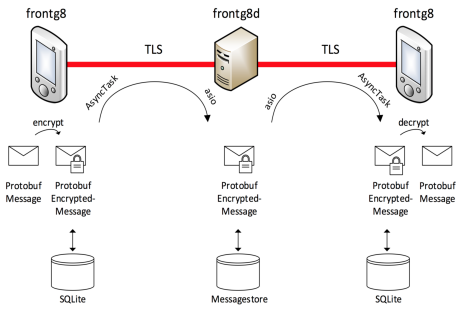

Ueli Bosshard

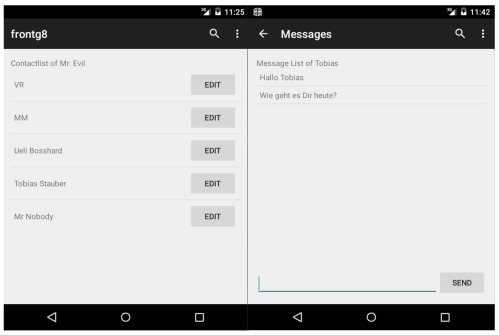

Tobias Stauber

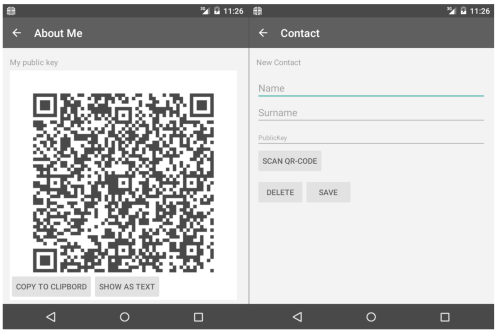
Diplomanden	Ueli Bosshard, Tobias Stauber
Examinator	Prof. Dr. Andreas Steffen
Experte	Tobias Brunner, HSR ITA, Rapperswil, SG
Themengebiet	Sicherheit

frontg8

Chatsystem mit hohen Anforderungen an die Privatsphäre







Ausgangslage: Frontg8 ist ein aus einer Server- und einer Clientkomponente bestehendes Chatsystem. Dabei fokussiert sich frontg8 primär auf die anonymisierte Kommunikation zwischen den Anwendern. Um die Privatsphäre zu wahren, ist es unerlässlich, jede beteiligte Komponente (Clients und Server) jederzeit vollständig unter eigener Kontrolle zu haben. Jede im System teilnehmende Person verfügt über ein aus öffentlichem Schlüssel (Publickey) und privatem Schlüssel (Privatekey) bestehendes Schlüsselpaar. Dieses wird eingesetzt um die Kommunikationspartner zu identifizieren und auch dazu die gemeinsamen Geheimnisse zu erarbeiten, welche fürs Verschlüsseln und Signieren der Nachrichten verwendet werden.

Vorgehen/Technologien: Um die Anonymität zu wahren, ist es unerlässlich, dass der Server nur so wenig wie möglich über die teilnehmenden Parteien in Erfahrung bringen kann. Durch diese Anforderung entsteht die Limitation, dass der initiale Schlüsselaustausch nicht über den Server durchgeführt werden kann. Die Teilnehmer müssen also ihre Publickeys auf einem anderen Weg austauschen. Wenn zwei Partner ihre Publickeys ausgetauscht haben, erarbeitet frontg8 daraus mittels Diffie-Hellman auf elliptischen Kurven (ECDH) je einen gemeinsamen symmetrischen Schlüssel für die Kryptographie und für das Unterschreiben der Nachrichten.

Ergebnis: In Software Engineering 2 Projekt wurden von uns bereits ein Server und ein Python-Client umgesetzt. In dieser Studienarbeit war es nun das Ziel, einen vollumfänglich kompatiblen, auf dem Mobile-Betriebssystem Android lauffähigen, Client zu entwickeln. Im Zentrum der Arbeit stand, die Privatsphäre zu wahren, sichere Verschlüsselung einzusetzen und eine einfache Bedienung zu ermöglichen. Dazu setzen wir zeitgemässe Verschlüsselungsalgorithmen und aktuelle API-Funktionen ein. Da Android einige interessante Möglichkeiten anbietet geheime Schlüssel zu speichern und zu verwalten, setzten wir uns im Verlauf der Arbeit intensiv damit auseinander um zu ergründen, ob es die angebotene Funktionalität erlaubt, den von uns gewünschten Funktionsumfang direkt mit Android-Bordmitteln umzusetzen. Das resultierte Produkt ist eine komplette Android Applikation, welche alle unsere Anforderungen erfüllt und es erlaubt, sichere und voll anonymisierte Kommunikation mit anderen Teilnehmern zu führen.