Grundlagen und Anwendungsgebiete von Chipkarten

Leitung: Adrian Spalka und Hanno Langweg
Autor: Sven Tantau, tantau@informatik.uni-bonn.de
Institut für Informatik III
Universität Bonn

Stand: 10. April 2002

Dieses Dokument ist Teil eines Seminars über Chipkarten im Rahmen des Informatikstudiums. Hierbei soll anhand des Buches *Handbuch der Chipkarten* das Thema der IT-Sicherheit bei Chipkarten diskutiert werden. Grundlage für diese Ausarbeitung sind die Kapitel 1 und 2 sowie 13 und 14.

Inhaltsverzeichnis

1 Einleitung

Diese Ausarbeitung beschreibt die Grundlagen und Anwendungsgebiete von Chipkarten.

Als erstes werde ich auf die verschiedenen Kartenarten eingehen und die Speicherkarte und die Mikroprozessorkarte näher beschreiben. Um die Materie verständlicher und interessant zu gestalten gebe ich einige Beispiele an. Bei der Mikroprozessorkarte wird zudem noch auf das Betriebssystem und das Dateisystem eingegangen.

Kapitel Nummer drei befasst sich mit Kartenterminals, wobei Sicherheitsfunktionen im Vordergrund stehen.

Im vierten Kapitel beschreibe ich den Lebenszyklus einer Chipkarte und gebe anhand eines Beispiels einen Einblick zum Thema Anwendungsdesign. Auch Vorüberlegungen bei einem Chipkartenprojekt werden angesprochen.

Die letzen drei Kapitel bestehen aus einer Zusammenfassung, einem Ausblick und dem Literaturverzeichnis.

2 Kartenarten

In diesem Kapitel werden die gebräuchlichsten Kartenarten vorgestellt. Dabei beschränke ich mich nicht auf Chipkarten, sondern gehe auch kurz auf andere Plastikkarten ein, auf denen Informationen gespeichert werden. Das in ISO 7811 beschriebene ID-1 Format ist das heute gebräuchlichste um einheitliche Kartenkörper herzustellen.

Da für die Wirtschaft der Kartenkörper als Werbeträger sehr interessant ist, werden sogar wiederbeschreibbare Kartenkörper entwickelt. Die Vorstellung, dass man seine Geldkarte im Kaufhaus zum Bezahlen in ein Terminal steckt und diese kommt mit einem neuem Aufdruck (beispielsweise Werbung für ein Sonderangebot) heraus, ist nicht weit hergeholt.

2.1 Hochgeprägte Karten

Hochgeprägte Karten ohne weitere Funktionen sind heutzutage selten. Vereinzelt finden sie noch als Kundenkarte oder Identifikationskarte Anwendung; in Bereichen, in denen die Sicherheit kaum eine Rolle spielt.

Bei dieser Kartenart werden relevante Informationen mit einem speziellen Verfahren auf die Karte geprägt. Dabei stehen die Buchstaben und Ziffern leicht nach außen, was einen Abdruck auf Papier leicht möglich macht. Da der Abdruck auf Papier ohne elektrische Energie möglich ist, hat diese Technik sehr zur Verbreitung und Akzeptanz von „Plastikgeld“ in der ganzen Welt beigetragen. Die Position der Prägung bei Kreditkarten ist in ISO 7811 nachzulesen. Da Hochprägung kaum vor Kopieren schützt, und die Kartendaten nicht elektronisch erfasst und verarbeitet werden können, braucht man für die Praxis zusätzliche Lösungen.

2.2 Magnetstreifenkarten

Da mit steigender Akzeptanz der Kreditkarte die Papierflut wuchs und die Verarbeitung immer teurer und aufwendiger wurde, bestand der Bedarf an einer Speicherungsmethode von Daten auf der Plastikkarte. Ein integrierter Magnetstreifen war eine gute Lösung, da die Daten digital gespeichert werden können und die Produktion kostengünstig ist.

Die Eigenschaften wie Kodiertechnik oder Lage sind in ISO 7811 dargestellt.
Der Streifen wird in drei Spuren unterteilt, wobei die ersten beiden nur für den Lesebetrieb und die dritte zusätzlich für den Schreibbetrieb gedacht ist. Es können ungefähr 1000 Bit gespeichert werden, was das Abbilden einer Hochprägung und das Speichern einiger Zusatzinformationen ermöglicht.

Da Daten auf einem Magnetstreifen sehr leicht ausgelesen, verändert oder kopiert werden können, gibt es in Kartenterminals, wie zum Beispiel Bankautomaten, oft zusätzliche Methoden um die Echtheit einer Karte festzustellen.
Wenn keine weiteren Methoden zum Prüfen der Echtheit einer Magnetstreifenkarte vorhanden sind, reicht ein Kopieren der Daten auf ein Magnetband (zum Beispiel von einer Videokassette) und das Positionieren von diesem auf einem passendem Stück Plastik oder Pappe.

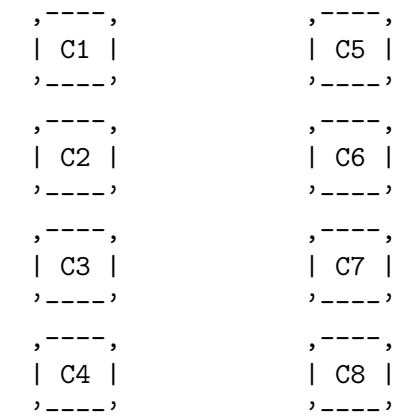
2.3 Optische Speicherkarten

Unter optischen Speicherkarten versteht man üblicherweise Kartenkörper, auf die eine reflektierende Schicht (Vergleichbar mit der Schicht auf einer üblichen CD) aufgetragen ist. In dieser Schicht werden die Informationen eingebrannt. Der Vorteil dieser Karten ist, dass im Vergleich zu anderen Kartenarten relativ preisgünstig viele Informationen gespeichert werden können.
Zum Einsatz kommen optische Speicherkarten zum Beispiel im Frachtverkehr. Dabei wird an die Kontainer die Karte geklebt und enthält Daten über den Inhalt oder die Reiseroute.
Problematisch an dieser Technik ist, dass die Karten nicht verschmutzen dürfen und die Lese-Terminals teuer und störanfällig sind.
Eine andere Art von optischen Speicherkarten stellen Karten mit aufgedrucktem Barcode oder ähnlichem dar.

2.4 Chipkarten

Chipkarten, also Kartenkörper mit eingebettetem Chip, sind im Begriff Magnetstreifenkarten ganz abzulösen. Der Vorteil von elektischen Schaltkreisen zur Speicherung von Daten gegenüber den anderen Methoden ist, dass die gespeicherten Informationen gegen unberechtigtes Auslesen oder Manipulation stark geschützt werden können. Dies geschieht meist durch kryptografische Methoden. Neben der Speicherung von Daten sind sogenannte Mikroprozessorkarten zudem in der Lage Daten logisch zu verarbeiten.

Eine übliche Chipkarte hat auf dem Chip 8 oder 6 Kontakteinrichtungen.



C1: Betriebsspannung
C2: Reset/Steuerleitung
C3: Takt
C4: Für spätere Anwendungen reserviert.
C5: Masse
C6: Programmierspannung (wird normalerweise nicht benutzt)
C7: Datenleitung I/O
C8: Für spätere Anwendungen reserviert.
(C4 und C8 sind optional)

Neben kontaktbehafteten Karten, bei denen eine direkte elektrische Verbindung zwischen dem Terminal und dem Chip zur Kommunikation genutzt wird, gibt es noch kontaktlose Karten, die nicht Problemen wie statischer Elektrizität oder Oxidation ausgesetzt sind.
Kontaktlose Karten kommunizieren mit dem Terminal „drahtlos“. Die Stromversorgung der Karte wird durch eine induktive Kopplung hergestellt. Dabei erzeugt das Terminal ein elektromagnetisches Hochfrequenzfeld. In der Karte ist eine Spule, an der durch das elektromagnetische Feld eine Spannung induziert wird. Durch einen Schwingkreis auf beiden Seiten und einen

Gleichrichter kann man diese Spannung nutzen um die Karte mit Energie zu versorgen.

Es entfallen viele Probleme der kontaktbehafteten Karte, und es ergeben sich Vorteile wie zum Beispiel, dass die Orientierung der Karte beim Einstecken in ein Terminal unwichtig ist. Die Möglichkeit des Auslesens auf Entfernungen bis zu einigen Metern, je nach Kartenart, kann Vorteile und Nachteile haben. Ein Vorteil ist, dass es möglich ist Terminals zu bauen, die nicht verschmutzen. Ein Nachteil ist, dass eine Person, die eine Karte in der Tasche mit sich trägt, unter Umständen ohne ihr Wissen erfasst werden kann.
Für die Wirtschaft ist der Wegfall der sichbaren Elektronik und der Gewinn an potentieller Werbefläche sicherlich auch ein Aspekt der die Verbreitung dieser Technik fördert.
Aus den genannten Gründen sind diese Karten zum Beispiel schon als Skipass oder Mensa-Karte in Gebrauch.

2.5 Speicherkarten

Speicherkarten sind die erste Generation von Chipkarten. Bei ihnen ist es nur möglich Daten zu speichern oder zu lesen. Es gibt allerdings auch Speicherkarten, bei denen ein Sicherheitssystem integriert ist.

Die bekanntesten Speicherkarten sind die Krankenversichertenkarten, bei denen die Daten einfach gelesen und geschrieben werden können und die Telefonkarte, bei der die Funktionen teilweise durch eine Sicherheitslogik geschützt sind. Da Chipkarten im Bereich von 3-5 Volt arbeiten, ist es leicht möglich, den Parallelport eines Heimcomputers zum auslesen und beschreiben von Speicherkarten zu gebrauchen, was einen schnellen Einstieg in die Materie ohne großen finanziellen Aufwand oder das Verlassen des Hauses möglich macht. Anleitungen für den Bau von Kartenlese- und Schreibgeräten finden sich leicht im Internet.
Für die regelmäßige Anwendung ist der Kauf eines Kartenterminals zu Empfehlen, da man auf einer höheren logischen Ebene arbeiten kann und die Preise unter Euro 50,- liegen.

2.5.1 Aufbau

Eine Speicherkarte besteht aus drei Bereichen.
Einer Adress- und Sicherheitslogik, einem ROM und einem EEPROM.
Die Adress- und Sicherheitslogik entscheidet unter Einbeziehung der Daten von ROM, in dem Identifizierungsdaten sind, und EEPROM, in dem Anwendungsdaten sind, ob die Operation zulässig ist.
Die Kommunikation mit dem Chip wird über 3 Leitungen geregelt: RST, CLK und I/O. I/O gibt den Wert des EEPROM an, auf den der Adresszähler zeigt, der entweder erhöht oder auf 0 gesetzt werden kann.
In ISO 7816 ist dafür ein synchrones Übertragungsprotokoll definiert.

2.5.2 Anwendungen

Anwendung finden Speicherkarten zum Beispiel im Bereich Bezahlfunktion (Telefonkarte) oder zum Transport von Daten (Krankenversichertenkarte).

2.5.3 Beispiel Krankenversichertenkarte

Die Chipkarten, die die verschiedenen Krankenversicherungen in Deutschland verteilt haben, sind momentan synchrone 256-Bit Speicherkarten und enthalten keine Sicherheitslogik. Die Daten können also von jedem gelesen und neu geschrieben werden. Einzige Sicherheit gegen eine Veränderung ist eine 8-Bit-XOR-Prüfsumme über den Datensatz. Die Karte dient dazu, den Patienten dem Arzt gegenüber zu identifizieren und eine elektronische Erfassung der Daten zu ermöglichen. Die enthaltenen Daten sind öffentlich,

was eine Grundvoraussetzung für die Zulassung war.
Alle Daten liegen in einem EF[1], das man durch Angabe von Speicherbereich und Länge auslesen kann.
Die Datenelemente der Krankenversichertenkarte:

Tag	Name	Laenge	
80h	Krankenkassenname	2..28	
81h	Krankenkassennummer	7	
82h	Versichertennummr	6..12	
83h	Versichertenstatus	4	
84h	Titel	0..15	*
85h	Vorname	0..28	*
86h	Namenszusatz	0..15	*
87h	Familienname	2..28	
88h	Geburtsdatum	8	
89h	Strasse+Hausnummer	0..28	*
8Ah	Wohnsitz-Laendercode	0..3	*
8Bh	Postleitzahl	4..7	
8Ch	Ortsname	2.22	
8Dh	Gueltigkeitsdatum	4	
8Eh	Pruefsumme	1	**
8Fh	VKNR	5	
90h	Statusergaenzung O/W	0..3	(O/W = Ost/West)

* Felder mit der Laenge 0 sind optional
** XOR-Summe ueber den gesamten Datensatz

[1] EF=elementary file: vergleichbar mit einer Datei

2.5.4 Beispiel Telefonkarte

Die Telefonkarte, die in Deutschland von der Telekom ausgegeben wird, ist eine Speicherkarte mit einer Sicherheitslogik. Die Datenübertragung verläuft synchron nach ISO 7816. Es wurden seit den ersten Tests 1983 viele Millionen Stück ausgegeben und in fast jeder Stadt in Deutschland findet sich eine Telefonzelle, die nur die Telefonkarte akzeptiert.
Im Speicher des Chips sind folgende fünf Datenfelder enthalten:
-7-stellige Seriennummer
-Herstellungsdatum
-Herstellercode
-Startguthaben
Restguthaben (in diesem Bereich kann nur „gelöscht“ werden)

Die Sicherheitslogik in der Karte hat den Zweck der Telefonzelle zu bestätigen, dass es sich um eine echte Telefonkarte handelt und um eine Manipulation des Datenverkehrs feststellen zu können. Dies geschieht dadurch, dass auf der Telefonkarte ein geheimer Algorithmus implementiert ist, ebenso in der Telefonzelle. Wie dieses System funktioniert, möchte ich an dem Beispiel eines Telefonanrufes mittels Telefonkarte erörtern.

Wenn man die Telefonkarte in die Telefonzelle steckt, wird der Shutter[2] geschlossen und die Kontaktfelder der Karte werden mit der Telefonzelle verbunden.
Als erstes schickt die Telefonzelle Reset an die Karte. Wenn diese mit einem ATR[3] antwortet kann die Telefonzelle feststellen, ob es eine synchrone Karte ist, die nach ISO 7816 arbeitet.
Dann fragt die Telefonzelle nach den fünf Datenfeldern und schickt unteranderem die Seriennummer über eine Datenverbindung an ein Hintergrundsystem, wo diese mit einer Sperrliste[4] verglichen wird.
Die Telefonzelle erzeugt eine „zufällige“ Zahl und schickt diese an die Karte. Mit den fünf Datenfeldern und der Zufallszahl als Eingabe berechnen Karte und Telefonzelle mit dem geheimen Algorithmus eine Zahl x.
Die Karte schickt die Zahl x an die Telefonzelle und diese prüft, ob sie das gleiche Ergebnis hat. Wenn das der Fall ist, kann die Telefonzelle davon ausgehen, dass es sich um eine echte Telefonkarte handelt, da nur eine echte Karte den geheimen Algorithmus enthält. Dieses Sicherheitsverfahren trägt auch den Namen „Challenge-Response“.
Für den Fall einer echten Karte würde die Telefonzelle jetzt das Guthaben

[2] Ein Shutter schließt den Kartenschlitz und soll das herausführen von Kabeln verhindern.

[3] ATR=Answer To Reset

[4] Wenn die Seriennummer in der Sperrliste steht, wird entweder keine Telefonverbindung zugelassen oder die Verbindug wird erstellt und die Polizei zu der Telefonzelle geschickt.

anzeigen und die Leitung freischalten.
Sobald eine Telefonverbindung zustande kommt, setzt die Telefonzelle das Guthaben der Karte herab[5], liest es wieder aus und prüft, ob der Stand verringert wurde.
Danach schickt die Telefonzelle wieder eine neue Zufallszahl. Mit dem geheimen Algorithmus wird jetzt wieder eine Zahl x berechnet.
Wenn die nachfolgende Prüfung der Zahl ein positives Ergebnis hat, wiederholt sich das System, bis die Karte kein Guthaben mehr aufweist oder die Telefonverbindung unterbrochen wird.

Die Sicherheit von Telefonkarten hängt maßgeblich von der Geheimhaltung des Algorithmus ab.
Nur mit diesem Wissen ist es einem Angreifer möglich, kostenlos zu telefonieren, da alle benutzen Kartennummern in die Sperrliste eingetragen werden und es folglich keine gleichen geben darf.

Früher wurden die letzen beiden Stellen der Seriennummer nicht mitgespeichert. Das hatte zur Folge, dass immer 100 gleicher Karten im Umlauf waren.
Folgende Probleme ergaben sich:
Wenn bekannt war, dass eine Karte manipuliert ist, konnte man sie nicht sperren, da sonst 99 andere Karten auch gesperrt werden.
Ein anderes Problem, war die Möglichkeit zur Manipulation:
Um sich eine Gebühreneinheit zu erschleichen, brauchte man 2 Karten mit gleicher Seriennummer.
Die erste Karte ist „voll“ und die zweite Karte ist um eine Gebühreneinheit verringert. Man verbindet die erste Karte mit der Telefonzelle und sobald das Signal zum Schreiben der ersten verbrauchten Einheit kommt, fängt man dieses ab und verbindet danach die zweite Karte mit der Telefonzelle. Diese liesst die Daten aus und stellt fest, dass eine Einheit abgebucht wurde. Alle Berechnungen zur überprüfung der Echtheit der Karte fallen positiv aus.

Im folgenden beschreibe ich das Senden einer Challenge und das empfangen einer Response bei einem Eurochip SLE4436, welcher in der heutigen Telefonkarte eingesetzt wird.
1. Als erstes wird ein Reset durch einen Impuls von 1 μS CLK während 5 μS RST an die Karte gesendet.
2. 110 Impulse auf CLK geben, um an Bitposition 110 zu kommen.
3. Durch einen gleichzeitigen Impuls auf RST und CLK wird die Schreibsequenz eingeleitet.
4. 10 μS warten.
5. 177 Impulse auf CLK geben.

[5]Der Wert der Gebühreneinheit wird der Telefonzelle durch das interne Modem mitgeteilt.

6. Die 48 Bit der Challenge werden einzeln gesetzt durch Schreiben und einem nachfolgendem CLK.
7.Um die 16 Bit Response zu lesen, muss man für jedes Bit 160 CLK Impulse schicken und dann I/O lesen.

2.6 Mikroprozessorkarten

Mikroprozessorkarten oder auch Smartcards sind eine Weiterentwicklung von Speicherkarten. Neben der Funktion, dass Daten gespeichert werden können, enthält diese Art von Karten zudem noch die Möglichkeit, Daten logisch zu verarbeiten.

Da in Smartcards praktisch ein kleiner Computer implementiert ist, sind die zukünftigen Entwicklungen kaum abzusehen.

2.6.1 Aufbau

Eine Mikroprozessorkarte besteht normalerweise aus Prozessor und Speicher.
Der Prozessor (meist 8-Bit) ist mit den üblichen Methoden zur Manipulation von Registern ausgestattet und wird von einem Coprozessor unterstützt, der für komplexe mathematische Operationen benutzt wird.
Der Speicher besteht aus einem ROM, in dem das Betriebssystem und Anwendungen gespeichert werden; einem nicht flüchtigen[6] Bereich (Größe etwa 2 bis 8 KB), in dem feste Daten, wie zum Beispiel die letzen 10 Buchungen, gespeichert werden und einem flüchtigen RAM (bis zu 1 KB), das von Anwendungen genutzt werden kann.

2.6.2 Anwendungen

Eine Mikroprozessorkarte bietet die Möglichkeit, eine kleine Rechenmaschine in der Brieftasche zu tragen. Die Anwendungsmöglichkeiten sind im Hinblick auf die fortschreitende Miniaturisierung von Schaltkreisen kaum alle aufzuzählen oder vorstellbar. Bekannte Anwendungen sind die digitale Signatur, die Geldkarte oder die Verwendung von Algorithmen, die man nicht veröffentlichen möchte.

2.6.3 Sicherheitstechniken

Die meisten Anwendungen sind mit dem Gebiet der IT-Sicherheit thematisch verbunden. Das liegt daran, dass die Chipkarte bei vernünftiger Implementierung gespeicherte Daten oder Algorithmen effizient vor Missbrauch schützen kann. Besonders von Vorteil ist, dass Terminals für Chipkarten billig zu kaufen oder zu basteln, oder in vorhandener Hardware wie zum Beispiel einer Tastatur schon enthalten sind.
Die Sicherheit einer Chipkarte besteht aus der Verknüpfung von verschiedenen Teilbereichen:
Bei der Benutzeridentifizierung soll sichergestellt werden, dass die Karte

[6] Hersteller geben meist 10 Jahre an

nur von befugten Personen verwendet werden kann. In der Praxis geschieht dies meist durch die Eingabe einer PIN[7]. Karten, wie sie zum Beispiel in Mobiltelefonen vorkommen, fragen nach einer 4-stelligen Geheimnummer. Wenn diese zu oft falsch eingegeben wurde, sperrt sich die Karte und es wird eine PIN mit deutlich mehr Stellen abgefragt. Dieses System und eine Zeitverzögerung bei der Eingabe machen ein systematisches Ausprobieren aller Kombinationen als Angriff auf die Karte unsinnig.
In Bezug auf Sicherheit spielt die Authentisierung des Kartenterminals eine wichtige Rolle um einen Mißbrauch zu verhindern. In der Presse waren Berichte über falsche Bankautomaten zu finden, die Betrüger aufgestellt hatten, um Kartendaten zu kopieren und die Geheimzahl abzufangen. Bei dem Design von Anwendungen muss darauf geachtet werden, dass theoretisch der gesamte Datenverkehr zwischen Karte und Terminal abgehört oder manipuliert werden kann.
Man unterscheidet zwischen symmetrischen und asymmetrischen Kryptoverfahren zur Authentisierung.

Authentisierung durch ein symmetrisches Kryptoverfahren, kann einseitig geschehen. Das bedeutet, dass entweder nur die Karte das Terminal auf Echtheit prüft oder umgekehrt. Beidseitige Authetisierung mit symmetrischen Kryptomethoden, bezeichneit eine gegenseitige Prüfung auf Echtheit.

Authentisierung mit asymmetrischen Kryptoverfahren unterscheidet zwischen dem statischen und dem dynamischen Verfahren.
Bei dem statischen Verfahren werden bei jedem Gebrauch der Karte die selben Daten zur Authentisierung verwendet, was einem Angreifer unter Umständen die Gelegenheit gibt, Daten widereinzuspielen.
Dynamische Verfahren verwenden bei jedem Gebrauch neue Daten.
Natürlich können asymmetrische Methoden einseitig oder beidseitig angewendet werden.

Ein weiterer Schutzmechanismus neben dem der laufenden Anwendung und dem des Beriebssystems ist auf der Hardwareebene zu finden.
Es muss dafür gesorgt werden, dass spezielle Speicherbereiche nicht ausgelesen oder gelöscht werden können. Des weiteren sollte man keine Rückschlüsse auf Daten oder Architektur aufgrund von Temperaturschwankungen oder Energieverbrauch ziehen können.
Da man bei einigen Anwendungen wie Telefon- oder Geldkarten mit einem hohen Bedrohungspotential rechnen kann, prüfen Spezialisten eine Hardwarearchitektur auch unter den Gesichtspunkten, dass es einem Angreifer möglich ist einen Chip mit gleicher oder sogar besserer Technik zu analysieren. Beispielsweise kann man davon ausgehen, dass ein Angreifer einen Chip

[7]PIN=personal identification number: Geheimzahl

bis zu einem gewissen Grad freilegen kann und dann gezielt Leiterbahnen[8] unterbricht.

Es ist zu bemerken, dass eine Smartcard meist nur Teil eines Sicherheitskonzepts ist und dort oft Schwachstellen existieren, die einen direkten Angriff auf die Chipkarte unnötig machen. Wenn die Karte zum Beispiel dazu dient einen Raum abzusichern, würde sich ein Angreifer nicht auf die Kartentechnik konzentrieren, wenn zu dem Raum ein Fenster gut erreichbar offen steht.

2.6.4 Betriebssystem

Betriebssysteme für Mikroprozessorkarten (COS[9]) gibt es von vielen Herstellern. Besonders interessant sind Varianten, die es erlauben Daten mit Programmcode nachzuladen, die vom System interpretiert werden. Die Programme müssen nicht zwingend in Assembler geschrieben werden, da es auch Karten gibt, die Hochsprachen wie C, Basic oder Java verwenden können.
Das COS hat folgende Aufgaben:
-Die Kommunikation zwischen der Karte und dem Terminal wird geregelt.
-Den Ablauf von Kommandos steuern.
-Die Verwaltung von Daten und Zugriffsrechten, sowie
die Verwaltung und Ausführung von kryptographischen Algorithmen.

Schön ist, dass einige COS schon plattformübergreifend arbeiten und es beispielsweise möglich ist auf eine Karte mit mehr oder weniger Speicher umzusteigen, wenn Bedarf besteht oder um Kosten für Speicher zu senken, weil man diesen nicht braucht.

Um Fehler bei der Entwicklung einzugrenzen werden Betriebssysteme modular entwickelt. Wichtige Teile werde ich kurz erläutern.

Die I/O-Schnittstelle, welche eine serielle Übertragung durchführt, benutzt den I/O-Manager für die Fehlerkorrektur.
Der Secure-Messaging-Manager ist für die Ver- und Entschlüsselung der Kommunikation mit dem Terminal und Authentisierung zuständig. Zudem wird dort die Benutzeridentifikation durchgeführt und es werden kryptografische Algorithmen für zum Beispiel die digitale Signatur, durch Zugriff auf eine Kryptobibliothek, zur Verfügung gestellt.
Der Kommandointerpreter ermittelt aus den Daten die Befehle und zugehörige Parameter, die er an den Logical-Channel-Manager weiterleitet. Ist es nicht möglich einen gültigen Befehl zu extrahieren, schickt ein Returncodemanager eine Fehlermeldung an das Terminal.

[8] Leiterbahnen sind etwa 1 tausendstel Millimeter dick
[9] COS = chipcard operating system

Der Logical-Channel-Manager ermittelt den angewählten Kanal und schaltet dessen Zustände.
In einem Zustandsautomat wird geprüft, ob ein empfangener Befehl mit zugehörigen Parametern im aktuellen Zustand erlaubt ist. Wenn die Prüfung positiv verläuft, gehen die Daten an das Modul Anwendungsbefehl.
Im Modul Anwendungsbefehl werden die eigentlichen Befehle ausgeführt.
Wie bereits erwähnt, gibt es auch Chipkarten, die es erlauben Programme nachzuladen. Das dazu benötigte Modul bezeichnet man als Codeinterpreter.
Der schon angesprochenen Returncode-Manager hat die Aufgabe, Fehlermeldungen von den einzelnen Modulen an das Terminal weiterzuleiten.

2.6.5 Dateisystem

Um eine physikalische Adressierung aus Sicht des Terminals zu vermeiden, bieten moderne Chipkartenbetriebssysteme Dateisysteme an, in denen Daten gespeichert werden können. Wie bei bekannten Dateisystemen kann man Dateien in anderen Dateien ablegen und diese relativ zur eigenen Position oder absolut zu einer Hauptdatei ansprechen beziehungsweise indizieren.

Die üblichen Dateitypen werden folgedermaßen bezeichnet:

-Master File (MF)
In der Hierarchie der Dateien an oberster Stelle.

-Dedicated File (DF)
Vergleichbar mit einem Verzeichnis.

-Elementary File (EF)
Vergleichbar mit normalen Dateien.

Elementary Files können noch nach dem Kriterium “für die Außenwelt“ und „für das Betriebssystem“ unterschieden werden.

2.6.6 Datenübertragung

Im Gegensatz zu Speicherkarten geschieht die Kommunikation der Karte mit dem Terminal asynchron. Details zu verschiedenen Protokollen können in ISO7816 nachgelesen werden.
Am bekanntesten ist das Protokoll T=0, welches in der GSM-Karte verwendung findet und byteorientiert arbeitet.
Ein weiteres oft verwendetes und international als sehr sicher angesehenes

Protokoll zur Datenübertragung ist T=1, bei dem streng nach einem Schichtenmodell gearbeitet wird. Dadurch ist es für Anwendungen sehr einfach Daten zu verschlüsseln, weil die Anwendung nur die richtige Schicht wählen muss und die Daten dann zum Beispiel von einer darunterliegenden Schicht verschlüsselt werden. Benutzt wird dieses Protokoll unter anderem bei der digitalen Signatur mit Smartcard.

2.6.7 Kommandos

Die Kommunikation mit einer Chipkarte verläuft immer nach dem Verfahren, dass das Terminal eine Aufforderung an die Karte schickt, die die empfangenen Daten verarbeitet und das Ergebnis zurückschickt.
Die Daten werden in Pakete oder Einheiten mit dem Namen APDU[10] verpackt und transportiert. Die Kommandos, die eingebettet sind, erlauben zum Beispiel das Selektieren von EFs anhand einer eindeutigen Nummer (FID), das Lesen und Schreiben von Dateien oder den Zugriff auf komplexere Datenstrukturen.

2.6.8 Beispiel Mobiltelefone

Ein Anwendungsgebiet von Mikroprozessorkarten ist die Mobiltelefonie.
Die Karte sorgt für Gebührenerfassung, Verschlüsselung und frei belegbaren gesicherten Speicherplatz. Um zu verstehen, welche Rolle die Chipkarte dabei genau spielt, ist ein wenig Hintergrundwissen nötig. Ich erläutere die Thematik am Beispiel des GSM-Netzes.

Das GSM-Netz ist ein Mobilfunknetz, bei dem die Daten digital und verschlüsselt im 900 oder 1800 MHz Bereich in der Modulationsart FMN[11] übertragen werden. Das Funknetz besteht aus Zellen mit maximal 40 km Durchmesser. Es wird grundlegend zwischen der „Mobile Station (MS)“ und der „Base Station (BS)“ mit einem Hintergrundsystem unterschieden.
Die MS besteht aus dem Mobiltelefon (ME[12]) und der Chipkarte, die Subscriber Identity Module (SIM) genannt wird. Die SIM-Karte liegt üblicherweise nicht im ID-1 Format sondern im ID-000 Format vor, wobei sich nur die Größe des Kartenkörpers unterscheidet.
Die SIM-Karte hat die primäre Aufgabe, die MS gegenüber der BS zu identifizieren. Dies geschieht durch eine im GSM-Netz einzigartige, maximal 8 Byte große Nummer, die „International Mobile Subscriber Identity (IMSI)“ genannt wird.

[10] APDU = application protocal data unit
[11] FMN: frequency modulation narrow
[12] ME: mobile entity

Wenn ein Gespräch geführt werden soll, dann stellt die MS eine Verbindung zur nächsten BS her und überträgt an sie die IMSI.
Wenn die IMSI bei der BS registriert und gültig ist, schickt die BS an das ME eine Zufallszahl, die an die SIM-Karte weitergereicht wird.
Die SIM-Karte berechnet mit der IMSI und einer geheimen Zahl Ki mit einem geheimen Algorithmus $A3$ eine Zahl, die an die BS geschickt wird.
Die BS errechnet mit $A3$, der IMSI und der Zufallszahl einen Wert, der mit dem erhaltenen Wert übereinstimmen muss. Wenn dies der Fall ist, ist die Authentifikation abgeschlossen und die MS berechtigt zu telefonieren.
Um die Daten auf der Funkstrecke verschlüsselt zu übertragen, führen sowohl SIM als auch BS mit einem Algorithmus $A8$ und der Zufallszahl und IMSI als Eingabe eine Berechnung durch. Das Ergebnis wird von der SIM-Karte an das ME weitergereicht, welches mit einem Algorithmus $A5$ die Sprachdaten verschlüsselt bzw. entschlüsselt.

Neben der Erzeugung von Schlüsseln für die Authentifikation und Verschlüsselung regelt die Karte auch wichtige Funktionen wie Benutzeridentifikation oder die Speicherung von Telefonnummern um mehrere Telefone mit den gleichen Daten benutzen zu können.
Die SIM-Karte hat auch die Funktion, dass Betreiber neue Programme oder Funktionen per Funknetz in die Karte speisen können[13]. Dies geschieht durch Einbetten der Anweisungen in eine SMS[14], die automatisch erkannt wird. Eine Beispielanwendung ist die Möglichkeit einen Webserver auf der Karte zu implementieren um ein Abfragen per Web-Browser möglich zu machen.
Im April 1998 stellte der Chaos Computer Club der Öffentlichkeit eine Anleitung zur Verfügung, die es ermöglicht, eine GSM-Karte zu klonen[15]. Diesen als „GSM-Hack“ bekannt gewordenen Angriff möchte ich kurz erläutern.
Die Sicherheit des GSM-Netzes beruht zum Großteil auf der Geheimhaltung des Algorithmus $A3$ (zur Authentifikation) und des Algorithmus $A8$ (für die Datenverschlüsselung auf der Funkstrecke). Marc Briceno von der Smart Card Developers Association hatte durch aufgetauchte Unterlagen und Reverse Engineering[16] herausgefunden, dass es einen Algorithmus COMP128 gibt und wie dieser funktioniert. Dieser Algorithmus wird für $A3$ und $A8$ von vielen Netzbetreibern als Referenzimplementation genutzt. Ian Goldberg und Dave Wagner vom ISAAC Forschungszentrum in Berkeley hatten ei-

[13] Die Möglichkeit der Fernwartung einer Chipkarte wurde 2001 von einem Pay-Tv-Anbieter genutz, um systematisch einen Code auf nachgemachte Karten zu laden, der diese unbrauchbar gemacht hat.

[14] SMS (oder nur short message) ist die Bezeichnung für eine Kurzmitteilung im GSM Netz

[15] als klonen bezeichnent man das kopieren oder simulieren einer vorhandenen Chipkarte

[16] Beim Reverse Engineering wird versucht durch systematisches Testen einen möglichst genaue Vorstellung davon zu bekommen, wie ein Chip Aufgebaut ist.

ne Schwachstelle in COMP128 entdeckt, die es ermöglicht, durch ca. 150000 Anfragen an eine Chipkarte den darin enthaltenen geheimen Schlüssel Ki zu erlangen.
Mit dem Wissen um den geheimen Schlüssel Ki und der IMSI, welche einfach ausgelesen werden kann, ist es nun möglich, einen Personal Computer zum Simulieren einer echten GSM-Karte zu nutzen.

2.6.9 Beispiel Digitale Signatur

Dadurch, dass kryptografische Algorithmen auf einer Mikroprozessorkarte implementiert werden können und dass gegen unbefugtes Auslesen gesicherte Daten dort untergebracht werden können, ist die Smart Card für die Anwendung bei der digitalen Signatur gut geeignet.

Ich setze voraus, dass die Grundprinzipien bei der digitalen Signatur bekannt sind.
Da die Leistungsfähigkeit von Chipkarten nicht immer ausreichend groß ist, um alle kryptografischen Funktionen auszuführen, werden viele Aufgaben wie das Generieren von Schlüsseln extern vollzogen.
Karten die dem deutschen Signaturgesetz genügen, müssen ihre Schlüssel intern erzeugen, da dies weiter Sicherheit[17] bietet.
Der Ablauf beim digitalen Signieren mit einer Chipkarte ist folgender:
Die Datei, die später signiert werden soll, wird auf dem Personal Computer erstellt. Dann wird das „Signaturprogramm“ gestartet und fordert dazu auf, die Chipkarte in das Laufwerk zu stecken und eine PIN einzugeben. Wenn die Benutzeridentifikation postiv verläuft, bildet die Software mittels einer Reduzierungsfunktion eine Prüfsumme über die erstellte Datei und schickt diese an die Karte zur Signatur. Die Karte benutzt den im Inneren gespeicherten privaten Schlüssel zum Signieren dieser Prüfsumme und liefert das Ergebnis zurück, welches die digitale Signatur der Datei darstellt.

Besonders sicherheitskritisch bei diesem System ist nicht die Chipkarte an sich, sondern der Personal Computer, auf dem Schadprogramme laufen können. Die PIN kann leicht von der Tastatur abgefangen werden oder das angreifende Programm ersetzt die Prüfsumme, welche von der Software an die Karte geschickt wird, um so an eine gültige Signatur für andere Daten zu kommen.
Da Personal Computer heutzutage sehr komplexe Systeme sind, ist es selbst mit einem Betriebssystem welches ein gutes Rechtemanagement bietet, in der Praxis kaum möglich, sichere Kryptografie zu implementieren.
Eine Verkleinerung der Angriffsfläche ist durch Benutzen einer speziellen Tastatur oder einem Display auf der Karte/Terminal möglich.

[17] Der Schlüssel ist immer in der Karte und kann nicht ausgelesen werden.

3 Karten-Terminals

Terminals spielen für Chipkarten naturgemäß eine wichtige Rolle. Dabei ist zwischen Terminals zu unterscheiden, die speziell für eine Anwendung gebaut werden und solchen, die das Bearbeiten von vielen Kartentypen erlauben und im Computerhandel für jeden erhältlich sind.
Eine Sonderstellung nehmen kontaktlose Terminals ein. Diese haben den besonderen Vorteil, dass sie gut gegen Vandalismus geschützt werden können. Nachteilig ist, dass die Karte fast nur mit kryptografischen Methoden authentisiert wird.
Viele Karten, wie zum Beispiel die Telefon- oder Geldkarte, werden so konstruiert, dass einige Funktionen für alle Kartenleser nutzbar sind und die sicherheitsrelevanten Funktionen nur mit einem Spezialterminal benutzt werden können.
Im Folgenden gehe ich auf einige Systeme ein, die von Spezialterminals genutzt werden, um zu identifizieren und Manipulationen oder unberechtigtes Ausspähen von Daten zu verhindern.

3.1 Sicherheitssysteme

Um zu verhindern, dass Karten in ein Terminal eingeführt werden, an denen Kabel nach außen geführt werden, gibt es sogenannte Shutter. Bei diesen Systemen wird die Karte tief in das Innere des Terminals befördert und die Öffnung verschließt sich.
Um die Echtheit einer Karte zu überprüfen gibt es zahlreiche Methoden.
Bei Magnetstreifenkarten gibt es unsichtbare Markierungen und der Anfang der „nur-Lesen“ Sektionen ist gesondert gekennzeichnet.
In Telefonzellen werden die Seriennummern mit einem Hintergrundsystem abgeglichen und die Telefonkarte wird Extemsituaionen ausgesetzt, wodurch auch die Echtheit überprüft wird.
Zudem messen verschiedenste Terminals physikalische Eigenschaften der Karte und prüfen dabei zum Beispiel Stromverbrauch, Wärmeentwicklung oder die Masse.

3.2 Probleme von Terminals

Problematisch bei Terminals (auch zum Beispiel bei biometrischen Systemen) ist, dass man eine gewisse Toleranz für Fehler zulassen muss, um eine Technik in der Praxis einzusetzen. Wenn bei Systemem, wie eine Zugangskontrolle in einer Firma mit 50 Mitarbeitern, eine Fehlerquote von einem Promille hat, ist dies kein großes Problem. Wenn diese Fehlerquote allerdings bei einem System mit Millionen von Nutzern auftritt, ist dies ein wirtschaftlicher Verlust, bei der Annahme, dass Angreifer weniger Schaden

anrichten können.
Optische Sensoren[18] haben zum Beispiel das Problem, auf eine bestimmte Temperatur und Luftfeuchtigkeit[19] angewiesen zu sein, um zuverlässig zu arbeiten.
Auch die Shuttertechnik der Telekom bei Telefonzellen ist nicht sicher genug, da es immer wieder Anleitungen gibt, wie man den Shutter offen hält und zum Beispiel mit einem Draht spezielle Sensoren zur Prüfung austrickst.
Wenn ein Kartensystem auch einige Zeit unabhängig von einem Hintergrundsystem funktionieren soll, wie beispielsweise die Bankkarte mit Geldautomaten als Terminal und einem Hintergrundsystem, dann hat ein Angreifer oft eine größere Angriffsfläche, wenn er durch Tricks eine Verbindung zu einem Hintergrundsystem unterbindet oder manipuliert. Auch diese Technik wurde schon benutzt um Kreditkarten-Kunden um ihr Geld zu bringen.

[18] Optische Sensoren haben oft die Funktion für das menschliche Auge unsichtbare Sicherheitsmerkmale zu überprüfen.

[19] In den südlichen Regionen können optische Sensoren deshalb oft nicht zuverlässig eingesetzt werden.

4 Chipkarten Fertigung und design von Anwendungen

Der Lebenszyklus einer Chipkarte wird in 5 Phasen unterteilt.

1. Herstellung von Chip und Karte.
2. Kartenvorbereitung.
3. Anwendungsvorbereitung.
4. Kartenbenutzung.
5. Ende der Kartenbenutzung.

Da in der Praxis Aufgaben wie das Aufspielen des Beriebssystems bzw. Anwendungen und die Personalisierung nicht alle von einer einzigen Firma getätigt werden, sind die Chips mit Transportcode ausgestattet, die einen unberechtigten Zugriff oder Manipulation verhindern.

4.1 Design von Anwendungen

Das Design einer Anwendung entscheidet über Erfolg und Misserfolg eines Chipkartenprojekts.

Wenn man zu dem Schluss gekommen ist, dass eine Chipkartenlösung für ein Problem eine Lösung darstellt, muss man sich einige Fragen beantworten:
-Welche Sicherheitstechnik setze ich ein?
Diese Frage ist immer abhängig von den Kosten für mehr Sicherheit und den Kosten im Falle eines Missbrauchs. Firmen sollte beim Kauf von Sicherheit klar sein, warum etwas Geld kostet und was die erbrachte Leistung für das Unternehmen wert ist. Eine Tür mit Chipkartenschloss und einer biometrischen Überprüfung der Person für tausende Euro hat keinen Wert, wenn ein Fenster offen ist, durch das ein Angreifer Zutritt bekommen könnte.
-Kann meine Anwendung auf der Chipkarte in annehmbarer Zeit ihre Arbeit leisten?
Es hat sich gezeigt, dass Menschen glauben, ihre Chipkarte sei kaputt, wenn die Operation länger als eine Sekunde dauert. Es gibt Formelsammlungen, die ein Abschätzen von Ausführungszeiten bei der Planung erlauben. Durch von der Chipkarte unabhängige visuelle Maßnahmen kann man dem Benutzer vorspielen, dass er etwas von der Aktivität mitbekommt, was zu ein wenig mehr Geduld auf der menschlichen Seite führt. Wenn der Anwender aufgrund eines Shutters die Karte nicht herrausziehen kann, ist dieses Problem zu vernachlässigen.
-Gibt es wirtschaftlich bessere Alternativen?
Bevor man sich Türöffnungssysteme auf der Basis von Chipkarten anschafft, sollte man wissen, was normale Schlösser kosten.
Desweiteren sollte man bedenken, was bei Verlust von Karten geschieht und

wer bei Problemen haftbar ist.

4.2 Beispiel Design

In vielen Fällen ist es sinnvoll, wenn sich ein Anwender sicher sein kann, dass ein Terminal „offiziell“ ist. Im Folgenden werde ich einen Vorschlag aus der DIN-Spezifikation für die deutsche Signaturkarte vorstellen.

Diese Methode kann nur gefälschte Terminals erkennen, aber nicht solche, die manipuliert wurden.
Die Idee ist, dass dem Benutzer nachdem sich die Chipkarte und das Terminal gegenseitig authentisiert haben, ein geheimer Satz auf einem Bildschirm angezeigt wird, den nur der Anwender kennt. Natürlich ist man bei dieser Methode nicht davor sicher, dass jemand den geheimen Satz ausspäht und eine gezielte Fälschung für eine bestimmte Karte baut.

Für das Design von Anwendungen stehen viele Hilfsmittel zur Verfügung wie zum Beispiel Software, die eine Chipkarte und ein Terminal simuliert, auf der Anwendungen getestet werden können. Zudem gibt es Programme zum Erstellen von Dateistrukturen und Programmierung.
Für unser Beispiel müssten wir 1 EF anlegen in einem DF für die Anwendung „SicheresTerminal“.
Der Ablauf unserer Anwendung:
1. Terminal schickt Reset an Karte.
2. Karte schickt ATR an das Terminal.
3. Das Terminal prüft: wenn ATR richtig ist, wird fortgesetzt.
4. Eine beidseitiges Authentisierung wird angewendet.
5. Wenn die Authentisierung erfolgreich war, darf das Terminal den geheimen Satz aus dem EF lesen und ihn es dem Benutzer anzeigen.
6. Jetzt könnte eine PIN Abfrage kommen und dann eine nützliche Anwendung.

5 Zusammenfassung

Zusammenfassend ist zu sagen, dass die Chipkarte noch Platz für viele Anwendungen bietet. Nach „Moore's Law“ verdoppelt sich die Rechnerleistung alle 18 Monate oder vertausendfacht sich nach etwa 15 Jahren. Deshalb ist damit zu rechnen, dass bald vollständige Kryptosysteme auf dem Chip Platz finden werden.

Der Stand der Technik ist, dass normale Speicherkarten wie die vorgestellte Krankenversichertenkarte aussterben. Durch Massenproduktion sind billige Mikroprozessorkarten auf dem Markt, die dem Käufer viele Vorteile bieten wie zum Beispiel Authentisierung oder Identifikation.

6 Ausblick

In der Zukunft werden auf uns noch sehr viele Chipkarten zukommen.
Es wird schwer sein sich dagegen zu wehren, da die Vorteile von der Wirtschaft in den Vordergrund gestellt werden. Die Nachteile sind die Aufgabe der Anonymität, beispielsweise beim Zahlungsverkehr. Viele Automaten wie zum Beispiel Telefonzellen oder Fahrscheinautomaten am Bahnhof bieten keine Möglichkeit mehr mit konventionellem Geld zu bezahlen. Da Daten teilweise zentral zusammengeführt und gespeichert werden, ist es ein Leichtes über Anwender ein Profil zu erstellen. Auch kontaktlose Chipkarten, die über weite Entfernungen ausgelesen werden können und über deren Inhalt man sich nicht genau im Klaren ist, sind kritisch zu betrachten.
Wünschenswert für die Zukunft wäre eine Chipkarte, die voll dokumentiert ist und Platz für viele verschiedene Anwendungen bietet. Dabei sollte der Anwender selber bestimmen können, welche Anwendungen darauf laufen. Die Möglichkeit private Schlüssel ohne dritte Parteien einzuspielen sowie ein möglichst hoher Grad an Anonymität sind für mich persönlich die wichtigsten Punkte. Denn aus der Verknüpfung von Daten solch einer Karte lassen sich Profile erstellen, die über Mobilität, Kommunikation, Kaufverhalten und Vorlieben einer Person Auskunft geben.

Literatur:

W. Rankl, W. Effing — Handbuch der Chipkarten (3. Aufl.)
1999 Carl Hanser Verlag München Wien

mr crash — How to read the response from Eurochip SLE4436 and SLE 5533 chips.
http://www.geocities.com/ResearchTriangle/Lab/1578/ssn7.htm

Stephane Bausson — ISO7816 asynchronous smartcard information
1995
http://www.hut.fi/Misc/Electronics/docs/smartcard/iso7816.txt

Chaos Computer Club — CCC klont D2 Kundenkarte
1998
http://www.ccc.de/gsm/index

Chaos Computer Club (15. Chaos Communication Congress in Berlin) – Chipcard Hacking
ftp://ftp.ccc.de/congress/15c3/doku/mp3/chipcard_hacking_teil2.mp3