Secode für sichere **PIN-Eingabe** am Geldautomaten

Von Moritz Brandes, Jennifer Diez, Linda Gernhard, Stefan Henne, Florian Horsch, Anja Mayer, Philipp Mikat und Maike Sonnek

Acht Studierende der Dualen Hochschule Baden-Württemberg in Heidenheim haben im Rahmen einer Projektarbeit ein Konzept entwickelt, mit dem die PIN-Eingabe am Geldautomaten sicherer werden soll. Kern ist ein mit einer Polarisationsfolie versehenes Encrypting-PIN-Pad, bei dem die Anordnung der Ziffern für die PIN-Eingabe nach dem Zufallsprinzip wechselt. Das soll das Ausspähen aufgrund der Handbewegungen sowie das Abfilmen der PIN-Eingabe unmöglich machen. Ein Patent ist angemeldet. Red.

In der heutigen Zeit ist Datensicherheit ein heikles Thema. Betrüger entwickeln immerzu neue Methoden, um an persönliche Daten, insbesondere die Bankdaten, ihrer Opfer zu gelangen. Dies geschieht in zahlreichen Fällen durch Skimming, welches eine Vorgehensweise ist, bei der die Daten der ec- oder Kreditkarte und die zugehörige PIN am Geldautomaten ausgelesen und gespeichert werden. Deutschlandweit gab es laut Statista 2014 rund 57 000 Geldautomaten, an denen jährlich etwa 2,2 Millionen Transaktionen (Stand 2013) durchgeführt werden. 2015 wurden 118 der Bankautomaten in Deutschland manipuliert, um an die Bankdaten der Nutzer zu gelangen. Solche Manipulationen brachten nach Angaben von Euro Kartensysteme 2014 einen Schaden von 2,7 Millionen Euro mit sich. Im Ausland sind die Sicherheitslücken weitaus größer, wodurch NCR zufolge 2015 eine Schadenssumme von 2,6 Milliarden Euro weltweit entstand. Europaweit wurden in Italien, der Türkei und Frankreich besonders viele Skimming-Fälle registriert.

Statistiken zeigen, dass die Anzahl der Betrugsfälle in den vergangen Jahren deutlich zurückging. Während 2012 noch 520 Fälle von Skimming in Deutschland registriert wurden, waren es 2013 nur noch 341 Fälle. Im Ausland sank die Zahl der Fälle von 830 (2012) auf 487 Fälle (2013). Dies ist unter anderem auf die Einführung des EMV-Chips, der von Europay International, Mastercard und Visa entwickelt wurde, zurückzuführen. Dennoch bleiben die Schadenssummen enorm, denn auch die Betrugsmethoden entwickeln sich mittels neuer Technologien immer weiter. Dadurch sehen 39 Prozent der Bundesbürger im ec-Kartenbetrug durch manipulierte Bankautomaten ein großes Risiko, das Statista zufolge auch 2016 im Ranking noch vor Terroranschlägen, Computerviren, ansteckenden Krankheiten und Naturkatastrophen steht. Über die Hälfte aller Befragten befürchtet, dass der ec-Kartenbetrug durch manipulierte Bankautomaten zunehmen wird.

Zu den Autoren

Moritz Brandes, Jennifer Diez, Linda Gernhard, Stefan Henne, Florian Horsch, Anja Mayer, Philipp Mikat, Maike Sonnek, Studenten des Studiengangs Wirtschaftsingenieurswesen, Duale Hochschule Baden-Württemberg, Heidenheim

Wirtschaftliche und technische Machbarkeit nachgewiesen

Eine Gruppe aus acht Studierenden des Studiengangs Wirtschaftsingenieurwesen der Dualen Hochschule Baden-Württemberg (DHBW), Heidenheim, beschäftigt sich derzeit mit dieser Problematik und entwickelt unter dem Namen „SeCODE – Secure Code System" ein Encrypting PIN-Pad, welches das Ziel verfolgt, die Sicherheit bei der PIN-Eingabe am Bankautomaten zu erhöhen. Das Encrypting PIN-Pad ist ein Eingabefeld zur Eingabe der persönlichen PIN, beispielsweise am Bankautomaten, welches die PIN verschlüsselt zum Bankenserver weiterleitet, der diese kontrolliert.

Bevor die Projektidee, ein sicheres Encrypting PIN-Pad mit einer wechselnden Ziffernanordnung zu entwickeln, um die Sicherheit beim Abhebevorgang zu erhöhen, in die Realisationsphase ging, wurde die technische, finanzielle und wirtschaftliche Machbarkeit seiner Idee nachgewiesen. Außerdem wurde ein Patent (mit dem Ak-

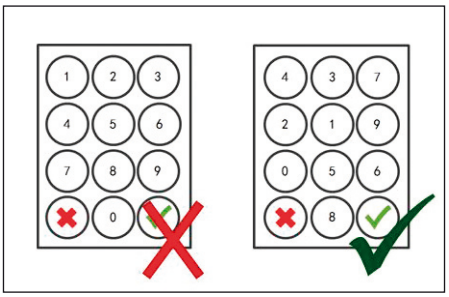
tenzeichen 10 2015 005 503.8) für das entwickelte System angemeldet.

Zufällige Ziffernanordnung auf dem PIN-Pad

Um die PIN-Eingabe sicherer zu gestalten, verbindet Secode verschiedene Komponenten. Der Hauptbestandteil ist die Software, welche eine wechselnde Anordnung der Ziffernabfolge bei der PIN-Eingabe ermöglicht. Dies bedeutet, dass die Zahlen nicht wie gewohnt angeordnet sind, sondern durch den Fisher-Yates-Zufallsalgorithmus die Reihenfolge ändern (siehe Abbildung). Dies geschieht pseudozufällig. Der Algorithmus betrachtet immer zwei Ziffern und entscheidet nach zufälligen Faktoren, ob die Position der beiden Ziffern gegeneinander vertauscht wird oder nicht. Da alle Ziffernpaare separat betrachtet wurden, ist sichergestellt, dass sich nach dem Mischvorgang keine der Ziffern an ihrer ursprünglichen Position befindet.

Für die Verschlüsselung wird das sogenannte „triple DES"-Verfahren verwendet. Dies ist ein symmetrisches Verschlüsselungsverfahren, welches denselben Schlüssel für die Verschlüsselung und die Entschlüsselung der PIN verwendet. Die Überprüfung der eingegebenen PIN erfolgt durch den Server der Bank, der sich außerhalb des Geldautomaten befindet. Die Informationsübermittlung zwischen dem Rechner des Bankautomaten und dem Bankenserver erfolgt in verschlüsselter Form, um die Datensicherheit gewährleisten zu können.

Beispiel für die Anwendung von Secode



Neben der Einhaltung aller Bankenstandards stellte die Implementierung und fehlerfreie Umsetzung der Verschlüsselung eine der größten Herausforderungen dar. Innerhalb eines halben Jahres wurde der Algorithmus für Secode implementiert und kontinuierlich verbessert. Durch die zufällige Anordnung der Ziffern auf dem Encrypting PIN-Pad ist es für Personen im Bereich des Bankautomaten nicht mehr möglich, anhand der Handbewegung des Nutzers zu erahnen, welche Zahlenkombination dieser eingibt, da außer dem Nutzer keiner die angezeigte Ziffernanordnung kennt.

Polarisationsfolie auf dem Touchpad

Eine Polarisationsfolie, die auf dem Touchpad angebracht wird, dient dazu, weitere Betrugsmöglichkeiten, wie beispielsweise das Abfilmen der eingegebenen PIN, zu verhindern. Diese Polarisationsfolie schränkt den Einsichtswinkel so ein, dass nur die Person, welche ihre PIN eingibt, erkennen kann, was auf dem Display zu sehen ist.

Zudem bietet sie die Möglichkeit, die Eingabe der PIN auf einem Touchpad auch für Personen mit eingeschränktem Sehvermögen benutzerfreundlich zu gestalten, indem ähnlich wie bei den derzeit gängigen Encrypting-PIN-Pads Erhöhungen an festgelegten Positionen integriert werden. Um ihnen die Ziffernanordnung zu übermitteln, kann das Audiosystem genutzt werden, welches sich bei den aktuellen Geldautomaten bereits im Einsatz befindet. In der Zukunft kann das Touchpad durch ein spezielles Touchpad ersetzt werden, welches die Brailleschrift anzeigt, um die Nutzung des Encrypting PIN-Pad von Secode für Blinde zu erleichtern.

Um die Annahme des Systems am Markt möglichst einfach zu gestalten, werden das Touchpad und der zugehörige Rechner, auf dem der Code programmiert ist in einem Gehäuse geliefert, sodass das bestehende Encrypting-PIN-Pad ohne großen Aufwand ausgetauscht werden kann. Der fertiggestellte Prototyp wird am Mittwoch, den 18. Mai 2016, bei der Abschlusspräsentation in der Dualen Hochschule Baden-Württemberg, Heidenheim, vorgestellt.

Um nachhaltig zur Verbesserung der Sicherheit beim Geldabhebevorgang beizutragen, ist das Team **(info@secode-system.de)** derzeit noch auf der Suche nach einem Kooperationspartner, welcher bereit ist, die Markteinführung zu unterstützen. Im Gegenzug wird dieser von der Technologie und dem angemeldeten Patent profitieren.