NFC-Schließsysteme auf Basis von FIDO U2F und EMV

Betreuung: Michael Roland

Josef Ressel Center for User-friendly Secure Mobile Environments (u'smile)

Motivation

Viele elektronische Schließsysteme setzen auf den Einsatz von Near Field Communication (NFC), RFID bzw. kontaktloser Chipkarten um eine möglichst einfache Handhabung und eine geringe machanische Beanspruchung zu erzielen. Als Schlüsselmedien kommen dabei üblicherweise proprietäre RFID-Token und Smartcards (z.B. MIFARE Classic oder MIFARE DESFire) zur Anwendung. Insbesondere im privaten Bereich ist das Sicherheitsniveau dieser proprietären Technologien oft sehr gering (z.B. RFID-Token mit einfacher Seriennummer oder die seit Jahren obsolete MIFARE Classic Technologie). Dabei tragen wir bereits jetzt eine Vielzahl moderner und sicherer NFC-Smartcards mit uns herum. Beispiele dafür sind NFC-Bankomatkarten (Maestro PayPass) und NFC-Kreditkarten (MasterCard PayPass, Visa payWave). Darüber hinaus treibt die FIDO Alliance die Verbreitung dedizierter NFC-Token als zusätzlicher Faktor bei der Authentisierung gegenüber Webanwendungen voran. Alle diese Token bzw. Smartcards sind nichts anderes als kryptographische Schlüssel auf Basis asymmetrischer Kryptosysteme. Es ist daher naheliegend, dass sich diese auch als Schlüsselmedien für Schließsysteme eigenen würden.

Aufgabenstellung

Im theoretischen Teil der Arbeit soll genau diese Eignung als Schlüsselmedien für Schließsysteme evaluiert werden. Dabei sind sowohl Schließsysteme zu betrachten, bei denen eine große Anzahl an Schlössern zentral verwaltet und die Berechtigungen zentral geprüft werden, als auch dezentrale Systeme, bei denen Berechtigungen von jedem Schloss individuell verwaltet werden. Besonderes Augenmerk soll dabei auf die Registrierung neuer „Schlüssel" sowie den Widerruf verlorener oder gestohlener „Schlüssel" gelegt werden.

Im praktischen Teil der Arbeit soll der Prototyp für ein Schloss implementiert werden, welches mittels U2F-Token und EMV-Smartcards (Maestro/MasterCard und Visa) gesperrt werden kann. Das Schloss soll die Registrierung neuer und das Löschen bestehender Schlüssel ermöglichen. Als Basis für das Schloss kann beispielsweise ein Raspberry Pi mit einem NFC-Lesegerät herangezogen werden.

Ziele

- >> Auseinandersetzung mit dem FIDO U2F-Protokoll sowie den EMV-Protokollen für Bezahlsysteme
- >> Analyse der Möglichkeiten und Risiken durch den Einsatz von U2F-Token und EMV-Smartcards in Schließsystemen (insbesondere in Hinblick auf die Registrierung neuer Schlüssel sowie den Widerruf registrierter Schlüssel)
- >> Implementierung des Prototyps eines Schlosses welches mittels U2F-Token und EMV-Smartcards gesperrt werden kann

Literatur

[1] Bergem, M., Maury, F.: A first glance at the U2F protocol. In: SSTIC 2016 (Jun 2016)

[2] EMVCo: https://www.emvco.com/

[3] EMVCo: EMV Contactless Specifications for Payment Systems – Book A: Architecture and General Requirements, Version 2.5 (Mar 2015)

[4] FIDO Alliance: https://fidoalliance.org/

[5] FIDO Alliance: FIDO NFC Protocol Specification v1.0, Implementation Draft (May 2015)

[6] FIDO Alliance: Universal 2nd Factor (U2F) Overview, Proposed Standard (May 2015)

Themenfelder

- >> Near Field Communication und Chipkarten
- >> FIDO Universal 2nd Factor
- >> Embedded Systeme
- >> Hardware, Software
- >> Kryptographie

Kontakt

Dr. Michael Roland
+43 (0)50804-27149
michael.roland@fh-hagenberg.at