

Ali Sunyaev

Lehrstuhl für Wirtschaftsinformatik Prof. Dr. Krcmar
Technische Universität München

27.09.2007

Die elektronische Gesundheitskarte und die Sicherheit: Ein Vorschlag zur entwicklungsbegleitenden Sicherheitsevaluation aus Anwendersicht

Gesundheitstelematik und eGK

Bremen, 27. September 2007

Munich Competence Center eHealth (MCCeH)

- Munich Competence Center eHealth (www.ehealth-tum.de)



Die Lehrstühle für Wirtschaftsinformatik ([Prof. Dr. Krcmar](#)) und Medizinische Informatik ([Prof. Dr. Kuhn](#)) der Fakultät für Medizin und der Fakultät für Informatik der Technischen Universität München, bündeln ihre Fachkompetenz in den Bereichen Informations- und Kommunikationstechnologie (IKT) für Entwurf, Implementierung, Evaluation und Wirtschaftlichkeit von eHealth Lösungen.

- Sicherheitsanalyse des Telematikpilotprojektes zur elektronischen Gesundheitskarte im Raum Ingolstadt



Einführung

- Das größte Telematik-Projekt der Welt.
- Schrittweise Einführung der elektronischen Gesundheitskarte in Deutschland.



Die neuen Gesetzesanforderungen des §291a erfordern eine umfangreiche Funktionalität und Komplexität der Gesundheitskarte

Identifikation

Name, Geburtsdatum	ALT
Anschrift	ALT
Geschlecht	NEU
Unterschrift	ALT
Lichtbild	NEU

Medizinische Informationen

Medizinische Notfalldaten	NEU
Elektronischer Arztbrief	NEU
Pointer zur elektronischen Patientenakte	NEU
Arzneimitteldokumentation	NEU
Zusätzliche Daten von oder für Versicherte	NEU

Administration

Einheitliche Krankenversichertennummer	NEU
Ausstellende Krankenversicherung	ALT
Kassenärztliche Vereinigung	NEU
Versichertenstatus für Versichertengruppen	ALT
Zuzahlungsstatus	NEU
Tag des Beginns des Vers.-Schutzes	NEU
Ggfls. Fristablaufdatum Versicherungsschutz	ALT
Dokumentationsfeld für widerrufbare Einwilligung des Versicherten	NEU
Löschung einzelner medizinischer Daten auf Verlangen, ggfls. Zugriffsbeschränkungen	NEU
Einzug der Karte bei Kassenwechsel o. ä.	NEU
Daten über in Anspruch genommene Leistungen und vorläufige Kosten	NEU
Umfassende Informationspflicht (Funktionsweise, Daten)	NEU
Behandlung im europ. Ausland (E-111)	NEU

Sicherheit

Verschlüsselung	NEU
PIN	NEU
Digitale Signatur	NEU
Zugriff nur mit Signaturkarte (HPC o. SMC)	ALT
Auslesung einzelner Daten auf bestimmte Nutzerkreise beschränkt	NEU
Authorisierung des Zugriffs durch den Versicherten (PIN) außer bei Notfalldaten	NEU
Protokollierung der letzten 50 Zugriffe zur Datenschutzkontrolle	ALT
Zugriff von Versicherten auf von ihnen oder für sie eingestellte Daten	NEU

E-Rezept

Elektronisches Rezept	NEU
-----------------------	-----

ALT

Bisher schon auf der KVK

NEU

Komplett neue Funktionalität

- Der **administrative Teil der Information** wird **von den Krankenkassen** auf die Karte gebracht

- Die **medizinischen Daten** sind **freiwillig** und werden **durch Leistungserbringer** bzw. die Versicherten eingebracht

- Die **Infrastruktur** für alle Daten **muss mit der Karte harmonisiert** werden

Quelle: GMG

Die neuen Gesetzesanforderungen des §291a erfordern eine umfangreiche Funktionalität und Komplexität der Gesundheitskarte

Sicherheit

Verschlüsselung	NEU
PIN	NEU
Digitale Signatur	NEU
Zugriff nur mit Signaturkarte (HPC o. SMC)	ALT
Auslesung einzelner Daten auf bestimmte Nutzerkreise beschränkt	NEU
Authorisierung des Zugriffs durch den Versicherten (PIN) außer bei Notfalldaten	NEU
Protokollierung der letzten 50 Zugriffe zur Datenschutzkontrolle	ALT
Zugriff von Versicherten auf von ihnen oder für sie eingestellte Daten	NEU

Aktueller Stand

- Aktuelle Probleme
 - Verzögerung
 - Akzeptanzprobleme von Seiten der Leistungserbringer (Ärzte) und der Leistungsempfänger (Patienten)
 - Negative Medienberichterstattung
 - Unsicherheit in der Bevölkerung
 - ➔ Schaffung der Transparenz



- Testregion Ingolstadt: zum 1. Oktober 2007 offizieller Beginn des Feldtestes

Problemstellung

- Unter Berücksichtigung der spezifischen Situation im Testgebiet gilt es festzustellen, inwiefern die in den bisherigen Spezifikationen festgelegten Sicherheitsanforderungen ausreichend und praktisch umsetzbar sind.
 - Welche Eigenschaften der zentralen technischen, organisatorischen und ökonomischen Kriterien können für eine derartige Sicherheitsanalyse identifiziert werden?
 - in der Modellregion Ingolstadt nutzergruppenspezifisch (Patienten, Leistungserbringer, Kostenträger) systematisiert werden?
 - Wie können die definierten Sicherheitsanforderungen in der Testregion Ingolstadt umgesetzt werden? Wie ist die dafür notwendige Prozessreorganisation in der Modellregion zu gestalten?
 - Wie kann die Verteilung der analysierten Sicherheitsanforderungen auf die verschiedenen Teilkomponenten der Gesundheitstelematikinfrastruktur im Raum Ingolstadt definiert werden? Wie wird die soziotechnische und ökonomische Vorteilhaftigkeit von Sicherheitskonzepten abgeschätzt?

Fachzeitschrift	Zusammenfassung	Detaillierte Untersuchung	Von Interesse
ACM Computing Surveys	1	1	1
ACM Transactions on Information and System Security	38	1	0
Bank Accounting & Finance	2	1	0
Communications of the ACM	54	8	1
Computers & Security	92	32	2
European Journal of Information Systems	4	1	1
HMD Praxis der Wirtschaftsinformatik	7	5	0
IEEE Security & Privacy	21	4	0
IM Information Management & Consulting	3	1	0
Information and Organization	2	1	0
Information Management & Computer Security	33	9	1
Information Systems Journal	13	2	2
Information Systems Management	12	1	0
Information Systems Security	41	9	0
Information Security Management	29	1	0
Internal Auditor	21	1	0
International Journal of Network Management	28	1	0
International Journal of Medical Informatics	9	2	0
Journal of Computer Security	7	1	0
Journal of Management Information Systems	4	1	0
Journal of Research and Practice in Information Technology	2	1	0
Strategic Finance	7	1	0
Andere	11	10	2
Summe Fachzeitschriften	441	95	10
Wissenschaftliche Arbeiten von Firmen/Verbänden/Behörden	19	19	2
Dissertationen/ Diplom-/ Masterarbeiten/universitäre Working Paper	39	39	5
Konferenzen/Workshops	13	4	1
Summe gesamt	512	157	18

Kontext Evaluation

1. Rahmenbedingungen ermitteln

2. Ziele definieren

3. Entwicklung eines Evaluationsrahmens

4. Kriterien definieren

Nutzergruppen

ökonomische

organisatorische

technische

5. Kennzahlen zur Evaluation bilden

8. Feldzugang gewinnen

7. Vorgehen festlegen

6. Soll-Zustand definieren

Prozess Evaluation

9. Felduntersuchung

10. Externes Material sammeln

Analyse

14. ökonomische

13. organisatorische

12. technische

15. Nutzergruppen

11. Ist-Zustand dokumentieren

Produkt Evaluation

16. Sicherheitsanalyse des Gesamtsystems und dessen Teilkomponenten

17. Dokumentierte Evaluation und Handlungsempfehlungen

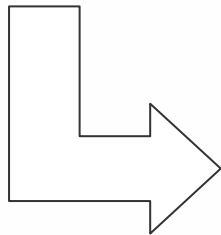
18. Abschätzung der ökonomischen, technischen und organisatorischen Vorteilhaftigkeiten von Sicherheitskonzepten

Evaluationsvorbereitung

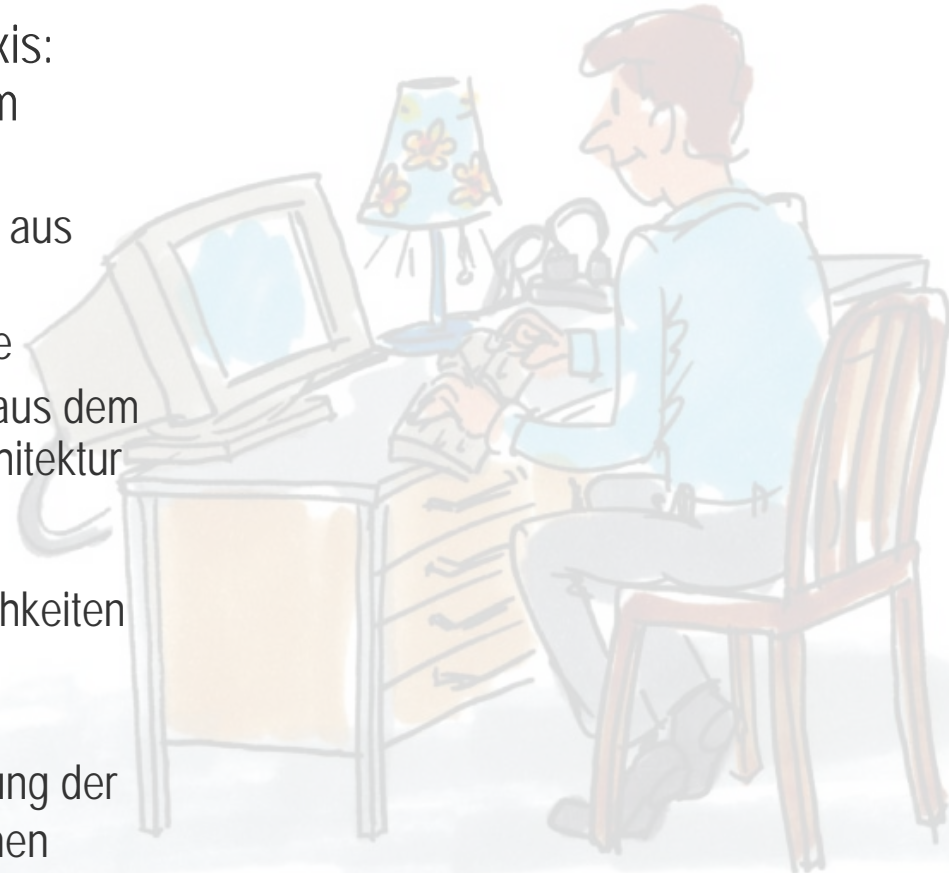
Danke für die Aufmerksamkeit

Nächste Schritte – „kontrolliertes Hacking“

- Nachbildung einer Referenz-Arztpraxis:
sicherheitsrelevante Angriffe in einem kontrollierten Umfeld
 - Ein Praxisverwaltungssystem (PVS) aus dem Bereich der Primärsysteme
 - Ein Prototyp eines Konnektors sowie
 - Ein Prototyp eines Kartenterminals aus dem dezentralen Bereich der Gesamtarchitektur



- Evtl. Lösungsmöglichkeiten bei vorhandenen Schwachstellen
- Subjektive Bestätigung der Erfüllung der technischen Sicherheitsanforderungen



Nächste Schritte – „kontrolliertes Hacking“

- Folgende Ansatzpunkte für Angriffe sind hierbei vorstellbar:
 - a. *Praxisverwaltungssystem*
 - Angriff auf möglicherweise unzureichend gesicherte Eingabemasken (vor allem vor dem Hintergrund, dass es sich nach derzeitigen Angaben um ein webbasiertes System handeln wird)
 - Informationsgewinnung über Patientendaten mittels versteckter Kanäle (ungewollter, versteckter Informationsaustausch über das Dateisystem)
 - Angriffsmöglichkeiten durch etwaige Implementierungsfehler der Schnittstellen zum Konnektor
 - Angriffe auf direkte Kommunikation mit Mehrwertdiensten etc. die direkt mit der Telematik Infrastruktur, durch den Konnektor getunnelt, stattfinden
 - b. *Konnektor*
 - Unterbinden der Verfügbarkeit für das PVS durch geeignete Angriffe (Konkret z.B. Syn-Flooding etc.)
 - Unterbinden des Verbindungsaufbaus zur Telematik Infrastruktur durch geeignete Angriffe (Konkret z.B. Syn-Flooding, DNS Spoofing, ...)
 - Verkehrsflussanalysen, um z.B. Zuordnung von Telematik-Dienstzugriffen zu Patienten herzustellen
 - Angriffe auf mögliche Implementierungsfehler der durch die Gematik spezifizierten Protokolle durch die Hersteller
 - Angriffe auf Updatefunktionalität der Firmware
 - Angriff / Umleitung / Manipulation der Trusted Viewer Komponente
 - c. *Kartenterminal*
 - Angriffe auf mögliche Implementierungsfehler der durch die Gematik spezifizierten Protokolle durch die Hersteller
 - Unterbinden der Verfügbarkeit hinsichtlich des Zugriffs durch den Konnektor (Siehe Vorgehen Konnektor)
 - Angriffe auf Updatefunktionalität der Firmware
 - Angriffe durch manipulierte Karten (vor allem hinsichtlich der Verfügbarkeit)

Nächste Schritte – „kontrolliertes Hacking“

d. *Verbindungen zwischen den 3 Komponenten*

- Angriffe auf die verwendeten kryptographischen Protokolle (zumindest deren voraussichtliche Unmöglichkeit erläutern)
- Man-In-The-Middle Angriff, um die eingesetzten kryptographischen Mechanismen evtl. zu umgehen
- Verkehrsflussanalysen, um z.B. Zuordnung von Telematik-Dienstzugriffen zu Patienten herzustellen
- Session Hijacking in irgendeiner Form

e. *Generelle Angriffsideen*

- Versuch die Daten auf der Karte zu verändern (vor allem eRezept)
 - Angriff auf die Anonymität der Daten. Konkret: Zuordnung von Informationen jeglicher Art zum zugehörigen Patienten
 - Wiedereinspielungsangriffe in jeglicher Hinsicht
 - Mehrfacheinlösung von eRezepten
 - Evaluierung ob und welcher Schaden durch loggen von PVS Eingaben / Ausspionieren der PIN erzeugt werden kann
-
- Auf Basis der erzielten Ergebnisse werden bei vorhandenen Schwachstellen Lösungsmöglichkeiten erarbeitet, andernfalls die Erfüllung der Sicherheitsbedürfnisse bzw. die Konformität zu IT Sicherheitsstandards aus unserer Sicht bestätigt.

(Die verletzten Sicherheitsziele werden nicht separat zu jedem Angriff aufgeführt. Einige Angriffe beziehen sich auf mehrere oder alle Sicherheitsziele.)

Nächste Schritte – organisatorische Sicherheitsaspekte

- Unter Berücksichtigung der spezifischen Situation im Testgebiet, gilt es festzustellen inwiefern die in den bisherigen Spezifikationen festgelegte organisatorische Sicherheitsanforderungen ausreichend und praktisch umsetzbar sind. Folgende Problemstellungen sind denkbar:
 - a. komplexere Abläufe
 - o mehr und aufwändigere Arbeitsschritte z.B. bei der Ausstellung eines Rezepts
 - o zusätzliche Aufgaben durch das neue System z.B. Wartung, Kontrolle der Sicherheitsmaßnahmen, Nacherfassung der Daten nach einem Systemausfall
 - b. unzureichend spezifizierte Abläufe
 - o z.B. in Bezug auf die Nutzung von HBA und eGK
 - c. unzureichend festgelegte Zugriffsrechte für die durchzuführenden Aufgaben
 - o z.B. ungenügende Zugriffsrechte für Angestellte der Leistungserbringer
 - d. Probleme bei der Umsetzbarkeit der organisatorischen Maßnahmen
 - o zu hoher Zeitaufwand
 - o fehlendes Know-How
 - o zu große Einschränkung der Benutzbarkeit
 - o unzureichende Möglichkeiten die Einhaltung zu kontrollieren
- → Erhebung von Sicherheitsanforderungen für das Prozessmodell des Kartenhandlings in der Testregion Ingolstadt

