Bankensektor

4 Security ist eine Lösung zur manipulations- und fälschungssicheren Erfassung von biometrischen Daten
Jederzeit integrierbar in die bisherige EC-Kartenstruktur
Geringe Integrations- und Betriebskosten bei maximaler Sicherheit

Die Probleme des bestehenden EC-Kartensystems (Maestro):

Das bisherige EC-Kartensystem mit Magnetstreifen und PIN ist ein System aus Zeiten, in denen das Wort Computerkriminalität noch kein Thema war. 4-stellige PIN-Nummern galten zwar damals als sicher, können aber heute den Missbrauch nicht mehr wirklich ausschließen, zumal die PIN mit Hilfe des Kartencodes errechnet wird.
Sicherungsmerkmale, die auf biometrischen Daten beruhen waren damals nicht denkbar. Man war froh, überhaupt die beim EC-Verfahren notwendigen Datentransferraten und Verarbeitungsgeschwindigkeiten zu erreichen. Es gibt zwar mittlerweile EC-Karten, die durch einen auf der Karte aufgebrachten Chip angeblich fälschungssicher sind, dennoch hilft dies nicht gegen den Kartendiebstahl. Der EC-Kartenbetrug – wie er sich heute darstellt – beruht auf einem Ausspähen oder Erfassen der PIN und einer Abtastung des Magnetstreifens der Karte. Es würde aber keinesfalls für Personen mit derartiger krimineller Energie ein Problem darstellen, die Karte zu entwenden.
An den Problemen im Automobilbereich mit „Tachojustagen“ bei angeblich fälschungssicheren Tachometern erkennt man, dass auch ein angeblich fälschungssicherer Chip dies nur auf Zeit sein kann. Nachdem diese Karten – und damit die dort aufgebrachten Chips – zu Hunderttausenden, wenn nicht gar Millionen verbreitet sind und es damit keine Kontrolle über den verbleib dieser Karten gibt, findet sich sicher jemand, der das unmögliche möglich macht.

Das Problem ist aber nicht nur die tatsächlich zu geringe Sicherheit. Vielmehr macht sich bei der Bevölkerung eine gewisse Angst beim Umgang mit diesem System breit.

Ein weiteres Problem stellen Missbrauchskosten auf Seiten der Bank dar. Ein System, das missbraucht wird sorgt für Kosten auf Seiten der Banken und der Kunden. Selbst wenn die Bank nicht haften muß, so wird sie sich das Vertrauen der Kunden im Missbrauchsfall verspielen.

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com

Neue EC-Karten sind nicht wirklich sicherer, aber sie kosten das 3-fache (laut Angabe der Sparkassen, die sich für deren Einsatz entschieden haben) wie die alten Karten.
Ein derart dramatischer Kostenanstieg ist aus Gründen der Wettbewerbsfähigkeit wohl kaum hinnehmbar. Darum scheuen sich auch die anderen Banken (noch) vor der Einführung.

Diesem System bleibt das Problem, dass mehr oder weniger – über die Verbreitung – allgemein zugängliche Daten als Sicherheitsmerkmale eingesetzt werden und die beliebten 4-stelligen PINs derart unsicher sind, dass eher von Unsicherheitssystemen, denn von Sicherheitssystemen gesprochen werden kann, denn eine Chance von 1 zu 10.000 für die richtige PIN ist wahrlich kein Sicherheitsfaktor und öffentlich zugängliche Systeme werden immer manipulierbar bleiben.

Die Lösung

Ein höheres Sicherheitsniveau bei den Karten ist nur eine Neuauflage des Hase und Igel Spiels. Neu eingeführte Sicherheitsmerkmale können – da sie ja offen da liegen – jederzeit geknackt werden. Die Kartensicherheit ist also indirekt durch ein zentral gespeichertes biometrisches Merkmal zu ergänzen, das in keiner Verbindung zu den Kartendaten steht. Nur im Zentralsystem können Kartendaten und Fingerabdruck einander zugeordnet und abgeglichen werden. Somit ist sichergestellt, dass selbst, wenn es zu einem unbemerkten Kartenverlust kommt, Kartenmissbrauch unmöglich ist, da hierfür der Fingerabdruck des Besitzers notwendig ist. Seinen Finger verliert man nicht unbemerkt.

Ein Fingerabdruck ist etwas einmaliges. Nicht umsonst ist er ein unumstrittenes gerichtsrelevantes Beweismittel. Man kann zwar einen Fingerabdruck abnehmen und kopieren. Diese Kopien können jedoch durch eine einfache Hautwiderstands-messung, die es ermöglicht, organische lebende Strukturen von anderen Strukturen zu unterscheiden, aufgedeckt werden.

Das größte Problem stellt jedoch dann immer noch eine Manipulation oder ein Missbrauch der Daten dar. Hierzu haben wir die eigentliche Lösung geschaffen:

Betrachtet man die derzeitige Anwendungsstruktur herkömmlicher Fingerprint-scanner, so wird bei herkömmlichen Systemen ein Bild erstellt – oder auch ein Auszug, der die wichtigen Merkmale enthält – und dieses über den Rechner, an dem der Scanner angeschlossen ist, zu einer Zentralstelle übertragen, oder gleich in diesem System verglichen. Zumindest der zum Rechner erzeugte Datenstrom kann jederzeit mitgeschrieben werden und somit – anstatt eines echten Fingerabdruckes – wieder verwendet werden.

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com

Die Daten müssen vor jeglichem Missbrauch geschützt werden!

Das heißt auch der Rechner hinter dem Scanner, das angeschlossene Netzwerk und alle anderen sich zwischen dem Scanner und dem Zentralsystem befindlichen Stellen müssen von der Nutzung ausgeschlossen werden. Eine normale Verschlüsselung würde beim selben Fingerprint wieder das selbe Muster erzeugen. Ein Mitschreiben und Widerversenden wäre also hierbei jederzeit möglich.

Unsere Lösung sorgt dafür, dass mitgeschriebene Daten absolut wertlos sind. Durch alternierende Keys – sowohl von der Zentrale, als auch an der Fingerprintscan- und Verschlüsselungseinheit sorgen dafür, dass keine Mustererkennung stattfinden kann. Die hier übertragenen Daten könnten - theoretisch – selbst über das Internet ohne weitere Sicherungsmaßnahmen übertragen werden.
Weitere Sicherheitsmaßnahmen sorgen dafür, dass jeglicher Manipulationsversuch erkannt und protokolliert wird.

Die Fingerprintdaten bekommen lediglich in der Zentrale wieder einen Wert.

Unterschiedliche Sicherheiten für unterschiedliche Einsatzzwecke:

Für eine Sicherung von Geldtransfers käme eine 3-stufige Sicherheitsabstufung in Betracht. So sollte nach Geräteeinsatz unterschieden werden:

1. Innerhalb der Banken (z.B. am Schalter) und an Geldautomaten

   Hier bestehen die umfangreichsten Möglichkeiten. Mit dem Fingerprint können hier elektronische Unterschriften geleistet werden, Barabhebungen vorgenommen, Überweisungen, Abbuchungen und Abbuchungsaufträge, sowie sämtliche weiteren Bankgeschäfte bestätigt werden.
   Diese bankinternen 4 Security – Systeme haben Ihre eigene Verschlüsselung, werden exakt inventarisiert und ihr Verbleib überwacht. Für die Inbetriebnahme, die Inbetriebhaltung und ihre Entsorgung gibt es ein fest vorgeschriebenes Protokoll.

2. 4 Security POS

   Für POS – Systeme bzw. Systeme im Firmeneinsatz wird eine zweite Sicherheitsstufe definiert. Diese Systeme bekommen ihren eigenen Verschlüsselungsalgorhythmus und werden nur verliehen bzw. zur Verfügung gestellt. Das Eigentum verbleibt entweder bei der Bank oder der Betriebsgesellschaft. Diese Systeme müssen sich mindestens einmal pro Monat am Hauptsystem rückmelden. Ihr Verlust muß angezeigt werden. Bei Defekt werden diese Geräte zurück an die Bank versandt, dort als nicht mehr aktiv

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com

gekennzeichnet und entsorgt werden. Durch den Verbleib der Systeme im Eigentum des Betreibers ist ein jederzeitiger Zugriff auf Systeme im Falle eines Manipulationsverdachts gewährleistet. Mit diesen Systemen sind Abbuchungen von fremden Konten möglich, bzw. die normalen EC-Kartendienste, wie sie an POS-Systemen üblich sind.

3. 4 Security Home

   Dies werden die meistverbreitetsten Systeme sein. Sie lösen PIN / TAN bzw. HBCI Strukturen ab und sorgen beim Kunden für ein hohes Sicherheitsempfinden. Wieder mit einem eigenen Algorhythmus versehen sind dies Kaufsysteme, oder Systeme, die von der Bank zur Verfügung gestellt werden. Der Vertrieb erfolgt ausschließlich über die Banken. Jedoch ist ein von einer Bank vertriebenes Gerät – über die Eintragung im Zentralsystem – jederzeit für andere Banken mitverwendbar. Die Geräte werden nur unter Angabe der persönlichen Daten vertrieben. Bei einem Weiterverkauf muß dies inkl. der Personendaten der Bank oder Zentralstelle gemeldet werden. Der Weiterverkäufer haftet für die Richtigkeit der Daten, bzw. für eventuelle Folgeschäden. Mit diesem System können die normalen Heimbankgeschäfte getätigt werden. Bankabbuchungen würde ich dem 4 Security POS vorbehalten.

Warum dieser Aufwand?

Nur mit guten Worten und im Vertrauen auf eine zweifelsohne sehr manipulationssichere Technik allein funktioniert ein System nicht auf Dauer. Jeder Algorhythmus ist knackbar. 4 Security ist aber ein Proaktives System. Wir können bereits den Versuch einer Manipulation aktiv feststellen und darauf reagieren. Es besteht also die Möglichkeit, zu einem Zeitpunkt einzugreifen, in dem noch kein Schaden entstanden ist. Das spart sehr viel Geld. Durch die Registrierung der einzelnen Systeme besteht die Möglichkeit, den Manipulator ausfindig zu machen und somit zu verhindern, dass dieser im Verborgenen weitermachen kann.
Solche Manipulatoren kommen auf eine Sperrliste und erhalten keine 4 Security Systeme mehr. Man kann sie ebenfalls – durch die Protokollierung nachgewiesen – der Justiz zuführen und somit ihrem schädlichen Treiben ein Ende machen. Bei EC-Karten Manipulation oder beim Internetbanking bestehen derartige Möglichkeiten bisher nicht.

Kosteneffizienter Einsatz:

Im Gegensatz zu Millionen neuen Karten müssen bei einem solchen System nur die Bankautomaten und die Auszahlungsschalter nachgerüstet werden. Die Kosten hierfür halten sich im Rahmen.

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com

Weiterer Nachrüstungsbedarf besteht im Einzelhandel. Auch besteht die Möglichkeit, dieses System anstatt von HBCI einzusetzen. Diese Kosten träfen dann aber nicht mehr die Bank. Im Gegenteil kann hier die Bank durch die Vermietung dieser Systeme sogar Einnahmen erzielen.
Weitere Kosten fallen durch den Aufbau und den Betrieb des Zentralsystems an. Diese halten sich aber im Rahmen, bzw. können über Sicherheitsdienstleistungen kompensiert werden.

Wie kann der Übergangsprozeß aussehen?

Für den Übergang kann – ähnlich wie bei den sichereren EC-Karten eine Prüfung vorgeschaltet werden, ob der Kunde denn bereits eine Fingerprint – Registrierung hat. Die Bank kann durch das Anbieten einer sicheren Alternative die Haftung für den Missbrauch der bisherigen Lösung deutlich reduzieren. Hierzu dürfte der Hinweis auf die Verfügbarkeit einer sicheren Alternative genügen.
Der Einzelhandel wird Druck seitens der Kunden bekommen. Auch wäre es denkbar, dass man EC-Kartengeschäfte, die noch mittels PIN abgewickelt werden nur noch unter Vorbehalt erledigt, die mit dem Fingerprint gesicherten jedoch ohne diesen Vorbehalt zulässt.
Im Privatbereich wird durch 4 Security Phishing oder eine Datenerlangung mit Hilfe von Trojanern so gut wie unmöglich gemacht. Mit einem einfachen Hinweis auf die Sicherheit wird wohl dadurch eine Verbreitung im Privatbereich sehr wahrscheinlich.

Möglicher Zusatznutzen:

Dieses System kann auch auf Dauer zu einem Internetbezahlsystem werden, dass nicht nur Sicherheit verspricht, sondern sie auch einhält. Dadurch gäbe es für die Banken einen Zukunftsmarkt, der bisher noch von nicht gesicherten Bankabbuchungen oder über Kreditkarten funktioniert. Die Authentifizierung des Fingerprints kann als kostenpflichtiger Dienst den E-Commerce Plattformen zur Verfügung gestellt werden. Diese erkaufen sich damit die Sicherheit einer eindeutigen, rückverfolgbaren Willenserklärung und einer gesicherten Bezahlung, bzw. Identifikation des Bestellers. Missbrauch wird somit eingedämmt.

Zusammenfassung:

Man kann sagen, dass dieses zum Patent angemeldete System die Basis für funktionierende elektronische Banking- und Bezahlsysteme werden kann und – auf Grund der bestechenden Preis- / Leistungsrelation auch werden wird. Bei einer

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com

überschaubaren Investition ist maximale Sicherheit gewährleistet. Diese geht soweit, dass sogar der Versuch, das System zu manipulieren aufgezeichnet und damit verfolgbar gemacht wird.

Dies ist definitiv die Basis für eine moderne digitale Gesellschaft.

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com