

Sicherheit bei Smartcards

Chair-Woei Miu

Willinghusener Landstraße 48a
22885 Barsbüttel
0049 40/ 6700242

5miu@informatik.uni-hamburg.de

ABSTRACT

Wenn man von einer Chipkarte spricht, meint man aber meistens eine Smartcard, oder eine Art von Smartcard.

Dieses Paper beschäftigt sich mit dem Aufbau und besonders der Sicherheit bei Smartcards. Es wird in diesem Paper zwischen logischer- und physikalischer Sicherheit unterschieden.

Im letzten Teil werden verschiedene Angriffsmöglichkeiten gezeigt.

General Terms

Sicherheit, Angriffsmöglichkeiten

Keywords

Smartcards, Geldkarte, Synchron- und Asynchrone Smartcards

1. EINLEITUNG

Smartcards, welche im Deutschen auch gerne als Chipkarten bezeichnet werden, werden in vielen Bereichen der Geschäftswelt verwendet. Es handelt sich um die Chipkarten die z.B. als Geldkarte von den Kreditinstituten an die Kunden ausgegeben werden. Smartcards werden auch in Firmen eingesetzt, als so genannte ID-Cards, welche es erlauben in Räume einzutreten, die nur für bestimmte Personen zugänglich sind. Auch in Mobiltelefonen stecken Smartcards in Form einer SIM-Karte.

Es gibt zwei, bzw. drei Erfinder, die die Geschichte der Smartcards sehr geprägt haben.

1. Die beiden deutschen Erfinder: *Jürgen Dethloff* und *Helmut Gröttrup*, wollten im Jahre 1968 in eine Identifikationskarte einen Schaltkreis einbauen.
2. Der französische Erfinder *Roland Moreno* wollte ein elektronisches Objekt entwickeln, worauf er persönliche und streng vertrauliche Daten speichern kann. Diese sollten aber erst aufrufbar sein, wenn der Eigentümer einen Code (PIN) eingibt. [1][2]

2. AUFBAU DER SMARTCARDS

Die Smartcards sind mit einem Mikrochip bestückt, welcher das Einsatzgebiet der Smartcards bestimmt. Die Geldkarte verwendet z.B. einen Mikrochip, der speziell für den zentralen Kreditausschuss (ZKA) hergestellt wird..

Der Mikrochip ist normalerweise komplett in der Plastikkarte integriert. Die Verbindung zur Außenwelt wird durch das Chipkartenmodul ermöglicht. Die Kontakte des Chipkartenmoduls werden fälschlicherweise öfters als Chip bezeichnet. Das Chipkartenmodul besitzt entweder sechs oder acht Kontakte, obwohl meistens fünf zur Kommunikation schon ausreichen.

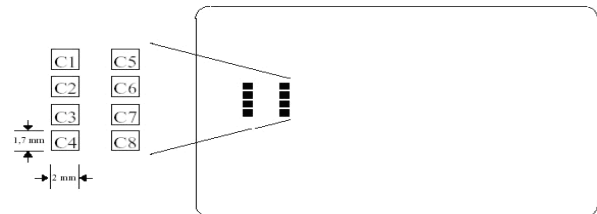


Abbildung 1: Eingänge einer Smartcard [1]

Tabelle : Erläuterung der Chiipeingänge [1]

Kontakt	Signal	Anmerkung
C1	Vcc	Versorgungsspannung
C2	RST	Reset-Signal
C3	CLK	Taktsignal
C4	RFU	Reserviert für zukünftige Anwendungen
C5	GND	Masse
C6	Vpp	Programmierspannung
C7	I/O	Dateneingang/ -ausgang
C8	RFU	Reserviert für zukünftige Anwendungen

Es gibt drei verschiedene nach ISO 7816 genormte Größen, die die Chipkarten haben sollten:

- **ID-1:** Die am meisten genutzte Größe (85,60 × 53,98 mm) wird bei Kreditkarten, Telefonkarten, EU-Führerscheinen und bei Krankenversicherungskarten genutzt.
- **ID-00:** Die Größe (66mm × 33mm) wurde bisher selten oder noch nicht genutzt.
- **ID-000:** Das Kleinste Format misst gerade mal 25mm × 15mm und wird üblicherweise in Mobiltelefonen als SIM-Karte eingesetzt. [1][2]

2.1 Synchrone Smartcards

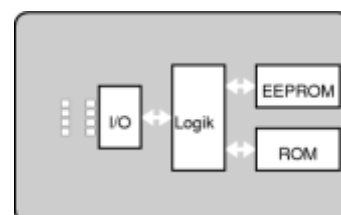


Abbildung 2: Blockschaltbild einer synchronen Smartcard [2]

Die synchronen Smartcards besitzen nur einen Speicher, welcher beschrieben oder ausgelesen werden kann. Es ist möglich, über die I/O Schnittstelle auf einzelne Speicherzellen zuzugreifen. Synchronen Smartcards finden z.B. in Telefonkarten oder Krankenkassenkarten ihren Platz.

Diese Smartcards werden nur verwendet, um Daten zu speichern, nicht um komplexe Vorgänge abzuwickeln.

2.2 Asynchrone Smartcards

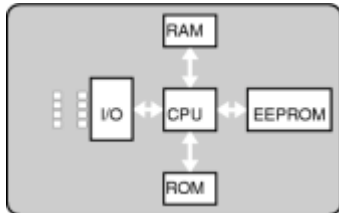


Abbildung 3: Blockschaltbild einer asynchronen Smartcard [2]

Die asynchronen Smartcards besitzen im Gegensatz zu den synchronen Smartcards einen Mikroprozessor. Über den Mikroprozessor ist es möglich, auf die gespeicherten Daten zuzugreifen.

Es ist nicht möglich den Datenspeicher direkt auszulesen, man muss den Weg über den I/O (Ein- und Ausgang), und über die CPU (Prozessor) gehen.

Der Vorteil der asynchronen Smartcards liegt darin, dass man mit Hilfe des Prozessors kryptographische Verfahren entwickeln kann, um die gespeicherten Daten vor fremdem Zugriff zu schützen. Wenn der Chip einmal fertig hergestellt wurde, ist es nicht mehr möglich, das auf der Smartcard laufende Programm zu ändern. [1][2]

3. ANGRIFFSMÖGLICHKEITEN

Um an Daten, welche auf der Smartcard gespeichert sind, zu gelangen, gibt es verschiedene Angriffsmöglichkeiten.

In den folgenden Untertiteln werden einige Angriffsmöglichkeiten vorgestellt.

3.1 Angriff des Terminals gegen den Karteneigentümer

Bei diesem Angriff wird z.B. bei einer Geldkarte nicht der eingegebene Betrag abgebucht, sondern ein anderer. Der Karteneigentümer bekommt davon erstmal nichts mit, da auf der Anzeige nur der eingegebene Betrag als abgebucht angezeigt wird und nicht der wirklich abgebuchte Betrag.

Dann gibt es noch eine Art Angriff des Terminals gegen den Kontoeigentümer. Man hängt ein Schild auf das richtige Terminal auf, worauf steht, dass dieser defekt sei und man solle an einen anderen gehen. Da nur ein anderer da steht, wird dieser dann vom ahnungslosen Kartenhalter genutzt. Dieser ist aber so präpariert, dass der Karteninhaber seine Karte hinein steckt und seinen PIN eingibt, daraufhin wird dann eine Fehlermeldung erscheinen und die Karte wieder ausgegeben, oder zieht diese gleich ein. [3][4]

3.2 Angriff des Karteneigeninhaber gegen den Dateneigentümer

Bei diesem Angriff geht es darum die auf der Karte gespeicherten Daten auszulesen, verändern oder gar zu kopieren.

Solche Angriffe finden z.B. in Smartcard geschützten Firmen statt. So könnte man einem Arbeiter der Firma die Karte stehlen, kopieren und unbemerkt wieder zurückgeben. Somit hätte man Zugang zu der Firma, ohne, dass jemand davon was mitkriegt. Bei Geldkarten kann solch ein Angriff auch stattfinden. Es wäre möglich den geladenen Geldbetrag zu verändern, um damit Profit zu machen.

3.3 Versuch an den kartenspezifischen Schlüssel zu gelangen

Den kartenspezifischen Schlüssel benötigt man um Daten auslesen zu können. Dieser ist aber an einem speziell geschützten Bereich der Smartcard gespeichert. Also ist es sehr schwer an diesen zu kommen.

Es gäbe die Möglichkeit die Sicherung, die bei der Herstellung der Karte durchgebrannt wurde, wieder herzustellen. Dadurch würde die Karte sich wieder in den Testmodus schalten, worin man die Gespeicherten Daten Auslesen und Verändern kann. [3][4]

4. Sicherheit bei Smartcards

Die Sicherheit bei Smartcards ist sehr wichtig, besonders, wenn es um Geldkarten, SIM-Karten oder ID-Cards geht.

Die Smartcard sollte sicher vor unbefugten Zugriff auf die gespeicherten Daten sein. Bei der Geldkarte wäre es z.B. fatal, wenn es möglich wäre, den geladenen Geldstand zu verändern. Deshalb sind die Smartcards mehrfach gesichert.

4.1 Physikalische Sicherheit

Bei den Smartcards sollen physikalische Sicherheitsmaßnahmen das Analysieren und das Manipulieren der Karte verhindern. Dieses wird durch Sensoren, die die Funktions- und Speicherelemente überwachen ermöglicht.

Durch eine sehr hohe Transistordichte wird der Informationsgewinn über die Struktur des eingebauten Mikrocontrollers erschwert, bzw. unmöglich macht. Die Verbindung zwischen Speicher und dem Mikroprozessor darf von Außen nicht kontaktierbar sein, da man sonst direkten Zugriff auf den Speicher hätte.

Die Leistungsaufnahme, bei verschiedenen Befehlen des Prozessors darf keinen großen Schwankungsbereich haben, sonst wäre es möglich, durch verschiedene Leistungsaufnahmen auf kryptographische Schlüssel zu schließen.

Es werden noch die Adress- und Datenleitungen komplett ungeordnet verlegt um die Zuordnung zu den einzelnen Funktionselementen zu erschweren.

Es wird nach Eingabe der benötigten Informationen, je nach Einsatzgebiet der Karte, eine Sicherung im Inneren des Chips durchgebrannt, um das spätere ändern der Daten unmöglich zu machen. Im EEPROM (siehe dazu auch Abbildungen 2 und 3) wird vermerkt, dass sich diese Karte nicht mehr in den Testmodus zurückschalten lässt. Dieses ist sehr wichtig, da es möglich ist, im Testmodus die gespeicherten Daten zu verändern.

Auf den Chip wird noch eine Passivierungsschicht aufgetragen, um eine Manipulation von außen zu verhindern. Wenn diese Schicht entfernt wird, wird die Karte deaktiviert.

Das Fehlen der Schicht wird durch Widerstands, bzw. Kapazitätsmessungen der Smartcard bemerkt.

Es wird noch die Eingangsspannung von der Smartcard selbst geprüft, um sicherzustellen, dass die nicht mit einer falschen Spannung betrieben wird und ungewünscht Informationen preisgibt.

Die angelegte Taktfrequenz wird auch gemessen. Wenn diese ein bestimmtes Minimum unterschreitet, wird die Karte automatisch deaktiviert.

4.2 Logische Sicherheit

Um die logischen Sicherheitsanforderungen auf einer Smartcard zu realisieren, muss eine Datensicherung und eine sichere Kommunikation gewährleistet sein.

Die Kommunikation wird durch kryptographische Verfahren gesichert.

Die Datensicherung wird dadurch realisiert, dass man nur, wie in Kapitel 3.2 beschrieben, über den I/O und dann durch den Prozessor auf den Speicher zugreifen kann.

Dazu kommt noch, dass nicht das ganze Betriebssystem auf dem ROM gespeichert wird. Das Betriebssystem wird erst bei der Initialisierung der Smartcard komplettiert.[1]

5. ABSCHLUSS

Smartcards sind eigentlich sehr sichere Karten, wenn man sie nicht in verdächtige Kartenterminals hinein steckt. Sie werden ständig weiterentwickelt und werden somit auch immer sicherer.

Eine Weiterentwicklung der Smartcards sind die Javacards.

Diese macht es möglich, mehrere Anwendungen auf einer Karte laufen zu lassen. Damit hat man mehrere Karten in einer, was das Kartengewirr in den Brieftaschen um einiges erleichtert.

6. REFERENZEN

- [1] Marcel Selhorst
Die Geldkarte eine „sichere“ elektronische Geldbörse?!(Seminararbeit)
http://www.prosec.rub.de/staff/selhorst/geldkarte_selhorst.pdf
am: ?? ?? 2002
- [2] Wikipedia.
Chipkarte
<http://de.wikipedia.org/wiki/Smartcard>
am: 03.01.2006
- [3] Bruce Schneier
Breaking Hard to Do: Modeling Security Threats for Smart Cards
https://www.usenix.org/publications/library/proceedings/smartcard99/full_papers/schneier/schneier.pdf
am: 10-11.05.1999
- [4] Philipp Gühring
Sicherheitsprobleme bei Smart Cards
<http://www3.futureware.at/smartcard/smartcard.pdf>
am: 19.10.1999

