Sicherheitsanalyse von Kreditkarten am Beispiel von EMV

Zidu Wang, Christopher Wolf und Jörg Schwenk
Lehrstuhl für Netz- und Datensicherheit
Horst Görtz Institut für IT-Sicherheit der Ruhr-Universität Bochum
www.nds.rub.de, www.hgi.rub.de

Der vorliegene Artikel gibt eine Zusammenfassung der Sicherheitsmechanismen moderner Kreditkarten wie z.B. Mastercard, Visa oder Eurocard. Zentral für Kreditkarten ist ein sicherer Authentifikationsprozess, da jede Kreditkarte ja letztendlich einen Geldwert darstellt. Daran schließt sich ein möglicher Angriff mittels gefälschter Terminals sowie Möglichkeiten zu dessen Behebung an.

1 Einleitung

Im täglichen Leben nimmt die Benutzung von Kreditkarten, wie beispielsweise die Mastercard oder Visacard, immer mehr zu und spielt in der heutigen modernen Gesellschaft eine bedeutende Rolle. Es ist sehr bequem, Zahlungen mit der Kreditkarte durchführen zu können. Daher gibt es immer mehr Menschen, die Kreditkarten nutzen. Doch mit der Verwendung der Kreditkarte entstehen auch Gefahren. Um eine Kreditkarte verwenden zu können, muss diese erst im Terminal gelesen werden, bevor eine endgültige Zahlung erfolgen kann. Dieses Terminal kann durch kriminelle Aktivitäten missbraucht werden und so dem Besitzer der Kreditkarte schaden [DM07]. Die Sicherheit der Benutzung einer Kreditkarte wird hier also bewertet. Besonders in der Kreditwirtschaft wird eine hohe Sicherheit verlangt. Um einen Missbrauch ausschließen zu können, wird daher eine Migration von Magnetstreifenkarte zu Chipkarte durchgeführt. Mit der Chiptechnik können kryptographische Verfahren im Kartenzahlungssystem verwendet werden, um die Sicherheit zwischen der Karte und dem Terminal zu garantieren. Europay International, MasterCard und VISA (EMV), die als größte Zahlungskarten-Organisationen gelten, entwickelten gemeinsam den nach ihnen benannten EMV-Standard, der den Standard für Chipkarten-Applikationen und Chipkarten-Terminals darstellt [uWG05]. Im Juni 2008 wurde die Version 4.2 der EMV-Spezifikation veröffentlicht.

Da die EMV-Spezifikation aus vier Büchern besteht ist sie sehr umfangreich. In diesem Artikel geben wir daher einen komprimierten Überblick über kryptographisch wichtige Funktionen von Kreditkarten gemäß EMV-Spezifikation. Danach zeigen wir wie die vorhandene Spezifikation verbessert werden kann um den Nutzer besser vor gefälschten Terminals zu schützen.

2 EMV Infrastruktur

2.1 Systembeschreibung

Die Kommunikationsparteien einer Kredittransaktion bestehen aus einer ICC, einem Terminal, einem Issuer und einem Acquirer. Im Folgenden werden die 4 Parteien näher vorgestellt:

- Die ICC ist die Abkürzung für *Integrated Circuit Card*. In der Spezifikation stellt die ICC genau die Kredit-Chipkarte dar.
- Das Terminal steht mit der ICC in direkter Kommunikation. Zudem ist das Terminal mit dem Hintergrundsystem verbunden.
- Der Issuer ist der Kartenaussteller und somit auch die Kundenbank, die die Kreditkarte dem Karteninhaber ausstellt.
- Der Acquirer ist die *Acquiring Bank*, die das Terminal zum Händler zuteilt.

Der Kunde eröffnet ein Konto bei der Kundenbank, die dem Kunde eine mit dem Konto verbundene ICC ausstellt. Gleichfalls beantragt der Händler ein Konto bei der Acquiring Bank, die dem Händler ein Terminal zuteilt. Der Kunde bezahlt mit der ICC im Laden des Händlers und die Transaktionsdaten wird durch das Terminal des Händlers zum Hintergrundsystem übertragen. Das Hintergrundsystem ist nähmlich die Acquiring Bank und die Kundenbank. Bei einer erfolgreichen Transaktion wird das Geld von dem Kundenkonto auf das Händlerkonto überwiesen. Die EMV-Spezifikation ist ein Standard besonders für das Kommunikationsverhalten zwischen der ICC und dem Terminal. Die kryptographischen Maßnahmen werden in den Authentifikationen in der EMV-Spezifikation ausgeführt, um die Echtkeit der Karte, die in der Karte gespeicherten Informationen und den Karteninhaber zu authentifizieren.

2.2 Authentifikationsprozess

Unterschiedliche offline Authentifikationen (CDA, DDA, SDA, PIN-Verschlüsselung) werden ausgeführt, um die Kartenechtkeit zu prüfen und den richtigen Karteninhaber zu identifizieren. Die Abbildung 1 zeigt die verschiedenen Authentifikationen.

- Kartenechtkeitsprüfung
  Es gibt drei Authentikationen, um die Kartenechtkeit zu prüfen.

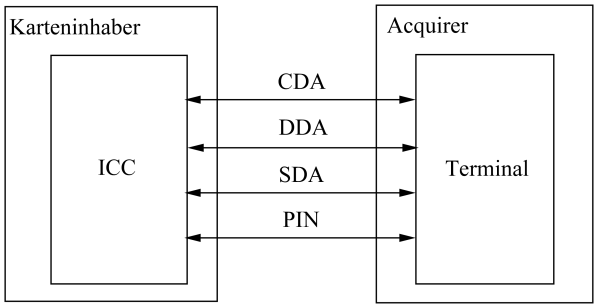

Abbildung 1: Transaktionsphase

1. SDA (*Static Data Authentication*) [EII08, S.49]
   Die SDA ist die einzige Art der *Offline Static Data Authentication*. Bei der SDA werden die Echtkeit der statischen Daten geprüft, die vom Issuer in der ICC gespeichert werden (z.B. Kartenummer und Gültigkeitszeitraum etc). Allerdings ist es bei dieser Authentikation unmöglich, die Echtkeit der Karte zu prüfen.
2. DDA (*Dynamic Data Authentication*) [EII08, S.78]
   Die DDA ist die einfache Version der zwei Authentikationsarten der *Offline Dynamic Data Authentication*. Bei der DDA besitzt die ICC ein eigenes Schlüsselpaar, dadurch können nicht nur die statischen Daten geprüft werden, sondern auch die dynamischen Daten, die von ICC und Terminal generiert werden, mit der von ICC erzeugten Signatur verifiziert werden.
3. CDA (*Combined DDA/Application Cryptogram Generation*) [EII08, S.82]
   Das *Application Cryptogram* wird für die Auswahl der Offline und Online Authentikationen verwendet. Die CDA schließt die DDA, die Generierung, den Austausch und die Verifizierung des *Application Cryptogram* ein. Die CDA verfügt nicht nur über die Funktion von der DDA, sondern auch die Authentikation mittels des *Application Cryptogram*.

- Benutzerauthentikation [EII08, S.93]
  Der Benutzer (Karteninhaber) wird durch die Eingabe seiner PIN (*Personal Identification Number*) auf dem PIN Pad des Terminals identifiziert. EMV erlaubt, dass das Terminal und die Karte offline die PIN des Benutzers prüfen. Bei der CDA und der DDA verschlüsselt das Terminal die

PIN des Benutzers mit dem öffentlichen Schlüssel der ICC und schickt die Verschlüsselung zur Karte. Die Karte entschlüsselt die verschlüsselte Datei und prüft, ob die erhaltene PIN mit der gespeicherten PIN identisch ist. Bei der SDA gibt es keine PIN-Verschlüsselung.

Alle Daten werden dabei mittels 3DES sowie RSA mit bis zu 2048 Bit abgesichert. Als Hash-Algorithmus wird SHA-1 eingesetzt. Einziger Kritikpunkt ist, dass als Verschlüsselungsexponent e die Werte 3 oder $65537{=}2^{16}+1$ fest voreingestellt sind. Ansonsten wurden aus unserer Sicht adäquate kryptographische Vorkehrungen getroffen.

3 Angriff mit gefälschtem Terminal

Das Sicherheitsmodell garantiert die sichere offline Transaktion zwischen dem Terminal und der Karte. Die offline Authentikationen werden ausgeführt, damit die folgenden Sicherheitszwecke für die Transaktion realisiert werden.

- SDA – Die Echtkeit der statischen Daten zu authentifizieren
- CDA und DDA – Die Echtkeit der dynamischen Daten zu authentifizieren
- CDA und DDA – Die Echtkeit der ICC zu authentifizieren
- PIN-Verschlüsselung – Die Echtkeit des Karteninhabers zu authentifizieren

Davon können die statischen und dynamischen Daten, die ICC und der Karteninhaber verifiziert werden. Aber es gibt keine Authentikation des Terminals. Wenn die ICC mit dem Terminal kommuniziert, kann das Terminal sich nicht authentifizieren. Daher ist es unklar, ob es sich überhaupt um ein richtiges Terminal handelt. Es besteht die Gefahr, dass die Daten der Karte vom Täter abgefangen werden können, sofern die Karte mit einem gefälschten Terminal in Verbindung gerät. Im Folgenden wird dargestellt, wie die statischen Daten während der Transaktion mit einem gefälschten Terminal ausgespäht werden können.

Das Terminal wird von der Acquirer Bank den Tankstellen, Supermärkten oder Restaurants etc. zugeteilt. Der Besitzer des Terminals wird bereits bei der Acquier Bank als Bevollmächtigter eingestuft, und es gilt normalerweise als verlässlich, dass der Kunde mit der Karte auf dem Terminal zahlt. Allerdings ist es auch möglich, dass irgendein Angestellter ein Täter ist, der das richtige Terminal mit einem gefälschten Terminal austauscht. Es ist auch nicht sehr schwierig, ein gefälschtes Terminal zu bekommen. Ein EMV-Terminal kann in

Ebay mit einem Preis von $50 gekauft werden. Im Gehäuse kann der Täter eine andere Schaltung anbringen, damit das Terminal nur SDA unterstützt und die statischen Daten der Karte während dem Bezahlungsvorgang gespeichert werden. Mit den gespeicherten statischen Daten kann eine entsprechende Magnetstreifenkarte hergestellt werden, mit der der Täter auf das Terminal zugreifen kann, wobei das EMV nicht unterstützt wird, und so eine Transaktion ausgeführt werden kann [DM07]. In manchen Ländern (z.B. Afrika) ist die EMV Migration noch ganz neu. Ein Terminal in solchen Ländern unterstützt lediglich die Magnetstreifenkarte. Der Täter kann dort mit der gefälschten Magnetstreifenkarte frei Geld abheben.

Das mögliche Szenario wird wie folgt dargestellt:

1. Der Täter ist ein Angestellter in einem Restaurant. Er kauft ein Terminal von Ebay und manipuliert es anschließend so, dass nur SDA unterstützt wird und die Daten der Karte während dem Bezahlungsvorgang gespeichert bleiben. Heimlich tauscht er das richtige Terminal mit seinem gefälschten Terminal um. Die anderen Angestellten bemerken das Vorhaben des Täters nicht, da das gefälschte Terminal gleich wie das originale Terminal aussieht. Wenn der Kunde bezahlen möchte, stellt der Täter das gefälschte Terminal dem jeweiligen Kunden zur Verfügung.

2. Der Kunde möchte sein Essen mit der EMV-Karte bezahlen. Er kann vom äußeren Erscheinungsbild nicht klar erkennen, dass das Terminal manipuliert wurde. Er steckt seine Karte also in das gefälschte Terminal und folgt den Anweisungen, die auf dem LCD des Terminals zu sehen sind. Der ahnungslose Kunde gibt also sein Passwort über das PIN-Pad ein, wobei dieses im gefälschten Terminal gespeichert bleibt.

3. Die Karte kommuniziert mit dem gefälschten Terminal. Da das Terminal nur SDA unterstürtzt, überspringt es die CDA und DDA und wählt daher die Karte und SDA aus.

4. Die ICC schickt in der Verifizierungsphase der SDA die Verifizierungsdaten zum Terminal (siehe Abbildung 2). Die statischen Daten werden als Klartext zum Terminal übertragen.

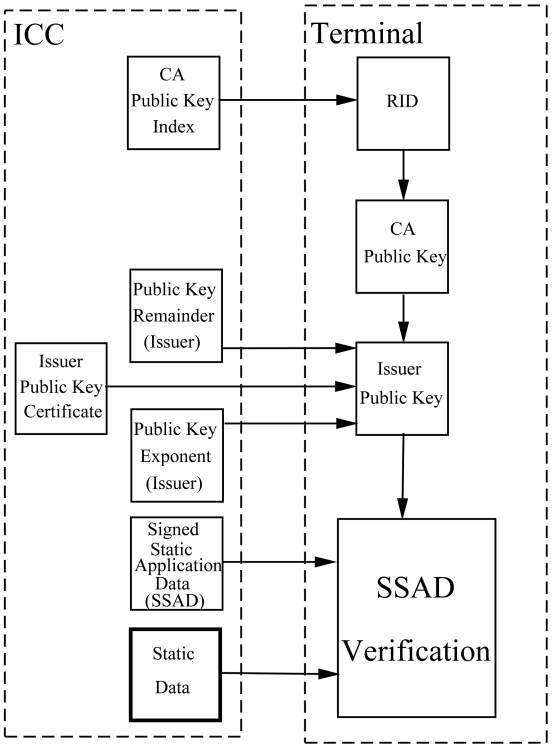

Abbildung 2: Verifizierungsphase der SDA

5. Nach der Transaktion wird auf dem LCD des Terminals angezeigt, dass die Bezahlung erfolgreich abgeschlossen wurde. Aber das Geld wurde nicht vom Konto des Kunden abgezogen.

6. Der Täter stellt eine gefälschte Magnetstreifenkarte mit den statischen Daten her. Er reist in ein Land, wo die EMV Migration noch nicht durchgeführt werden kann. Dort kauft er einen Diamanten mit Hilfe der gefälschten Karte.

4 Konzept zur Vermeidung des beschriebenen Angriffs

4.1 Beschreibung des Konzeptes

Um einen Angriff mit dem gefälschten Terminal zu verhindern, ist die Authentikation des Terminals notwendig. Die Terminal-Authentikation soll vor den anderen Authentikationen ausgeführt werden (siehe Abbildung 3), damit die ICC sicher ist, dass sie ihre Verifizierungsdaten zum richtigen Terminal sendet. Wenn die Terminal-Authentikation nicht erfolgreich ausgeführt wird, stoppt die ICC die Transaktion und die folgende Authentikationen werden auch nicht weiter ausgeführt. Damit können die Verifizierungsdaten nicht vom gefälschten Terminal abgefangen werden.

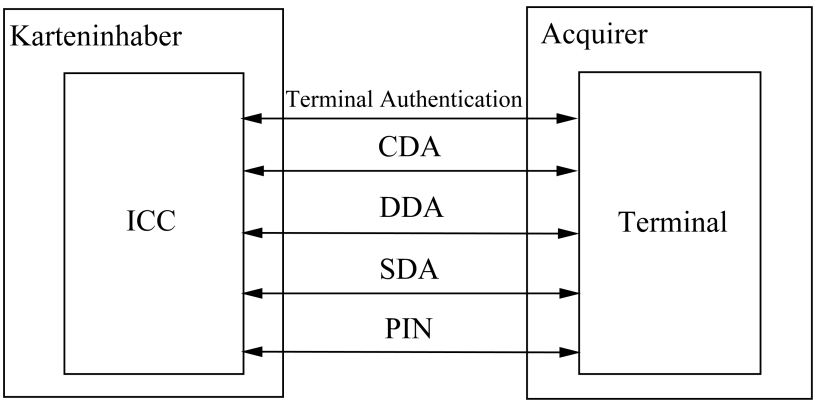

Abbildung 3: Authentikationen (mit der Terminal-Authentikation)

Im Folgenden wird eine mögliche Terminal-Authentikation entworfen. In dieser Terminal-Authentikation besitzt die CA, die Acquirer Bank und das Terminal drei asymmetrische Schlüsselpaare. Die CA erstellt das Zertifikat für die Acquirer Bank, wobei die Acquirer Bank das Zertifikat für das Terminal erstellt. Genau wie die anderen Authentikationen besteht die Terminal-Authentikation aus der Vorbereitungsphase, der Abfragephase und der Verifizierungsphase. In der Vorbereitungsphase werden die Zertifikate ausgestellt und die Verifizierungsdaten im Terminal gespeichert. In der Abfragephase berechnet die ICC mit den Zertifikaten den öffentlichen Schlüssel des Terminals. In der Verifizierungsphase verifiziert die ICC die vom Terminal signierten Daten. Die drei Phasen werden im Folgenden ausführlich vorgestellt:

4.1.1 Vorbereitungsphase der Terminal-Authentikation

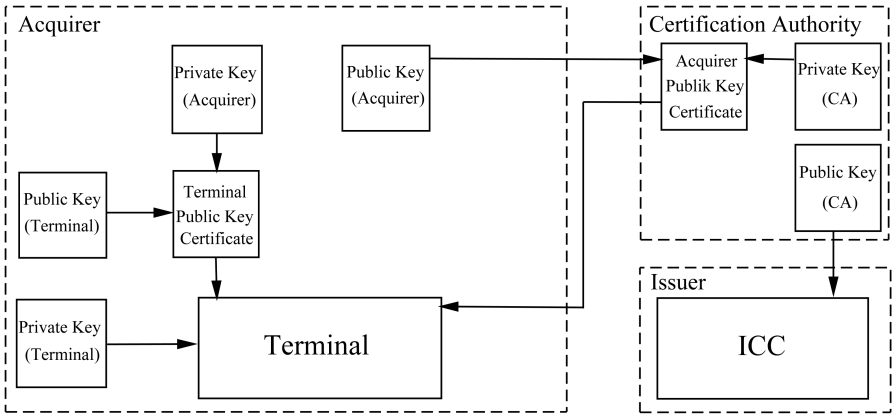

Abbildung 4: Vorbereitungsphase der Terminal-Authentikation

Die Vorbereitungsphase der Terminal-Authentikation wird in Abbildung 4 vorgestellt. Die Schritte werden folgendermaßen ausführlich beschrieben:

1. Der Acquirer schickt seinen öffentlichen Schlüssel zum Terminal. Das Terminal erstellt das Zertifikat für den Acquirer.

2. Der Acquirer erstellt das Zertifikat für den öffentlichen Schlüssel des Terminals. Das Zertifikat des Acquirers, das Zertifikat des Terminals und der private Schlüssel des Terminals werden im Terminal gespeichert.

3. Der öffentliche Schlüssel der CA wird durch den Issuer in der ICC gespeichert.

Nach der Vorbereitungsphase besitzt das Terminal das Zertifikat des Acquirers, das Zertifikat des Terminals und seinen privaten Schlüssel. Die ICC besitzt nur den öffentlichen Schlüssel der CA. Danach wird das Terminal der Acquirer Bank dem bevollmächtigten Ort (z.B. Tankstellen, Supermarkt oder Restaurant etc) zugeteilt, wobei die ICC der Issuer Bank zur Person (Karteninhaber) zugeteilt wird.

Wenn der Karteninhaber mit der ICC auf dem Terminal bezahlt, wird die Terminal-Authentikation zuerst ausgeführt. Die Abfragephase wird zunächst ausgeführ, damit die ICC den öffentlichen Schlüssel des Terminals erfährt.

4.1.2 Abfragephase der Terminal-Authentikation

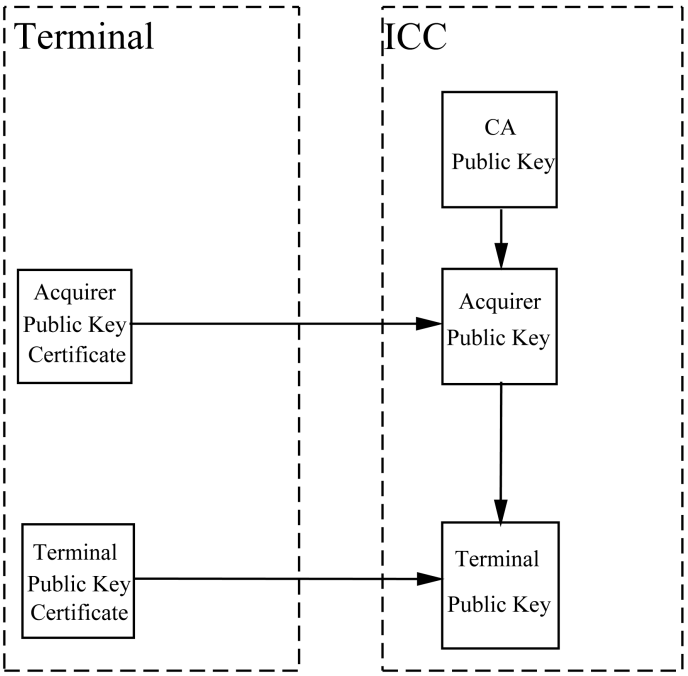

Abbildung 5: Abfragephase der Authentikation des Terminals

Die Abfragephase der Terminal-Authentikation wird wie in Abbildung 5 vorgestellt. Die Schritte werden im Folgenden beschrieben:

1. Die ICC verifiziert das Zertifikat des Acquirers mit dem öffentlichen Schlüssel der CA. Dadurch erhält sie den öffentlichen Schlüssel des Acquirers.
2. Die ICC verifiziert das Zertifikat des Terminals mit dem öffentlichen Schlüssel des Acquirers. Dadurch bekommt sie den öffentlichen Schlüssel des Terminals.

Nach der Abfragephase erhält die ICC den öffentlichen Schlüssel des Terminals, mit dem die ICC die vom Terminal signierten Daten in der Verifizierungsphase verifiziert.

4.1.3 Verifizierungsphase der Terminal-Authentikation

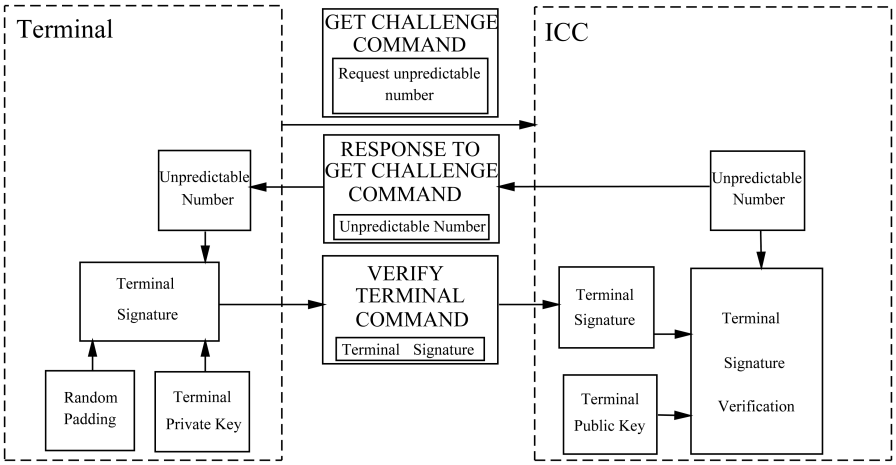

Abbildung 6: Verifizierungsphase der Authentikation des Terminals

Die Verifizierungsphase der Terminal-Authentikation wird wie in Abbildung 6 beschrieben. Die Schritte werden wie folgt dargestellt:

1. Das Terminal schickt der ICC den GET CHALLENGE Befehl, um eine unvorhersagbare Nummer anzufordern.

2. Die ICC stellt eine nicht vorhersagbare Nummer zusammen. Mit dem RESPONSE Befehl schickt sie die unvorhersagbare Nummer zum Terminal zurück.

3. Das Terminal verkettet die unvorhersagbare Nummer mit einem zufälligen Padding zusammen. Die Verkettung wird mit dem privaten Schlüssel des Terminals signiert. Das Terminal schickt die Signatur im VERIFY TERMINAL Befehl zur ICC zurück.

4. Die ICC verifiziert die Signatur mit dem öffentlichen Schlüssel des Terminals. Wenn die unvorhersagbare Nummer in der Signatur mit der Originalen identisch ist, ist die Terminal-Authentikation erfolgreich.

4.2 Gegenmaßnahme zur Manipulation des Terminals

Es besteht zudem die Möglichkeit, das Terminal zu manipulieren. Der Täter kann einen Mithörer im Terminal installieren oder er kann die Schaltung im Terminal umbauen, um die verschiedenen Angriffe durchführen zu können. Es ist sehr daher sehr wichtig, eine Manipulation des Terminals zu verhindern.

Das Terminal wird von der Acquirer Bank bevollmächtigt und dann den Supermärkten, Tankstellen oder Restaurants etc. erteilt. Bei der Terminal-Authentikation wird ein privater Schlüssel im Terminal gespeichert. Mit diesem Schlüssel signiert das Terminal die Verifizierungsdaten, damit es von der ICC verifiziert wird. Ohne den privaten Schlüssel kann das Terminal nicht verifiziert werden und die ICC stoppt in diesem Fall die Transaktionen.

Es wird hier vorgeschlagen, die Schutzmaßnahme des privaten Schlüssels mit den Gegenmaßnahmen der Manipulation des Terminals zu verbinden. Wenn der Täter das Terminal öffnet, um es zu manipulieren, wird der private Schlüssel im Terminal selbst gelöscht. Ohne den privaten Schlüssel kann die Transaktion nicht ausgeführt werden. Mit dieser Maßnahme kann die Manipulation des Terminals verhindert werden.

5 Fazit

Durch die Analyse der Sicherheitsaspekten der EMV-Spezifikation wird es festgestellt, dass es keine Authentikation des Terminals gibt. Zu diesem Punkt wurde ein möglicher Angriff vorgestellt und als Gegenmaßnahme eine Terminal-Authentikation entworfen. Mit dieser Terminal-Authentikation kann das Terminal sich gegen die Karte authentifizieren und kann die Manipulation des Terminals verhindert werden.

Es ist derzeit noch unklar, wie es im Praxis umgesetzt wird. Es ist daher nur einen theoretischer Vorschlag, um das Ausspionieren von Verifizierungsdaten der ICC mit einem gefälschten Terminal sowie die Manipulation des Terminals zu verhindern. Allerdings sind die vorgeschlagenen Mechanismen alle praxistauglich, was die Chance ihrer Implementierung deutlich verbessert.

Literatur

[DM07] Saar Drimer and Steven J. Murdoch. Keep your enemies close: Distance bounding against smartcard relay attacks. *USENIX Security*, page 3, 2007.

[EII08] MasterCard International Europay International and Visa Interna-

tional. Book 2, Security and Key Management. In *Integrated Circuit Card Specification for Payment Systems, Version 4.2*. EMV, 2008.

[uWG05] Sandro Amendola und Waldemar Grudzien. Sicherheitsdienstleistungen bei karten-zahlungssystemen. In *9. Deutscher IT-Sicherheitskongress des BSI*, page 1, 2005.