Grundlagen von Chipkarten

Marcin Korzen
Hochschule für Technik Stuttgart

04. November 2007

Inhaltsverzeichnis

1 Einleitung

Chipkarten spielen eine immer größere Rolle im gesellschaftlichen Leben von Menschen.

Die Geschichte von Chipkarten begann Mitte der 50-er Jahren in den USA mit der Einführung der ersten Geldkarten Visacard und Mastercard auf den amerikanischen Markt. Seit damals haben Chipkarten sehr an Bedeutung gewonnen.

Heutzutage sind die üblichen Zahlungsmittel, wie z.B. Bargeld, durch Chipkarten auf den zweiten Plan verschoben. Der Grund dafür ist die Bequemlichkeit. Man braucht kein Bargeld mehr dabei zu haben, um seine Rechnungen bezahlen zu können.

Der Anwendungsbereich von Chipkarten ist vielfältiger und breiter geworden. Chipkarten kommen nicht nur in dem Bereich des Zahlungsverkehrs zum Einsatz, sondern auch im Bereich der Zugangskontrolle und der Datenspeicherung.

In dieser Arbeit soll untersucht werden, ob Chipkarten eine sichere und ausgereifte Technologie geworden sind. Zunächst werden die Grundlagen von Chipkarten erläutert. Dabei werden als erstes die unterschiedlichen Typen von Chipkarten geschildert. Dann wird der Aufbau von Chipkarten beschrieben. Im Anschluss daran werden Sicherheitsmechanismen vorgestellt und schließlich die Arten von Chipkartenanwendungen erwähnt.

2 Typen von Chipkarten

Chipkarten lassen sich bezüglich des Chiptyps in Speicherkarten und Chipkarten einteilen. Der Unterschied bezieht sich auf deren Aufbau. Außerdem muss auch zwischen drei Funktionsweisen unterschieden werden. Nämlich zwischen kontaktbehafteten, kontaktlosen und dual-interface Chipkarten.

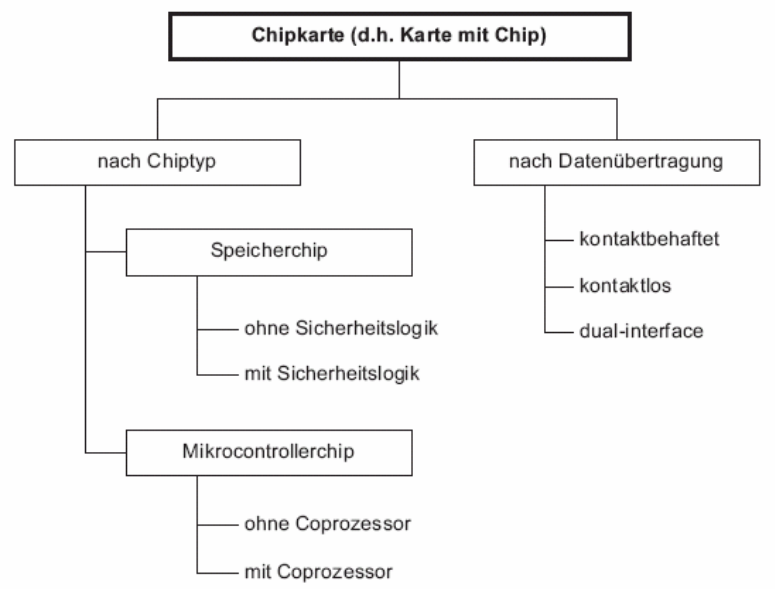

Abbildung 1: Klassifizierung von Chipkarten differenziert nach Chiptyp und Datenübertragung [1].

2.1 Speicherkarten

In Speicherkarten wird ein Speicherchip eingebaut. Durch eine Sicherheitslogik wird es sichergestellt, dass die so genannte Speicherzelle nur einmal geschrieben und nicht mehr gelöscht werden kann.

Speicherkarten können überall eingesetzt werden. Die bekanntesten Beispiele für den Einsatz von Speicherkarten sind Telefonkarten und Krankenversicherungskarten. Im Falle von Telefonkarten wurde die Sicherheitslogik noch erweitert, beispielsweise durch die Eingabe eines PIN. Krankenversicherungskarten sind auch Speicherkarten. Bevor Speicherkarten in diesem Bereich eingesetzt wurden, waren persönliche Daten auf dem Krankenschein eingetragen. Zurzeit werden die Daten auf dem Chip gespeichert. Mit Hilfe eines Lasergerätes können die problemlos gelesen werden[1].

Dadurch, dass der Chip billig ist, werden die Speicherkarten günstiger als Prozessorkarten, was der größte Vorteil des Typs von Chipkarten ist. Der Nachteil bezieht sich auf die Hauptsache, dass die Speicherzelle nur einmal geschrieben und nicht mehr gelöscht werden kann. Beispielsweise können dadurch Telefonkarten nicht neu geladen werden.

Zusammenfassend lässt sich sagen, dass die Speicherkarten auf Grund deren niedrigen Preises dort eingesetzt werden, wo der Kaufpreis eine große Rolle spielt. Was bei einer Massenfertigung einen großen Gewinn verursachen kann.

2.2 Prozessorkarten

Im Gegenteil zu den Speicherkarten besitzen Prozessorkarten, außer einem Chip, noch einen Mikroprozessor. Dadurch können sie frei programmiert werden.

Die heutigen Geld- und Kreditkarten gehören im Allgemeinen zu diesem Typ. In diesem Fall können unterschiedliche komplexe Kryptoalgorithmen und Verschlüsselung von geheimen Schlüsseln eingesetzt werden. Die einzige Beschränkung ist der verfügbare Speicherplatz und was sich damit verbindet, eine begrenzte Recherleistung. Jedoch durch die so schnell entwickelnde Technologie werden der Speicherplatz und die Recherleistung mit der Zeit immer größer.

Außerdem können die Prozessorkarten beispielsweise nach dem Verbrauch des Guthabens wieder aufgeladen werden, weil die Speicherzelle mehrere Male geschrieben und gelöscht werden kann. Als Beispiel können SIM-Karten erwähnt werden, die in jedem Mobiltelefon zum Einsatz kommen und nach dem Verbrauch des Guthabens aufgeladen werden können.

Auch die Möglichkeit im Internet sicher bezahlen zu können, haben wir Prozessorchipkarten zu verdanken. Durch den Einsatz von Kryptoalgorithmen und Verschlüsselung von geheimen Schlüsseln können Internetzahlungen mit hohem Sicherheitsniveau realisiert werden.

Zusammenfassend lässt sich sagen, dass durch die Vorteile von Prozessorkarten, wie die Verschlüsselung von Daten, Einsatz von Kryptoalgorithmen, die Zukunft den Prozessorkarten offen steht. Es werden immer neue Bereiche entdeckt, in denen Prozessorkarten eine neue bessere Qualität ermöglichen.

2.3 Kontaktbehaftete Karten

Die Kommunikation zwischen einer Karte und einem Terminal erfolgt durch das Einstecken der Karte in einen Kartenleser.

Die Funktionsweise ist in manchen Fällen gewünscht. Beispielsweise bei Zahlungsvorgängen. In diesem Fall soll die Karte ins Terminal eingesteckt und die Bestätigung gedruckt werden, was mit einer Willenserklärung gleichbedeutend ist. Wäre es möglich Zahlungsvorgänge kontaktlos durchzuführen, könnten beispielsweise Betrüger ohne Wissen des Kontoinhabers das Geld aus dessen Karte abzubuchen [1].

2.4 Kontaktlose Karten

Heutzutage können sowohl Speicher- als auch Mikroprozessorkarten kontaktlos arbeiten.

Kontaktlose Speicherkarten funktionieren in einem Abstand bis zu 1 Meter von Terminal. Das ist ein großer Unterschied im Vergleich zu kontaktlosen Mikroprozessorarten, weil die Entfernung von Terminal, bei diesem Typ, auf ein paar Zentimeter beschränkt ist [1].

Kontaktlose Chipkarten kommen vor allem im Bereich der Zugangskontrolle zum Einsatz. Der Grund dafür ist, dass sich die Karte beispielsweise in einem Geldbeutel oder in einer Tasche befinden kann und der Nutzer die nicht in der Hand halten muss, um seine Identifikation durchführen zu können.

2.5 Dual-Interface-Karten

Chipkarten dieses Typs funktionieren sowohl kontaktbehaftet als auch kontaktlos. Das ist durch die Integration beiden Funktionen auf einem Chip möglich. Die Dual-Interface-Karten können deswegen auf beide Weisen mit einem Terminal arbeiten [4].

3 Aufbau von Chipkarten

3.1 Speicherkarte

Eine Speicherkarte besteht aus mehreren Komponenten, die folgende Aufgaben haben:

- Adress- und Sicherheitslogik – Kontrolle des Zugriffs auf den Speicher
- EEPROM - Ablegung von erforderlichen Daten für die Anwendung
- I/O Schnittstelle - Übertragung von Daten
- ROM – enthält Identifizierungsdaten

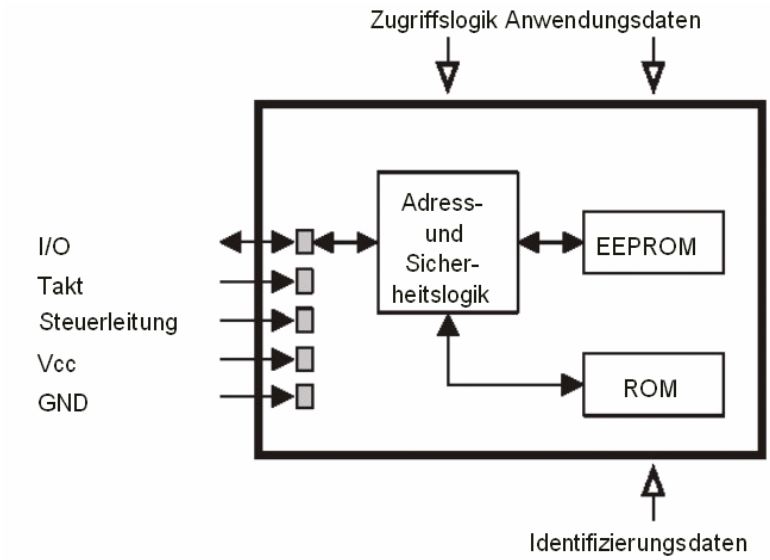

Abbildung 2: Architektur einer kontaktbehafteten Speicherkarte mit Sicherheitslogik [1].

3.2 Prozessorkarte

Eine Prozessorchipkarte besteht aus folgenden Komponenten:
- CPU – ein Mikroprozessor zur Verarbeitung von Daten
- NPU– ein Kryptoprozessor zur effizienten Ausführung von Kryptoverfahren
- I/O Schnittstelle – Übertragung von Daten
- ROM – enthält das Betriebssystem des Chips, kann nicht gelöscht werden
- RAM – Arbeitsschpeicher des Prozessors, nicht löschbar und flüchtig
- EEPROM – Speicherung von Anwendungsdaten, z.B. kryptographische Schlüssel oder Zertifikate, kann vielfach beschrieben werden und ist nicht flüchtig.

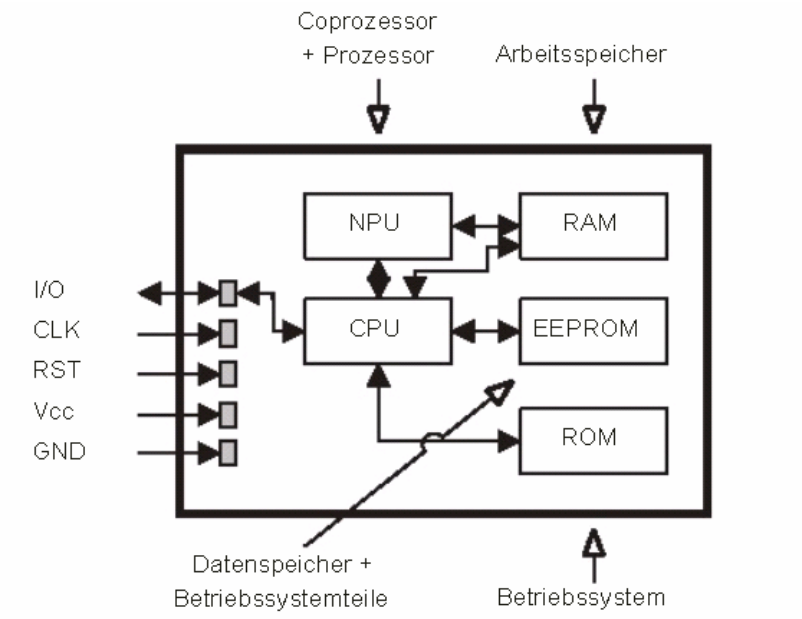

Abbildung 3: Architektur einer kontaktbehafteten Mikroprozessorkarte mit Koprozessor [1].

4 Sicherheit von Chipkarten

Die Sicherheit ist eine der wichtigsten Anforderungen an Chipkarten. Es muss sichergestellt werden, dass die Technologie eine sichere Nutzung von Chipkarten ermöglicht. Deshalb sind die Anforderungen an ihre Sicherheit besonders hoch. Das bedeutet, dass das Extrahieren von Informationen aus einer Chipkarte von einem Angreifer mit einem großen finanziellen und zeitlichen Aufwand verbunden werden muss.

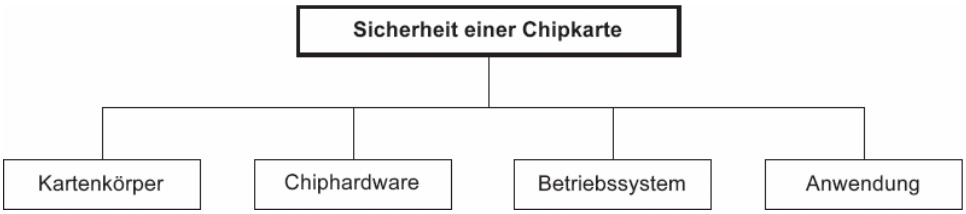

Abbildung 4: Vier Segmente, die die Sicherheit einer Chipkarte garantieren [1].

Das erste Segment ist der Kartenkörper, in dem sich ein Chip befindet. Die Prüfung der Sicherheitsmerkmale kann nicht nur maschinell sondern auch visuell von Menschen erfolgen.

Die drei weiteren Segmente Chiphardware, Betriebssystem und Anwendung sind für das Schutz der Daten und Programme, die sich in dem Mikroprozessor der Chipkarte befinden, verantwortlich.

Die Überprüfung des ersten Segments kann ausfallen, falls die Chipkarte in einem Bereich ohne Menschlichen Kartenprüfung genutzt wird.

Die drei übrig bleibenden Segmente sind unbedingt nötig, um die physikalische und logische Angriffssicherheit der Chipkarte gewährleisten zu können. Wenn nur eins der Segmente ausfällt, ist die Chipkarte nicht mehr sicher [1].

4.1 Angriffsmöglichkeiten

Es kann zwischen unterschiedlichen Angriffsmöglichkeiten unterschieden werden:

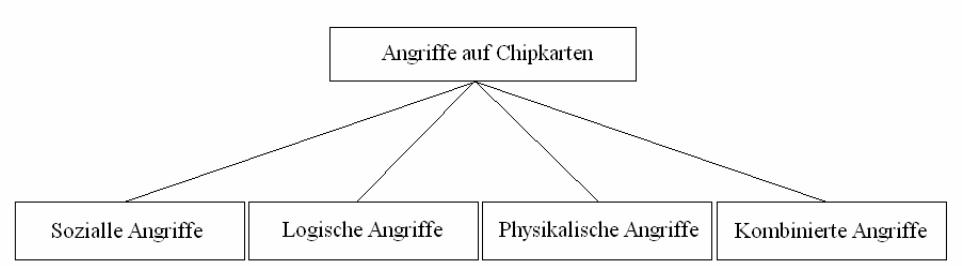

Abbildung 5: Angriffsmöglichkeiten auf Chipkarten

Soziale Angriffe

Die Art von Angriffen richtet sich an Personen. Das können sowohl Entwickler, als auch Kartenbesitzer sein. Das Ziel könnte es beispielsweise sein, wichtige Informationen von diesen Personen zu bekommen. Um die sozialen Angriffe zu beschränken, wurden unterschiedliche Maßnahmen eingeführt, die einen Angreifer von einem sozialen Angriff abwahren sollen [4].

Beispielsweise werden Programmierverfahren bekannt gegeben. Der Grund dafür ist, dass die Sicherheit nur von den geheimen Schlüsseln abhängt. Das führt dazu, dass das Wissen eines Programmierers dem Angreifer nichts bringt.

Logische Angriffe

In diesem Fall wird es versucht, durch die Schnittstelle auf den Speicher einer Chipkarte zuzugreifen. Es kann auch durch einen Fehler in der Implementierung von eingesetzten Protokollen versucht werden, auf den Speicher einer Chipkarte zuzugreifen. Um die Risiko eines erfolgreichen Angriffs zu beschränken, müssen Chipkarten unterschiedliche Tests überstehen [4]. Erst nach dem intensiven Testen können sie zum Einsatz kommen.

Heutzutage gibt es keine bekannten, erfolgreichen, logischen Angriffe.

Physikalische Angriffe

Um die Informationen aus einer Chipkarte auslesen zu können, wird es auch versucht auf die gespeicherten Informationen physikalisch zuzugreifen. Das ist beispielsweise durch den Einsatz von speziellen Lesegeräten möglich. Der Grund dafür, dass die physikalischen Angriffe praktisch unmöglich sind, ist das, dass sich die Geräte nur in speziellen Labors befinden und nur einige Spezialisten zu denen einen Zugang haben [4].

Kombinierte Angriffe

Die kombinierten Angriffe sind eine Mischung aus mehreren unterschiedlichen Angriffen. Beispielsweise kann ein physikalischer Angriff als Vorbereitung für den nachfolgenden logischen Angriff dienen [4].

4.2 Benutzeridentifizierung

Es kann zwischen folgenden Sicherheitsmechanismen unterschieden werden:

Prüfung einer Geheimzahl
Die am meisten benutzte Benutzeridentifizierung ist die Eingabe einer PIN. Die Länge einer PIN soll zwischen 4 und 12 Stellen haben, damit die Wahrscheinlichkeit gering ist, dass jemand die PIN einfach errät [5].

Zur Eingabe einer PIN wird die Tastatur eines Terminals benutzt. Der Wert der PIN wird von Terminal zur Chipkarte geschickt, wo sich ein Referenzwert befindet. Die beiden Werte werden verglichen und das Ergebnis wird an Terminal gesendet.

Die PIN kann entweder statisch oder veränderbar sein. Bei den statischen PINs kann der Wert nicht geändert werden. In Falle von veränderbaren PINs kann der Wert so oft wie gewünscht geändert werden.

Wie schon früher erwähnt wurde, ist die Eingabe einer PIN gleichbedeutend mit Willenserklärung. Der Nutzer erklärt sich mit der Eingabe einer PIN, dass er, sozusagen, weiß, was er tut.

Die Formel für die Wahrscheinlichkeit des Erratens einer PIN:

$$P = \frac{i}{m^n}$$

dabei:
i – Anzahl der Versuche
m – Anzahl der möglichen Zeichen pro Stelle
n – Anzahl der Stellen

Als Beispiel beträgt die Wahrscheinlichkeit, bei dreimaligem Versuch eine vierstellige PIN zu erraten, 0,03% [1].

Biometrische Verfahren
Da viele Menschen Probleme haben, um sich eine PIN zu merken, werden von Manchen biometrische Verfahren favorisiert. Die Verfahren sind weder schneller auch sicherer als die Eingabe einer PIN [1].

Der Unterschied ist, dass es keine Geheimzahl mehr gebraucht wird, um die Identifizierung eines Nutzers durchzuführen, sondern die Person kann auf Grund ihrer einzigartigen, biologischen Merkmalen identifiziert werden.

Die biometrischen Verfahren werden besonders dadurch interessant, dass sie eigenartig und unänderbar sind.

Um eine Person zu identifizieren eignen sich nur die Merkmale, die alle folgenden Punkte erfüllen:
- technisch gut messbar
- eindeutige Zuordnung einer Person
- keine Veränderung des Merkmals möglich

- sehr geringe Veränderung des Merkmals mit der Zeit
- Akzeptanz der Messmethode und des Merkmals durch Benutzer

5 Anwendungstypen

5.1 Speicherbasierte Anwendungen

Bei dem Typ von Anwendungen ist der Zugriff auf den gesamten Speicher möglich. Das Terminal kann auf dem Speicher sowohl lesen, als auch schreiben. Der Speicherchip bestimmt die notwendige Zugriffslogik, die nicht geändert werden kann.

Der Typ von Anwendungen findet vor allem den Einsatz bei einfachen Anwendungen. Der Grund dafür ist, dass einerseits Speicherkarten kostengünstig sind, andererseits ihre Komplexität aber begrenzt ist. Das führt dazu, dass sie nicht in allen Bereichen zum Einsatz kommen können [2].

5.2 Dateibasierte Anwendungen

In den dateibasierten Anwendungen werden Prozessorkarten mit einem Chipkarten-Betriebssystem genutzt. Eine dateibasierte Anwendung besteht aus Datendateien in einer Verzeichnisdatei. Die Zugriffsrechte auf die Datendateien wie Lesen, Löschen, Schreiben und Erzeugen werden festgelegt und in einem Regelsatz gespeichert.

Die Eigenschaften von den dateibasierten Anwendungen erfüllen alle Anforderungen, damit komplexe Anwendungen ohne Programmkode erstellt werden können [2].

5.3 Kodebasierte Anwendungen

Die kodebasierten Anwendungen charakterisieren sich dadurch, dass sie im Vergleich zu den dateibasierten Anwendungen noch ein Programmkode haben, der an die Anwendungsspezifikation angepasst wurde.

Der Vorteil ist, dass der Anwendungsentwickler den Kode selbst programmieren kann, um eine gewünschte Funktionalität zu bekommen. Die Tatsache führt jedoch dazu, dass die kodebasierten Anwendungen fehlerhaft werden können. Dadurch entstehen neue Sicherheitslücken. Es lässt sich sagen, dass der Typ von Anwendungen erst dann eingesetzt werden soll, wenn es sichergestellt wird, dass die dateibasierten Anwendungen die Anforderungen nicht erfüllen können [2].

6 Zusammenfassung

Die zurzeit verwendeten Sicherheitsmassnahmen bieten keinen 100%-igen Schutz gegen Angreifer an. Zwar erschweren sie deutlich Angriffsversuche, können die aber nicht vollständig unterbinden.

Der Angreifer muss jedoch mit dem riesigen, zeitlichen und finanziellen Aufwand rechnen, der nötig ist, um Informationen aus einer Chipkarte extrahieren zu können.

Daraus lässt sich schließen, dass trotz des nicht 100%-igen Schutzes gegen Angriffsversuche, Chipkarten eine sichere und ausgereifte Technologie sind. Die Nutzer müssen sich nicht fürchten, ob ihr Daten oder Geld gefährdet sind.

Literatur

[1] Wolfgang Rankl, Wolfgang Effing: *Handbuch der Chipkarten (4. Auflage)*, 2002, Carl Hanser Verlag München Wien.

[2] Wolfgang Rankl, *Chipkarten-Anwendungen - Entwurfsmuster für Einsatz und Programmierung von Chipkarten*, 2006, Carl Hanser Verlag München Wien.

[3] Krister Helbing, *Sichere Kommunikation und Authentifizierung in medizinischen Netzwerken mit Hilfe von Mikroprozessorkarten*, 2005, Bachelorarbeit, Georg-August-Universität Göttingen, - http://www-archiv.informatik.uni-goettingen.de/cms-content/gaug-zfi-bm-2005-05.pdf
Abgerufen am 11.10.2007

[4] D21 Arbeitsgruppe 5, *Mehr Sicherheit, Mobilität und Effizienz durch den Einsatz von Chipkarten*, 2002, - http://kommforum.difu.de/upload/files/ beitraege_aufsaetze/186/Initiative%20D21_SmartcardsReport.pdf
Abgerufen am 11.10.2007

[5] Lars Morres, *Sicherung von Chipkarten*, 2002, - http://www.humboldtschule-berlin.de/unterricht/inf/pdf/chipkarten.pdf
Abgerufen am 11.10.2007