# 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

**Abstract:** 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.

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 . 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. 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.