Grundlagen von Chipkarten

Marcin Korzen
Hochschule für Technik Stuttgart

19. Oktober 2007

Inhaltsverzeichnis

1 Einleitung

Chipkarten spielen immer größere Rolle im gesellschaftlichen Leben von Menschen.

Die Geschichte von Chipkarten begann in den 50-er Jahren in den USA mit der Einführung der ersten Geldkarten Visacard und Mastercard auf den amerikanischen Markt. Von daher bis heute 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 zum Einsatz nicht nur in dem Bereich des Zahlungsverkehrs, 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. Als erstens werden 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 in Speicherkarten und Chipkarten einteilen. Der Unterschied bezieht sich auf deren Aufbau. Außerdem muss auch zwischen zwei Funktionsweisen unterschieden werden. Nämlich zwischen kontaktbehafteten und kontaktlosen Chipkarten.

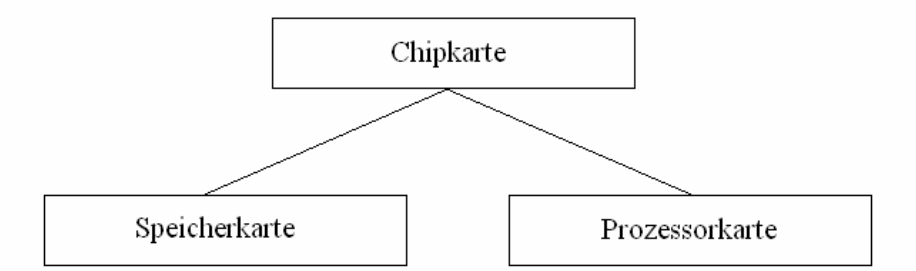

Abbildung 1: Typen von Chipkarten

2.1 Speicherkarten

In Speicherkarten wird kein Mikrocontroller eingebaut, sondern nur ein Speicherchip. 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 Chipkarten sind Telefonkarten und Krankenversicherungskarten. In dem Fall von Telefonkarten wurde die

Sicherheitslogik noch erwartet, beispielsweise durch die Eingabe eines PIN. Krankenversicherungskarten sind auch Speicherkarten. Persönliche Daten werden auf dem Chip gespeichert und mit Hilfe eines Lasergerätes gelesen [1].

Dadurch, dass der Chip klein 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.

2.2 Prozessorkarten

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

Die sich heutzutage in Benutzung befindenden Geld- und Kreditkarten gehören zu dem 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.

Auch die Möglichkeit im Internet sicher bezahlen zu können, haben wir Prozessorchipkarten zu bedanken [1].

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 Kontaktlose Karten

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

Kontaktlose Chipkarten kommen zum Einsatz vor allem im Bereich der Zugangskontrolle. Der Grund dafür ist, dass sich die Karte beispielsweise in einem Geldbeutel oder in einer Tasche befinden kann und der Nutzer die nicht im Handy halten muss, um seine Identifikation durchführen zu können [1].

2.4 Dual-Interface-Karten

Chipkarten dieses Typs besitzen die Kommunikationsschnittstelle sowohl der kontaktbehafteten, als auch der kontaktlosen Speicherkarten. 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

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

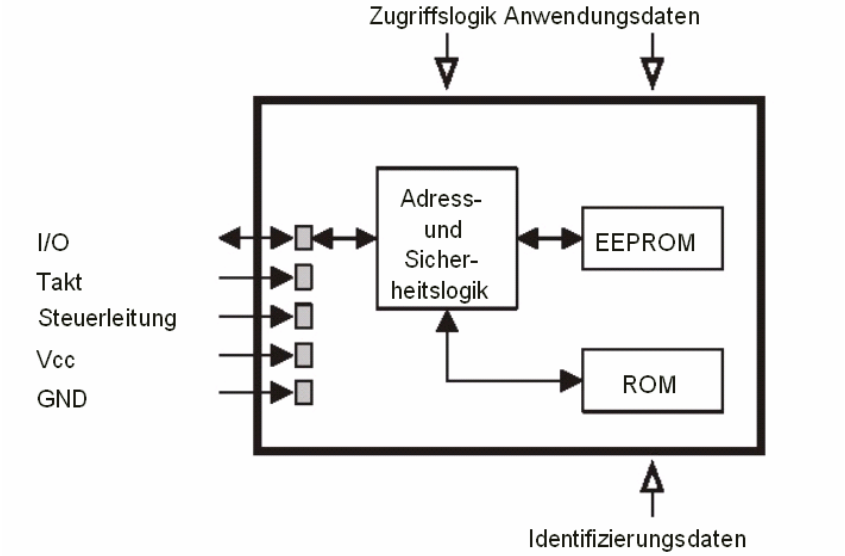

Abbildung 2: Typische Architektur einer kontaktbehafteten Speicherkarte mit Sicherheitslogik [1].

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.

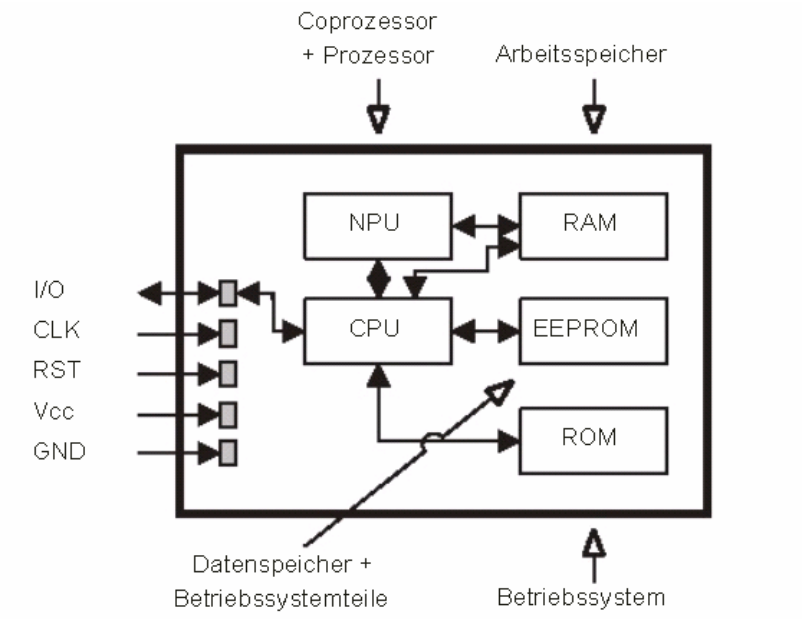

Abbildung 3: Typische Architektur einer kontaktbehafteten Mikroprozessorkarte mit Koprozessor [1].

4 Sicherheit von Chipkarten

Die Sicherheit ist eine von den 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.

Es kann zwischen unterschiedlichen Angriffsmöglichkeiten unterschieden werden:

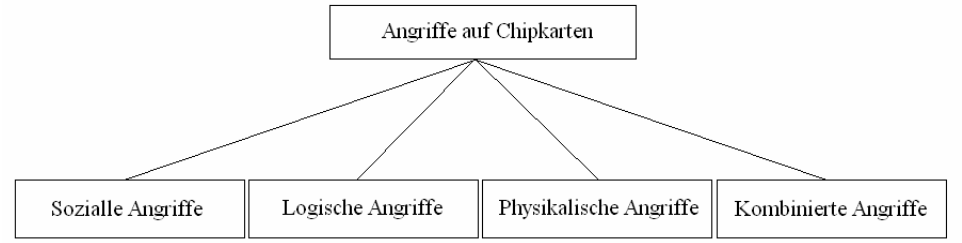

Abbildung 4: Angriffsmöglichkeiten auf Chipkarten

4.1 Soziale Angriffe

Die Art von Angriffen richtet sich an Personen. Das können sowohl Entwickler, als auch Kartenbesitzer sein. 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.

4.2 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, was das beste Beispiel dafür ist, dass durch das Testen logische Angriffe verweigert werden können.

4.3 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 Geräten 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].

4.4 Kombinierte Angriffe

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

5 Anwendungen von Chipkarten

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, Schreiben, Löschen, Schreiben, 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, falls der Anwendungsentwickler nicht genug Erfahrung hat.

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

[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