

| H. Schomäcker GmbH, Postfach 906 105, 51127 Köln

An alle Nutzer von Mifare®
Standardkarten-
systemen

| H. Schomäcker GmbH

Heidestraße 183
51147 Köln

Fon 0 22 03 / 9 25 76 _ 0
Fax 0 22 03 / 9 25 76 _ 50

www.schomaecker-gmbh.com

ralf.schomaecker@schomaecker-gmbh.com

Köln, den 16.04.008

Betreff: Sicherheit von Mifare® Kartensystemen

Basierend auf Untersuchungen verschiedener Personen und Institutionen erschien in der Zeitschrift ct 8/2008 ein Artikel, der auf gravierende Sicherheitsmängel der kontaktlosen Mifare® Classic Karten hinweist und diverse Angriffsszenarien erläutert.

Status der heutigen Karte:

Zur Verschlüsselung der Datenübertragung zwischen der Mifare® Karte und Kartenlesern wird der sogenannte CRYPTO1 Chiffrieralgorithmus eingesetzt.

Details zu diesem Algorithmus wurden bislang von der Firma NXP / Philips, **nicht** veröffentlicht.

Durch obiges Hardwareanalyseverfahren eines Mifare® Chips gelang es nun, den Schaltplan des Zufallszahlengenerators und der Verschlüsselungseinheit, in Erfahrung zu bringen. Dabei stellte sich heraus, dass der Zufallszahlengenerator deutliche Schwächen hat, voraussehbar ist und der Chiffrieralgorithmus heutigen Sicherheitsanforderungen nicht genügt.

Zudem gibt es Zusammenhänge zwischen der Karten-ID und dem Cryptoschlüssel. Damit besteht die Möglichkeit, wenn entsprechende technische Gerätschaften und Kenntnisse vorhanden sind, aus der Datenübertragung zwischen einem Leser und Karte die Sektorzugriffsschlüssel der Anwendung zu ermitteln.

Die heute meist verwendete Mifare® Karte entspricht dem Typ von Karten, dessen Schwächen aufgedeckt wurden.

Allgemeine Risiken:

Aufgrund dieser Informationen sind verschiedene Angriffszenarien möglich:

1. Es könnte versucht werden, die Datenübertragungen zwischen Geldaufwerter und der Karte aufzuzeichnen und missbräuchlich zu verwenden.
2. Es könnte versucht werden, Karteninformationen auf andere Datenträger zu kopieren
3. Nach Kenntnis der Sektorzugriffsschlüssel könnten Karten geklont werden

Spezielle Risiken für Schomäcker-Kunden:

Im Markt der Studentenwerke arbeiten wir mit den Systemen der **Firma tl1** zusammen. Durch die Aufzeichnung aller Umsätze fallen manipulierte Aufwertungen auf. Die Karten können im Manipulationsfall an allen vernetzten Kartenlesern gesperrt werden.

Fazit:

Für vernetzte Systeme ist das Manipulationsrisiko als nicht so hoch einzustufen, weil eine Manipulation feststellbar ist.

Bei Systemen ohne Hintergrundkonto ist das Risiko einer Manipulation höher, da hier die einzelne Manipulation prinzipbedingt nicht auffällt. Dafür sind die Umsätze in der Regel gering und lohnen nicht den Aufwand der Manipulation.

Fazit:

Für nicht vernetzte Systeme, ist das Manipulationsrisiko vorhanden, aber aus unserer Einschätzung heraus, als relativ gering einzustufen.

Sie als Kunde müssen entscheiden, ob der potentielle Schaden im Verhältnis zu dem Migrationsaufwand auf eine neue Karte einen Wechsel rechtfertigt.

Was bietet Schomäcker Card Solutions heute schon?

Als verfügbare Alternative bieten wir die kontaktlose Mifare DESfire® Karte an. Die MifareDESfire® hat folgende Merkmale:

Entspricht ISO /IEC 14443A

Kann bis zu 28 verschiedene Applikationen speichern.

Die Karte verwendet den hohen Standard des 3DES Chiffrieralgorithmus.

Die Karte ist kompatibel zu den Schomäcker Mifare-Kartenlesern .

Diese Karte verwendet TrippleDES zur Authentifizierung. Den Namen verdankt das Verfahren der Art seiner Anwendung. Der Algorithmus DES wird 3x hintereinander auf das zu Verschlüsselnde angewendet. Ab Sommer 08 wird auch eine AES-Verschlüsselung unterstützt.

Diese Chiffrieralgorithmen sind gründlich geprüft und gelten für die nächsten Jahre als sicher.

Schomäcker Card Solutions versteht sich als innovatives Unternehmen.

Daher sind alle aktuellen Produkte hardwaremäßig in der Lage kontaktlose Karten nach ISO 14443A zu unterstützen.

Ein kurzfristiger Umstieg für unsere Kunden ist jederzeit möglich.

Sofern ein Wartungsvertrag mit uns besteht, ist die Firmwareumrüstung aktueller Kartenleser kostenfrei. Für alle anderen Kunden arbeiten wir an einer Migration, die einen kostengünstigen Umstieg ermöglicht.

Schomäcker Card Solutions bietet weitere Karten-Optionen!

Wir werden gegen Ende des Jahres auch den Nachfolger der Mifare® Classic, die Mifare® Plus Karte unterstützen, wenn sie verfügbar ist.

Eine zusätzliche Option bieten die modernen Legic® Advant Karten, wie wir sie bereits in größeren Umgebungen einsetzen. Unsere Kartenleser sind auf diese Technologie jederzeit umrüstbar. Allerdings fallen hier (höhere) Migrationskosten bei Hard- und Software an.

Falls Sie Fragen zu diesem Thema haben, rufen Sie uns gerne an. Wir stehen Ihnen jederzeit gerne zur Beratung und Information zur Verfügung.

Weitere Informationen im Netz finden Sie unter:

www.mifare.net

www.nxp.com