

Überweisungstrick: NFC-Bankomatkarten lassen sich hacken

GEORG PICHLER
9. Jänner 2014, 11:46

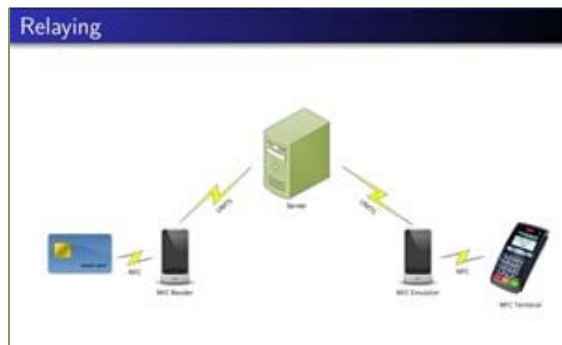


foto: dieter vymazal

Das grundsätzliche Set-up eines Angriffs via NFC-Relaying.

Praktisches Risiko gering – auslesbare Informationen aber datenschutztechnisch heikel

Wie zuletzt bekanntgeworden ist, ist es derzeit möglich, mit einer einfachen Handy-App via NFC von neueren Bankomatkarten Daten abzurufen. So kann man etwa eine Übersicht über die letzten Transaktionen oder das Quick-Guthaben erhalten. Es ist aber auch möglich, mit einem gezielten Angriff Überweisungen zu initiieren.

Szenario

Der WebStandard hat beim Experten Dieter Vymazal von der Fachhochschule Hagenberg nachgefragt, der die Schwäche aufgedeckt hat. Er erklärt den Angriff folgendermaßen:

Benötigt werden zwei Personen mit NFC-fähigen Smartphones.

Eine muss sich in räumlicher Nähe zum Opfer befinden, um ihr Telefon Kontakt mit der Karte herstellen zu lassen – etwa durch das Heranführen an die Geldtasche an der Kasse eines Supermarkts. Das Handy gibt sich dabei als Bankomat aus und stellt eine Zahlungsanfrage an die Karte des Opfers.

NFC-Relaying

Die Karte bestätigt diese, sofern sie maximal 25 Euro beträgt, automatisch und schickt sie an das Telefon zurück. Dieses leitet die signierte Verifikation per Internet an das Telefon der zweiten Person weiter, die ihr Gerät wiederum bei einer echten NFC-fähigen Bankomat (von welcher die ursprüngliche Zahlungsanfrage ausgeht) platziert hat und sich gegenüber dieser als Karte ausgibt.

Die Kasse empfängt nun die Bestätigung und erkennt sie als authentisch. Die Zahlungsanfrage wird an die jeweilige Bank weitergegeben und die Abbuchung durchgeführt. Man spricht bei dieser Form von Angriff auch von "NFC-Relaying".

Kaum lohnenswert

Da die Attacke verhältnismäßig aufwändig durchzuführen ist und im erfolgreichsten Falle hintereinander fünfmal 25 Euro (insgesamt also 125 Euro) abgebucht werden können, ist die praktische Gefahr laut Vymazal als gering einzustufen. Problematischer wird es, wenn es den Angreifern im Vorfeld gelungen ist, den PIN der Karte auszuspähen. Dann ließen sich fünf Überweisungen mit dem für die Karte von der Bank festgelegten Betragslimit ausführen.

Beweisfälschung möglich

Eine erfolgreiche gefälschte Überweisung könnte aber auch einen anderen Zweck erfüllen als bloßen Geldgewinn. Sie ermöglicht es theoretisch, über die bestätigte Zahlung einen falschen Beweis dafür zu schaffen, dass das Opfer des Angriffs zu einem bestimmten Zeitpunkt an einem bestimmten Ort einen Einkauf getätigt hat, ohne tatsächlich dort gewesen zu sein. So ließe sich, zum Beispiel mit der Zahlungsbestätigung eines Sex-Shops, belastendes Material generieren.

Eine Möglichkeit, solchen Angriffen vorzubeugen, sieht Vymazal darin, aufseiten der Bank die Dauer einer Transaktion zu überprüfen, da die Durchführung hier üblicherweise merkbar länger dauert als bei einer normalen Zahlung. Dies böte aber wiederum das Potenzial für Fehlalarme und den Abbruch eigentlich legitimer Überweisungen. Auch spezielle Schutzhüllen können helfen.

Datenschutzbedenken

Generell ortet Vymazal aber auch bei der bisher schon gegebenen Möglichkeit, einfach Daten auszulesen, datenschutzrechtliche Bedenken. Zudem ist es bei NFC-aktivierten Kreditkarten möglich, deren Nummer (nicht aber die CVC-Nummer) auszulesen und mit dieser herauszufinden, um welchen Kartentyp es sich handelt, und die

zuständige Bank zu ermitteln.

Informationen, die Potenzial für Missbrauch – etwa durch Social Engineering – bieten. Auf den neuen Karten, die in wenigen Monaten ausgeliefert werden sollen, werden die letzten Buchungen nicht mehr gespeichert. Die Payment Services Austria hat mittlerweile gegenüber dem Ö1-"Morgenjournal" Stellung bezogen und erkennt keine "Gefahr in der Praxis". (Georg Pichler, derStandard.at, 09.01.2014)

Links

FH OÖ / Campus Hagenberg

Payment Services Austria

Near Field Communication (Wikipedia)

Nachlese

Der Schnüffel-Chip im Geldbörsel

Smartphone-App liest Bankomatkarten aus

ADVERTORIAL



Neue Gesichter der Stadt

Die WK Wien holt neue Unternehmen aus Wien vor den Vorhang! Oder sind Sie selbst auf Standortsuche? Dann gibt es Unterstützung.

BEZAHLTE ANZEIGE

© derStandard.at GmbH 2014

Alle Rechte vorbehalten. Nutzung ausschließlich für den privaten Eigenbedarf.
Eine Weiterverwendung und Reproduktion über den persönlichen Gebrauch hinaus ist nicht gestattet.

.