Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

InIT Institut für angewandte
Informationstechnologie

Zipper Instant Messenger - Generieren von digitalen Signaturen mittels Smartphone und Sicherheitschip

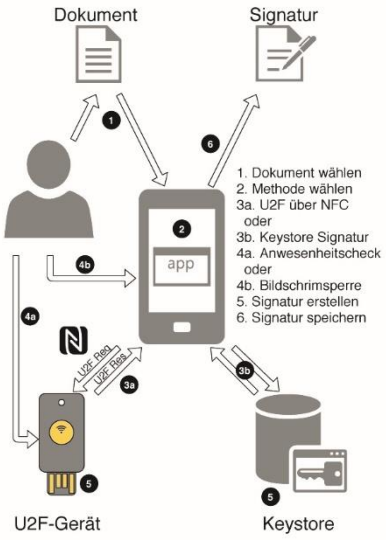
Diplomierende
Thomas Brown
Kay Friedli

Dozierende
Bernhard Tellenbach
Kevin Lapagna

Digitale Signaturen werden immer öfter in moderne Geschäftsprozesse integriert. Gleiches gilt für Smartphones und Instant-Messenger, welche zunehmend Teil der Arbeitsumgebung werden. Die Firma zipper.im möchte sich in diesem aufkommenden Markt mit ihrem Produkt zipper Instant Messaging etablieren. Um das Produkt auch auf Smartphones anbieten zu können, gilt es, die Möglichkeiten zur Erstellung von Signaturen auf solchen Geräten zu evaluieren. Dabei sollen sowohl die Möglichkeiten der internen Kryptographie-Hardware des Smartphones, als auch das U2F-Verfahren über NFC untersucht werden.

In dieser Arbeit wurde eine Applikation für Android entwickelt, mit der entsprechende Signaturen erstellt werden können. Die Applikation ist in Java geschrieben, nutzt den Android Keystore als Schnittstelle zur internen Kryptographie-Hardware und implementiert ein angepasstes U2F-Verfahren. Der Prototyp dient als Machbarkeitsstudie und Vorlage für eine eigene Umsetzung durch zipper.im. Um eventuelle Schwachstellen zu identifizieren, wurde der Prototyp einer Sicherheitsanalyse unterzogen. Die Sicherheitsanalyse basiert auf Attack-Trees und umschreibt relevante Angriffsszenarien.

Der Prototyp zeigt, dass U2F über NFC auf Android umsetzbar ist. Auch der Keystore bietet auf moderner Hardware ein hohes Mass an Sicherheit und ist eine valide Alternative zu externer Krypto-Hardware. Probleme mit U2F zeigen sich bei der korrekten Implementation der FacetID, die nicht erreicht werden konnte. Die Analyse der Implementationen weist zudem auf Schwachstellen im verwendeten U2F-Verfahren hin. Da U2F nicht für Signaturen konzipiert wurde, zeigen sich Risiken bezüglich Nonrepudiation und ein potenzielles Angriffsszenario mit eingespielten Signatur-Anfragen. Der Keystore wiederum ist anfällig für bestimmte DoS-Angriffe. Insgesamt ist eine Umsetzung von Signaturen auf einem Smartphone realisierbar, es sind jedoch die damit verbundenen Risiken zu berücksichtigen.



Ablaufdiagramm für das Erstellen einer Signatur mit der Prototyp-Applikation. Die Signatur kann mittels einem externen U2F-Gerät (angesteuert über NFC) oder mit der internen Krypto-Hardware des Smartphones erstellt werden.