Bankkarten und Sicherheit: Immer noch ein Thema?

Zeit und Ort: Freitag, 17. September 2004, 9.00 Uhr, HS 105

Moderation: Herr Prof. Dr. Dipl.-Ing. Manfred Pausch

Referenten:

Das „neue“ PIN-Verfahren bei ec-Karten

Ab 1998 wurde in Deutschland ein sogenanntes „neues“ PIN-Verfahren eingeführt. Dabei wird für die Verschlüsselung ein Triple-DES-Verfahren eingesetzt, das zwei längere Schlüssel verwendet. Theoretisch ist bei diesem Verfahren eine Errechnung der verwendeten Schlüssel mit derzeitig allgemein verfügbarer Rechnerkapazität nahezu ausgeschlossen. Jede PIN ist gleichwahrscheinlich vorhanden, so dass die Chance die richtige PIN zu treffen theoretisch bei 1/10.000 liegt.

Nach Darstellung der deutschen Kreditwirtschaft wird das neue PIN-Verfahren seit 1998 eingesetzt. An der Wahrhaftigkeit dieser Behauptung bestehen jedoch begründete Zweifel. Die Presse in Deutschland hat darüber berichtet, dass das alte PIN-System trotz offizieller Dementies seitens der Kreditwirtschaft intern als korrumpiert betrachtet wurde[1]. Die Beklagte hat sich allerdings im Verfahren 4 C 412/00 vor dem Amtsgericht Werl geweigert dem vom Gericht bestellten Sachverständigen Zutritt zu ihrem Rechenzentrum zu gewähren, wo dieser sich von dem korrekten Einsatz des neuen PIN-Verfahrens überzeugen sollte. Sie hat dann die Klageforderung anerkannt.

Unabhängig von der Ausgestaltung des neuen PIN-Verfahrens im einzelnen, ist zur Beurteilung der Sicherheit zuerst zu überprüfen, wie Transformation hexadezimaler Zahlen in das Dezimalsystem durchgeführt wird.

Zur Erklärung für Mathematik-Laien: Das Hexadezimal-System kennt insgesamt 16 Zustände (Ziffern), während das Dezimalsystem nur über 10 Ziffern verfügt. Bei einer Transformation vom Hexadezimalsystem müssen somit 16 Zustände in 10 Zustände abgebildet werden. Dazu stelle man sich vor, dass jeder Zustand eine Kugel mit einem einzigartigen Symbol ist, die in Kästchen abgelegt werden müssen. Das Problem der hexadezimal-dezimalen Wandlung besteht nun darin die 16 Kugeln auf die 10 Kästchen zu verteilen.

Es ist offensichtlich, dass 6 Kästchen je 2 Kugeln und 4 Kästchen nur je eine Kugel aufnehmen müssen. Deshalb ist die Wahrscheinlichkeit, eine Kugel mit einem gewünschten Symbol zu finden, in 6 Kästchen doppelt so hoch wie in den 4 restlichen. Wenn man nun weiß, welche "überzähligen" Symbole als zweite Kugel in welche Kästchen abgelegt werden, erhöht sich die Wahrscheinlichkeit die richtige Verteilung zu erraten dramatisch. Dieses war auch eines der von mir kritisierten Probleme des alten PIN-Systems.

[1] DER SPIEGEL 36/1997 Seite 104: "Spätes Eingeständnis"

Die Konzeption des neuen PIN-Verfahrens lässt sich folgendermaßen beschreiben: Es gibt kein vom ZKA[2] vorgeschriebenes Verfahren, das für alle Kartenarten (Kreditkarten, ec-Karten und Kundenkarten) identisch ist. Die Verbände (BdB, BVR, DSGV, VöB) haben eigene Verfahren entwickelt, die zudem noch - neben der Kartenart - unterschiedlich für verschiedene Nutzerkreise sein können.

Beispielhaft sei das Verfahren zur PIN-Erzeugung und PIN-Prüfung eines Institutes aus dem Bereich der öffentlichen Banken für ec-Karten erläutert[3]:

Für jedes Institut wird mit einem Zufallsgenerator ein Masterschlüssel erzeugt. Dieser sollte in einem Sicherheitsbereich verwahrt und nur für die PIN-Erzeugung benutzt werden. Mit einem Datenblock, der aus den auf der Karte enthaltenen Daten gebildet wird, wird mit dem Masterschlüssel ein kartenindividueller Schlüssel erzeugt. Mit diesem wird dann die PIN dieser Karte berechnet, indem kartenindividuelle Daten mit dem Masterschlüssel verschlüsselt werden. Aus dem so gewonnenen Verschlüsselungsergebnis wird dann die PIN abgeleitet.

Die PIN-Prüfung unterscheidet sich von der PIN-Erzeugung. Bei der PIN-Prüfung werden zwei Institutsschlüssel verwendet, die vom Verfalljahr der Karte abhängen. Aus dem übermittelten Datenblock der in das Lesegerät eingeführten Karte und der dazu gehörenden PIN wird ein Textblock erstellt, der in einem Triple-DES-Verfahren mit den beiden Institutsschlüsseln verschlüsselt wird. Aus den beiden Verschlüsselungsergebnissen werden zwei vierstellige Werte abgeleitet, die auch auf dem Magnetstreifen der Karte enthalten sind.

Die eingegebene PIN wird zur Berechnung der Prüfwerte verwendet. Stimmen die errechneten Prüfwerte und die vom Kartenleser übertragenen beiden vierstelligen Werte überein, so wird die Zahlung autorisiert.

Die PIN-Generierung bei Kreditkarten

Im Prinzip entspricht die Generierung der PIN bei Kreditkarten dem bei der ec-Karte angewandten Verfahren. Jedoch kann bei Kreditkarten aus kartenindividuellen Daten die eingesetzte Single-DES-Verschlüsselung leichter gebrochen werden. Hierfür sind für einen versierten Täter nur einige Karten und eine leistungsfähige Computeranlage nötig.

1998 führte die "Electronic Frontier Foundation" öffentlich ein DES-Cracking durch. Die benötigten Schlüssel wurden bereits nach kurzer Zeit (im letzten veröffentlichten Versuch nach 5 Stunden!) gefunden. Die eingesetzte Computeranlage wurde sehr ausführlich beschrieben.[4]

Risiko: Theoretisch hohe Sicherheit bezüglich der Berechenbarkeit der PIN bei ec-Karten. Die Einhaltung der behaupteten Verfahren konnte jedoch bisher nicht von unabhängigen Sachverständigen zertifiziert werden. Bisher hat die Kreditwirtschaft die Korrumpierung von Schlüsseln kategorisch bestritten, doch die Realität war mindestens beim alten System anders[5]. Wenn es einem Angreifer gelingt in den Besitz der Schlüssel zu gelangen, so sind ihm während der Dauer der Verwendung dieser Schlüssel alle Möglichkeiten gegeben:

---

[2] ZKA = Zentraler Kredit-Ausschuss, in dem alle Verbände der deutschen Kreditwirtschaft zusammengeschlossen sind

[3] Die Varianten des neuen PIN-Systems sind im Detail nicht alle öffentlich bekannt

[4] Cracking DES. Secrets of Encryption Research, Wiretap Politics Chip Design. Electronic Frontier Foundation. O´Reilly 1998. ISBN 1-56592-520-3.

[5] Der Spiegel 36/1997: Spätes Eingeständnis (Anlage)

Er benötigt dann "vor Ort" nur noch wenige Sekunden für die Berechnung der jeder PIN, die mit diesen Schlüsseln generiert wurde.

Bei Kreditkarten ist das theoretische Risiko der Berechenbarkeit der PIN wegen der Verwendung von kurzen Schlüsseln wesentlich höher als bei ec-Karten. Wenn in Deutschland trotzdem weniger Missbrauchsfälle mit Kreditkarten bekanntgeworden sind, so liegt das offensichtlich daran, dass die Deutschen in der Regel mit ihrer zum Konto gehörigen ec-Karte Geld aus dem Automaten holen und mit der Kreditkarte Waren und Dienstleistungen (wie ein Unternehmen der Branche wirbt: "mit dem guten Namen") bezahlen.

Das "Erraten" der PIN

Die PIN ist zur Zeit sowohl für ec-Karten als auch für VISA-Kreditkarten vierstellig. Folglich gibt es theoretisch 10.000 Möglichkeiten der Variation, so dass sich die Wahrscheinlichkeit eine richtige PIN zu erraten mit 1:10.000 ergeben würde. Weil jedoch die PIN 0000 nicht vorkommt und drei Fehlversuche bis zur Einziehung der Karte möglich sind, erhöht sich die Wahrscheinlichkeit auf 1:3.333. Durch die Dezimalisierung des DES-Ergebnisses, das für die PIN herangezogen wird, erhöht sich die Trefferwahrscheinlichkeit darüber hinaus. Der genaue Wert kann zur Zeit nicht angegeben werden, weil das konkrete Verfahren nicht offengelegt wird. Ein "Serientäter" der viele Karten in seinem Besitz hat, hat also gute Chancen einen Treffer zu landen. Man muss dabei noch berücksichtigen, dass das angegebene Risiko rein statistisch, d. h. im Durchschnitt bei unendlich vielen Versuchen, zu sehen ist. In Wirklichkeit kann schon der erste Versuch – wie jeder Lotto-Spieler hofft und was auch wirklich eintreten kann - bei einer Karte ein Treffer sein.

Es muss darauf hingewiesen werden, dass in Verfahren, in denen der Verfasser als Sachverständiger tätig war, wiederholt behauptet wurde bei der Umstellung des PIN-Verfahrens habe sich die PIN im Einzelfall nicht geändert. Wenn diese Behauptung richtig ist, so sind Zweifel an der richtigen Durchführung des neuen PIN-Verfahrens angebracht. Denn, wenn die PIN-Generierung nach einem Zufallsprinzip arbeitet, kann das nicht sein. Mit der Übernahme der alten PIN, die bestimmte Vorzugsziffern enthält, erhöht sich die Wahrscheinlichkeit der Erratung der PIN dramatisch auf ca. 1:150.

Aus gutem Grund haben die Banken im Interbankenverkehr eine sechsstellige PIN gewählt. Diese ist viel sicherer als die der Karten.

Risiko: Geringe Sicherheit aufgrund der Verwendung vierstelliger PIN. Hier sind auch "Zufallstreffer" im Einzelfall nicht auszuschließen, weil sich die statistische Aussage nur auf große Mengen bezieht.

Die Plastikkarte

Die Plastikkarte selbst hat die Abmessungen von min. = 85,78 mm und max. = 86,42 mm in der Breite, sowie min. = 53,98 mm und max. = 54,51 mm in der Höhe. Sie kann mit Zeichen oder Bildern bedruckt sein, die in keiner Art ausgewertet werden, aber auch Merkmale enthalten, die geprüft werden können und somit eine gewisse Fälschungssicherheit bewirken. Die mannigfaltigen Möglichkeiten von Sicherheitsmerkmalen seien am Beispiel einer Musterkarte des Kuratoriums Deutsche Kartenwirtschaft veranschaulicht:

Die heute technisch möglichen Sicherheitsmerkmale sind durch rote Markierungen bezeichnet. Hologramme bzw. nicht sichtbare Merkmale können hier nicht dargestellt werden. Es ist bedauerlich und beinhaltet eine nicht zu übersehende Betriebsgefahr, dass die aufgezeigten Sicherheitsmerkmale üblicherweise nicht eingesetzt werden. Dadurch ist das Risiko des Missbrauchs von Debit- und Kreditkarten durch Kopien nicht zu unterschätzen[6].

Darüber hinaus enthält eine Karte in der Regel auch noch Datenspeicher: den Magnetstreifen, den Chip und das MM-Merkmal.

Der Magnetstreifen

Der auf der Kartenrückseite oft braun zu erkennende Magnetstreifen enthält drei Spuren. Bei VISA-Debitkarten interessiert nur Spur 2, bei ec-Karten enthält Spur 3 die wichtigen Daten.

Spur 2:

ABA track =	American Banking Association
	Standard Spur
Urspr. Norm:	ISO 3554 (USA=ANSI X4.16 – 1976)
Verfahren:	F2F
Dichte:	73 bpi +/- 3%
Code:	5 bit code (einschl. 1 odd parity bit)
Kapazität:	40 numerische Zeichen
Verwendung:	Nur Lesen

Spur 3:

MINTS track =	Mutual Institution National Transfer System
Urspr. Norm:	ISO 4909, DIN 4909
Verfahren:	F2F
Dichte:	210 bpi +/- 5%
Code:	5 bit code (einschl. 1 odd parity bit)
Kapazität:	107 numerische Zeichen
Verwendung:	Lesen und Schreiben

[6] Bundeskriminalamt:“EC-Karte einfach kopiert“ in Wiesbadener Kurier /Geld Kurier vom 15.2.2003

Risiko: Beide Spuren können mit handelsüblichen, frei erhältlichen Karten-Lese-/Schreibgeräten erstellt, ausgelesen und verändert wwerden. Die Bedeutung der einzelnen Daten ist allgemein bekannt.

Der Chip

Zur weiteren Erhöhung der Sicherheit hat man bei neueren Karten einen Microchip integriert. Dieser wird über 5 Kontakte angesteuert. Jedoch ist sein Inhalt verschlüsselt und besonders gesichert. Da das Steuerprogramm auch nicht vollständige im Chip abgelegt ist und auch die externen Befehle verschlüsselt ankommen, ist eine relativ hohe Sicherheit gegeben. In der Regel wird dieser Chip jedoch zur Zeit nur für die Geldkartenfunktion genutzt.

Ab dem Jahr 2005 soll der Chip für die Durchführung von VISA Kreditkarten-Buchungen (EMV-Applikationen) genutzt werden. Über die Verwendung für ec-Karten ist zur Zeit noch nichts bekannt. Somit wird es ab 2004 für Plastikgeld bezüglich der Sicherheit ein Zweiklassensystem geben: Kreditkarten werden sicherer sein als ec-Karten. Während der Übergangszeit auf das Chip-System wird im Magnetstreifen der Kreditkarten ein Zeichen abgespeichert sein, das ggf. auf den vorhandenen Chip hinweist, so dass dieser genutzt werden kann.

Erst wenn eine vollständige Ausstattung aller GAA in Europa mit EMV-Applikationen sowie eine vollständige Ausstattung der Kreditkarten mit EMV-Chips erfolgt ist, kann auf die Daten des Magnetstreifens verzichtet werden.

Risiko: Der elektronische Chip verfügt über gute Schutzfunktionen. Er kann nich mit handelüblichen Geräten im sensiblen Bereich ausgelesen werden. Er bietet deshalb eine hohe Sicherheit.

Das MM-Merkmal

Zur Personalisierung der Plastikkarte wird bei deutschen ec-Karten ein karten-individueller Code in einem nichtmagnetischen Streifen eingeprägt, der nur mittels eines kapazitiven Verfahrens gelesen werden kann. Durch Verknüpfung dieses Codes mit den Daten des Magnetstreifens kann so eine individuelle Prüfziffer generiert werden, die die Verwendung von Blankketten (leeren Plastikkarten, wie man sie in einschlägigen Geschäften kaufen kann) unmöglich macht. Denn beim Kopieren der Kartendaten des Magnetstreifens kann keine gültige Prüfziffer erzeugt werden.

Leider wird das MM-Verfahren im Ausland mit wenigen Ausnahmen überhaupt nicht und in Deutschland (wegen des Temperatur- und Feuchte-abhängigen Dielektrikums) nicht immer eingesetzt.

Risiko: Während die Daten im Chip und das MM-Merkmal nur sehr schwer verändert werden können, sind die Daten des Magnetstreifens mit einfachen Mitteln (Lese-/Schreibegeräte) zu verändern. Sicherheit gegen Kopieren wird im wesentlichen durch nichtmagnetische Sicherheitsmerkmale erhöht. Verfälschungen werden durch Verknüpfungen von magnetischen und nichtmagnetischen Daten erschwert. Jedoch wird das MM-Merkmal im Ausland - und auch in einigen nachgewiesenen Fällen sogar in Deutschland – nicht berücksichtigt. In diesen Fällen kann mit einfachen Mitteln eine Kopie der Daten auf eine andere Karte übertragen werden. Diese ist dann voll einsatzfähig.

Die Ablauforganisation

Das Sicherheitsmanagement
Um zu erschweren, dass der Masterschlüssel öffentlich bekannt wird, verwalten üblicherweise zwei Mitarbeiter des Instituts jeweils einen halben Schlüssel. Dabei sollte sichergestellt sein, dass diese Mitarbeiter, die Key-Management-Administratoren (KMA), nicht an der Planung und/oder Durchführung der Verfahren beteiligt sind. Die Schlüssel sollten in einem Tresor verwahrt werden, der sich im Sicherheitsbereich des Instituts befindet.

In diesem Sicherheitsbereich befinden sich auch die Geräte, mit denen die PIN erzeugt und geprüft wird. Die notwendigen Schlüssel sind hier in Sicherheitsmodulen abgelegt, deren Manipulation oder gewaltsame Öffnung üblicherweise ihre Zerstörung bewirkt. Aber auch in diesen Sicherheitsmodulen sollten die Schlüssel nur wiederum mit einem Transportschlüssel verschlüsselt abgelegt werden. Dieser Transportschlüssel ist selbst in zwei Teilschlüssel zerlegt, die getrennt verwaltet werden.
Auch für die Weitergabe der Schlüssel an den zuständigen Verband gilt das „Vier-Augen-Prinzip“. Zudem müssen die betrauten Mitarbeiter besonders zur Geheimhaltung verpflichtet werden.

Risiko: Wenn die Verfahren wie beschrieben eingehalten werden, ist das **Risiko sehr gering**.

Der Versand der Karten und der PIN

Üblicherweise werde die Karten als Massendrucksachen zur Post gegeben. Sie sind deshalb leicht erkennbar, was in der Vergangenheit wiederholt dazu geführt hat, dass sie von Postmitarbeiter ausgefiltert wurden. Die PIN-Briefe werden auf die selbe Weise dem Karteninhaber zugestellt. Es ist bekannt, dass wiederholt auch diese Briefe ausgefiltert wurden. Die missbräuchliche Benutzung der entwendeten Karten und zugehörigen PIN war dann nur noch eine Formsache. Deshalb sind einige Institute nach Eigenbekundung dazu übergegangen, die Sendungen an unterschiedlichen Orten aufzugeben.
Es sei darauf verwiesen, dass in anderen Ländern, z. B. in Frankreich, Karte und PIN-Brief vom Kontoinhaber in den Geschäftsräumen des Kreditinstitutes persönlich (gegen Vorlage des Ausweises o. ä. Dokumente) abgeholt werden müssen. Das wäre zur Erhöhung der Sicherheit auch den deutschen Kunden zuzumuten.

Risiko: Der Versand von Karte und PIN auf dem Postweg ist in Deutschland als sehr riskant zu bezeichnen.

Verwahrung von Karte und zugehöriger PIN
Nach den „Allgemeinen Geschäftsbedingungen AGB“ der Kreditinstitute müssen die Karte und die PIN immer getrennt aufbewahrt werden bzw. die PIN nach Kenntnisnahme vernichtet werden.

Dem muss teilweise widersprochen werden. Denn wenn Karte und PIN in einem verschlossenen Behältnis (Schrank bzw. Tresor) gemeinsam verwahrt werden, hat Der rechtmäßige Inhaber nach meiner Meinung seiner Sorgfaltspflicht Genüge getan. Gegen einen Wohnungs-Einbruch z.B. kann man sich üblicherweise kaum schützen. Zum anderen kann die Vernichtung des PIN-Briefes nicht generell in AGBs verlangt werden, weil kein Durchschnittsbürger seine PIN bei Besitz mehrerer Karten und nur gelegentlicher Nutzung jeder Karte im Gedächtnis behalten kann. Die Aufbewahrungsart von Karte und PIN im Zeitpunkt des Abhandenkommens ist deshalb immer im Einzelfall zu würdigen.

Risiko: Im Streitfall kann der Karteninhaber i. d. R. nicht beweisen, dass sich die PIN zum Zeitpunkt des Abhandenkommens nicht in unmittelbarer Nähe zur Karte befand.

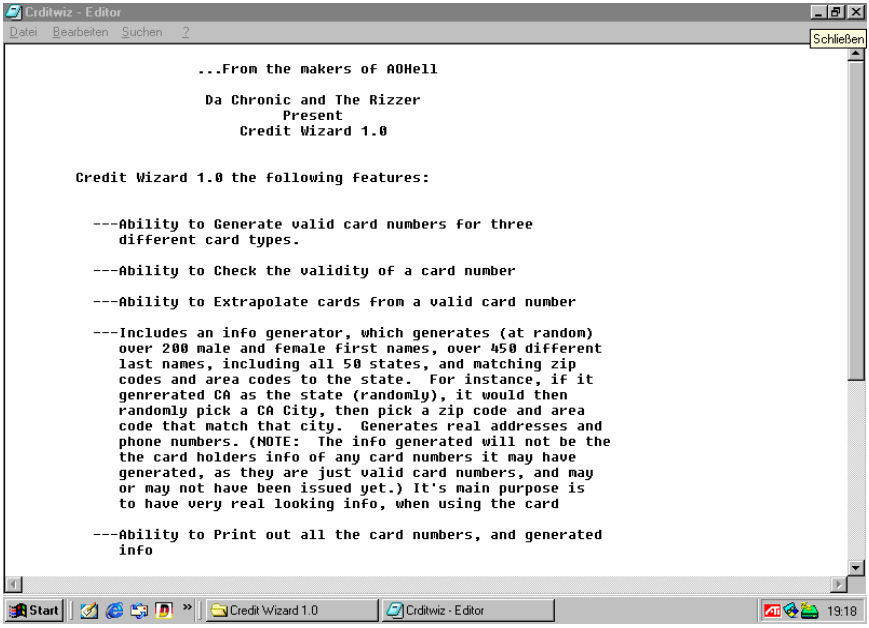
Einkauf mit Kreditkarten oder ec-Karten im Internet

Das durch die Preisgabe der Kredit- oder ec-Kartennummer im nationalen und internationalen Verkehr über das Internet begründete Risiko ist in den Medien hinreichend unter Bezug auf aktuelle Ereignisse beschrieben worden. Es darf deshalb zur Zeit als das größte Risiko für Missbrauch von Karten angesehen werden.

Hierfür werden Kundennamen und Kartennummern oft auch aus dem Abfall von z. B. Restaurants oder an Tankstellen gewonnen, weil häufig sorglos mit den Belegen umgegangen wird.

Auch die sogenannten geschlossenen Systeme bieten nur geringen Schutz. Die Hacker lauern überall und haben selbst zur Generierung gültiger Kreditkarten-nummern aufwendige Computerprogramme geschaffen, wie der Bildschirm-Ausdruck veranschaulicht. In diesem Programm ist die Generierung von Karten der Beklagten enthalten. Ich habe die Beklagte seinerzeit darauf aufmerksam gemacht. Ob und evtl. welche Gegenmaßnahmen getroffen wurden, ist mir unbekannt.

Risiko: Die Preisgabe und Übertragung von Kartendaten im Zahlungsverkehr über den allgemein zugänglichen Bereich des Internet ist äußerst riskant! Wenn nicht ein überzeugendes Schutzsystem durch den Partner angeboten wird, sollte die Preisgabe von Kartennummern in keinem Fall über das Internet erfolgen.



Online-/Offline-Übertragung von Daten

Die Banken behaupten, dass die Übertragung der Daten vom Geldautomaten zum Rechenzentrum des Kreditinstitutes ausschließlich online erfolgt, weil die Kontoführende ❷②⑤② ⑤⑩ ⑩⑫⑥②②⑩⑤ prüfen und ggf. autorisieren müsse. Dazu sei das Nationale Online Verfahren (NOV) seit Ende der 90er Jahre eingerichtet worden. Das mag in der Regel für Deutschland gelten. Doch ist es nicht überzeugend, dass eine Online-Autorisierung durch die Konto führende Bank von jedem Automaten auf der Welt durchgeführt wird. In jedem Falle sind deshalb die Transaktionsprotokolle des Automaten und der Konto führenden Stelle im Original durch einen Sachverständigen zu prüfen.

Auch wird immer wieder von den Kreditinstituten in Fällen der missbräuchlichen Benutzung im Ausland gestohlener Karten behauptet, dass es mindestens einige Stunden dauere bis eine Kartensperre im Ausland greift. Bei einem tatsächlichen Online-Verkehr ist diese Behauptung absolut absurd.

Da die Sperre bei der Konto führenden Stelle wirksam sein sollte, würde bei einer Online-Übertragung aus dem Ausland die Autorisierung der beabsichtigten Transaktion verweigert und die Karte müsste nach den Regeln sofort eingezogen werden.

Risiko: In der Regel ist der beweispflichtige Kunde als Laie vor Gericht nicht in der Lage die tatsächlichen Details der Datenübermittlung (Online/Offline) darzulegen. Auch an einen Sachverständigen werden hohe Anforderungen gestellt, so dass nicht jeder EDV-Sachverständige hierzu in der Lage ist. Der Sachverständige muss in jedem Fall die Original-Protokolle der streitgegenständlichen Transaktionen des GAA und des Rechenzentrums überprüfen. Um auszuschließen, dass ein technischer Mangel vorliegt, müssen die Protokolle auch vorausgehende und nachfolgende Transaktionen (ggf. in anonymisierender Form durch Kürzung der Kontonummern) enthalten. Das zeitliche Eintreten der Wirksamkeit einer Sperre ist ebenfalls an beiden Enden der streitgegenständlichen Transaktion zu analysieren.

Die kundenzugängliche Hardware

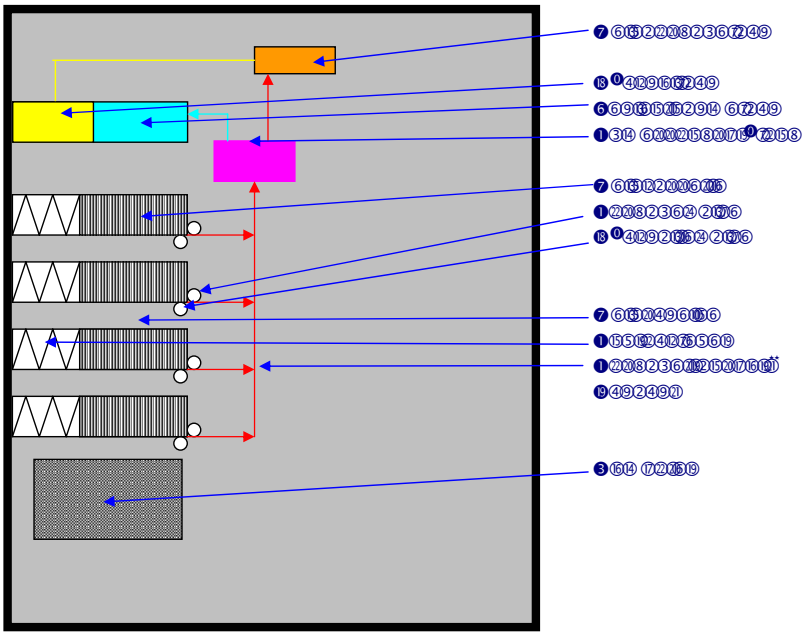
2.5.1 Der Geldausgabeautomat (GAA)

Von einem Geldausgabe-Automaten (GAA) werden üblicherweise drei Dinge erwartet:
1. Er soll die korrekte Geldmenge herausgeben.
2. Er soll den Vorgang schnell abwickeln.
3. Die Scheine sollen echt sein.

Dabei wird jedoch in der Regel übersehen, dass er aufgrund seiner Bauart auch die „Betriebsgefahr“ nach dem heutigen Stand der Technik so gering wie möglich halten soll. Das ist leider heute in der Regel zu bezweifeln.

Betrachten wird deshalb die technische Funktionsweise eines Geldausgabe-Automaten näher:

Funktionsweise eines Geldausgabe-Automaten (GAA)



Es ist technisch grundsätzlich möglich, falsche Scheine im GAA auszusortieren, doch wird dadurch die Ausgabe stark verzögert. Deshalb beziehen die Kreditinstitute die Geldscheine von der Landeszentralbank, wo das Geld vom Stapel maschinell gezählt und auf Echtheit geprüft wird. Ein häufig eingesetzter Geladausgabe-Automat enthält fünf Geldkassetten. Das sind längliche Kassetten, die übereinander angeordnet sind. Diese Kassetten werden nach den örtlichen Anforderungen durch das aufstellende Kreditinstitut mit Noten unterschiedlichen Wertes bestückt: Wenn überwiegend jugendliche Kunden den Automaten vor der Diskothek benutzen, so werden überwiegend kleine Scheine in die Kassetten gegeben. Grundsätzlich gibt es je ein Magazin für Zehner, Zwanziger, Fünfziger und Hunderter. Daraus stellt der Automat den gewünschten Betrag zusammen.

Wenn die Geldkassetten in den Automaten eingesetzt werden, geben sie – ähnlich wie die Videokassette im Rekorder – eine Entnahmeöffnung frei. Die oberste Kassette bleibt dabei leer. Dem Computer wird dann der Anfangsbestand jeder der vier bestückten Kassetten mitgeteilt. Er berechnet dann fortlaufend den aktuellen Bestand und stellt die gewünschten Mengen für die Ausgabe bereit. Falls eine Kassette leer sein sollte, so wird er automatisch die gewünschte Menge in kleinerer Stückelung zusammenstellen.

Üblicherweise stehen die Geldscheine, wie in einem Karteikasten, fein säuberlich hintereinander. Dabei drückt eine Feder in Richtung der Entnahmeöffnung der Kassette, wo sie sich gegen eine gummierte Walze abstützen. Bei einer Entnahme beginnt sich die Walze zu drehen

und zieht so den ersten Geldschein nach unten. Damit nicht mehrere Geldscheine entnommen werden, werden diese durch eine gegenlaufende Gummiwalze vereinzelt.

Der vereinzelte Schein gleitet über Schienen auf Gummibänder, die ihn zur Abmessungsüberprüfungs-Station transportieren. Diese zusätzliche Prüfung ist charakteristisch für Geldautomaten. Denn obwohl sich die Vereinzelung von Blättern mit gegenlaufenden Gummiwalzen in der Drucktechnik und bei Kopierern hervorragend bewährt hat, kommt es doch hin und wieder vor, dass ein Schein durchschlüpft. Besonders neue Noten können so fest an einander haften, dass eine weitere Prüfung unbedingt erforderlich ist. Bei der Abmessungsprüfung werden dann die Breite und die Dicke des entnommenen Scheins vermessen.

Beide Messungen sind unbedingt nötig, weil zum einen zwei Schein exakt übereinander liegen könnten. Dadurch ergibt sich eine doppelte Dicke. Zum anderen könnten zwei Scheine gegen einander verschoben sein, so dass sich andere Abmessungen ergäben. Es könnte aber auch sein, dass sich versehentlich ein anderer Wert unter die Scheine in einer Kassette geschlichen hat. Dieser würde ebenfalls durch die Feststellung der exakten Abmessungen ausgesondert werden können.

Bei der Dickenmessung wird der entnommene Schein unter einem Nocken hindurchgeführt, der am kürzeren Arm eines Hebels befestigt ist. Das Hebelverhältnis übersetzt Dickendifferenzen von Hundertstel Millimetern in Weglängen von einigen Millimetern, so dass der Rechner auch kleinste Dickendifferenzen gegenüber einem vorgegebenen Sollwert verarbeiten kann. Der Sollwert wird beim Einlegen der Kassette in den Automaten ermittelt. Durch Probeentnahmen wird das Gerät auf die aktuelle Dicke der eingelegten Scheine justiert. Auf dieser Grundlage wird die Zeit berechnet, die ein Schein zum Passieren einer Fotozelle bei konstanter Fördergeschwindigkeit benötigt. Dies ist dann das Maß für die Sollgröße des Scheins.

Gelangen dann tatsächlich einmal zwei Scheine in diese Prüfstation, so werden sie – wie die bei der Justierung benutzten Scheine – in das Fehlentnahmefach (Reject-Fach) der leeren Kassette abgelegt. Für den Kunden wird sofort ein neuer Schein nachgeschoben. Dieser Vorgang verzehrt nur Sekunden, so dass der Kunde in der Regel hiervon nichts merkt. Der Sachverständige kann diesen Vorfall erst durch eine Zeitanalyse feststellen, wenn keine Fehlermeldung ausgegeben wird.

Die einwandfreien, vereinzelten Geldscheine gelangen auf eine Sammelablage, von der der angeforderte Betrag an das Ausgabefach weitergeleitet wird. Entnimmt der Kunde das Geld nicht in der durch das Programm vorgegebenen Zeit (was relativ häufig vorkommt!), so wird der Betrag automatisch wieder eingezogen und in das Rückholfach (Retract-Fach) abgelegt.

Alle Vorgänge werden durch den eingebauten Computer erfaßt und protokolliert, so dass eine ständige Aktualität des im Geldausgabe-Automaten verfügbaren Bestandes gewährleistet ist. In regelmäßigen Abständen sollte die ursprünglich leere Kassette überprüft werden und ein Bestandsabgleich erfolgen.

Manipulation von Geldautomaten (GAA) und Risiken aus deren Bauart

Es sind mehrere Methoden von Automaten-Manipulationen bekannt geworden, die als Risiken dargestellt werden.

Risiko:

- Der Geldausgabeschacht wird verstopft, so dass der Täter nach dem Fortgang des Kunden das Geld „herausfischen“ kann ("Marlboro-Methode").
- Der Geldausgabeschacht wird mit einer Vorrichtung versehen, die die Rückgabe der Karte verhindert ("Algerische Schlinge"). Durch Hilfsangebot der Täter wird die PIN ausgespäht. Diese Methode ist sehr aktuell (siehe Warnung des BKA Juni 2003, Video Raiffeisenkasse, SAT1 am 15.09.2003).
- Wenn das Kreditinstitut keine Trennblätter zwischen den Vorgängen einfügt, so gibt es Möglichkeiten ohne Kontenbelastung Geld zu entnehmen.
- Bei sogenannten Touch Screen Pads gibt es „daktyloskopische“ Methoden die vorher eingegebene PIN mit hoher Wahrscheinlichkeit richtig herauszufinden.

Ausspähung der PIN am GAA

Durch die Bauart und die Aufstellung wird die Ausspähung der PIN des Kunden auch ohne technische Hilfsmittel wie Minikamera o. ä. in vielen Fällen begünstigt.

Risiko:

- Aus Betriebsgefahr = **sehr hoch**

Darüber hinaus muss auch darauf hingewiesen werden, dass viele Fälle von Ausspähungen mit technischen Hilfsmitteln bekannt geworden sind. An dieser Stelle soll nur die Möglichkeit der Ausspähung mit Mikro-Videokameras erwähnt werden. Diese Kameras werden im Katalog eines deutschen Elektronik-Händlers derzeit mit den Abmessungen von 32 x 32 x 14 mm zu einem Preis von 79,95 EURO angeboten.

Risiko:

- Ausspähung mit technischen Hilfsmitteln (Kameras, Vorsatzgeräte) = **hoch**

Diebstahl von Geldausgabeautomaten (GAA)

Am 13. Februar 2003 wurde im Fernsehen auf Kanal HR3 berichtet, dass in der Nacht zum 12.02.2003 in Alsfeld (Hessen) ein 700 kg schwerer Geldautomat in der Sparkasse aus der Wand gebrochen und abtransportiert wurde. Es wurde von einer Beute in Höhe von 38.000 € berichtet.

Wenn man von dem finanziellen Schaden für das Kreditinstitut absieht, stellt sich die Frage, welche weiteren Risiken dem Kunden durch einen Automatendiebstahl erwachsen.

Risiko für Kartenbesitzer:

Hier ist folgende Möglichkeit offensichtlich:

- Der Automat wird ausgeschlachtet und - mit neuem Innenleben versehen – wieder aufgestellt (Methode Mailand-Mall). Bei Benutzung werden die Kartendaten und die zugehörige PIN eingelesen und abgespeichert. Damit werden dann Blanketten erstellt und die Konten der Kunden geplündert. Diese Methode funktioniert nur, wenn das MM-Merkmal und/oder der Chip nicht verwendet werden.

Die Software zum Betrieb von Geldautomaten

Es sind inzwischen mehrere Fälle bekannt geworden, in denen die Eingabe von nachweisbar falschen PIN zur Ausgabe des abgeforderten Betrages am GAA geführt haben. Der Verfasser hat mit einem Fernsehteam des ZDF einen Fall in Berlin dokumentiert und aufgearbeitet, der auch von der Redaktion WISO gesendet worden ist. Dabei hat der Karteninhaber mehrere unterschiedliche – vom Team spontan erfundene - PIN eingegeben. In jedem Falle wurde

vom GAA der angeforderte Betrag ausgegeben. In anderen Städten sind ebenfalls solche Fälle bekannt geworden. Da von den betroffenen Kreditinstituten niemals nachgewiesen wurde, dass der behauptete Softwarefehler behoben worden ist, ist auch heute nicht auszuschliessen, dass dieser Fehler noch auftreten kann.

Es ist deshalb im Schadensfall jedes Mal unbedingt das **Original-**Protokoll des GAA von einem neutralen Sachverständigen auszuwerten. Für eine abgesicherte Beweisführung sind Kontenauszüge, nachgefertigte Bildschirmausdrucke oder sonstige EDV-Derivatbelege des Kreditinstitutes nicht akzeptabel. Gleichermassen sind auch die Originalprotokolle des kontenbearbeitenden Rechenzentrums zu prüfen. Diese Urkunden sind in der Fachwelt allgemein als Transaktionsprotokolle bekannt.

Risiko: Auch Computer können bekanntlich versagen; Software kann Fehler enthalten, die unter bestimmten Umständen unvorhersehbare Aktionen (Ausgabe von Geld bei falscher PIN-Eingabe!) auslöst. Dieses Risiko kann nicht aussagefähig quantifiziert werden, doch sind in meiner Praxis bereits zwei nachweisbare Fälle bekannt geworden.

Karten-Lesegeräte

Lesegeräte, die die Daten im Magnetstreifen von Debit- und Kreditkarten lesen und ggf. ändern können, kommen im System des elektronischen Zahlungsverkehrs in unterschiedlichsten Bauformen zum Einsatz.

Bekannt sind zum Beispiel die Handgeräte bei der Deutschen Bahn und in ausländischen Restaurants (z.B. Frankreich). Da diese Geräte die Daten per Funk an einen in der Nähe stehenden Empfänger senden, besteht hier grundsätzlich die Möglichkeit diese Daten elektronisch mitzuhören und abzuspeichern.

Häufig werden die Daten aber auch erst gesammelt, bis sie an das Rechenzentrum übermittelt werden (Offline-Verkehr). Diese Methode wird aus Kostengründen oft von kleineren Unternehmen im sogenannten POS-Verfahren verwendet.

Da die Handheld-Geräte in der Regel über keine Sichtschutzeinrichtungen (Sichtblenden) verfügen, ist es leicht möglich die PIN-Eingabe auszuspähen.

Aber auch die älteren Abrollgeräte stellen ein hohes Risiko der Datenausspähung dar. Oft lassen die Gäste die Belege zurück, so dass sich die notwendigen Kartendaten leicht aus dem Abfall eines Restaurants fischen und kopieren lassen.

Die gleichen Risiken bestehen grundsätzlich auch bei Desktop-Geräten, wie sie üblicherweise in Tankstellen verwendet werden. Wegen der häufig dicht stehenden eiligen Kunden ist die PIN-Eingabe relativ einfach auszuspähen. Darüber hinaus ist es auch schon vorgekommen, dass betrügerischen Angestellte PIN und Kartendaten systematisch ausgespäht und abgespeichert haben.

In zunehmendem Maße werden Lesegeräte wegen ihrer miniaturisierten Bauform auch als Vorsatzgeräte verwendet um Zugang zu Geldautomaten zu ermöglichen (Fall Axmann, Köln). Dabei werden die Daten ausgelesen und abgespeichert. Diese Methode wird aber nur ausserhalb der Geschäftszeit eines Kreditinstitutes angewandt. Kunden sollten deshalb besonders

wachsam sein und auf keinen Fall die PIN eingeben, wenn sie an einem Display dazu aufgefordert werden.

Risiko: Die am häufigsten zu vermutende Ursache für missbräuchliche Benutzung von Karten ist die Ausspähung mit und ohne Hilfsmittel. Sie wird durch die Bauart und den Aufstellungsort des GAA begünstigt. Dadurch ist eine erhebliche Betriebsgefahr gegeben, die der Aufsteller des GAA zu tragen hat. Bei mangelnder Video-Überwachung ist die Verantwortung des Aufstellers noch höher zu bemessen. Insgesamt ist das Risiko „GAA“ als **sehr hoch** zu bewerten.