

Fachseminar Sommersemester 2005
bei Professor F. Mattern

Smarte Objekte und smarte Umgebungen

Titel:
Privatsphäre und RFID

Studentin: Jutta Bonan
Betreuer: Christian Flörkemeier

Motivation	2
RFID – Radio Frequency Identification	3
Anwendung RFID	4
Probleme: Privatsphäre von RFID	5
Existierende Problemlösungen	6
Das Hash-Based RFID Protokoll	7
Verbesserung von Avoine und Oechslin	9
Der RFID-Reisepass	11
Challenge-Response Authentifikations-Protokoll	11
Zusammenfassung	13
Quellenangabe	14

Motivation

Mit RFID kann man Daten durch Funk übertragen. Es können biometrische Daten gespeichert werden. Diese Vorteile werden unter anderem in Bibliotheken, bei Skipässe, im Handel und im Reisepass genutzt. Doch diese Vorteile sind auch mit Nachteile verbunden, da die Privatsphäre der Bürger verletzt wird. Ziel dieses Seminar ist, die Vorteile und die damit verbundenen Nachteile bezüglich der Privatsphäre von RFID aufzuzeigen. Lösungsvorschläge werden diskutiert und zwei Protokolle zur Lösung des Privatsphärenproblems vorgestellt.



RFID – Radio Frequency Identification

Das RFID-System besteht aus zwei Komponenten: das Lesegerät und der Transponder (im Weiteren als „Tag“ bezeichnet).

Das Tag kann irgendwo angebracht werden und von einem Lesegerät ausgelesen, beziehungsweise wieder beschrieben werden. Das Tag hat eine Speicherkapazität bis zu 2 kBytes. Es speichert zum Beispiel eine eindeutige Identität (ID), den Namen des Objektes an dem er behaftet ist und den Hersteller des Objektes. Die eindeutige ID benötigt das Tag, damit es „ansprechbar“ ist. Bei der Reichweite wird zwischen aktive und passive Tags unterschieden. Aktive Tags sind teurer, da sie selber eine Batterie beinhalten. Passive Tags hingegen sind energielos und deshalb billig. Ihre Reichweite beträgt von 1mm bis maximal 10m. In diesem Seminar werden nur passive Tags behandelt. Damit passive Tags „antworten“ können, werden sie vom Lesegerät mit Energie (elektromagnetische Wellen) aufgeladen. In jedem Tag hat es eine kleine Antenne, welche die Energie vom Lesegerät empfängt. Die Datenübertragungsrate ist ca. 5 kBytes pro Sekunde. Es können dem Lesegerät 10 bis 100 Tags pro Sekunde antworten. Das hängt von verschiedenen Faktoren ab, wie zum Beispiel: Rauschempfindlichkeit, viele Kollisionen. Auch kann es Leseschwierigkeiten haben, wenn das Tag in einer Metalltasche verborgen ist oder unter Wasser steht, da die elektromagnetische Wellen nicht hindurch können. Sie funktionieren unzuverlässig. Die Haltbarkeit eines RFID-Tags ist länger als Smartkarten, welche über Kontakte funktionieren. Der Einsatzbereich von RFID ist sehr gross und viel gefragt. Im Handel wird RFID viel eingesetzt, z.B. um den Warenbestand zu zählen. In der Bibliothek um die Bücher einfach zu verwalten. Im Tourismus beispielsweise, für den Skipass. Im Einkaufszentrum an der Kasse, um die Wartezeit zu reduzieren. Und seit 2004 wird sogar RFID für den Pass eingesetzt.

Vorteile: Speicherkapazität auf kleinstem Raum, höhere Speicherkapazität als Barcodes, kontaktlose Identifikation zum Objekt, haltet lange und ist billig

Anwendung RFID

Bibliothek, Handel

RFID kann verwendet werden, um Bücher über Funk zu identifizieren. Dies hat den Vorteil, dass man Bücher in einer Bibliothek selbständig ausleihen kann. Man braucht nicht mehr Schlange zu stehen. Verlässt man die Bibliothek wird über das Lesegerät in der Bibliothek automatisch notiert, welche Bücher man genommen hat. Das Buch muss nicht extra aufgemacht werden, man kann es einfach einpacken und nach Hause gehen. [siehe Abbildung]. Das gleiche gilt im Handelsbereich. In einem Einkaufszentrum beispielsweise, kann der Einkaufswagen voll bepackt werden. RFID erspart das Herausnehmen der Einkäufe. Alles wird beim Ausgang automatisch gelesen, da jeder Artikel mit einem RFID-Tag versehen ist. Auch kann es benutzt werden, um den Warenbestand in einem Lager festzustellen. In der Bibliothek und im Handel wird vor allem der Vorteil von RFID ausgenutzt, dass es klein, überall angebracht werden kann und über Funk erkennbar ist. Man braucht keinen optischen Zugriff auf die Waren und kann kontaktlos mit ihnen „kommunizieren“.



RFID-Reisepass

RFID kennt auch einen ganz anderen Anwendungsbereich. Der RFID-Reisepass. Hier werden die Vorteile von RFID ausgenutzt, indem man auch biometrische Daten im Tag speichert. Typischerweise werden Gesicht und Fingerabdrücke gespeichert. Die Beziehung zwischen dem Reisepass und dem Inhaber des Passes wird dadurch gestärkt. Der Pass wird fälschungssicherer. Da RFID über Funk geht, ist die Haltbarkeit des Tags lang, da kein physischer Kontakt zwischen Lesegerät und Tag existiert und er dadurch nicht abgenutzt wird. Im Gegensatz zum Handel, ist hier eigentlich kein Interesse vorhanden, dass Pässe von weitem gelesen werden können.

Probleme: Privatsphäre von RFID

Die Privatsphäre von RFID ist gefährdet, wenn Tags von nicht autorisierten Lesegeräten gelesen werden können, oder Tags werden von verschiedenen Lesegeräten an unterschiedlichen Orten gelesen. Davon kann man Rückschlüsse bilden, wo die Person, welche den Tag auf sich hat, überall gewesen ist.

Man unterscheidet zwischen der Locations-Privacy (Ortungs-Privatsphäre) und der Data-Privacy (Daten-Privatsphäre).

Locations-Privacy

Die Vorteile von RFID, dass man einen Tag überall anbringen und unbemerkt lesen kann, wird zum Hauptproblem der Locations-Privacy. Kauft die Person X beispielsweise ein paar Schuhe, in welche ein Tag klebt, bleibt seine Privatsphäre weiterhin geschützt. Das Problem ergibt sich erst, wenn zwischen der Person X und den Schuhen ein Zusammenhang gemacht wird und Person X aufgrund seiner Schuhe identifiziert werden kann. Jedes Mal wenn ein Lesegerät ein paar Schuhe mit dieser Tag-ID liest, weiss es, dass diese Schuhe Person X gehören. Es ist möglich Person X aufgrund seiner Schuhe, welche einen Tag besitzen zu verfolgen.



Data-Privacy

Die Vorteile von RFID werden auch beim Reisepass zu einem grossen Problem. Wer möchte schon, dass seine Daten im Reisepass von jedem Lesegerät gelesen werden können? Mit RFID passiert dies unbemerkt und ohne persönlichem Einverständnis. Im extremen Fall könnte man Personen in einer Menschenmenge identifizieren. Wird jemand polizeilich gesucht, ist dies sicher ein Vorteil. Doch ein durchschnittlicher Bürger ist seiner Privatsphäre komplett beraubt.

Existierende Problemlösungen

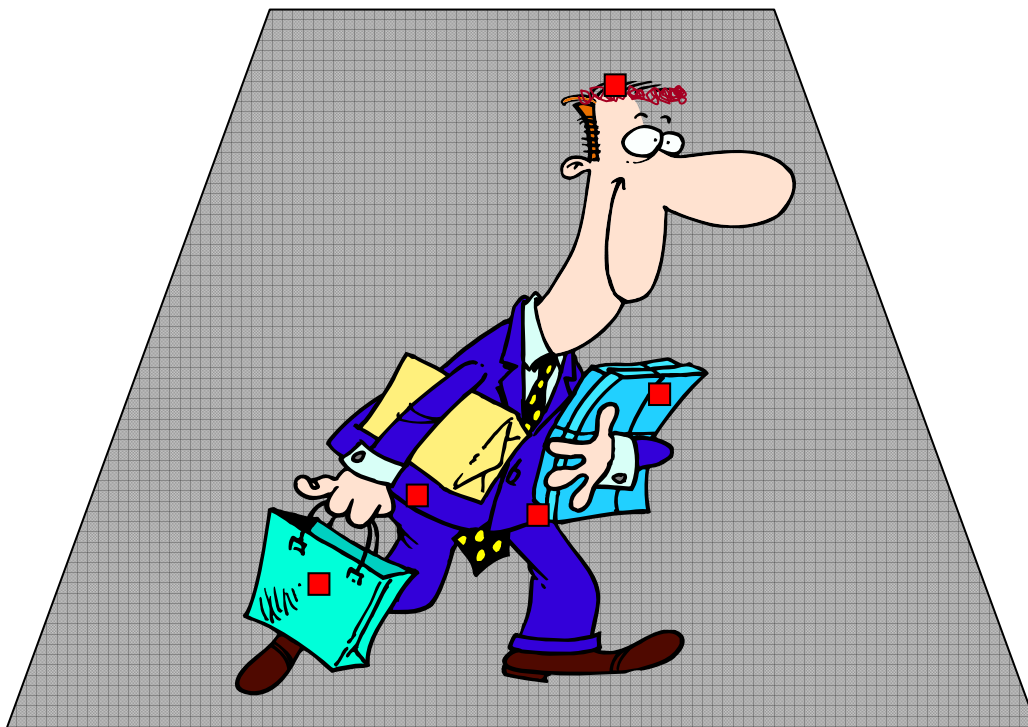
Kill-Tag

Das Tag wird vernichtet. Somit ist die Privatsphäre des Benutzers gewährleistet. Leider ist das tolle Tag zerstört und es ist nicht mehr möglich es weiter zu verwenden. Die Idee mit der Verwaltung einer Bibliothek durch RFID geht nicht. Nachdem die Tags bei der Ausleihe gekillt werden, ist ein neuer Tag bei der Rückgabe erforderlich. Im Einkaufszentrum könnte ein Unbefugter die Tags schon vor dem Bezahlen killen und dann ohne Gefahr die Ware stehlen.

Tags in Metallfolie

Werden die Tags in einer Metallfolie eingehüllt, dann besteht keine Gefahr mehr, dass sie gelesen werden. Der Benutzer muss das Tag persönlich freigeben, indem er die Metallfolie wegnimmt. Diese Idee ist beim Reisepass sicher ein Teil einer Lösung. Bei dem Bibliothekbeispiel könnte man die Bücher nach der Ausleihe in einer Alutasche stecken. Doch wird damit das Entwenden von Büchern vereinfacht, indem jemand die Alutasche in die Bibliothek mit hereinnimmt und die Bücher mitnimmt, ohne dass sie ausgelesen wurden. Alle Artikel, welche einen Tag enthalten, mit einer Metallfolie zu überdecken, sehe ich als sehr umständlich [siehe Abbildung].

Deshalb werden zwei weitere Lösungen vorgestellt, bei welchen der Tag erhalten bleibt und unbefugte Lesegeräte die Tags nicht lesen können.



Das Hash-Based RFID Protokoll

Ohkubo, Suzuki und Knoshita haben ein Protokoll vorgeschlagen, in welchem Privacy garantiert wird. Avoine und Oechslin definieren:

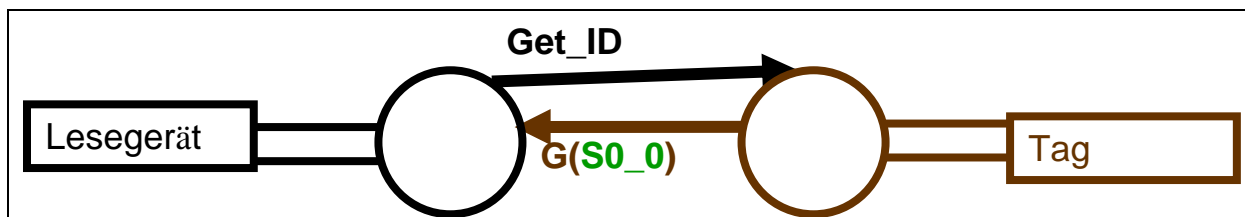
Privacy

Wird die Identität eines Tags gelesen, kann daraus nicht auf seine wahre Identität geschlossen werden. Nur autorisierte Lesegeräte können dies.

Forward-Privacy

Wird zum Zeitpunkt t die Identität des Tags ermittelt, können rückwirkend alle Daten, die zum Zeitpunkt $t' < t$ gelesen wurden, der Person nicht zugeordnet werden.

Das Hash-Based RFID Protokoll hat zum Ziel Privacy und Forward-Privacy zu gewährleisten. In diesem Protokoll speichert das Tag seine Anfangs-ID und wechselt dann nach jeder Anfrage eines Lesegerätes seine ID. Die Lesegeräte welche autorisiert sind das Tag auszulesen, speichern ebenfalls die Anfangs-ID des Tags. Ein Lesegerät hat eine Liste mit allen Anfangs-ID der Tags, welche es berechtigt ist auszulesen. Beide Komponenten, Lesegerät und Tag, speichern zwei Hashfunktionen G und H , welche öffentlich bekannt sind. Fragt das Lesegerät das Tag nach seiner ID (siehe Abbildung), schickt das Tag, falls es seine erste Anfrage ist, seine Anfangs-ID zurück, auf welche die Hash-Funktion G zuerst angewendet wurde (siehe Abbildung).



Jedesmal, wenn das Tag seine aktuelle Identität weitergegeben hat, wechselt es seine Identität. Die neue Identität berechnet sich wie folgt: sei der Anfangswert $S0_0$ so ist der nächste Wert $S0_1 := H(S0_0)$. Somit gibt das Tag nie zweimal den gleichen Wert als Identität an. Wie weiss aber das Lesegerät, welche wahre Identität hinter dem erhaltenen Hashwert verborgen ist?

Das Lesegerät, hat wie erwähnt, alle wahren Identitäten von den Tags, auf welchen es autorisiert ist, gespeichert. Es berechnet für alle diese Identitäten den Wert $G(Si_0)$ und schreibt sie in eine Tabelle. Die erste Spalte der Tabelle enthält die Werte $G(Si_0)$, die zweite Spalte die Werte $G(H(Si_1))$, die dritte $G(H(H(Si_2)))$ und so weiter bis zu $G(H(H...(Si_m)...))$. Jedesmal vergleicht das Lesegerät alle Werte einer Spalte mit dem erhaltenen Hashwert des Tags. Stimmt die Zahl mit einem Wert der Tabelle überein, dann kennt das Lesegerät die wahre Identität des Tags, indem es ganz Links in die 0-te Spalte auf der gleichen Zeile den wahren ID-Wert ausliest. Findet es den Wert nicht, so rechnet es Spalte für Spalte weiter. Avoine und Oechslin nehmen eine obere Schranke m an. Die Schranke m bezeichnet die Anzahl der Spalten in der Tabelle oder anders gesagt, die Anzahl Male, welches ein Tag gelesen werden darf.

Tabelle im Lesegerät

Wahre Id = Si_0	G(Si_0)	G(H(Si_0))	G(H(H(Si_0)))	...	G(H(H...(Si_m)...))
S0_0					
S1_0					
S2_0					
...					
Si_0					

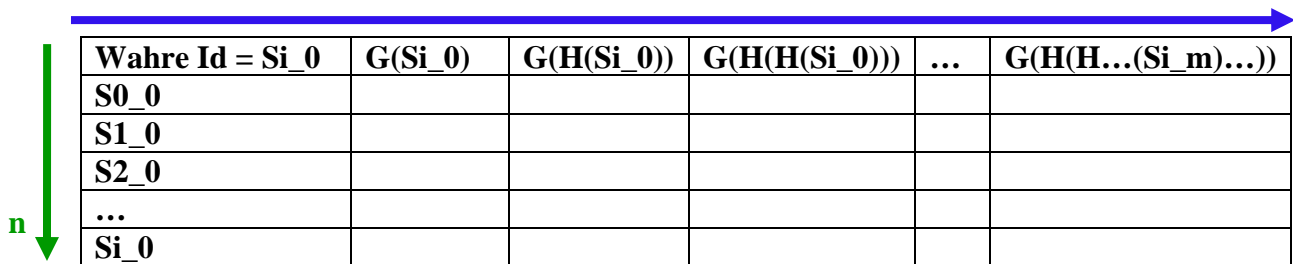
Fazit

Privacy ist gewährleistet. Da das Tag jedes mal einen anderen Hashwert als aktuelle Identität dem Lesegerät rüberschickt, kann es von einem unberechtigten Lesegerät nicht verfolgt werden. Denn dieser kann keinen Zusammenhang zwischen den verschiedenen Werten erkennen.

Forward-Privacy ist mit diesem Protokoll ebenfalls gewährleistet. Findet jemand den aktuellen ID-Wert eines Tags heraus, so kann er rückwirkend keinen Zusammenhang der Werte erkennen. Ist beispielsweise der Wert S0_2 bekannt, so kann kein Zusammenhang auf S0_1 geschlossen werden. Das Tag kann von jetzt an weiterverfolgt werden, aber nicht rückwirkend.

Verbesserung von Avoine und Oechslin

Avoine und Oechslin haben dieses Protokoll auf ein Bibliotheksbeispiel angewendet und die Ausführungszeit berechnet. Es wird angenommen, dass in der Bibliothek 1 Million Bücher ($n = 2^{20}$) sind, die einen Tag haben. Weiter wird angenommen, dass das Tag m mal gelesen wird ($m = 2^{10}$). Das System soll 2^{24} Hashoperationen pro Sekunde ausführen können. Die Durchschnittszeit berechnet sich: $n \cdot m / 2 = 2^{29}$. Das ergibt eine Ausführungszeit von 2^5 und ist ca. eine 1/2 Minute lang.



Wahre Id = Si_0	G(Si_0)	G(H(Si_0))	G(H(H(Si_0)))	...	G(H(H...(Si_m)...))
S0_0					
S1_0					
S2_0					
...					
Si_0					

Wird die Länge des Schlüssels Si_0 im Tag mit 128 Bits = 2^7 angenommen. So benötigt das Speichern von 1 Million Tag-Identitäten **16 MBytes**.

Dieses Beispiel ist mit 1 Million Tag gerechnet worden, wenn aber dieses Protokoll im Handel eingesetzt würde, wo jeder Artikel mit einem Tag versehen ist, wie lange würde es für die Berechnung dauern?

Deshalb haben Avoine und Oechslin vorgeschlagen, dass die Hashwerte schon im Voraus berechnet werden sollen. Das hat den Vorteil, dass das Lesegerät nur einen sequentiellen Scan über die Tabelle machen muss, um den erhaltenen Wert zu vergleichen. Der Nachteil ist, dass so eine Tabelle in unserem Bibliotheksbeispiel $m \cdot 16$ MBytes = 4 GBytes benötigen würde und im Handel noch viel mehr Speicher. Der Speicherplatz würde immer grösser werden.

Time-Memory Trade-Off

Avoine und Oechslin haben einen Trade-Off gemacht. Sie haben versucht, ein optimales Verhältnis zwischen vorausberechneten, abgespeicherten Hashwerten zu finden und Werten, die jedes Mal neu berechnet werden müssen zu finden. In dem oben erwähnten Bibliotheksbeispiel sind sie auf eine Berechnungszeit von nur 1.6 Millisekunden für eine Identitätsabfrage gekommen und haben somit den Zeitaufwand erheblich reduzieren können.

Fazit

Eine Schwäche im System ist die angenommene obere Schranke m . Wer bestimmt, wie viele Male ein Tag ausgelesen werden darf? Was passiert, wenn der Tag ausgelesen ist? Nimmt der Tag dann wieder seinen Anfangswert als Identität an? Ein unberechtigtes Lesegerät könnte einen Tag so lange auslesen, bis das Tag wieder seinen Anfangswert annimmt. Das Lesegerät speichert sich die Zahlenreihenfolge die immer die gleiche sind, wenn der Anfangswert gleich ist und somit ist die Privacy und Forward-Privacy des Tags verletzt. Lässt man aber m ins unendliche gehen, so kann ein Lesegerät unendlich lange rechnen und wenn das Tag nicht zu „seinen“ Tags gehört, dann rechnet dieses Lesegerät unendlich lange.

Eine andere Möglichkeit wäre dem Lesegerät eine Zeitlimite für die Berechnungszeit der Tagserkennung zu geben. Dann werden aber die Tags nach einiger Zeit nicht mehr von den autorisierten Lesegeräten erkannt, denn sie sind ausser der Zeitlimite der Lesegeräte gekommen, wenn deren n zu gross wird.

Ein andere Nachteil dieses Verfahren ist, dass der Tag teurer wird. Denn das Protokoll, sowie die Hashfunktionen müssen abgespeichert werden.

Die Lesegeräte müssen die wahren Identitäten der Tags als Geheimnis hüten.

Der RFID-Reisepass

Ab November 2005 wird der RFID-Reisepass in EU-Länder obligatorisch sein. In der Schweiz kann man noch bis September 2005 einen alten Pass kaufen. In die USA kann man in Zukunft nur noch mit einem RFID-Reisepass ohne Visum einreisen.

Das neue an diesem Pass ist, dass er biometrisch ist. Das digitale Gesichtsbild und später auch die Fingerabdrücke werden darin gespeichert. Wie der Name schon sagt, wird in jedem Pass ein RFID-Tag vorhanden sein. Das Ziel ist, eine stärkere Bindung zwischen der Person und dem Reisepass zu haben. Der Pass wird fälschungssicherer sein, da zusätzliche Signaturen angebracht werden. Die Haltbarkeit des Passes mit einem RFID-Tag ist länger als mit einer Smartkarte, welche über Kontakte funktioniert.

Vorteile von RFID werden auch hier zu Nachteile. Es muss unbedingt verhindert werden, dass der Speicher des Tags von jedem Lesegerät ausgelesen werden kann. Sonst wird die Data-Privacy stark verletzt und man könnte von jeder Person alle Daten kennen, ohne dass sie die Erlaubnis dazu erteilt hat.

Lösungsvorschlag zu Data-Privacy

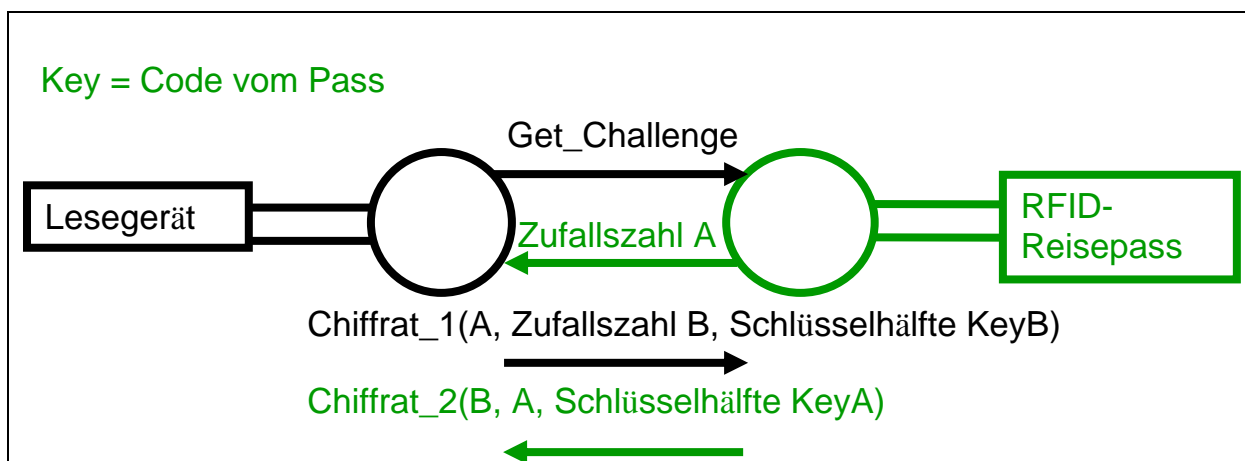
Eine Möglichkeit ist, keine zusätzliche Schutzfunktion anzubringen, sondern den Lesebereich vom Lesegerät zum Tag stark einzuschränken. Dagegen spricht, dass manipulierte Lesegeräte auch von weiterer Distanz den Pass auslesen könnten. Auch kann ein passives Mithören der Kommunikation nicht verhindert werden.

Challenge-Response Authentifikations-Protokoll

Kügler hat das Challenge-Response Authentifikation-Protokoll vorgeschlagen, um unberechtigtes Auslesen des Reisepasses, sowie unerlaubtes passives Mithören, durch unberechtigte Lesegeräte zu verhindern.

Der eindeutige Code des Passes wird in diesem Protokoll als gemeinsamer Schlüssel genommen. Das Lesegerät erhält diesen Schlüssel, indem der Passinhaber den Pass öffnet und dem Lesegerät optischen Zugriff darauf erlaubt. Der Passinhaber kann somit selber bestimmen, wem er den Zugriff auf seinem Pass gibt und wem er es verweigert.

Protokoll Skizze



Protokoll Beschreibung

	Lesegerät	RFID-Reisepass
1	Gib mir eine Zufallszahl	
2		Schickt Zufallszahl A
3	Nimmt Zufallszahl A, eine Zufallszahl B und wählt eine Schlüsselhälfte KeyB. Es verschlüsselt alles mit dem Key und schickt das Chiffirat_1	
4		Entschlüsselt Chiffirat_1 und kontrolliert, ob Zufallszahl A korrekt ist. Nimmt Zufallszahl B, Zufallszahl A und wählt eine Schlüsselhälfte KeyA. Er verschlüsselt alles mit dem Key und schickt Chiffirat_2
5	Entschlüsselt Chiffirat_2 und kontrolliert ob Zufallszahl B korrekt ist.	
6	Verschlüsselte authentifizierte Kommunikationskanal ist aufgebaut mit Schlüssel KeyAKeyB	

So authentifizieren sich Lesegerät und RFID-Reisepass, da nur diese beiden den Key kennen. Für die weitere Kommunikation wird der längere Schlüssel KeyAKeyB verwendet. Der geheime Code des Passes wird nur einmal über einen sicheren (optischen) Kanal übertragen.

Fazit

Dieses Protokoll garantiert Data-Privacy. Der Tag wird viel teurer, da das ganze Protokoll auf dem kleinen Chip realisiert werden muss.

Ist der geheime Code des Passes einer Person bekannt. So kann sie bei einem Lesegerät dabeistehen und jedes Mal auf jeder Tag-Anfrage mit diesem Code antworten. Falls der Passinhaber, von diesem Code, an dem Lesegerät vorbeikommt, dann meint er, dass das Lesegerät geantwortet hat. Tatsächlich ist es aber diese Person gewesen. Die Privacy ist verletzt, da diese Person, den Passinhaber auf diese Weise verfolgen kann. Diese Frage steht noch zur Diskussion offen.

Zusammenfassung

Zwei Vorteile von RFID werden unterschieden. Erstens das automatische und unsichtbare Auslesen eines Tags. Zweitens die Möglichkeit biometrische Daten abzuspeichern und die längere Haltbarkeit von RFID, da sie kontaktlos funktioniert.

Die Vorteile von RFID werden zu Nachteilen: Location- und Data-Privacy Probleme.

Lösungsansatz durch das RFID Hash-Based – Protokoll und Verbesserung durch Avoine und Oechslin. Der RFID-Reisepass und das Challenge-Response Authentisierungsprotokoll werden, durch Dr. Dennis Kügler im CT, vorgestellt.

Quellenangabe

A Scalable and Provably Secure Hash-Based RFID Protokoll (Avoine and Oechslin, EPFL)

Cryptographic approach to „privacy-friendly“ tags. In RFID Privacy Workshop (M. Ohkubo, K. Suzuki, and S. Kinoshita, MIT, USA, 2003)

Risiko Reisepass? (Dr. Dennis Kügler)

Risiken und Chancen des Einsatzes von RFID-Systemen (Bundesamt für Sicherheit in der Informationstechnik)

RFID-Handbuch, Klaus Finkenzeller

Bilder: Internet,

http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker_slides.pdf

Interessanter Link: <http://stoprfid.foebud.org/htm/forder2.html#gefahren>