Sichere Speicherung von Patientendaten mittels Chipkarten

Stefan Rass · Raphael Wigoutschnigg · Peter Schartner

Alpen-Adria-Universität Klagenfurt
{stefan.rass | raphael.wigoutschnigg | peter.schartner}@uni-klu.ac.at

Zusammenfassung

In Zeiten, in denen sich die Digitalisierung und Speicherung von Krankendaten als potentieller Wirtschaftszweig herausstellt, ist es in der Verantwortung der Systementwickler dafür Sorge zu tragen, dass diese sensiblen Informationen nicht zum Nachteil der Patienten verwendet werden können. Um die Wirtschaftslücke, die durch den Wunsch der Speicherung dieser persönlichen Daten enstanden ist, zu füllen, bieten viele Plattformen eine zentrale Speicherung der Krankendaten an. Jedoch ist diese Variante aus Datenschutzsicht bedenklich. Diese Arbeit beschäftigt sich mit der Frage, wie man schutzbedürftige Daten bei einem Notfall auch ohne Zutun des Karteninhabers einem Arzt zugänglich machen kann ohne dabei Gefahr zu laufen, dass diese Informationen jeder Person offen stehen. Des Weiteren soll sichergestellt sein, dass der Karteninhaber immer die Kontrolle über seine Daten besitzt und bei Bedarf diese auch löschen kann, sodass niemand mehr darauf Zugriff besitzt.

1 Einführung

Die erfolgreiche Erstversorgung von Patienten in Notfällen erfordert häufig rasches Ergreifen medizinischer Massnahmen verschiedenster Art. Die Verabreichung von Medikamenten kann unter gewissen Umständen zu allergischen Reaktionen bzw. zu gefährlichen Wechselwirkungen mit bestehenden Medikationen führen. Beispiele hierfür sind Penicilin-Allergien oder Diabetes. Patienten, welche eine Vielzahl von Medikamenten einnehmen, sind unter Stress eventuell nicht in der Lage, die Liste ihrer Medikationen lückenlos anzugeben. In Fällen, in denen der Patient ohne Bewusstsein ist, besitzt der Arzt keine Möglichkeit einer Anamnese vor Ort, sofern nicht Angehörige oder Bekannte zur Verfügung stehen, welche die erforderlichen Auskünfte erteilen können. Fehlende Information kann damit das Leben eines Patienten zusätzlich gefährden, wenn keine Speicherung der Informationen in einer im Notfall zugreifbaren Art und Weise vorliegt. Beispiele von Informationen, deren Verfügbarkeit im Notfall kritisch sein können, sind Allergien, Medikationen, Organ-Fehler (Herzfehler oder fehlende Organe), ansteckende oder chronische Krankheiten (Hepatitis, HIV, Diabetes, etc.), frühere Operationen (beispielsweise sind Computer-Tomographien bei Vorhandensein von metallischen Implantaten nicht möglich) und viele mehr.

Ein inhärentes Problem bei der Speicherung derartig sensibler Daten ist der Zugriff durch unbefugte Dritte. Beispielsweise kann der Träger einer Karte bei einer Bewerbung um eine Stelle von seinem zukünftigen Arbeitgeber erpresst werden, seine Krankheitsgeschichte offen zu legen. Die Speicherung von Krankendaten auf einer Chipkarte (beispielsweise der österreichischen e-card [Soz09]) muss derartige Szenarien mit beweisbarer Sicherheit ausschliessen.

P. Horster · P. Schartner (Hrsg.) · D•A•CH Security 2009 · syssec (2009) 185-194.

Es sei an dieser Stelle explizit darauf hingewiesen, dass sämtliche Sicherheitsmechanismen den Nutzern und Nutzerinnen der Karte optional zur Verfügung gestellt werden können, abhängig von deren Wünschen und Schutzbedürfnissen.

2 Analyse aktueller Lösungen

Aktuelle Vorschläge und Lösungen [MCW08c, MCW08a, MCW08b] gehen häufig von einer zentralen Speicherung der Krankenakten bzw. Notfalldaten aus und erlauben den webbasierten Zugriff auf diese Informationen. Somit ist es – beispielsweise bei notfallkarte.at – dem Notarzt möglich, die Daten mithilfe der Informationen, die auf der Notfallkarte aufgedruckt sind, auszulesen, ohne, dass dafür ein Passwort oder Ähnliches benötigt wird. Geht diese Karte verloren und wird nicht rechtzeitig gesperrt, sind die Daten vor Missbrauch nicht mehr geschützt. Der Kunde kann auf diese drei zusammengehörigen Produkte (notfallkarte.at, befundkarte.at, medikamentenkompass.at) mittels eines Web-Zugangs zugreifen und in Teilbereichen Änderungen vornehmen. Hierfür ist ein persönliches Passwort notwendig. Einen Teil der Daten, wie beispielsweise die der Krankenakte, können nur berechtigte Ärzte ändern, womit gewollte Manipulationen großteils verhindert oder erschwert werden.

Kunden, die einen großen Wert darauf legen, die Hoheitsgewalt über ihre Daten zu besitzen (sie wollen die Daten löschen können, wann immer sie wollen), werden sich eventuell an der zentralen Speicherung stoßen. Auch wenn der Anbieter versichert, die Daten auf Anfrage zu löschen, kann sich der Kunde dessen nicht sicher sein. Die Einbeziehung des Kunden in derartige Entscheidungen sollte daher entweder auf rechtlichem oder technischem Wege erfolgen, sofern dies gewünscht wird.

Ein weiteres Problem besteht darin, dass die zentral gespeicherten Daten besonders gut geschützt sein müssen, weil sonst eventuell die Gefahr eines massiven Datendiebstahles besteht. In der Vergangenheit wurden genügend Skandale um Datenlecks bekannt, die ein gewisses Maß an Skepsis hervorrufen sollten. Wenn Gesundheitsdaten zudem auch im Ausland gespeichert werden, erhöhen sich die Gefahrenpotentiale. Beispielsweise wäre hierfür HealthVault von Microsoft [Micr09] oder Google Health [Goog09] zu nennen.

Einen anderen Weg beschreitet Medids.com [Medi08]. Hier werden die Krankendaten auf einem USB-Speicher abgelegt und können im Notfall oder bei einer Routineuntersuchung vom Arzt eingesehen werden. Da die Daten jedoch im Klartext auf dem Gerät abgelegt werden und es auch keine Schutzmechanismen gibt, ist man gegen keinerlei Angriffe geschützt. Aufgrund der dezentralen Struktur hat man hier die vollständige Kontrolle über die Daten und kann diese jederzeit löschen oder verändern.

Ein weiterer Vorschlag [RNGB+07] beschäftigt sich mit der zentralen, pseudonymisierten Speicherung von Krankendaten. Hierbei werden die Krankendaten zwar nicht verschlüsselt abgelegt, jedoch die Verknüpfung zu den Patientendaten wird durch den Einsatz kryptographischer Mechanismen für einen Angreifer unbrauchbar gemacht. Erst durch die Hinzunahme eines Schlüssels kann die Zuordnung für einen bestimmten Patienten wieder hergestellt werden. Dieses System erlaubt auch eine Aufteilung des Schlüssels (durch ein Sharing-Verfahren) auf mehrere Administratoren bzw. die Wiederherstellung des selben durch redundante Speicherung der einzelnen Teile. Diese Aufteilung erfolgt durch ein (k, n)-Secret-Sharing. Weiters ist dem System nicht bekannt, welcher Administrator welche Shares hält, was die Chance eines betrügerischen Verhaltens reduziert. Ein Angreifer kann somit nicht gezielt Share-Holder bestechen, um den gewünschten Schlüssel zu bestimmen.

Die Datenbank mit dem Anamnesedaten ist für einen Angreifer nutzlos, weil er dadurch nur die Krankheiten der Gesamtheit der Patienten kennt. Die Krankendaten sind jedoch nicht informationstheoretisch sicher, weil die Pseudonyme (bzw der Schlüssel der dahinter steht) mit genügend großem Einsatz dem entsprechenden Patienten zugeordnet werden können. Ein Diebstahl der Daten kann sich dadurch in vielen Jahren (auch wenn der Schlüssel vernichtet wurde) zum Nachteil der Patienten entwickeln, sollte die technische Weiterentwicklung ein Brechen heutiger kryptographischer Verfahren ermöglichen.

3 Anforderungen

Wir unterteilen die Daten eines Patienten grob in drei Kategorien: freigegebene Daten, Notfalldaten und persönliche Daten (z.B. die Krankengeschichte). Freigegebene Informationen sollen von jedem (insbesonders von einem Notarzt) gelesen werden können und ergeben bei Offenlegung für den Besitzer keine negativen Folgen. Notfalldaten sollen nur im Ernstfall von z.B. einem Notarzt ausgewertet werden können, um den Patienten durch die Erstversorgung nicht zusätzlich zu gefährden. Die persönlichen Daten umfassen alles, was der Kartenbesitzer als sensibel definiert und bei einer Veröffentlichung zu negativen Konsequenzen führen kann. Für die Speicherung von personenbezogenen Daten ergeben sich daher folgende Anforderungen:

- Die öffentlichen Daten dürfen nur vom Patienten selbst (oder mit dessen Autorisierung) auf die Karte geladen werden, um es niemandem mit geeigneter Hardware zu ermöglichen, diese Daten zu manipulieren und dadurch im Ernstfall Schaden anzurichten.
- Die Notfalldaten auf der Karte dürfen vom Besitzer der Karte selbst nicht gelesen oder verändert werden können: Erstere Anforderung schließt die Erpressbarkeit des Trägers aus, letztere Anforderung schließt eine Manipulation der Daten zu Gunsten des Trägers aus (beispielsweise die Verschleierung von Sucht-Verhalten). Die Notfalldaten müssen ohne Zutun des Besitzers gelesen werden können, falls die betreffende Person ohne Bewusstsein ist.
- Optional kann die zentrale Buchführung über sämtliche Aktivitäten betreffend die Daten erzwungen werden, sofern der Eigentümer der Karte dies wünscht. Diese unumgehbare Meldepflicht kann bei Verlust auch die nicht-autorisierte Verwendung der Karte anzeigen und offeriert damit eine zusätzliche Alarm-Funktionalität.
- Die Krankengeschichte (oder andere als geheim eingestufte Informationen) darf nur mit dem Einverständnis des Kartenbesitzers verändert und gelesen werden.

Darüber hinaus ist zu klären, wie die Daten bei Verlust der Karte geschützt werden können bzw. wie eine Beschädigung der Informationen auf der Karte erkannt oder vermieden werden kann. Dies kann durch den Einsatz von Prüfsummen, sowie fehlerkorrigierenden Codierungen [McSa81] geschehen. Sofern Informationen durch Abkürzungen oder international gültige Codes (siehe [Orga08]) platzsparend auf der Karte untergebracht werden, darf das Kippen von Bits im Speicher der Karte nicht die darauf enthaltenen Informationen in eine veränderte aber gültige Form umwandeln.

4 Technische Umsetzung

Aus den in Kapitel 3 definierten Anforderungen leiten sich für die öffentlichen und geheimen Daten folgende Regeln ab.

- Vom Besitzer freigegebene Daten können im Klartext auf der Karte abgelegt werden. Dadurch ist gewährleistet, dass im Ernstfall jedem Notarzt mit entsprechender Hardware diese Daten rasch zur Verfügung stehen. Um unbefugte Manipulationen zu verhindern, werden die Daten durch eine PIN vor dem Verändern geschützt.
- Der Zugriff auf persönliche Daten (z.B. über einen Schlüssel) wird ebenfalls durch eine PIN geschützt. Somit ist es nur dem Karteninhaber möglich, diese Daten zu lesen und zu schreiben. Bei einem Arztbesuch muss der Patient wissentlich die Daten freigeben. Als weitere Maßnahme, um den Karteninhaber vor Erpressung zu schützen, kann die Chipkarte bei falscher Authentifizierung entweder den Zugriff auf ungültige Daten lenken oder die Karte unbrauchbar machen (Gefahr einer unbeabsichtigten Falscheingabe). Die Datenhaltung kann auf verschiedenste Arten erfolgen. Als Beispiele seien eine zentral verschlüsselte, eine lokale (z.B: USB-Datenspeicher) oder eine kombinierte Speicherung (z.B: durch Secret-Sharing) genannt. In einigen Arbeiten bzw. Projekten [FHK08, MeSc04, HeSS07] wird bei der Speicherung der Patientendaten von einer zentralisierten Architektur inklusive Trust Center ausgegangen, die es dem Benutzer erlaubt, online auf seine Informationen zuzugreifen.

Für die Verwaltung der Notfalldaten ergibt sich die Notwendigkeit, die Daten auf mehrere Instanzen aufzuteilen. Der Einsatz geeigneter Verfahren zum Secret-Sharing ist ein natürlicher Ansatz, um den obigen Forderungen bezüglich der Notfalldaten Rechnung zu tragen. Folgende Instanzen können an dem System beteiligt sein:

- der Inhaber der Karte
- der Hausarzt/die Hausärztin des Patienten/der Patientin
- die gesetzliche Krankenversicherung
- Krankenhäuser
- andere, als vertrauenswürdig erachtete Instanzen

Die Erpressung der Daten seitens eines unbefugten Dritten kann unterbunden werden, wenn ein k-aus-n-Secret-Sharing zum Einsatz kommt (mit $k \geq 2$), welches eine Rekonstruktion der Daten unmöglich macht, wenn nicht wenigstens k der n Instanzen bei der Aufdeckung kooperieren. Ein direkter Erpressungsversuch durch eine dritte Person kann damit vermieden werden, da diese zumindest eine andere Instanz (die Krankenkasse oder das Krankenhaus) dazu bewegen müsste, an der Rekonstruktion teilzunehmen. Die Erpressung kritischer Daten bei einer Stellenbewerbung ist damit de facto ausgeschlossen. Dennoch kann die Person eventuell unter Zwang als Berechtigte andere Instanzen dazu bringen an der Rekonstruktion teilzunehmen. Ein möglicher Schutz ist die Vergabe mehrerer PIN-Codes, welche verschiedene Ergebnisse liefern, die nicht unterscheidbar sind. Sofern der Patient nicht in der Lage ist, seine PIN einzugeben, kann sich ein Ersthelfer gegenüber der Chipkarte ausweisen und so auch Zugriff auf die Daten erhalten. Ein betrügerisches Verhalten eines Arztes oder Ersthelfers kann hierbei nicht ausgeschlossen, jedoch durch die Protokollierung der anderen Instanzen im Nachhinein aufgedeckt werden.

Wird der Träger der Karte erpresst die Daten preiszugeben (also zu rekonstruieren), so wird dies nicht zum Erfolg führen (auch wenn der Träger die korrekte PIN eingibt). Grund hierfür ist, dass der Karteninhaber nur einen Share besitzt und dieser keinerlei Information enthält. Somit müsste zumindest ein Arzt oder Ersthelfer, der Zugriff auf die Share-Datenbank besitzt, betrügerisch handeln, um eine Rekonstruktion der Daten zu bewerkstelligen. Bei Bedarf kann

auch der Zugang zur Karte durch die Ersthelfer untersagt werden, was bedeutet, dass nur durch die PIN-Eingabe die Rekonstruktion angestoßen werden kann. In diesem Fall ist jedoch kein Zugriff auf die Daten ohne aktives Zutun des möglicherweise bewusstlosen Unfallopfers möglich.

Die Übertragung der Shares der beteiligten Instanzen zur Chipkarte des Patienten kann durch eine sichere End-zu-End Verschlüsselung geschehen. Dadurch ist ausgeschlossen, dass ein Angreifer die übertragenen Shares zwischenspeichern kann, um diese später wieder einzuspielen. Dies stellt keine Beeinträchtigung des Verfahrens dar, weil sowieso nur die Chipkarte des Patienten die Daten rekonstruieren können soll und somit niemand (auch nicht der Arzt) die Shares der anderen beteiligten Parteien kennen muss. Um gewöhnliche Übertragungsfehler zu erkennen, bieten sich fehler-korrigierende Codes als Mittel zum Zweck an. Es kann gezeigt werden (siehe [McSa81]), dass Reed-Solomon Codierung äquivalent zu Shamir's Secret-Sharing ist, was die Möglichkeit eröffnet, fehlerhafte Shares durch Anwendung von Fehler-Korrekturalgorithmen zu identifizieren. Geeignete Algorithmen wurden im Rahmen der Theorie der fehler-korrigierenden Codes entwickelt und sind einfach zu implementieren.

Die Buchführung über die Verarbeitung der Patientendaten kann durch das Festlegen einer geeigneten Zugriffsstruktur bei dem eingesetzten Secret-Sharing Verfahren erzwungen werden. Herkömmliche Threshold-Verfahren wie jenes von Shamir vorgeschlagene Schema [Sham79], erlauben es beliebigen k oder mehr Instanzen, das Geheimnis zu rekonstruieren. Wenn wir die Anwesenheit einer bestimmten Instanz erzwingen möchten, so können wir dies stets durch ein 2-stufiges Sharing erreichen, wobei wir die Rohdaten zunächst mit Hilfe eines $(2, 2)$-Summensharing aufteilen. Jene Instanz, welche die Buchführung übernimmt, erhält einen Share, während der andere auf die anderen Instanzen, wie oben genannt (Hausarzt, Krankenhaus, etc.), weiter aufgeteilt wird. Es besteht keine Notwendigkeit der Trennung der überwachenden Instanz und den oben genannten, d.h. eine der Parteien kann beide Rollen übernehmen. Die Rekonstruktion kann dann zunächst durch die Chipkarte des Patienten erfolgen, welcher die rekonstruierten Daten nur in Verbindung mit der buchführenden Instanz korrekt decodieren kann. Es ist auch denkbar, Teile der Notfalldaten mit verschiedenen Schwellwerten zu verteilen, um die Sicherheit gegen betrügerisches Verhalten zu erhöhen.

4.1 Szenarien

Im Folgenden beschreiben wir eine Reihe von Szenarien, welche im Rahmen der bereits umrissenen technischen Umsetzung bewältigt werden können:

Notfallversorgung: Der Erstversorger kontaktiert das Krankenhaus bzw. die zuständige Gebietskrankenkasse und authentifiziert sich. Er erhält von der Instanz einen Share, und kann die kritischen Informationen mit Hilfe des Shares des Verunfallten rekonstruieren (in diesem Fall wäre der Schwellwert k des Secret-Sharing gleich 2).

Zerstörung der Informationen auf der Karte: Sollte der gespeicherte Share durch einen Defekt der Karte (z.B. durch eine Veränderung) unbrauchbar sein, ist eine Rekonstruktion der Notfalldaten nicht mehr möglich. In diesem Fall muss (mithilfe des Hausarztes) eine Chipkarte mitsamt neuer Shares (auch für die anderen beteiligten Instanzen) erzeugt werden. Abhilfe würde eine Backup-Lösung bringen. Diese könnte derart implementiert werden, dass in dieser gesicherten Datenbank weitere Shares liegen, die die Rekonstruktion auch ohne die Chipkarte des Patienten erlauben. Dies wirft natürlich weitere Probleme auf, da rein theoretisch auch ohne Zutun des Patienten und seiner Chipkarte die Notfalldaten rekonstruiert werden können. Auf Basis der Ergebnisse von [McSa81] ist es möglich, die Korrektheit von Shares zu verifizieren,

um Fehler im Speicher der Chipkarte aufzudecken.

Verlust der Karte: Wird vom Besitzer der Karte deren Verlust gemeldet, so können die übrigen Instanzen die Rekonstruktion der Informationen durchführen (sollte es eine Backup-Lösung geben), das Sharing neu berechnen und die alten Shares zerstören. Die verlorene Karte kann ersetzt werden, wobei der Share auf der verlorenen oder gestohlenen Karte nutzlos wird, da keine passenden anderen Shares mehr existieren. Für den Fall, dass keine Backup-Lösung für diesen Patienten existiert, müssen die Daten mithilfe des Hausarztes neu erfasst werden.

Wechsel des Hausarztes: Da der Hausarzt selbst keine Shares hält sondern nur den Zugriff auf die Shares bietet, ist der Wechsel des Hausarztes ohne Probleme möglich. Durch geeignete Zugriffsregeln kann dem alten Hausarzt der Zugriff auf die Shares der Patienten verwehrt werden.

Überweisung zu Fachärzten: Funktioniert ohne Einschränkung weiterhin, da der Facharzt sich gegenüber den beteiligten Instanzen als autorisiert ausweisen kann um Einsicht in den Krankenakt zu nehmen.

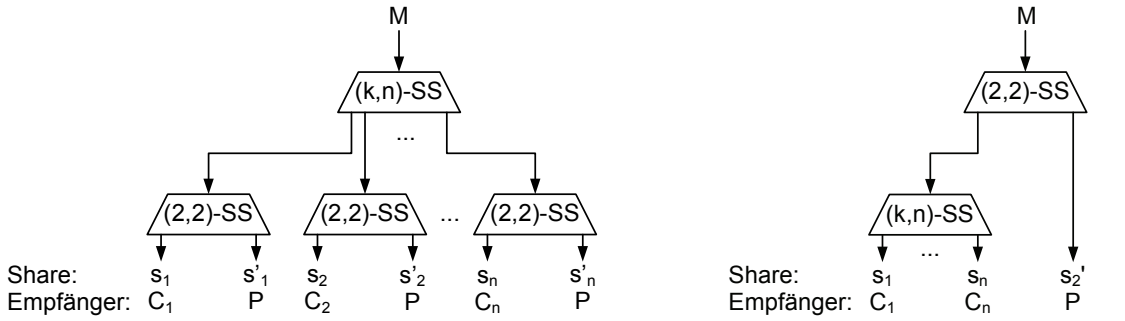
Erpressungsversuche: Diese sind ausgeschlossen, sofern die erpressende Partei nicht wenigstens $k-1$ andere Instanzen zur Mitwirkung zwingen kann. Der Besitzer oder die Besitzerin der Karte kann durch Angabe eines falschen PIN-Codes ungültigen Daten liefern, die der Angreifer nicht als solche identifizieren kann.

Vernichtung der Daten: Für den Fall, dass keine Backup-Shares vorhanden sind, kann der Kartenbesitzer den Zugriff auf seine Daten für immer verhindern, indem er die Chipkarte zerstört.

Um dem Kartenträger die Möglichkeit zu geben, den gewünschten Schutz individuell festzulegen, kann ein mehrstufiges Secret-Sharing eingesetzt werden. Soll beispielsweise eine bestimmte Person (z.B. ein Sachwalter) in alle Zugriffe auf die Notfalldaten involviert sein, so können sämtliche Shares zwischen der angegebenen Partei und den anderen Parteien aufgeteilt werden. Soll wenigstens eine Person aus einem angegebenen Personenkreis an jeder Rekonstruktion teilnehmen (beispielsweise in Szenarien, in denen der Sachwalter nicht erreichbar ist, und ein Stellvertreter einspringen muss), so kann auch das durch Festlegen entsprechender Zugriffsstrukturen leicht erfolgen. Die Menge der auf der Karte zu speichernden Daten wird davon nicht beeinflusst, da die oben beschriebene Rolle niemals dem Kartenträger selbst zukommen wird.

Wir illustrieren das Festlegen der Zugriffsstruktur anhand einiger Beispielszenarien. Im Folgenden bezeichnet M die zu speichernden Notfalldaten, und $s_1, \ldots, s_n$ seien die Shares, welche auf k aus Parteien aufgeteilt werden. Als (k, n)-Schwellwert-Schema (kurz: SS), wobei wenigstens beliebige k aus n Shares für die Rekonstruktion notwendig sind, bietet sich Shamir's Secret-Sharing an. Im Falle $k = n$ kann einfacher und effizienter aufgeteilt werden, durch Wahl von $n-1$ Zufallszahlen $r_1, \ldots, r_{n-1}$, welche die ersten $n-1$ Shares darstellen. Der letzte Share ergibt sich durch $s_n := M \oplus r_1 \oplus \cdots \oplus r_{n-1}$. Die im Folgenden verwendeten $(2, 2)$-Sharing Schemata können so effizient realisiert werden.

Szenario 1: Festlegen einer Instanz P, die verpflichtend bei jeder Rekonstruktion eingebunden werden muss. Jeder Share $s_1, \ldots, s_n$ wird durch Anwendung eines weiteren Secret-Sharing Verfahrens in zwei weitere Shares zerlegt, wobei einen Share die Partei C_i, und den anderen Share, die Partei P erhält. P muss damit n Shares speichern, und bei jeder Rekonstruktion den entsprechenden Share zur Verfügung stellen. Alternativ kann die Aufteilung von M auch zuerst erfolgen, sodass P einen Share s_1 zu M erhält, und der verbleibende Share s_2 entsprechend aufgeteilt wird. Beide Varianten sind bildlich in Abbildung 1(a) und 1(b) dargestellt.



(a) Szenario 1, Variante 1

(b) Szenario 1, effizientere Variante 2

Abb. 1: Secret-Sharing Varianten

Szenario 2: Wenigstens eine Person aus einem definierten Kreis von Personen muss an jeder Rekonstruktion teilnehmen. Beispiele hierfür wären das Einbinden eines Familienmitgliedes (Vormund), welcher das Einverständnis zur Offenlegung der Daten geben muss. Sofern die betreffende Person über keine Möglichkeit verfügt, die Daten in online-zugreifbarer Form zu speichern, kann eine Speicherung auf der Chipkarte der betreffenden Person erfolgen.

Szenario 3: Keine erzwungene Einbeziehung bestimmter Instanzen in die Offenlegung. In diesem Fall reicht ein herkömmliches (k, n)-Schwellwert-Verfahren aus.

5 Erpressung und Diebstahl

Die Einwilligung einer Person ihre Daten auf einer Chipkarte zu speichern, erfordert vollkommenes Vertrauen in die Sicherheit der angebotenen Datenspeicherung. Chipkarten gelten als technologisch abgesichert gegen das Auslesen von Daten, bzw. Manipulationen im Allgemeinen. Beschränkungen des Zugriffs durch PINs sind eine weit verbreitete und weithin akzeptierte Variante der Absicherung, jedoch bietet ein derartiges Passwort-System keinen hinreichenden Schutz vor Erpressung der geheimen Zugangsdaten.

Ein Szenario, welches ein Argument gegen die Speicherung persönlicher Notfalldaten liefert, ist die Erpressung der Krankendaten seitens eines potentiellen Arbeitgebers. Gesundheitliche Beeinträchtigungen mögen bei einer Bewerbung nicht zwingend anzugeben sein, jedoch kann der Erfolg einer Bewerbung stark davon beeinflusst sein, wie der Bewerber gesundheitlich eingeschätzt wird. Sofern eine Chipkarte für die Notfallversorgung mitgeführt wird, besteht die Gefahr der Erpressung der darauf gespeicherten Daten unter dem Zwang, dass bei einer Weigerung, die Bewerbung unmittelbar abgelehnt wird. Hierfür müsste jedoch zumindest ein Arzt mithelfen, um den zweiten nötigen Share zu erhalten. Zusätzlich wird diese Anfrage von einer zentralen Instanz protokolliert was auch zu rechtlichen Konsequenzen für den Arbeitgeber führen kann (oder bei der Aufklärung helfen kann). Somit bietet dieses Verfahren auch eine Abschreckung für neugierige Arbeitgeber. Mechanismen zum Schutz gegen derartige Erpressungs-Szenarien sind vielfältig und existieren in diversen Kontexten. Elektronische Türschlösser können durch Vergabe eines zweiten Zugangscodes, welcher die Tür auch öffnet, jedoch stillen Alarm auslöst, abgesichert werden. Ein ähnliches Konzept wurde bei der Software TrueCrypt [LeAd08] umgesetzt zum Schutz gegen die Erpressung des Passwortes. TrueCrypt bietet sogenannte *hidden volumes* an, welche innerhalb eines gewöhnlichen verschlüsselten Festplattenbereichs angelegt werden können. Ein solcher versteckter Bereich kann mit einem

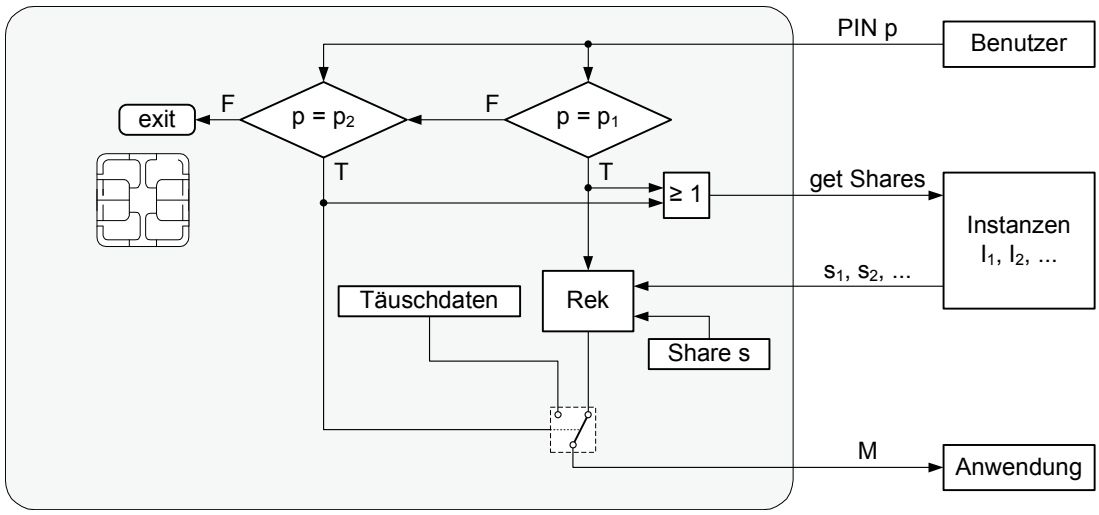


Abb. 2: Nutzung der Chipkarte (Variante 1)

Passwort wie ein normaler verschlüsselter Bereich geöffnet werden. Zusätzlich existiert ein zweites Passwort, welches im Erpressungsfall den Zugriff auf einen anderen Bereich freigibt, welcher in diesem Fall nur Informationen von geringem oder gar keinem Wert enthalten sollte. Im Idealfall bleiben die geheimen Daten damit geschützt, ohne einen Verdacht auf deren Existenz zu wecken.

In dieser Arbeit schlagen wir zwei Varianten zum Schutz der Daten auf der Chipkarte vor. In der ersten Variaten werden zwei dezidierte PINs verwendet. Ein PIN p_1 veranlasst die Chipkarte die Daten zu rekonstruieren, wogegen der zweite PIN P_2 einen vorbereiteten Datensatz liefert. Die Eingabe falscher PINs führt nach mehreren Fehlversuchen zur Sperrung des Zuganges durch die Chipkarte (und eventuell Löschung des Shares), wodurch sie unbrauchbar wird. Wird eine der beiden PINs eingegeben, so fragt die Chipkarte bei den anderen beteiligten Instanzen ($I_1 \ldots I_n$) um die fehlenden Share an, um auch im Erpressungsfall keinen Verdacht aufkommen zu lassen. Zusätzlich wird eine Information übertragen, die den anderen Instanzen mitteilt, ob es sich um eine Erpressung handelt, was zumindest einer späteren Aufklärung der Sachlage behilflich sein kann. Je nach eingegebener PIN (und dadurch eventuell erfolgtem stillen Alarm) senden die anderen Instanzen entweder die korrekten Shares oder aber im Erpressungsfall Zufallsdaten (oder ähnliche informationslose Daten) zur Chipkarte. Anhand der Länge der übertragenen Daten darf der Angreifer keine Informationen über Status des stillen Alarms erhalten. Im Normalfall rekonstruiert die Chipkarte die Daten (Funktion rek) und liefert sie dem Notarzt. Im Falle einer Erpressung werden lediglich Pseudoberechnungen durchgeführt und daraufhin die vorgefertigten Notfalldaten geliefert, welche der Angreifer aber nicht von den korrekten Daten unterscheiden kann.

Die zweite Methode erspart dem Karteninhaber die Notwendigkeit sich zwei PINs merken zu müssen. Hierbei existiert wiederum genau ein PIN p_1, der zu den korrekten Daten führt (analog zur Variante 1). Jedoch wird bei der Eingabe eines beliebigen anderen PINs ein zufälliger (aber fixer) Datensatz aus der Menge $T \cup M$ zurückgegeben. T enthält fix definierte und in der Chipkarte gespeicherte Täusch-Datensätze (analog zu dem einen Täusch-Datensatz auf Variante 1) und M enthält den korrekten Datensatz, der nach der Rekonstruktion (Funktion rek) entstanden ist. Bei einem Erpressungsversuch wird der Erpresste einen falschen PIN eingeben und somit

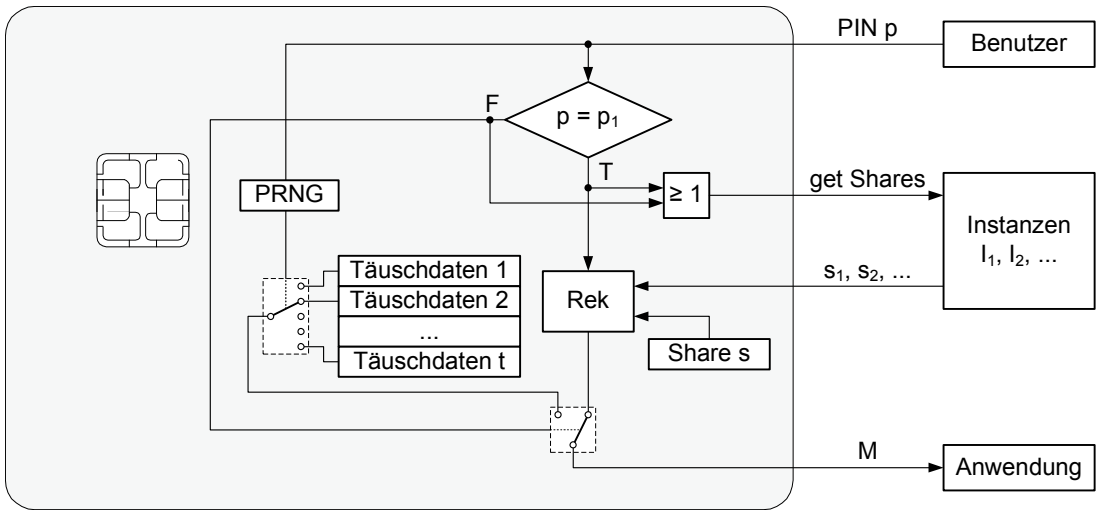


Abb. 3: Nutzung der Chipkarte (Variante 2)

ein Ergebnis provozieren, welches es dem Angreifer nicht erlaubt, Rückschlüsse auf die Krankendaten zu ziehen (der Angreifer weiß ja, dass er dem Ergebnis nicht vertrauen kann). Dieses Verfahren entspricht dem Bluffen im realen Leben (bei Variante 1 war es dagegen das Lügen). Voraussetzung zum Funktionieren dieses Bluffs ist, dass auf den selben PIN immer die selben Daten geliefert werden, damit der Angreifer den Bluff nicht durchschauen kann. Die Aufteilung der Datensätze auf die PINs darf auch keine Rückschlüsse auf die korrekten Notfalldaten zulassen (eventuell durch ein Ausschlussprinzip). Auch wenn der Angreifer oder der Erpresste den korrekten PIN eingibt, darf dies dem Angreifer nicht auffallen. Bei diesem Verfahren müssen im Gegensatz zum zuvor genannten die anderen beteiligten Instanzen ($I_1 \ldots I_n$) ihre Shares in jedem Fall übermitteln, weil die Rekonstruktion bei jedem PIN notwendig sein kann

Wir gehen von der Annahme aus, dass die Partei, welche die Chipkarte besitzt, an jeder Rekonstruktion teilnehmen muss (dies kann durch eines der dargestellten Verfahren leicht erzwungen werden). Das bedeutet, dass jedwede Rekonstruktion entweder mit der Zustimmung, oder ohne das Zutun des Karteninhabers erfolgt. Betrachten wir folgende Szenarien:

Rekonstruktion mit der Zustimmung des Karteninhabers: Nach Eingabe der korrekten PIN rekonstruiert die Chipkarte die Daten und stellt diese bereit.

Rekonstruktion ohne Mithilfe des Karteninhabers: Sofern die betreffende Person nicht in der Lage ist den PIN einzugeben (beispielsweise unter Bewusstlosigkeit im Notfall), kann der Notfallmediziner sich für die Rekonstruktion anders der Karte gegenüber legitimieren.

Rekonstruktion unter Druck (Erpressung): Die Eingabe eines falschen PIN gibt nur den Zugriff auf wertlose Daten frei. Der Angreifer hat aber keine technische Möglichkeit die Korrektheit der Daten zu verifizieren.

Verlust oder Diebstahl der Karte: Das Vortäuschen der Identität des Karteninhabers zur Rekonstruktion schlägt bei fehlender Kenntnis der PIN fehl, da jeder Versuch eine PIN einzugeben entweder fehlschlägt (Sperrung der Karte) oder aber einen stillen Alarm auslöst.

6 Resümee

Die vorgestellte Methode unterscheidet sich von den bisher vorgestellten Lösungen dadurch, dass die Kontrolle über die Daten vollständig in der Hand des Karteninhabers liegt. Durch diese Struktur ist es jederzeit möglich, die Daten durch eine Vernichtung der Smartcard zu löschen. Des weiteren ist auch ein Diebstahl der in zentralen Datenbanken gespeicherten Shares sinnlos, weil für jeden Share auch die dazugehörige Chipkarte besorgt werden müsste. Die Konsequenzen eines Datenlecks sind somit geringer, als bei einer vollständig zentralen Speicherung.

Literatur

[FHK08] FH Kärnten – Medizinische Informationstechnik (MedIT), CArinthian Notarzt Information System (CANIS). http://www.cti.ac.at/canis (2008).

[Goog09] Google.com: Google Health. http://www.google.com/health (2009).

[HeSS07] M. Heiligenbrunner, D. Slamanig, C. Stingl: Sicherheitskonzept für Notfalldaten unter Verwendung der eCard. *In: P. Horster (Hrsg.), DACH Security 2007*, syssec, Frechen (2007), 314–325.

[LeAd08] G. B. Le Roux, Paul, M. Adler: TrueCrypt – Free open-source disk encryption. http://www.truecrypt.org/ (2008).

[McSa81] R. McElice, D. Sarwate: On Sharing Secrets and Reed-Solomon Codes. In: *Communications of the ACM*, 24, 9 (1981), 583–584.

[MCW08a] Medical Computer Ware (MCW): Befundkarte. http://www.befundkarte.at/ (2008).

[MCW08b] Medical Computer Ware (MCW): Der Medikamentenkompass, eine Orientierungshilfe im Arzneimitteldschungel. http://www.medikamentenkompass.at/ (2008).

[MCW08c] Medical Computer Ware (MCW): Notfallkarte. http://www.notfallkarte.at/ (2008).

[Medi08] Medids.com: Med Flash USB Medical Alert tag, Medic ID, Medi alert. http://www.medids.com/Med-Flash-Medical-Records.html (2008).

[MeSc04] P. S. Merten, T. Schlienger: Eine eHealth Plattform – Einsatz von IKT im Gesundheitswesen. *In: P. Horster (Hrsg.), DACH Security 2004*, syssec, Frechen (2004), 345–358.

[Micr09] Microsoft.com: Welcome to Microsoft HealthVault. http://www.healthvault.com/ (2009).

[Orga08] W. H. Organization: WHO – International Classification of Diseases (ICD). http://www.who.int/classifications/icd/en/ (2008).

[RNGB+07] B. Riedl, T. Neubauer, G. Goluch, O. Boehm, G. Reinauer, A. Krumboeck: A secure architecture for the pseudonymization of medical data. In: *Availability, Reliability and Security, International Conference on*, 0 (2007), 318–324.

[Sham79] A. Shamir: How to share a secret. In: *Commun. ACM*, 22, 11 (1979), 612–613.

[Soz09] Sozialversicherungs-Chipkarten Betriebs- und Errichtungsgesellschaft m.b.H. SVC: e-card. http://www.chipkarte.at (2009).