Sascha Brendel – Bachelor-ITS – Matrikelnummer:

sascha.brendel@ruhr-uni-bochum.de

Exposé zum Paper
Mo(bile) Money, Mo(bile) Problems:
Analysis of Branchless Banking Applications in the Developing World

Zusammenfassung

Während in Europa nahezu jeder Bürger über ein Konto bei einer Bank verfügt, gibt es für viele Menschen in den sog. Entwicklungsländern keinen Zugang zu einem Bankkonto, wodurch diese auch nicht am bargeldlosen Zahlungsverkehr teilhaben können.
Mobile money oder auch **branchless banking** ist eine Möglichkeit, traditionelle Geldgeschäfte in Form von Überweisungen und Kontoführung zu abzuwickeln ohne eine Bank als Institution zu benötigen. Meist wird dies mit der Nutzung von Diensten bzw. Smartphone-Anwendungen (Apps) bestimmter Telekommunikationsanbieter realisiert.
Durch diese Anwendungen ist es den Menschen in diesen Gegegenden möglich, beispielsweise ihr Gehalt zu erhalten, ohne ein Bankkonto zu besitzen.

Während in unseren Breiten Banken in der Regel als sehr sicherheitsbewusst gelten und ihre Produkte gegen unberechtigten Zugriff durch Dritte oder Diebstahl absichern, werden *branchless banking* Anwendungen meist durch Telekommunikationsunternehmen entwickelt und herausgegeben.

In ihrem Paper, welches auf dem 24th USENIX Security Symposium im August 2015 in Washington D.C. veröffentlicht wurde, halten die Autoren Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor und Kevin R.B. Butler von der Universität von Florida ihre Ergebnisse zur Untersuchung der technischen Sicherheit dieser Applikationen fest.
Die Forscher untersuchten insgesamt 46 Android Apps von 246 *mobile money* – Anbietern und stellten dabei gravierende Mängel bezüglich der Sicherheit dieser Anwendungen fest, die von Millionen Menschen täglich genutzt werden.

Zur Analyse nutzten die Forscher sowohl automatisierte Verfahren als auch manuelle Code-Analysen der (de)kompilierten Anwendungen. Dabei untersuchten sie besonders die Phasen der Registierung, Anmeldung und Durchführung von Transaktionen. Aus den verfügbaren Android Apps wählten die Forscher dann 7 Anwendungen aus, die zusammen eine Nutzerbasis von über 1.3 Millionen Menschen aufweisen, um diese im Detail zu analysieren.

Das Paper gibt nach der Einführung in das Thema zunächst einen Überblick zu *mobile money* und *branchless banking*. Es schließt sich ein Kapitel an, welches die Auswahl der untersuchten Apps sowie deren Sicherheitsanalyse beschreibt. In den zwei darauffolgenden Abschnitten werden die Ergebnisse der Analysen dargestellt und diskutiert. Abschnitt 6 klärt die rechtlichen Grundlagen der Haftung bei Missbrauch dieser Anwendungen. Abschließend stellen die Autoren Verknüpfungen zu anderen Sicherheitsanlysen her und ziehen ein Fazit bezüglich der Sicherheit der untersuchten Android Apps.

Motivation

Im 21. Jahrhundert ist es für das Alltagsleben von größter Bedeutung, nahezu jederzeit Zugriff auf das eigene Bankkonto zu haben, sei es um Geld zu empfangen oder selbst zu überweisen. In Europa und auch in den vereinigten Staaten von Amerika können wir relativ problemlos mit unseren Bankkarten, sei es die Giro- oder eine Kreditkarte, über unser Bankkonto verfügen. Es gibt jedoch einen ehrheblichen Teil der Menschheit, der auf keine Infrastruktur zur Nutzung eines Bankkontos zugreifen kann.

Mobiles und / oder dezentrales Geld könnte für diese Menschen eine erhebliche Vereinfachung des täglichen Lebens sowie der Teilnahme an Finanzgeschäften ermöglichen.

Auch wegen meines Studiums der IT-Sicherheit interessiert mich die Umsetzung solcher Lösungen sehr, besonders im Hinblick auf die Sicherheit solch kritischer Systeme. Die etablierten Banken haben über Jahre hinweg ein als sehr sicher geltendes System geschaffen, bei dem moderne Kryptographie und sichere Protokolle als Standard eingesetzt werden. In unseren Medien fallen Telekommunikationsunternehmen hinsichtlich der IT-Sicherheit desöfteren negativ auf.
Es stellt sich also die Frage, inwieweit man einem Telekommunikations-unternehmen sein Geld anvertrauen kann und welche Maßnahmen die Anbieter von *mobile money* einsetzen, um ihre Kunden vor unberechtigten Zugriffen und Transaktionen zu schützen.

Daher möchte ich gerne das oben genannte Paper im Rahmen meines Bachelor-Seminars bearbeiten und vorstellen.

Vorläufige Gliederung

In meiner Seminararbeit werde ich zunächst einen Überblick über die Verfügbarkeit von Finanzdienstleistungen sowie der Verbreitung von EC- und Kreditkarten geben und dabei die Problematik in den sogenannten Entwicklungsländern aufzeigen. Anschließend werde ich das Funktionsweise von *mobile money* erläutern und eventuell den Unterschied zu Kryptowährungen verdeutlichen.

Im Hauptteil meiner Arbeit und der Präsentation werden die Anlysen der Forscher vorgestellt und deren Vorgehen erklärt. Der Vortrag von Bradley Reaves auf dem USENIX Symposium 2015 dient dabei als Orientierung.

Bei der Zusammenfassung der vorliegenden wissenschaftlichen Arbeit möchte ich einige der gravierndsten Sicherheitslücken im Detail vorstellen.

Sollte es mir möglich sein, so würde ich gerne eine aktuelle Version eine, der für die Detailanalysen ausgewählten Apps, untersuchen. Dabei möchte ich herausfinden, ob und inwieweit die aufgezeigten Sicherheitslücken noch vorhanden sind.

Abschließend finde ich es wichtig, wie es bereits die Autoren getan haben, auf die Haftungsfragen bei Missbrauch der Anwendungen einzugehen, da die Nutzungsbestimmungen, meiner Meinung nach, bei der ungenügenden Sicherheitsimplementierung sich äußerst fatal auf die Nutzer auswirken können.