SECURITY ANALYSIS OF THE GERMAN ELECTRONIC HEALTH CARD'S PERIPHERAL PARTS

Ali Sunyaev, Alexander Kaletsch, Christian Mauro and Helmut Krcmar
Chair for Information Systems, Technische Universität München, Boltzmannstraße 3, 85748 Garching, Germany

Keywords: Security Analysis, Electronic Health Card, Health Care Telematics.

Abstract: This paper describes a technical security analysis which is based on experiments done in a laboratory and verified in a physician's practice. The health care telematics infrastructure in Germany stipulates every physician and every patient to automatically be given an electronic health smart card (for patients) and a corresponding health professional card (for health care providers). We analyzed these cards and the peripheral parts of the telematics infrastructure according to the ISO 27001 security standard. The introduced attack scenarios show that there are several security issues in the peripheral parts of the German health care telematics. Based on discovered vulnerabilities we provide corresponding security measures to overcome these open issues and derive conceivable consequences for the nation-wide introduction of electronic health card in Germany.

1 INTRODUCTION

During the next years in Germany the present health insurance card will be replaced by the new electronic health card (eHC) (Sunyaev et al., 2009). The introduction tends to improve the efficiency of the health system and the patients' rights (Bales, 2003, p.5). In order to reduce costs in the public sector and to create a homogeneous communication basis a nationwide system is created – the health care telematics infrastructure (TI). The eHC will not only contain administrative data but also detailed information about the patient and his treatments. These pieces of information, covered by the obligation of secrecy in the physician-patient relationship and highly protected by law (Berg, 2004, pp.412-413), will now be stored in central databases in order to improve services for the patients.

Digitizing this information bears risks (Mandl et al., 2007). Insurance companies, banks, employers or marketing firms are only a few of several organizations highly interested in health data (Huber et al., 2008, p.1). Getting to know people's state of health, etiopathology or congenital diseases could give them a remarkable competitive advantage. Each individual whose data are stolen could get into serious trouble (Blobel, 2004). As a consequence patients could possibly get significant issues when taking out a loan or trying to find insurance (Anderson, 2001). Furthermore, one's reputation could get tarnished when the wrong pieces of own sensitive medical information becomes publicly accessible (Schneider, 2004).

This paper is based on extensive laboratory experiments and on a detailed review of gematik's specifications (detailed information about health care telematics specifications can be found at the organization`s website - http://www.gematik.de). Based on ISO 27001 for Information Security Management Systems Standard and BSI Security Guidelines (BSI, 2004), we focus on security issues in the peripheral parts of the telematics system and verify them in practice. These concerns are categorized and possible solutions are presented in this paper.

After the introduction of the German health care telematics and its peripheral parts, the configurations of the laboratory and the physician`s practice are described in section 4. The results of the performed security analysis and possible consequences are presented in sections 5 and 6. Section 7 summarizes our key findings and provides recommendations for future work in this area.

Sunyaev A., Kaletsch A., Mauro C. and Krcmar H. (2009).
SECURITY ANALYSIS OF THE GERMAN ELECTRONIC HEALTH CARD'S PERIPHERAL PARTS.
In *Proceedings of the 11th International Conference on Enterprise Information Systems - Information Systems Analysis and Specification*, pages 19-26
DOI: 10.5220/0001854000190026

2 THE GERMAN HEALTH TELEMATICS INFRASTRUCTURE

As requested by law (SGB V, 2007, § 291b) the business organisation gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) was created in order to lead the introduction of the electronic health card in Germany. gematik created all specifications used in the health care telematics infrastructure.

A nationwide telematics project was set up in order to introduce the eHC in Germany. The health care telematics infrastructure is divided in the central part, which consists of data centres with central databases and the peripheral parts, which are at the different renderers of service – e.g. in physician's practice, hospitals or pharmacy (gematik, 2008e, p.8). Both will be connected via a VPN tunnel. At the client's side the connection is established from the so-called connector and at the central part accepted by the VPN concentrator (gematik, 2008e, p.8). The connector allows the primary systems and the card reader to interact, which are both components of the peripheral part as well.

The electronic health card has the same proportions as a normal plastic card, e.g. like a credit card. On the front side there are individual-related information, a picture of the insurant and the microchip. Also some recognition features like braille, the name and logo of providing insurance company are placed there. On the back there is the European health insurance card (EHIC) (Drees, 2007, p. 1).

The eHC is a smartcard, which means it has its own microprocessor with its own instruction set (Caumanns et al., p.343). This distinguishes it from the present health insurance card in Germany, which is only a memory card. Not only administrative data about the insurant is stored on the card, but also medical data like electronic prescriptions. The insurant can decide whether information for medical emergencies, pharmaceutical documentations, insurants receipts and medical reports will be stored and if whether directly on the eHC or on central databases (Neuhaus et. al., p.1).

3 PRIMARY SYSTEMS IN THE PERIPHERAL INFRASTRUCTURE

Primary systems are types of software which offer the eHC's functionality to the renderers of service, e.g. practice or hospital information systems. This software is usually installed on normal personal computers which are used in the reception and treatment rooms. As these are standard PCs also standard services and programs are offered, e.g. email and internet.

These facts make the primary systems' computers a highly interesting target for attackers who want to achieve access to patients' data (Sunyaev et al., 2008b, p.3). In experiments and reviews attacks were subdivided into three different target categories: users, hardware and software. Hardware can be stolen or hidden, keyloggers (e.g.: http://www.keyloggersdirect.com/ index.php?products) could be attached. Users could be blackmailed, corrupted or spied on. But the most likely scenario is that software could be manipulated. This could be done by trojans, viruses or spyware which infiltrate systems by accessing websites, emails or through other security vulnerabilities (Sunyaev et al., 2008a).

In order to handle these issues detailed security knowledge is needed, not only when setting up the systems, but also when using them. Practice personal has to be trained to use these systems securely (Schneider, 2004).

A big issue is that there is no present standard for secure practices. gematik shifts them into the service consumer tier (SCT) and in this vein they place the responsibility for the primary systems on the renderers of service. It is defined that SCT's systems are not part of the telematics infrastructure, but only use them (gematik, 2008d, p.71). This means that there are no rules defined for them at gematik (gematik, 2008c, pp.134-138) and there is no separate security concept as well. Also gematik states that it should not be a problem that primary systems can be unsupervised for up to 30 minutes (gematik, 2008b, p.22).

4 LABORATORY'S/PHYSICIAN'S PRACTICE CONFIGURATION

The laboratory consists of three main components: the connector, the card reader and the primary system. This is a standard configuration which is used in every physician's practice in Germany.

The connector is the central component in the peripheral part of the telematics infrastructure. If the primary system is to access an electronic health card placed into the card reader it has to call a connector's function in order to proceed. It is not

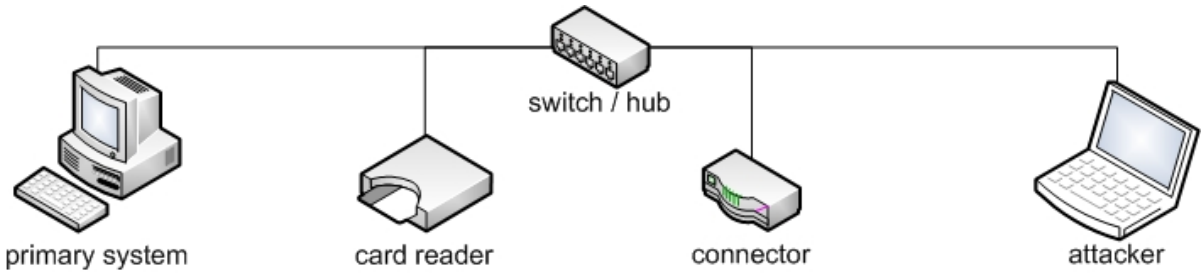

Figure 1: The laboratory's configuration (Source: own Figure).

possible to establish a direct connection between card reader and primary system. So if data have to be transferred into the central part of the health care telematics infrastructure only the connector can do so. The connector used in this test is part of the Futro S400 series by Siemens in version V1.07R4.5; hpscV1.07R4_build_2493_R13198.

The card reader Cherry SICCT Terminal in version 10037 is another component attached to the laboratory's network. At the card reader the electronic health card and the health professional card (HPC) can be inserted (Mauro et. al., 2008). It also has a keypad where numeric codes can be entered in order to gain access to these cards.

A usual personal computer was used as primary system which had an AMD Opteron Processor 144 with 1.81 GHz and 2.5GB RAM. Windows XP with Service Pack 2, DocConcept 8.2, DocConnect and Siemens Trusted Viewer are installed on the computer. With the practice software the connector's functions can be initialized in order to use the electronic health card's functionality. The functions allow the user to read administrative data, electronic prescriptions and emergency information stored on the eHC.

These components are normally connected by LAN via a standard switch. But when doing special network analyses this switch was replaced by a repeating hub (Figure 1).

A laptop acting as an attacker joined to the network was used for some experiments. It is equipped with a Core 2 Duo T74002x 2.16GHz processor and 2.0GB RAM. While running Windows Vista Business with Service Pack 1 as operating system, it has none of the tools which are normally used to connect to the electronic health card. But it has several tools installed which allow analyzing the network's traffic. Also an own client for the connector was developed.

In order to validate the results of the experiments tests were performed in a real physician's practice. A treatment room was used for the trials. Within these an attacker accessed the LAN by using a port behind a small commode. Figure 2 shows which hardware was found by analyzing the network and which of them were accessible.

As the practice has a well secured network, it was not possible to break into the windows domain which connected the practice computers, but it was possible to access the telematics hardware. That means that the attacker did not have access to any PC with practice software, but it was able to control the connector and with it every card reader in the practice.

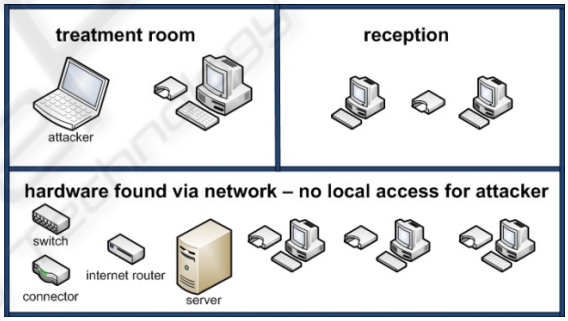

Figure 2: The Practice Network from the Attacker's Point of View (Source: own Figure).

5 THE NETWORK TRAFFIC ANALYSES AND ITS CONSEQUENCES

While analyzing the data sent over the network, all components were connected via a repeating hub. That means in contrast to a normal switch all data are sent to every attached device. Now, the use of tools like Wireshark (http://www.wireshark.org) or EttercapNG (http://ettercap.sourceforge.net) makes it possible to get a good impression of the network's dataflow.

The results show:

a) The connection between the card reader and connector is fully encrypted.

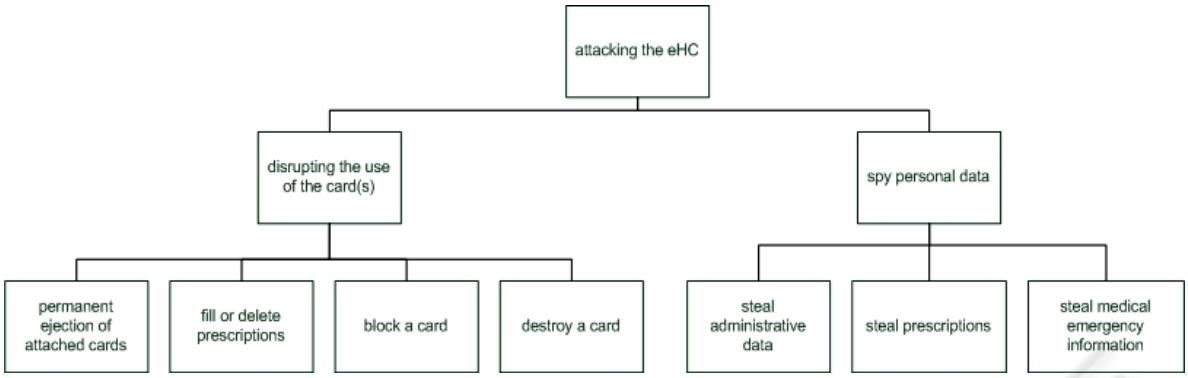

Figure 3: Attack Tree (Source: own Figure).

b) There is no encryption between the primary system and the connector.

The encrypted connection between the card reader and the connector is enforced by gematik (2008a, p.21). The missing encryption between primary system and connector is caused by a lack in the specification of gematik (2008b, pp.16-17; 2008c, p.297), which defines the use of a TSL encryption between connector and primary system as optional. As there is no encryption in the implementation all requests and answers from the primary system and the connector can be captured and looked at in plain text by a third party. This security issue is known at gematik (2008b, p.270), but it is labelled as a residual risk. It is left to the readers to decide if the possible theft of their private data, which includes administrative data as well as medical emergency information or electronic prescriptions, is an acceptable threat.

In addition to the fact that there is no encryption between the primary system and the connector there is also no enforced authentication. That means everyone can access the functions offered by the connector. Using PHP (http://www.php.net) as programming language in combination with the principles of extreme programming (Beck, 2000) an own client was implemented in order to fulfil derived attack scenarios. The program can be controlled via different interfaces, e.g. with a command line tool or a web interface.
There are three modes offered by the program:

- The “direct”-mode allows calling functions instantly.
- The “wait”-mode tries every three seconds to find an attached card and then sends the request.
- The “listen”-mode registers at the connector and waits for an event, which is triggered when a card is attached and then the request will be send to the connector.

The client is able to call all functions at the connector that could also be used by DocConnect 8.2. So it can act like a normal primary system and keeps itself quite well covered.

Abusing the functions provided by the connector leads to some strong attack scenarios.

6 ATTACKING THE GERMAN ELECTRONIC HEALTH CARD

The attack tree shown in Figure 3 denotes that the attacks can be classified into disrupting and spying types. The utilisation can be interrupted when permanently ejecting all cards, which get attached to a card reader. The deletion of prescriptions stored on the electronic health card is as possible as the blocking or destruction of the card itself. An attacker can also steal administrative data, prescriptions and medical emergency information stored on eHCs.

All attacks are based on the following scenario: The attacker can gain access to the physician’s practice network, e.g. through hacking the WLAN or just plugging into a socket. Also another common procedure is needed in order to call some functions: The physician unlocks his own health professional card (HPC) with his personal identification number (PIN) in the morning and locks the card in the evening, which means the card is ready to use for the whole day.

Table 1 shows the specifications of the functions that will be abused in the following in order to attack the German electronic health card.

Table 1: Connector's Functions that can be abused.

Permanent-Card-Ejection	
PIN needed:	None
supported card types:	All
Connector's function:	EjectCard
gematik's specification:	gematik 2008e, 200f; chapter 5.4.3.3.6
Delete or fill all prescriptions	
PINs needed:	HPC practice's PIN
Supported card types:	EHC
Connector's function names and their gematik's specification	• ReadVO: gematik 2008h, 73ff; chapter 6.2 • DeleteVO: gematik 2008h, 79ff; chapter 6.4 • DispenceVO: gematik 2008h, 76ff; chapter 6.3
Block a Card	
PINs needed:	PIN to change
Supported card types:	EHC, HPC
Connector's function:	ChangePin
gematik's specification:	gematik 2008e, 204f; chapter 5.4.3.3.8
Destroy a Card	
PINs needed:	PUK for locked PIN
Supported card types:	EHC, HPC
Connector's function:	UnblockPin
gematik's specification:	gematik 2008e, 209f; chapter 5.4.3.3.12
Steal private data from electronic health card	
PINs needed:	HPC practice's PIN
Supported card types:	• EHC
Connector's functions and their gematik's specification:	• ReadVSD: gematik 2008f, 52ff; chapter 7.1 • ReadVO: gematik 2008h, 73ff; chapter 6.2 • ReadNFD: gematik 2008g, 31ff; chapter 6.2

6.1 Permanent-Card-Ejection

The Attack. There are two ways to realize a permanent ejection. On the one hand it is possible to constantly call a function that ejects a card, e.g. every three seconds. On the other hand the registration to an event handler at the connector is possible. Then an event is triggered and immediate response can take place. Regardless of the way used it is not possible to attach any card to a card reader anymore (Figure 4).

A Possible Solution. As there is no additional benefit created when ejecting a card via the network this functionality could be easily removed. It is fully satisfying when a card can only be ejected locally at the card reader.

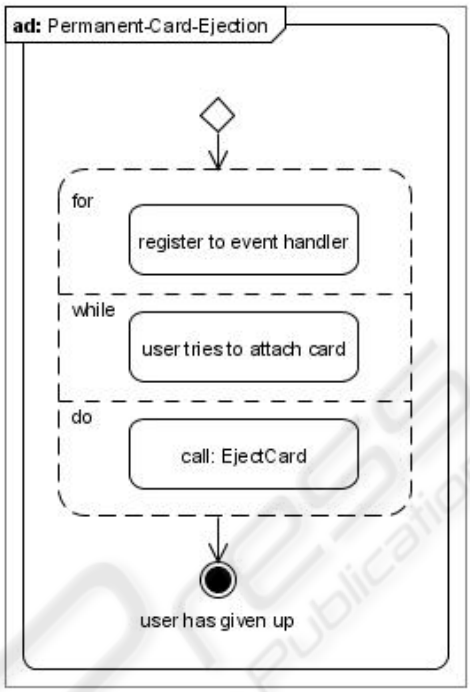

Figure 4: Activity Diagram - Permanent Card Ejection (Source: own Figure)

6.2 Fill or Delete Prescriptions

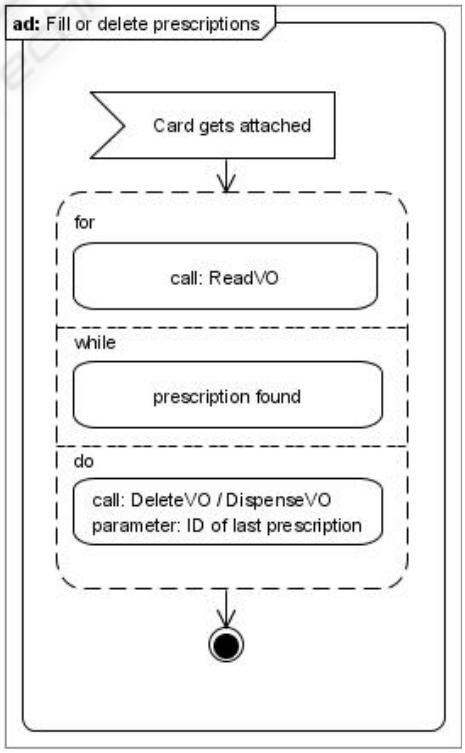

Figure 5: Activity Diagram - Fill or Delete Prescriptions (Source: own Figure).

The Attack. In order to delete or fill a prescription its Object ID is needed which is received from the connector in a first step. After the receipt the function for deleting or fulfilling the prescription can be called (Figure 5). As there is a maximum capacity of eight prescriptions on every electronic health card this procedure will repeat at most eight times then every prescription will be dispensed or deleted.

A Possible Solution. For writing or changing a prescription on an eHC the physician's signature personal identification number is needed. The usage of this PIN while deleting or dispensing electronic prescriptions would suppress a fully automated function call as described above. Therefore, the attack would not be possible anymore, because every action had to be authorized by a human on the card reader.

6.3 Lock a Card's PIN

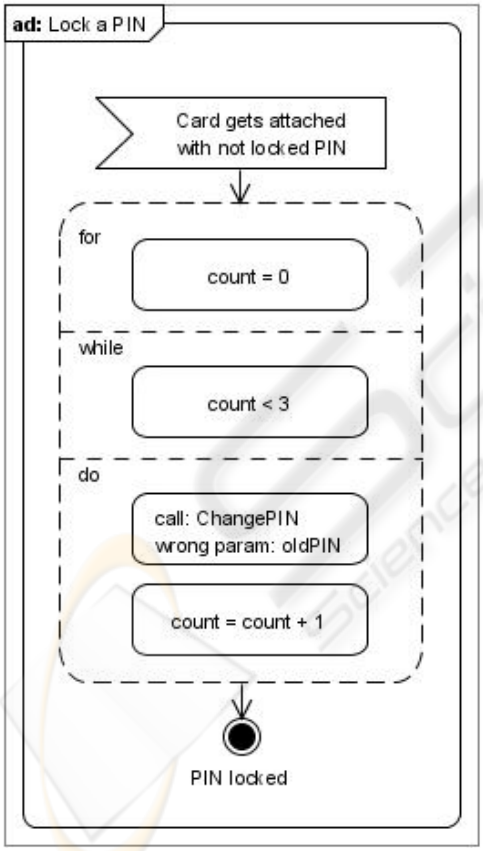

Figure 6: Activity Diagram - Lock a PIN (Source: own Figure).

The Attack. There is a connector's function which enables the user to change a card's PIN remotely. A PIN can be entered wrong three times before it is locked. This means abusing this functionality could block the card (Figure 6). In an experiment it took 350ms to call this function. That means within about one second a PIN can be locked.

A Possible Solution. As this function does not generate additional value and would be probably used very rarely, e.g. only initially, the function should be removed. It would be sufficient to be able to change the PIN only directly at the card reader.

6.4 Destroy a Card

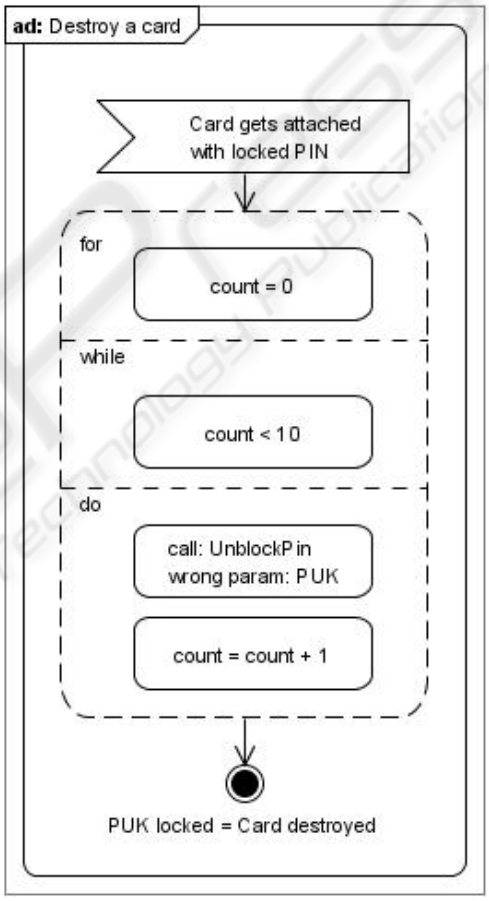

Figure 7: Activity Diagram - Destroy a card (Source: own Figure).

The Attack. When a PIN is locked, a function can be called which allows the user to unlock the PIN. As a parameter the personal unlocking key (PUK) is needed. It can only be used ten times before it becomes finally locked. So using this function with a wrong PUK for ten times on a locked PIN would lead to a locked PIN and a locked PUK. Not being able to unlock the PIN means that the card cannot be used anymore. The card is destroyed (Figure 7).

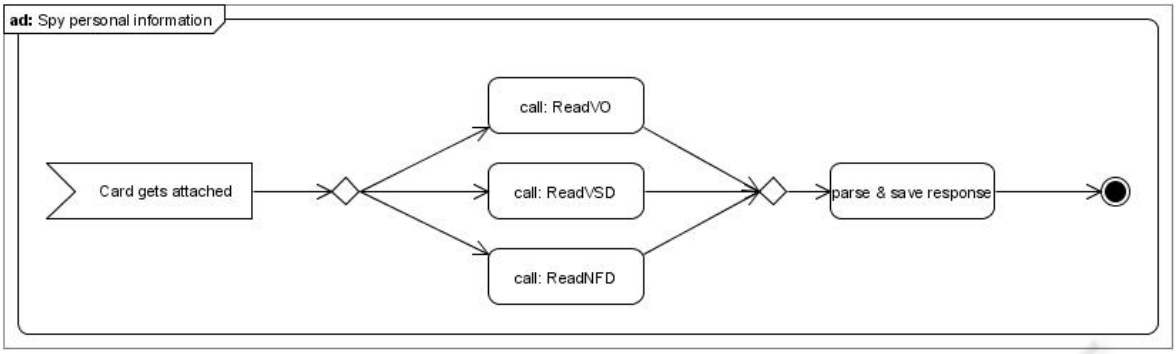

Figure 8: Activity Diagram - Spy Personal Information (Source: own Figure).

A Possible Solution. The case of a locked PIN should be an exception. So there is no real need to implement a function like this in the connector and the primary systems. Furthermore, it would be sufficient if the PIN can be unlocked directly on the card reader.

6.5 Spy Personal Information

As the thefts of *administrative data*, *electronic prescriptions* and *emergency information* work the same way they are all combined in Figure 8.

The Attacks. When a card is inserted, connector's functions can be called in order to steal administrative data, electronic prescriptions and emergency information (Figure 8). As response a XML file will be provided which can be easily parsed and saved. The collection of these data (see Table 2) gives the attacker private information about the patient and detailed knowledge about his state of health.

Table 2: Summary of Content that can be spied out.

administrative data	– insurant id – given name, family name – birthday, sex – full address – information about insurance coverage and the insurance company
electronic prescriptions	– date of issue – patient's and physician's administrative data – information about the prescription – name of medication – name of pharmacy – usage information
emergency information	– (past) diseases – medication (and incompatibility) – attending physician – persons to be notified – other notices (free text)

A Possible Solution. As these functions are essential they cannot be removed. Protecting them with a separate PIN would delay practice work. So only a secure connection between the primary system and the connector, which is encrypted and authenticated, will solve the problem.

7 CONCLUSIONS AND OUTLOOK

Table 3: Attacks tested in Laboratory and Practice.

Attack	Consequences
Permanent-Card-Ejection	Practice system cannot be used during an attack. This results in a work delay.
Delete all prescriptions	Patient looses all his prescriptions; this is very annoying, especially if he has had prescriptions form different physicians on the card.
Block Card	Unlocking with PUK is possible, but at first the PUK has to be send to the insurant by mail.
Destroy Card	The insurant has to order a new card at his insurance company.
Spy administrative data	Name, address, birthday and insurance data get stolen.
Spy prescriptions	Data which gets stolen can be used to deduce the recent state of health.
Spy emergency information	Information about medication intolerance, previous diseases and other highly private data gets stolen.

In the course of the present work critical security issues in the German electronic health card's system have been discovered. These have been tested in a laboratory and have been verified in a real physician's practice (Table 3). Therefore the following statements must be made:

– Patient's private and very sensible data stored on the German electronic health card are not secure and it is possible to steal them, because the card is used in an unsecured environment.
– Also manipulations of the eHC and health professional card are feasible.

Possible solutions to these security treatments have been given. It is undeniable that the connection between the connector and primary system must be encrypted and authentication has to be enforced. The given solutions are not extremely expensive or complicated. Also, it should be possible to implement them in time. In this regard rules and scenarios for primary systems should also be included in the specification in order to create a nationwide standard for practice information technology.

For future work, the components should also be exposed to further penetration tests. E.g. man in the middle attacks should be launched between the TLS encrypted network parts and hardware manipulations should be tried.

REFERENCES

Anderson, R. J., 2001. *Security Engineering: a Guide to Building Dependable Distributed Systems*. 1st. John Wiley & Sons, Inc.

Bales, S., 2003. *Die Einführung der Telematik im Gesundheitswesen als Herausforderung für die Weiterentwicklung der Patientenrechte in Deutschland*. [Talk] Bonn: gematik. Available at: http://www.dimdi.de/dynamic/de/ehealth/karte/downloadcenter/veroeffentlichungen/vortraege/bagh-bonn-bal-031107.pdf [Accessed 9 September 2008].

Beck, K., 2000. Extreme programming eXplained: embrace change. Reading, MA: Addison-Wesley.

Berg, W., 2004. Telemedizin und Datenschutz. *Medizinrecht*, 22 (8), pp. 411-414.

Blobel, B., 2004. Authorisation and access control for electronic health record systems. *International Journal of Medical Informatics*, Vol. 73 Nr. 3, pp. 251-257.

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

Caumanns, J. et al., 2006. Die eGK-Lösungsarchitektur Architektur zur Unterstützung der Anwendungen der elektronischen Gesundheitskarte. *Informatik-Spektrum*, 29 (5), pp. 341-348.

Drees, D., 2007: The Introduction of Health Telematics in Germany. In: European Commission Directorate General Information Society, *Information Security Solutions Europe/SECURE 2007 Conference*. Poland, Warsaw 25 27 September 2007. Vieweg: Wiesbaden.

Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008a. *Spezifikation eHealth-Kartenterminal*. Version 2.6.2.

Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008b. *Spezifisches Sicherheitskonzept der dezentralen Komponenten - Einboxkonnektor-Szenario*. Version 0.9.0 Kandidat.

Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008c. *Übergreifendes Sicherheitskonzept der Gesundheitstelematik*. Version 2.3.0.

Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008d. *Gesamtarchitektur*. Version 1.4.0.

Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008e. *Konnektorspezifikation*. Version 2.8.0.

Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008f. *Facharchitektur Versichertenstammdatenmanagement (VSDM)*. Version 2.6.0.

Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008g. *Facharchitektur Daten für die Nie Notfallversorgung (NFDM)*. Version 1.7.0.

Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008h. *Facharchitektur Verordnungsdatenmanagement (VODM)*. Version 1.5.1.

Huber, M., Sunyaev, A. & Krcmar, H., 2008. Security Analysis of the Health Care Telematics Infrastructure in Germany. In: INSTICC, *International Conference on Enterprise Information Systems 2008*. Spain, Barcelona 12-16 June 2008.

Mandl, K.D. et al., 2007. Indivo: a personally controlled health record for health information exchange and communication. *BMC Medical Informatics and Decision Making*, Vol. 7 Nr. 25.

Mauro, C. et al., 2008. A Proposed Solution for Managing Doctor's Smart Cards in Hospitals Using a Single Sign-On Central Architecture. In: HICSS 41, *Hawaii International Conference on System Sciences*. Hawaii, Big Island 7-10 January 2008.

Neuhaus, J., Deiters, W. & Wiedeler, M., 2006. Mehrwertdienste im Umfeld der elektronischen Gesundheitskarte. *Informatik-Spektrum*, 22 (5), pp.332-340.

Schneier, B., 2000. Secrets and lies: digital security in a networked world. John Wiley: New York.

SGB V, 2007. *Sozialgesetzbuch*. Fünftes Buch. DTV-Beck.

Sunyaev, A., von Beck, J., Jedamzik, S. & Krcmar, H., 2008a. *IT-Sicherheitsrichtlinien für eine sichere Arztpraxis*. Volume 1. Berlin: Shaker.

Sunyaev, A. et al., 2008b. Bewertung und Klassifikation von Bedrohungen im Umfeld der elektronischen Gesundheitskarte. In: Gesellschaft für Informatik, Informatik 2008. Germany, Munich 8-13 September. Gesellschaft für Informatik: Munich.

Sunyaev, A. et al., 2009. Analysis of the Applications of the Electronic Health Card in Germany. In*:* WI 2009, *Proceedings of Wirtschaftsinformatik 2009*, Austria, Vienna 25-27 February 2009.