Sicherheitsanforderung an Messenger Apps

Thomas Bötner[1] · Hartmut Pohl[1] · Markus Ullmann[2]

[1] softScheck GmbH
{thomas.boetner | hartmut.pohl}@softscheck.de

[2] Hochschule Bonn-Rhein-Sieg
markus.ullmann@h-brs.de

1 Motivation

Neben der Telefonie hat sich der Austausch kurzer Textnachrichten als mobiles Kommunikationsmittel etabliert. In Deutschland wurden 2014 über 27 Mrd. Textnachrichten über den Short Message Service (SMS) versendet [DCVA14]. Die Verbreitung der Smartphones und der damit verbundene Einzug des mobilen Internets ebneten den Weg für weitere Anwendungen zur Kommunikation: Zum einen werden traditionelle Instant Messaging (IM) Anwendungen, wie beispielsweise ICQ, MSN Messenger und Skype vom Personal Computer auf Smartphones portiert und zum anderen werden neue Anwendungen, wie WeChat, WhatsApp, iMessage, Joyn und Line angeboten. Das Over The Top (OTT) Modell beschreibt den Betrieb von Telekommunikationsdiensten über das Internet (hier der Nachrichtenaustausch), ohne dass der Anbieter über ein eigenes Telekommunikationsnetz verfügt oder ein solches mietet [BeCH11]. Ein Vorteil der OTT Anwendungen gegenüber der SMS liegt in den niedrigen Kosten für den Nutzer und der Möglichkeit, einfach Multimediainhalte auszutauschen. Dies führte zu einem schnellen Wachstum der Anzahl versandter Nachrichten. 2014 überholten die OTT Anwendungen die SMS in der absoluten Anzahl an Nachrichten pro Tag [PoRe14]. Nicht nur das Angebot der Anwendungen, sondern auch die Inhalte der Nachrichten haben sich verändert. So werden SMS als Authentifizierungswerkzeug im Internet verwendet: z.B. beim Online Banking oder bei Emailanbietern. Neben reinen Textnachrichten ist nun auch der Austausch von Bild, Video und Audio Daten möglich. Die Begrenzung von 160 Zeichen pro SMS Nachricht ist bei den OTT Anwendungen nicht mehr vorhanden. Auch werden die Inhalte intimer, was sich am Phänomen „Sexting“ erkennen lässt, das immer verbreiteter unter Jugendlichen und jungen Erwachsenen wird. Als „Sexting“ wird der private Austausch erotischer Fotos über Smartphones bezeichnet [WyCh11]. OTT Nachrichten werden nicht nur zahlenmäßig mehr, sondern auch vom Inhalt vertraulicher [HöGe03]. Diese Entwicklungen werfen neue datenschutztechnische Fragestellungen zum Schutz mobiler Kommunikation auf. Denn auf der einen Seite bedürfen vertraulichere Nachrichten eines stärkeren Schutzes, auf der anderen Seite ist die technische und rechtliche Situation des Datenschutzes aufgrund der großen Anzahl der global agierenden Anbieter unübersichtlich [DAV13]. Neben den Gesprächsinhalten fallen auch Verkehrsdaten (Datum, Uhrzeit, Statusinformationen, Benutzerkennungen und Aufenthaltsorte/IP-Adressen) an. Das Angebot an mobilen Messengern ist sehr groß. Einige Anbieter versuchen, sich durch das Qualitätsmerkmal IT-Sicherheit von der Konkurrenz abzugrenzen. Doch wodurch zeichnet sich eine sichere Messenger App aus? Diese Arbeit formuliert Sicherheitsanforderungen an Instant

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 241-252.

Messenger auf Basis des BSI IT-Grundschutzes [BSI15]. Dieser bietet eine Methode zur Formulierung der Sicherheitsanforderungen. Demnach wird aus einer Schutzbedarfsfeststellung der Sicherheitsbedarf abgeleitet. Der Sicherheitsbedarf dient als Grundlage für die Sicherheitsanforderungen. Abschließend wird der Messenger TextSecure anhand der ermittelten Sicherheitsanforderungen evaluiert. Ausgangspunkt für die Ableitung von Sicherheitsanforderungen sind einerseits die Analyse von Veröffentlichungen (siehe Kapitel 2) aber auch eigene Schwachstellenuntersuchungen der Open Source Messenger: Surespot, Telegram und TextSecure [Bötn14].

2 Related Work

In der Literatur finden sich eine ganze Reihe relevanter Arbeiten, die sich mit der Sicherheit mobiler Messenger bzw. Sicherheitslücken in mobilen Anwendungen auseinandersetzen.

Coull und Dyer [CoDy14] zeigen am Beispiel des Messengers iMessage, wie Informationen durch die Analyse der verschlüsselten Nachrichten abgeleitet werden können. Es lassen sich Informationen über Benutzeraktionen (beginnt Schreiben, beendet Schreiben oder Nachricht gelesen), Sprache, Länge und Art des Inhalts (Text oder Bild) einer Nachricht extrahieren. Diese Analysen lassen sich auch auf andere Messenger übertragen. Coul und Dyer zeigen dies für WhatsApp, Viber, und Telegram.

Sicherheitslücken u.a. schon im Security-Design wurden bereits in den Markführern identifiziert und veröffentlicht (WhatsApp [CoSW, SFK+12, Angl14, Alke13] und iMessage [Catt14]).

Bellovin et al. [BBCL14] stellen dar, wie Sicherheitslücken neue Überwachungsmethoden verschlüsselter IP-basierter Kommunikation ermöglichen, die mit traditionellen Überwachungsmaßnahmen nicht durchgeführt werden können. Sie sehen in der Ausnutzung von Sicherheitslücken zur Durchführung legitimierter Überwachungsmaßnahmen eine Alternative zu dem Ansatz einer rechtlichen Verpflichtung zum Einbau von Hintertüren in Kommunikationsprodukten.

Die Electronic Frontier Foundation bewertet in ihrer Secure Messaging Scorecard 40 Messenger Apps hinsichtlich dieser sieben Anforderungen[1]:

1. Verschlüsselter Transport der Nachrichten.
2. Verschlüsselt, sodass der Anbieter nicht mitlesen kann.
3. Können Kontakte verifiziert werden?
4. Ist vergangene Kommunikation sicher, falls Schlüssel gestohlen werden (Forward Secrecy)?
5. Ist der Quellcode für unabhängige Reviews verfügbar?
6. Ist das Security Design ordentlich dokumentiert?
7. Gab es ein unabhängiges Security Audit?

Diese Anforderungen sind nicht vollständig. Um die Sicherheit einer Messenger App bewerten zu können, fehlt beispielsweise eine Betrachtung der Verkehrsdaten. Auch werden alle Anforderungen als gleichwertig angesehen. Somit existiert bis dato keine vollständige Erhebung von Sicherheitsanforderungen für Messenger Apps, wie sie in dieser Arbeit vorgestellt wird.

[1] https://www.eff.org/secure-messaging-scorecard

2.1 Schutzbedarfsfeststellung

Ziel der Schutzbedarfsfeststellung ist eine qualitative Bewertung des Schutzbedarfs der Objekte eines IT-Systems in Bezug auf die einzelnen Schutzziele. Die Liste der zu schützenden Objekte ist das Ergebnis einer Analyse des Quellcodes und des Netzwerkverkehrs verschiedener Messenger Apps [Bötn14]. Die Objekte lassen sich in drei Gruppen Daten, IT-Systeme und Kommunikationsverbindungen einteilen. Den Gruppen werden die folgenden Objekte zugeordnet:

Daten:

- Nachrichteninhalt
- Kontaktdaten
- Öffentliche Schlüssel
- Private Schlüssel
- Geheime Schlüssel
- Passwörter
- Nutzer ID
- Push Client ID
- Verkehrsdaten:
  - Zeitpunkt des Versands, Empfangs, Schreiben und Lesen einer Nachricht
  - Ort des Versands, Empfang und Lesen einer Nachricht
  - Größe bzw. Länge einer Nachricht
  - Empfänger und Sender einer Nachricht
  - Statusinformationen (Nachricht versandt/empfangen/gelesen)
- Logdateien auf den Servern (enthalten Verkehrsdaten)

IT-Systeme:

- Smartphone der Nutzer
- Server der Messenger Anbieter
- Server Dritter (Google Could Messaging)

Kommunikationsverbindungen:

- Internetverbindung
- Mobilfunkverbindung

Primär bewerben die Anbieter die hohe Integrität und Vertraulichkeit der Nachrichteninhalte. Die Verfügbarkeit und der Schutz anderer Daten werden weniger stark beworben.

Tabelle 1 zeigt das Ergebnis der Schutzbedarfsfeststellung. Die Bewertung des jeweiligen Schutzbedarfs ist stark von dem Kontext, in dem die Messenger genutzt werden, abhängig. Die Messenger werden u.a. für den Zweck der Umgehung staatlicher Überwachung beworben. So wurde TextSecure von Aktivisten des arabischen Frühlings zur Organisation von Demonstrationen verwendet [Lemo11]. Da nach dem Maximumprinzip der Schaden mit den schwerwiegendsten Auswirkungen den Schutzbedarf bestimmt, wird hier von einem solchen Einsatzzweck ausgegangen.

Tab. 1: Schutzbedarfserstellung einer Messenger App

Objekt		Schutzbedarf			Begründung
Nr.	Name	Vertraulichkeit	Integrität	Verfügbarkeit	
D1	Nachrichten-inhalte	sehr hoch	sehr hoch	hoch	Je nach der Bedeutsamkeit des Inhalts kann eine Verletzung der Vertraulichkeit oder Integrität existenz- oder lebensbedrohlich sein.
D2	Kontaktdaten	sehr hoch	sehr hoch	hoch	Aus der Analyse der Kontaktdaten lassen sich Profile sozialer Beziehungen erstellen.
D3	Öffentliche Schlüssel	-	sehr hoch	hoch	Die Manipulation öffentlicher Schlüssel kann Man-in-the-Middle Angriffe ermöglichen.
D4	Private Schlüssel für asymmetrische Verschlüsselung	sehr hoch	sehr hoch	sehr hoch	Die Verletzung der Vertraulichkeit privater Schlüssel bedeutet die Verletzung der Vertraulichkeit von D1. Die Manipulation privater Schlüssel verhindert die Entschlüsselung der Nachrichten, sowie die korrekte Signatur.
D5	Geheime Schlüssel für symmetrische Verschlüsselung	sehr hoch	sehr hoch	hoch	Die Verletzung der Vertraulichkeit geheimer Schlüssel kann die Verletzung der Vertraulichkeit und Integrität von D1 bedeuten. Die Manipulation geheimer Schlüssel verhindert die Entschlüsselung der Nachrichten.
D6	Nutzerpass-wörter	sehr hoch	hoch	hoch	Die Verletzung der Vertraulichkeit kann die Verletzung der Vertraulichkeit der D5 bedeuten. Durch die Manipulation kann die Verfügbarkeit der anderen Objekte eingeschränkt werden.
D7	Nutzer ID	-	sehr hoch	hoch	Durch die Manipulation der Nutzer ID können Nachrichten an falsche Empfänger oder von falschen Sendern übermittelt werden.
D8	Push Client ID	-	hoch	hoch	Die Manipulation der Push Client ID wirkt sich auf die Verfügbarkeit anderer Objekte aus.
D9	Verkehrs-daten	sehr hoch	nor-mal	-	Aus der Analyse der Verkehrsdaten lassen sich Profile sozialer Beziehungen erstellen. Die Manipulation führt zu gefälschten Profilen.
D10	Logdateien auf Servern	sehr hoch	nor-mal	-	Logdateien enthalten Verkehrsdaten.
C1	Smartphone	sehr hoch	sehr hoch	hoch	Die Verletzung der Vertraulichkeit oder Integrität wirkt sich auf die Vertraulichkeit oder Integrität von D1-7 aus.
S1	Server der Anbieter	sehr hoch	sehr hoch	hoch	Die Verletzung der Integrität wirkt sich auf die Integrität von D3 aus.
S2	Server Dritter	-	hoch	hoch	Im schwerwiegendsten Fall kann durch Manipulation nur die Verfügbarkeit anderer Objekte eingeschränkt werden.
K1	Internet-Verbindung	-	hoch	hoch	Im schwerwiegendsten Fall kann durch Manipulation nur die Verfügbarkeit anderer Objekte eingeschränkt werden.
K2	Mobilfunk-Verbindung	-	hoch	hoch	Im schwerwiegendsten Fall kann durch Manipulation nur die Verfügbarkeit anderer Objekte eingeschränkt werden.

3 Sicherheitsanforderungen

Wie die Bewertung des Schutzbedarfs sind auch die Sicherheitsanforderungen abhängig von dem Kontext, in dem die Messenger Apps verwendet werden. Die hier formulierten Sicherheitsanforderungen können als allgemeine Mindestanforderungen oder als erweiterbare Grundlage angesehen werden.

Aus Tabelle 1 lassen sich die folgenden Sicherheitsanforderungen ableiten.

3.1 Identifizierung und Authentisierung

Jeder Nutzer muss sich gegenüber dem Server der Messenger Anbieter identifizieren und authentisieren.

Anforderung 1: Identifizierung und Authentisierung gegenüber Server
Jeder Nutzer muss sich gegenüber seinem Gesprächspartner identifizieren und authentisieren.

Anforderung 2: Identifizierung und Authentisierung gegenüber Gesprächspartner

3.2 Zugriffskontrolle

Durch einen Passwortschutz soll der Zugriff auf die Nachrichteninhalte, geheimen Schlüssel und Kontaktdaten durch Dritte verhindert werden.

Anforderung 3: Passwortgeschütze Anwendung
Durch eine passwortgeschützte Verschlüsselung lokaler und externer Daten wird der unberechtigte Zugriff auf Nachrichteninhalte und Kontaktdaten verhindert.

Anforderung 4: Verschlüsselung lokaler Daten

Anforderung 5: Verschlüsselung ggf. anfallender externer Daten (auf den Servern)

3.3 Verfügbarkeit der Server

Ist eine sichere Kommunikation über den Krypto-Messenger nicht möglich, besteht die Gefahr, dass der Nutzer auf einen weniger gesicherten Kommunikationskanal ausweicht.

Anforderung 6: Hohe Verfügbarkeit der Server
Gefordert wird eine vom Nutzer überprüfbare Verfügbarkeit des Dienstes. Folgende Statusinformationen wie Sende- und Empfangsnachweise unterstützen den Nutzer dabei:

- Status „Nachricht wurde gesendet“
- Status „Nachricht wurde empfangen“
- Status „Nachricht wurde gelesen“
- Status „Gesprächspartner ist online“
- Status „Gesprächspartner war zuletzt online vor …“

Anforderung 7: Statusinformationen
Werden Statusinformationen erstellt und übermittelt, so müssen diese gegen unberechtigten Zugriff geschützt werden.

Anforderung 8: Verschlüsselung der Statusinformationen
Der Versand der Statusinformationen

Anforderung 9: Option zur Deaktivierung der Statusinformationen

3.4 Übertragungssicherung

Um die Vertraulichkeit der Nachrichteninhalte zu schützen, ist eine Ende-zu-Ende Verschlüsselung notwendig.

Anforderung 10: Ende-zu-Ende Verschlüsselung der Nachrichten
Nur die an der Kommunikation beteiligten Subjekte dürfen auf die geheimen Schlüssel zugreifen können.

Anforderung 11: Sicheres Schlüsselmanagement
Je nach dem gewählten kryptographischen Verfahren kann eine Ende-zu-Ende Verschlüsselung die Integrität der Nachrichten sicherstellen. Ist dies nicht der Fall, muss die Integrität der Nachricht gesondert überprüft werden. Signaturen oder verschlüsselte Hashwerte der Nachrichten die an die Nachrichten, angehängt werden, sogenannte Message Authentication Codes (MAC), eignen sich zur Wahrung der Integrität.

Anforderung 12: Funktion zur Überprüfung der Integrität der Nachrichten

3.5 Datensicherung

Um die Verfügbarkeit der Nachrichten und Kontaktdaten sowie geheimer Schlüssel zu gewährleisten, müssen von diesen Sicherungskopien angelegt werden. So kann in dem Fall eines gestohlenen, verlorenen oder defekten Smartphones der Messenger auf einem anderen Smartphone verwendet werden.

Anforderung 13: Datensicherung und Wiederherstellung
Die Datensicherung muss gegen unberechtigten Zugriff geschützt werden.

Anforderung 14: Verschlüsselung der Datensicherung

3.6 Verkehrsdaten

Verkehrsdaten geben Aufschlüsse über soziale Beziehungen und das Kommunikationsverhalten und können teilweise Rückschlüsse auf Nachrichteninhalte liefern. Daher sollten nur Verkehrsdaten entstehen, die für den Betrieb des Messengers notwendig sind.

Anforderung 15: Vermeidung unnötiger Verkehrsdaten
Sofern Verkehrsdaten erhoben und gespeichert werden, müssen diese vor dem Zugriff unberechtigter Dritter geschützt werden.

Anforderung 16: Verschlüsselung von Verkehrsdaten
Besonders schützenswert sind Kontaktdaten. Kontaktdaten aus dem Smartphone sollen nicht ausgelesen und an den Server übertragen werden.

Anforderung 17: Kein Upload der Kontaktdaten

3.7 Datenschutzrechtliche Anforderungen

Obwohl aus Sicht der Nutzer eine Nachricht eines Messengers kaum von einer SMS oder MMS zu unterscheiden ist, ist eine Einordnung aus datenschutzrechtlicher Sicht aufgrund der technischen Unterschiede und ggf. eines ausländischen Unternehmenssitzes der Anbieter nicht direkt auf die Messenger übertragbar [DAV13].

Es ist umstritten, welches nationale oder internationale Gesetz in welchen Fällen anzuwenden ist. Für eine in Deutschland verwendete Messenger Anwendung kommen das Bundesdatenschutzgesetz (BDSG), das Telemediengesetz (TMG) und das Telekommunikationsgesetz

(TKG) in Betracht. Es ist nicht eindeutig geklärt, ob das BDSG trotz eines ausländischen Unternehmenssitz nach § 1 Abs. 5 S. 2 BDSG zumindest teilweise Anwendung findet, da Daten durch die Messenger Anwendungen in Deutschland erhoben werden. Die Rechtsprechung hierzu ist derzeit widersprüchlich [DAV13, RuFr13].

Aus der Komplexität und Unklarheit der juristischen Situation werden hier keine weiteren datenschutzrechtlichen Anforderungen abgeleitet. Zudem soll ein sicherer Messenger nicht nur ggf. geltende datenschutzrechtliche Bestimmungen einhalten, sondern darüber hinaus den Datenschutz als Ziel betrachten.

4 Evaluation des Messengers TextSecure

TextSecure wurde im Mai 2010 von der Entwicklergruppe Open Whisper Systems um den Sicherheitsforscher Moxie Marlinspike (Pseudonym) veröffentlicht. Mit TextSecure ließen sich zunächst nur SMS verschlüsseln. Diese Funktion ist in der aktuellen Version nicht mehr vorhanden. Zeitgleich wurde von Open Whisper Systems die Anwendung Redfone zur Ende-zu-Ende verschlüsselten Telefonie veröffentlicht.

Im November 2011 wurde Open Whisper Systems von Twitter aufgekauft. Twitter veröffentlichte im Dezember 2011 TextSecure und im Juni 2012 Redfone unter GPLv3/AGPLv3 Lizenzen. Beide Anwendungen erlangten größere Bekanntheit durch die Empfehlung des Guardian Projekts[2] und Edward Snowden[3]. Seit September 2013 ist TextSecure Bestandteil der alternativen Android-Firmware CyanogenMod und hat dadurch die Anzahl der Nutzer auf über 10 Mio. steigern können[4]. Ende Juli 2014 wurde die iOS Anwendung „Signal“ zur Ende-zu-Ende verschlüsselten Telefonie vorgestellt, die mit der Android Anwendung TextSecure kommunizieren kann. Eine Zusammenführung von Redfone, Signal und TextSecure zu einer Anwendung unter dem Namen Signal ist geplant[5].

Finanziert wird Whisper Systems durch den Open Technology Fund, ein Programm des Radio Free Asia zur Förderung eines globalen und freien Internets und zur Bekämpfung der Onlinezensur. Radio Free Asia ist ein nicht-kommerzieller Radiosender, der dem Broadcasting Board of Governors der USA untersteht, dessen Zusammensetzung direkt durch den Präsidenten der USA bestimmt wird. Open Whisper Systems erhielt bisher 455 Tsd. USD durch den Open Technology Fund[6].

Forscher der Ruhr Universität Bochum haben in 2014 das von TextSecure und das in der Anwendung verwendete Axolotl Protokoll untersucht und konnten das Erreichen der Schutzziele Authentizität und Vertraulichkeit bestätigen [FMB+14].

Anforderung 1: Identifizierung und Authentisierung gegenüber Server
Beim ersten Start von TextSecure werden zwei Schlüsselpaare, eines zur Verschlüsselung und eines zum Signieren aus Pseudozufallszahlen auf einer Cure25519 Kurve generiert. Daraufhin werden die beiden öffentlichen Schlüssel zusammen mit der Google Cloud Message ID und der Telefonnummer auf dem TextSecure Server verknüpft. Die Verifikation der Telefonnummer erfolgt einmalig durch eine

[2] https://guardianproject.info/apps/

[3] https://www.youtube.com/watch?v=UIhS9aB-qgU

[4] https://www.cyanogenmod.org/

[5] https://whispersystems.org/blog/signal/

[6] https://www.opentechfund.org/projects

SMS oder einen Anruf, die einen Verifikationscode enthalten [FMB+14, Bötn14]. So wird die Identifizierung und Authentisierung gegenüber dem Server gewährleistet.

Anforderung 2: Identifizierung und Authentisierung gegenüber Gesprächspartner
Die öffentlichen Schlüssel werden über den TextSecure Server verteilt. Die TextSecure Anwendung bietet die Option, die Hashwerte (Fingerprints) der Schlüssel über einen zweiten Kanal, z.B. mittels QR-Code, zu überprüfen. Somit können die Manipulation der Schlüssel auf dem Server und Man-in-the-middle Angriffe erkannt werden.

Anforderung 3: Passwortgeschütze Anwendung
Die lokale Verschlüsselung und der Passwortschutz der Anwendung sind optional. Aktiviert der Nutzer die lokale Verschlüsselung wird ein Masterkey generiert und verschlüsselt in den SharedPrefs gespeichert (s. Abbildung 1). Zunächst wird ein 128 Bit AES und ein 160 Bit MAC Schlüssel generiert. Die Konkatenation dieser beiden Schlüssel bilden dem sog. Masterkey.

Darauf wird die Anzahl der Iterationen bestimmt, indem die Anzahl an SHA1 Hashs gemessen wird, die das Android Gerät in 50 ms berechnen kann. Aus dem durch den Nutzer gewählten Passwort und zwei Pseudozufallszahlen SaltA und SaltB werden nach dem PKCS5s2 zwei Schlüssel KeyA und KeyB generiert.

Zunächst wird der Masterkey mit KeyA nach AES im Cipher Block Chaining (CBC) Modus verschlüsselt. Der verschlüsselte Masterkey wird darauf mit KeyB verschlüsselt und zusammen mit der Anzahl an Iterationen, SaltA und SaltB in die SharedPrefs geschrieben.

Die SharedPrefs werden für jede Anwendung in dem Android Gerät angelegt und können nur durch die jeweilige Anwendung gelesen und verändert werden. Dies gilt nicht für gerootete Geräte.

Anforderung 4: Verschlüsselung lokaler Daten
Wie der Passwortschutz ist auch die lokale Verschlüsselung optional.

Anforderung 5: Verschlüsselung ggf. anfallender externer Daten (auf den Servern)
Nach Angaben Whisper Systems werden anfallende Daten, wie die Kontaktdaten oder Logs nur kurzfristig auf den Servern gespeichert. Aufgrund der Ende-zu-Ende Verschlüsselung liegen die Nachrichten selbst immer nur verschlüsselt vor.

Anforderung 6: Hohe Verfügbarkeit der Server
Die Verfügbarkeit der Server wurde im Rahmen dieser Arbeit nicht untersucht.

Anforderung 7: Statusinformationen
Dem Nutzer wird angezeigt, ob eine Nachricht versandt sowie auch empfangen wurde. Darüber hinaus werden keine Statusinformationen erzeugt.

Anforderung 8: Verschlüsselung der Statusinformationen
Diese Statusinformationen werden verschlüsselt übertragen.

Anforderung 9: Option zur Deaktivierung der Statusinformationen
Statusinformationen lassen sich nicht deaktivieren.

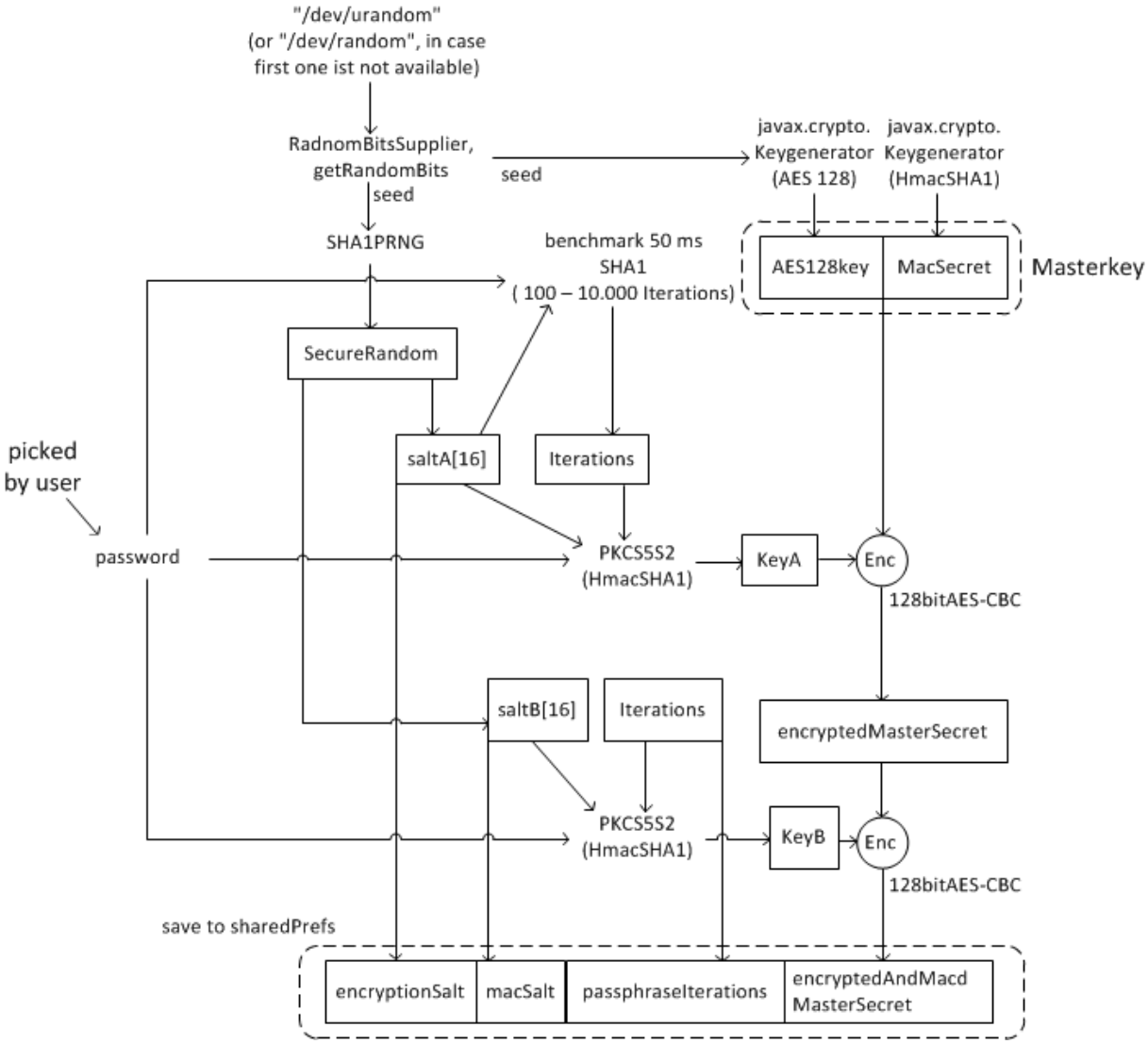

Abb. 1: Masterkey in SharedPrefs

Anforderung 10: Ende-zu-Ende Verschlüsselung der Nachrichten

TextSecure verwendet für die Verschlüsselung des Nachrichtenaustauschs das eigenentwickelte Axolotl Protokoll. Für jede neue Chatsession werden nach dem Elliptic Curve Diffie-Hellman Key Exchange Protokoll dreimal geheime Schlüssel generiert. Die Konkatenation dieser drei geheimen Schlüssel dient als Seed einer Key Chain (siehe Abbildung 2). Aus dieser Konkatenation wird durch die HMAC-based Extract-and-Expand Key Derivation Function (HKDF) ein 64 Byte großer Schlüssel generiert. Die ersten 32 Byte bilden den Root Key (RK), der nicht weiter verwendet wird. Die übrigen 32 Byte bilden den Schlüssel Chain Key (CK). Aus diesem wird durch die HKDF ein weiterer Schlüssel erzeugt. Die ersten 32 Bytes dieses Schlüssels bilden den Schlüssel Message Key (MK), mit dem die Nachricht nach AES256 im Counter Mode (CTR) ohne Padding verschlüsselt wird. Die übrigen 32 Bytes bilden den nächsten CK, aus dem der nächste MK für die nächste Nachricht und der übernächste CK generiert werden. Dieses Vorgehen gewährleistet nicht nur Ende-zu-Ende Verschlüsselung sondern auch Forward Secrecy und Future Secrecy.

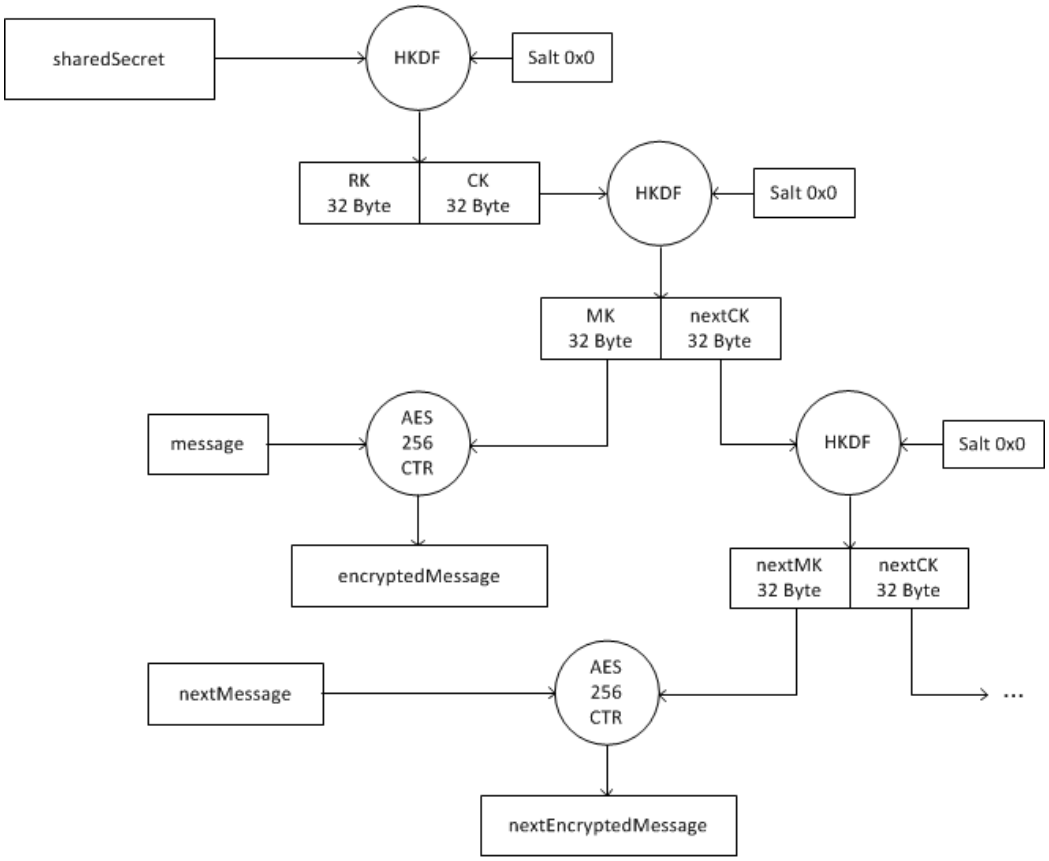

Abb. 2: Key Chain des Axolotl Protokoll

Anforderung 11: Sicheres Schlüsselmanagement
Die Authentizität und Integrität der öffentlichen Schlüssel kann durch den Nutzer manuell über einen zweiten Kanal überprüft werden. Zudem sind diese Schlüssel lokal verschlüsselt gespeichert, sofern die lokale Verschlüsselung aktiviert ist. Somit sind die Anforderungen an ein sicheres Schlüsselmanagement erfüllt.

Anforderung 12: Funktion zur Überprüfung der Integrität der Nachrichten
TextSecure bietet keine gesonderte Funktion zur Integritätsprüfung einer Nachricht. Jedoch gewährleistet das Axolotl Protokoll die Integrität der Nachrichten.

Anforderung 13: Datensicherung und Wiederherstellung
TextSecure biete die Funktion der Datensicherung und Wiederherstellung an.

Anforderung 14: Verschlüsselung der Datensicherung
Die Datensicherungen sind verschlüsselt.

Anforderung 15: Vermeidung unnötiger Verkehrsdaten
Der TextSecure Messenger überträgt nur die für die Kommunikation notwendigen Daten.

Anforderung 16: Verschlüsselung von Verkehrsdaten
Alle übertragenen Verkehrsdaten werden verschlüsselt übertragen.

Anforderung 17: Kein Upload der Kontaktdaten
Kontaktdaten (ausschließlich Telefonnummern) werden regelmäßig gehashed und an die TextSecure Server übertragen. Dort aber nur gegen eine Liste der Hashwerte der Telefonnummern aller TextSecure Nutzer abgeglichen und nicht gesondert gespeichert. Das Hashen bietet keinen ausreichenden Schutz, da die Anzahl aller möglichen Telefonnummern klein genug ist, um alle möglichen Hashwerte in überschaubarer Zeit zu berechnen.

Tab. 2: Bewertungsskala der Sicherheitsanforderungen

Nr.	Anforderung	erfüllt
1	Identifizierung und Authentisierung gegenüber Gesprächspartner	X
2	Identifizierung und Authentisierung am Server	X
3	Passwortgeschütze Anwendung	optional
4	Verschlüsselung lokaler Daten	optional
5	Verschlüsselung externer Daten (auf den Servern)	X
6	Hohe Verfügbarkeit der Server	wurde nicht untersucht.
7	Statusinformationen	X
8	Verschlüsselung der Statusinformationen	X
9	Option zur Deaktivierung der Statusinformationen	–
10	Ende-zu-Ende Verschlüsselung der Nachrichten	X
11	Sicheres Schlüsselmanagement	X
12	Funktion zur Überprüfung der Integrität der Nachrichten	X
13	Datensicherung und Wiederherstellung	X
14	Verschlüsselung der Datensicherung	X
15	Vermeidung unnötiger Verkehrsdaten	X
16	Verschlüsselung von Verkehrsdaten	X
17	Kein Upload der Kontaktdaten	–

5 Zusammenfassung

Messenger Apps haben die SMS-Nutzung überholt. Der Markt an Messenger Apps ist groß und unübersichtlich. Obwohl der Markt von als besonders sicher beworbenen Messenger Apps überschaubarer ist, fehlt ein vollständiger Kriterienkatalog als Grundlage für die Bewertung einzelner Messenger bezüglich ihrer Sicherheit.

In dieser Arbeit werden zunächst in einer Schutzbedarfserstellung alle schützenswerten Objekte bestimmt und eine qualitative Bewertung des Schutzbedarfs der Objekte vorgenommen. Daraus werden 17 Sicherheitsanforderungen an eine sichere Messenger App abgeleitet. Abschließend wird der Messenger TextSecure anhand der ermittelten Sicherheitsanforderungen evaluiert.

Literatur

[Alke13] T. Alkemade: Piercing through WhatsApp's encryption. Verfügbar unter : https://blog.thijsalkema.de/me/blog//blog/2013/10/08/piercing-through-whatsapp-s-encryption/ (2013).

[Angl14] C. Anglano: Forensic analysis of WhatsApp Messenger on Android smartphones. In Digital Investigation (2014).

[BBCL14] S. M. Bellovin, M. Blaze, S. Clark, und S. Landau: Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. In Nw. J. Tech. & Intell. Prop. 12 (2014).

[BeCH11] E. Bertin, N. Crespi, und M. L'Hostis: A few myths about telco and OTT models. In Intelligence in Next Generation Networks (ICIN) (2011) 6–10.

[Bötn14] Thomas Bötner: Sicherheit mobiler Instant Messenger. Bachelorarbeit an der Hochschule Bonn-Rhein-Sieg (2014).

[BSI15] Bundesamt für Sicherheit in der Informationssicherheit: IT-Grundschutz - Basis für Informationssicherheit. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/allgemein/einstieg/01001.html (2015).

[Catt14] C. Cattiaux: iMessage Privacy. Verfügbar unter: http://blog.quarkslab.com/imessage-privacy.html (2014).

[CoDy14] S. Coull, K. Dyer: Privacy Failures in Encrypted Messaging Services: Apple iMessage and Beyond. In arXiv preprint arXiv: 1403.1906 (2014).

[CoSW11] D. Cortjens, A. Spruyt, und W. F. Wieringa: WhatsApp Database Encryption Project Report. In Technical Report Verfügbar unter: https://www.os3.nl/_media/2011-2012/students/ssn_project_report.pdf (2011).

[DAV13] Deutscher Anwalt Verein: Stellungnahme des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht zur Anwendung des TKG auf neue Kommunikationsplattformen (bspw. WhatsApp). Verfügbar unter: http://www.anwaltverein.de/downloads/DAV-SN55-13.pdf (2013).

[DCVA14] Dialog Consult / VATM: 16. TK-Marktanalyse Deutschland 2014. Verfügbar unter: http://www.vatm.de/fileadmin/publikationen/studien/2014/VATM-TK-Marktstudie-2014.pdf (2014).

[FMB+14] T. Frosch, C. Mainka, C. Bader, F. Bergsma, J. Schwenk und T. Holz: How Secure is TextSecure? In Cryptology ePrint Archive Report 2014/904. Verfügbar unter: https://eprint. iacr. org/2014/904 (2014).

[HöGe03] J.R. Höflich und J. Gebhardt: Vermittlungskulturen im Wandel: Brief, E-mail, SMS. Frankfurt am Main: Lang (2003).

[Lemo11] R. Lemos: An App for Dissidents. MIT Technology Review. Verfügbar unter: http://www.technologyreview.com/news/422735/an-app-for-dissidents/ (2011).

[PoRe14] Portio Research: Mobile Messaging Markets 2014: Facebook, WhatsApp, SMS and OTT – the State of Play (2014).

[RuFr13] E.-O. Ruhle und N. Freund: Electronic communications services in the world of apps: Regulatory challenges. Verfügbar unter: http://www.econstor.eu/bitstream/10419/88519/1/77336918X.pdf (2013).

[SFK+12] S. Schrittwieser, P. Frühwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber und E. R. Weippl: Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications. NDSS (2012).

[WyCh11] D. K. Wysocki und C. D. Childers: Let my fingers do the talking: Sexting and infidelity in cyberspace, Sexuality & Culture, vol. 15, no. 3 (2011) 217–239.