former steps results. If these are already well documented during the preceeding steps, step six can be skipped.

In step seven, activities are chosen to minimize the risks implied by the uncovered vulnerabilities and weaknesses. This step has its counterpart in the *act* step of the PDCA approach, where also measures are implemented to improve the ISMS.

3.5 Mapping the Analysis Approach to PDCA

Figure 5 shows the coherence of the PDCA approach and the developed security analysis approach. Both are executed repeatedly, and the activities of the analysis steps overlap with activities of the PDCA approach.

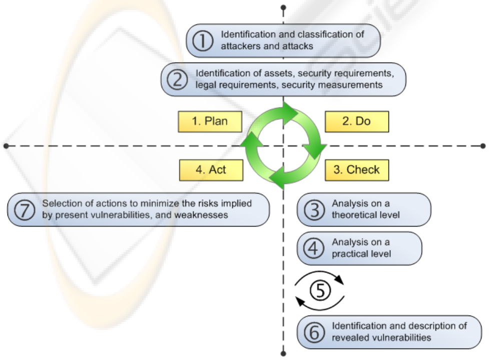
① Identification and classification of attackers and attacks
② Identification of assets, security requirements, legal requirements, security measurements
1. Plan
2. Do
4. Act
3. Check
⑦ Selection of actions to minimize the risks implied by present vulnerabilities, and weaknesses
③ Analysis on a theoretical level
④ Analysis on a practical level
⑤
⑥ Identification and description of revealed vulnerabilities

Figure 5: Mapping the developed approach to Plan-Do-Check-Act.

4 RESULTS OF THE ANALYSIS

4.1 Components an Documents Considered in the Analysis

The components considered in the security analysis are *eHC*, *Connector*, *Primary Systems*, *Card Readers* and the processes occurring during their interaction.

For the analysis, only publicly available documents were regarded. Of course, the analysis would be more complete, if also internal documents were considered, but by using only public sources, the security analysis is based on the same information level, any invader looking for an opportunity to attack this IT system is able to access. Furthermore, some internal development documents were marked as confidential at the point of analysis (november 2006 to november 2207) and thus could not be considered at all.

Altogether, the documents (SGB, 2007), (BDSG, 2003), (SigV, 2001), (SigG, 2001), (StGB, 2005), (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2007), (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2006a), (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2006b), (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2006c), (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2005b), (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2005a), (Neeb et al., 2004) have been considered for the analysis.

All Documents were at most dated to june 2007.

4.2 Identification and Classification of Attackers and Attacks

The identification and classification follows in large parts the indexing of (Schneier, 2004) and (Gerloni et al., 2004). The attackers were thereby classified by the criterions *available amount of time*, *know-how* and *available resources*. The attacks were divided into the topics *intention (criminal, publicity, etc.)*, *origin (internal/external)* and *technical basis* (Schneier, 2004). Furthermore, each attacker group and type of attack was brought into context with the eHC subject.

It emerged, that the biggest threats emanate from the groups *organised crime* and *cyber-terrorists* which seem to have the major interests and the largest financial resources.

4.3 Identification of Assets and Security Requirements

The identification of assets and security requirements was done by analysing public development documents, wordings which form the legal basis of the eHC and several basic IT security resources (cp. 4.1).

4.4 Analysis of the Components-Theoretical Level

4.4.1 Cross-component Analysis

The cross-component analysis was intended to analyse the processes, the mentioned components are involved in. Furthermore, the cross-component analysis included a critical review of the development documents from a security-based point of view.

Key for the Combination of Medical and Administrative Data. In (Neeb et al., 2004, p. 30)[3], it is mentioned, that security must not depend on the faith in one single person. In (Neeb et al., 2004, p. 20)[4] in contrast, a requirement can be found, which postulates, that the key for the combination of medical and administrative data of the insured, which are both stored separately, has to be kept by the ”Beauftrager fr den Datenschutz des Medizinischen Dienstes”, which obviously is represented by one single person.

Unauthorised Transfer of Medical Data. In (SGB, 2007, SGBV, 294a)[5], it is postulated, that under certain circumstances, medical data can be accessed by the insurance without approval of the insured. This exception is given by law, but conflicts with a general requirement mentioned in (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2006a, p. 63)[6], which says, that no one is allowed to access the medical data of an insured person without his or her approval. Although, this is a reasonable exception, it has at least to be communicated to the insured to fulfill another requirement found at (SGB, 2007, SGBV, 291a, para. 3)[7], demanding the insured to be told whatever happens with his medical data. These explanations can not be found in any of the considered documents.

Missing backup Method for Honoring Prescriptions. According to (Neeb et al., 2004, p. 19)[8], for every process in the HTI, there has to be at least one manually operated backup process. In (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2006b, p. 28)[9], there can be found one exception which combined with the following topic might result in severe problems concerning availability demands. There, the absence of an adequate backup process for honoring digital prescriptions is mentioned. Thus, an insured who has the prescription exclusively digitally on his eHC, has no opportunity to honor this prescription when the HTI is not available to the pharmacy. It is obvious, that this could lead to perilous situations, if prescriptions for immediately needed physics cannot be honored.

Possibility to Honor the Same Prescription Twice. If the availability drawback mentioned above would be resolved by strictly implementing the requirement of (Neeb et al., 2004, p. 19)[10] and thus establishing a manually operated backup process for honoring prescriptions, every insured would have on the one hand the digital copy of the prescriptions on his eHC, on the other hand a paper based copy to provide a manual backup process. This way, the insured could at first honor his or her digital prescription as usual and afterwards visit a pharmacy, where the HTI is not available due to technical problems for example. There, the insured could honor the paper based prescription, offending several requirements concerning accountability and non-repudiation[11].

Unassigned Assumption about the Security Implied by the used ”Zone-Concept”. The HTI and its related systems are divided into several zones. This division is made, to allow a discrete view on every zone concerning it security. As mentioned in (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2007, p. 32), each of these zones is considered as a closed area. However, each of these zones is related to others using a physical connection. Wherever there is a physical connection, there is also the possibility of (unauthorized) traffic between these zones, even if the chance for this kind of traffic might be very unlikely due to protection measures. Nevertheless, if there is the possibility of (unauthorized) traffic, it is not feasible to consider each of these zones for its own and even classify them differently.

[3] cp. requirement 004.So.A.AS in (Huber et al., 2008)

[4] cp. requirement 001.Vt.A.AS in (Huber et al., 2008)

[5] cp. requirement 010.So.A.AS in (Huber et al., 2008)

[6] cp. requirement 002.Vt.A.AS in (Huber et al., 2008)

[7] cp. requirement 011.So.A.AS in (Huber et al., 2008)

[8] cp. requirement 002.Vf.A.AS in (Huber et al., 2008)

[9] cp. requirement 008.Vf.K.AS in (Huber et al., 2008)

[10] cp. requirement 002.Vf.A.AS in (Huber et al., 2008)

[11] cp. requirements 003.Zu.A.AS, 004.Zu.A.AS and 005.Zu.A.AS in (Huber et al., 2008)

Thus, it should be contemplated, whether it might be reasonable to expand the view and consider the interaction between zones as well. Furthermore it might be reasonable to classify each interconnected zone the same, concerning security issues.

Adjustment of Minimum Standards happens Infrequently. As mentioned in (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2007, p. 28), the minimum security standards to be implemented on the HTI have to be adjusted annually. According to statistics of CERT[12], in the first quarter of 2007, there have been already 2,176 vulnerabilities announced. Regarding the estimated amount of more than 8,000 uncovered vulnerabilities during one year, a shorter period for adjusting the minimum security standards could improve security.

Inadequate Assumption about the Security of the Systems inside the HTI. In (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2006b, p. 60) it is mentioned, that all IT systems within the vpn provided by the HTI are considered to be secure. This argument is for example used to justify the missing authentication concerning the connection to the time servers of the HTI. As it is a fact that there are no completely secure IT systems[13], this argument is not acceptable. Also IT systems controlled and maintained by the HTI itself are vulnerable for example to malware, social engineering attacks, and so on.

Inconsistent with the claim cited above, in (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2007, p. 32), it is noted, that it is not possible to completely avoid threats and that there will continuously emerge new threats.

Security by Obscurity. In (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2007, p. 246), the Gematik claims, that *security by obscurity* is not a proper approach securing IT systems. Nevertheless, the software used for eHC purposes is classified as highly confidential in the same document. This classification results from parts of the software being intellectual property of the developing companies. Of course, copyright issues have to be regarded in the eHC environment as well, but also Shannon's maxime and Kerckhoff's principle[14] should be considered.

Thus, at least these parts of the eHC related IT systems, which contain security relevant processes, should be published completely and not kept secret to ensure intelectual property.

4.4.2 Analysis of the Connector

Imprecise Specification of the Blacklist Management. In the security concept of the Gematik, it is defined, that each Connector has to validate the certificate of the vpn concentrator of the central part of the HTI[15]. In this context, blacklists are used to identify Connectors with revoked certificates, which have to be updated periodical (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2007, p. 63). Besides this definition, no further information about implementation and handling of blacklists can be found in any of the considered documents. One of the most important issues is, where the Connector retrieves the blacklist information from. they can obviously not be provided by a server inside of the HTI, as fetching the blacklist information would come along with connecting to a potentially insecure vpn concentrator. Furthermore, there are several authentication requirements concerning the blacklist service, which have obviously not been considered yet. If insufficient authentication is used, an attacker could claim to be a blacklist-server and thus provide fake blacklists containing some or even all vpn concentrators of the HTI. Establishing such an attack, the HTI would not be reachable any more because of all of its vpn concentrators being blacklisted by an attacker.

Imprecise Specification of the Trusted Viewer Interface. According to (SigG, 2001, 2, no. 11 respectively 17, para. 2) and (SigV, 2001, 15, para. 1c, 2a and 2b) the Connector has to provide a trustworthy component - a so called *Trusted Viewer* component - , which enables the verification of signatures and the signed content. There are two possibilities of implementing this component. On the one hand, the Connector can contain a build in Trusted Viewer device, on the other hand, a Trusted Viewer component can be included as a separate component accessing an adequate Connector interface over the LAN.

Concerning the implementation of the Trusted Viewer and its interface, conflicting details can be found in the specification document (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2006b). On the one hand, it is postulated, that every Connector has to implement an interface for the Trusted Viewer no matter if it has a built in Trusted Viewer component or not (cp. (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2006b, p. 21)), on the other hand, the

[12] http://www.cert.org/stats

[13] cp. (Huber et al., 2008, p. 10)

[14] cp. requirement 002.So.A.AS in (Huber et al., 2008)

[15] cp. fig. 1

Connector has to implement the Trusted Viewer interface only if it does not contain a Trusted Viewer component on its own (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2006b, p. 45 and p. 136).

Security Issues Concerning the Communication with the Trusted Viewer. Between Connector and Trusted Viewer, all communication has to be secured by SSL according to (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2007, p. 172)[16], (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2007, p. 137)[17] and (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2006b, p. 137)[18]. In (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2006b, p. 137), it is mentioned, that the Trusted Viewer will most likely be implemented as a separate piece of software. Thus it would reputedly not be a security improvement to provide the this component with an own identity. According to this, the Trusted Viewer will de facto have no own identity which implies, that authentication between Connector and Trusted Viewer will be if at all one-sided, supporting man-in-the-middle attacks.

Nevertheless, in case there would be a two-way authentication, it might be possible, to use fake certificates for a man-in-the-middle attack between Connector and Trusted Viewer. So far, it is not specified, how the Trusted Viewer should verify the Connector's certificate and vice versa. Fourthermore it is not specified what happens, if a man in the middle attack between Connector and Trusted Viewer is established with fake certificates. Will the user be prompted that the certificate is fake? Where will he be prompted? How can be assured, that a user does not ignore the warning?

The worst case of a successful man-in-the-middle attack according to this issue could for example be the forgery of prescriptions.

A possible man-in-the-middle attack scenario based on the weakness described above can be found at (Huber et al., 2008, p. 73)

Security Issues Concerning the Communication with the Primary System. The problems illustrated in 4.4.2 can partially be adopted for the communication between Primary System and Connector. In none of the regarded documents, there can be found any requirement concerning an authentication between these two components besides the generally postulated use of SSL for the communication between components in the decentral part of the HTI (cp. (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2007, p. 172)[19], (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2007, p. 137)[20] and (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2006b, p. 137)[21]). If there will be an authentication between these two components, it probably would only be one-sided, due to the lack of a requirement demanding the Primary System to provide its own identity. The missing or just one-sided authentication enables the establishment of man-in-the-middle attacks between Connector and Primary System.

Even if there was an authentication between Primary System and Connector, at least the Primary System could not verify the Connectors identity. Therefore, the Primary System would have to verify the identity by using some kind of service, provided by the HTI. According to (Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2007, p. 177), the direct access of the HTI by a Primary System is strictly forbidden, and the Connector itself does actually not provide a service like this as well.

The worst case of a successful man-in-the-middle attack according to this issue could for example be the illegal retrieval of sensitive medical data of an insured person.

4.4.3 Analysis of the Primary System

Insufficient Classification of the Data Processed. Acoording to (Neeb et al., 2004, p. 21), the security level of the data processed by a Primary System is classified as low or medium. The requirements of these levels are allegedly covered by the security measures of an actual Primary System. According to the classification of IT-Grundschutz[22], the abuse of the concerning data would result amongst others in the following:

- the abuse would have only marginal legal consequences
- the effects on the social position and the financial circumstances of the person concerned would be insignificant
- the tolerable downtime of the Primary System would be 24 hours

[16] cp. requirement 005.In.K.AS in (Huber et al., 2008)

[17] cp. requirement 011.Vt.K.AS in (Huber et al., 2008)

[18] cp. requirement 026.In.K.AS in (Huber et al., 2008)

[19] cp. requirement 005.In.K.AS in (Huber et al., 2008)

[20] cp. requirement 011.Vt.K.AS in (Huber et al., 2008)

[21] cp. requirement 026.In.K.AS in (Huber et al., 2008)

[22] http://www.bsi.de/gshb/index.htm

- the financial loss of the institution using the Primary System would be tolerable

It is obvious, that the tolerable downtime of systems in the healthcare sector is in most cases not as long as 24 hours. Hospitals definately can not afford downtimes of their IT systems as long as 24 hours. Furthermore, the abuse of private, medical data of an insured can result in severe consequences - for example the anamnesis of a person in the hands of his or her employer or insurance company.

Unassigned Assumption about the Presence of Security Measures Provided by Present Primary Systems. According to (Neeb et al., 2004, p. 21), the security measures used in a present Primary Systems are sufficient to assure the postulated level of security for the processed data, which is classified as *normal* based on the categorisation of IT-Grundschutz[23].

To verify this claim, some of the major manufacturers of Primary Systems have been asked wheter they provide for example encryption of sensitive data or role based and password protected user access. 4 of 17 addressed companies answered and confirmed to provide some kinds of security measures in their products. So on the one hand, the claim has been verified, but on the other hand, the question comes up why the remaining companies did not respond at all and whether this behaviour is related to providing security features or not.

In contrast to the four companies providing security features in their products, the designee for data protection and freedom of information in Germany, Peter Schaar claims, that the present Primary Systems frequently do not offer any access control or encryption features (cp. (facharzt.de, 2005)).

4.4.4 Analysis of the Card Reader

As the used card reader is a *Secure Interoperable ChipCard Terminal*(SICCT) standardised, self-contained piece of hardware, its development is not part of the eHC development process and thus it would be no benefit to analyse it in detail. The terminals are being analysed during their development and certification process. Thus, the card terminals were only considered from a general point of view in the present work, whereas no weaknesses could be revealed. Due to its own digital certificate, the communication between other components and the card reader can be secured by a strong authentication. Furthermore, the card reader is sealed physically, so manipulation attempts can be detected easily.

Nevertheless, a practical analysis of this components might be interesting as thus, for example implementation deficiencies could be uncovered. As mentioned in 4.5, no card terminal was actually available for analysing activities, so these actions have to be done in future work.

4.4.5 Attack-Tree Analysis

As one tool of step three in the developed analysis approach, an Attack-Tree Analysis has been made to identify the most likely and easy attacks. Within the analysis, Attack-Trees for each of the components despite of the Primary System have been made. The Primary Systems were excluded from this analysis step due to the different kinds of available Primary Systems. There is no standardised Primary System due to the freedom of each manufacturer to implement a Primary System in his favourite way.

The result of the Attack-Tree analysis were two large Attack-Trees for the Connector and the card termiinal including over 600.000 attack-scenarios each.

The Attack-Trees can be used for further work, when the related components are present. Concerning the work in (Huber et al., 2008), it emerged, that attacks on a technical level are mostly very expensive or out of scale regarding the expenditure of time. As also some non or semi-technical ways to achieve an attackers goal have been included in the Attack-Tree Analysis for completeness, it showed up, that the most likely attacks are the ones using bribing, blackmailing or spying out confidential information like access data. These attacks in turn are typical for attackers belonging to the groups of organised crime and terrorism as mentioned in 4.2.

4.5 Analysis of the Components-Practical Level

At the beginning of the analysis in november 2006, it was planned to have some prototypes of the concerning components for analysing purposes within a few weeks. Unfortunately, just until the end of the analysis process, no hard- or software components usable for practical tests were available, mainly due to delays within the development process. Thus, none of the steps, planned for practical analysis activities could be executed and none of the revealed issues could be approved by further practical tests.

5 CONCLUSIONS AND OUTLOOK

In the course of the present work, a new approach was developed, to fit the needs of a security analysis from a technical point of view. This approach based on ISO

[23] http://www.bsi.de/gshb/index.htm

27001, was used to analyse the components Connector, Primary System, Card Terminal and some of their interaction processes wihtin the HTI. As a result of the analysis, 14 deficiencies could be revealed, including weaknesses, inconsistent and conflicting development documents and violation of security demands.

For future work, the analysis offers various starting points such as the constructed Attack-Trees or the revealed weaknesses which can and should be verified in practice as soon as the considered components are physically available for testing purposes.

REFERENCES

Anderson, R. (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley & Sons, 1 edition.

BDSG (2003). Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970).

BSI, British Standards Institution (1999). BS 7799-2 1999 Management von Informationssicherheit : Teil 2: Spezifikation fr Informationssicherheits-Managementsysteme.

BSI, Bundesamt für Sicherheit in der Informationstechnik (2004). Studie zu ISO-Normungsaktivitten ISO/BPM - Anforderungen an Information Security Management Systeme.

facharzt.de (2005). Datenschutzbeauftragter Schaar zur eCard: Es gibt keine 100prozentige Sicherheit. Interview von facharzt.de mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) Peter Schaar am 21.09.2005. *facharzt.de*.

Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (2005a). Gematik Fachmodell. Version 0.9.

Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (2005b). Gesamtarchitektur - Kryptographische Ziele der Telematik. Version 1.0.

Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (2006a). Einführung der Gesundheitskarte - Gesamtarchitektur. Version 0.2.0.

Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (2006b). Einführung der Gesundheitskarte - Konnektorspezifikation. Teil 1 - Allgemeine Funktionen und Schnittstellen des Konnektors. Version 0.6.0.

Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (2006c). Einführung der Gesundheitskarte - Spezifikation Infrastrukturkomponenten: Zeitdienst. Version 1.0.0.

Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (2007). Übergreifendes Sicherheitskonzept der Telematikinfrastruktur. Version 1.9.0.

Gerloni, H., Oberhaitzinger, B., Reier, H., and Plate, J. (2004). *Praxisbuch Sicherheit für Linux-Server und Netze*. Carl Hanser Verlag, München Wien.

Gollmann, D. (2006). *Computer Security*. Wiley, 2nd edition.

Haux, R. (2005). Health information systems - past, present, future. *International Journal of Medical Informatics*, 75:268–281.

Heeks, R. (2006). Health information systems: Failure, success and improvisation. *International Journal of Medical Informatics*, 75:125–137.

Huber, M., Sunyaev, A., and Krcmar, H. (2008). Arbeitspapier 32 - Technische Sicherheitsanalyse der elektronischen Gesundheitskarte. Technical report, Technische Universität München, Lehrstuhl für Wirtschaftsinformatik.

ITGI, IT Governance Institute (2007). Cobit 4.1.

Lorence, D. and Churchill, R. (2005). Incremental adoption of information security in health-care organizations: implications for document management. *Information Technology in Biomedicine, IEEE Transactions on*, 9(2):169–173.

Neeb, J., Bunz, H., and Biltzinger, P. (2004). Erarbeitung einer Strategie zur Einfhrung der Gesundheitskarte - Sicherheitsanforderungen.

Schabetsberger, T., Ammenwerth, E., Andreatta, S., Gratl, G., Haux, R., Lechleitner, G., Schindelwig, K., Stark, C., Vogl, R., and Wilhelmy, I. (2006). From a paper-based transmission of discharge summaries to electronic communication in health care regions. *International Journal of Medical Informatics*, 75:209–215.

Schneier, B. (2004). *Secrets and Lies : Digital Security in a Networked World*. Wiley.

Schweiger, A., Sunyaev, A., Leimeister, J., and Krcmar, H. (2007). Information systems and healthcare xx: Toward seamless healthcare with software agents. *Communications of the Association for Information Systems*, 19:692–709.

SGB (2007). *Sozialgesetzbuch*. DTV-Beck.

SigG (2001). Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) - Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 3 Abs. 9 des Gesetzes vom 7. Juli 2005 (BGBl. I S. 1970; änderung durch Art. 4 G v. 26.2.2007 I 179 zukünftig in Kraft).

SigV (2001). Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) - Signaturverordnung vom 16. November 2001 (BGBl. i S. 3074), geändert durch Artikel 2 des Gesetzes vom 4. Januar 2005 (BGBl. I S. 2).

StGB (2005). *Strafgesetzbuch*. DTV Deutscher Taschenbuch Verlag.