Instant-Messaging – Bedrohungen und Sicherungsmaßnahmen

Patrick Hartung · Daniel Fischer

Technische Universität Ilmenau
patrick.hartung89@gmail.com
daniel.fischer@tu-ilmenau.de

Zusammenfassung

Mobile Instant-Messaging-Dienste kommen nicht nur im Privat-, sondern zunehmend auch immer häufiger im Geschäftsleben zum Einsatz. Ein sicherer Umgang mit den über diese Dienste ausgetauschten Daten wird immer wichtiger. Mit Hilfe einer Bedrohungsanalyse ermitteln wir zunächst typische Bedrohungen bei der Verwendung mobiler Instant-Messaging-Dienste und dokumentieren diese in Form von Bedrohungsbäumen. Auf Grundlage einer Literatur- und Internetrecherche erstellen wir einen Katalog möglicher Sicherungsmaßnahmen, die gegen die identifizierten Bedrohungen wirken und geeignet sind, die Sicherheit der Datenkommunikation mit mobilen Instant-Messaging-Diensten zu erhöhen. Unser Katalog umfasst 25 Sicherungsmaßnahmen für Dienstanbieter und 14 Maßnahmen für Dienstnutzer. Darauf aufbauend haben wir anschließend für zwei mobile Instant-Messaging-Dienste untersucht, welche Sicherungsmaßnahmen durch deren Dienstanbieter aktuell umgesetzt sind.

1 Einleitung

Die tägliche Nutzung von Smartphones wird wesentlich von Instant-Messaging-Diensten (kurz: IM-Diensten) geprägt [Khal15, FePR14]. Dabei steht eine Vielzahl von Anbietern mit einem heterogenen Funktionsumfang in einem starken Wettbewerb. Bei der Auswahl eines IM-Dienstes orientieren sich Nutzer meist an deren Verbreitung und Benutzerfreundlichkeit, weniger an Sicherheitsaspekten [Trep13]. Mit der zunehmenden immer stärker auch öffentlich geführten Diskussion über das Thema „Privacy“ wird der sichere Umgang mit den über diese Dienste versendeten Daten wichtiger. Einige IM-Dienste konnten einen sicheren Umgang der Daten nicht immer gewährleisten und standen mit negativer Kritik in den Schlagzeilen [oV14a, oV14b, oV14c]. Um sich von der Konkurrenz zu differenzieren und den Kunden einen Mehrwert zu bieten, rücken viele Dienstanbieter die Sicherheit nun mehr in den Mittelpunkt [Medi15].

In diesem Beitrag erarbeiten wir einen Überblick über Bedrohungen und Sicherungsmaßnahmen von Instant-Messaging-Diensten für Smartphones. Insbesondere werden folgende Fragen diskutiert:

- Welche Bedrohungen gibt es bei der Benutzung eines IM-Dienstes?
- Welche Sicherungsmaßnahmen existieren, um sich gegen Bedrohungen schützen zu können?
- Welche IM-Dienste nutzen welche Sicherungsmaßnahmen und sind somit gegen welche Bedrohungen abgesichert?

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 107-119.

Im folgenden Abschnitt definieren wir Instant-Messaging-Dienste und grenzen unseren Untersuchungsgegenstand weiter ein. Des Weiteren erörtern wir kurz relevante Literatur zum Thema Sicherheit von IM-Diensten. Im dritten Abschnitt beschreiben wir die Durchführung unserer Bedrohungsanalyse. Anhand von Bedrohungsbäumen stellen wir typische Bedrohungen bei der Verwendung mobiler IM-Dienste dar. Des Weiteren ermitteln wir Sicherungsmaßnahmen (Gegenmaßnahmen zu den zuvor ermittelten Bedrohungen) und stellen diese in einem Maßnahmenkatalog zusammen. Zusätzlich stellen wir die Sicherungsmaßnahmen den ermittelten Bedrohungen in einer Kreuzreferenztabelle gegenüber, um zu verdeutlichen, welche Maßnahmen welchen Bedrohungen entgegenwirken. Im vierten Abschnitt untersuchen wir bei den IM-Diensten Telegram und Threema, welche Sicherungsmaßnahmen die Anbieter umgesetzt haben. Im letzten Abschnitt fassen wir die Ergebnisse des Beitrags kurz zusammen und nehmen eine kritische Würdigung vor.

2 Mobile Instant-Messaging-Dienste

Instant Messaging (IM) ist eine Kommunikationsmethode für zwei oder mehrere Personen über das Internet [Koll15, WaLL13, Ochs14, DaRS00]. Hierbei lassen sich zeichen- oder textbasierte Nachrichten sowie Dateianhänge, wie z.B. Bilder und Videos, an Personen aus einer Kontaktliste übertragen. Damit eine Kommunikation zwischen den Kommunikationspartnern erfolgen kann, muss zunächst ein IM-Client in Form einer Applikation auf den Geräten des Senders und Empfängers installiert werden [Mayb09]. Die IM-Clienten bauen eine Verbindung zu einem zentralen IM-Server des Dienstanbieters auf, authentifizieren sich an diesem und senden bzw. empfangen über diesen Server ihre Nachrichten. Die Besonderheit des Instant Messaging liegt darin, dass durch den Einsatz des Push-Verfahrens der Nachrichtenaustausch sofort, zeitlich unmittelbar stattfinden kann. Unterstützt wird aber auch eine zeitlich versetzte Übermittlung von Nachrichten, falls der Empfänger der Nachricht nicht erreichbar ist [Jend14, DaRS00, Far10]. Dann verweilt die versendete Nachricht auf dem Server des jeweiligen Dienstanbieters und wird erst übertragen, sobald der Empfänger mit dem IM-Server verbunden ist.

Im weiteren Verlauf des Beitrags beziehen wir uns ausschließlich auf mobile IM-Dienste, d.h. der Austausch der Nachrichten findet zwischen mobilen Endgeräten (z.B. Smartphones oder Tablets) statt.

Zur Systematisierung und Vereinfachung der Betrachtung unterscheiden wir folgende drei Phasen bei der Nutzung von IM-Diensten:

- Anmeldephase: Diese umfasst das Herunterladen der Applikation aus einem App-Store, die Installation und Anmeldung bei dem IM-Dienstanbieter, um für den Nachrichtenversand und -empfang bereit zu sein.
- Nachrichtenübermittlungsphase: In dieser Phase schickt der Sender eine Nachricht an einen Empfänger (über den IM-Server des Dienstanbieters) und der Empfänger erhält diese sofort oder zeitlich versetzt.
- Phase nach der Nachrichtenübermittlung: Nachdem der Empfänger die Nachricht erhalten hat, befinden sich die übermittelten Daten (Texte, Zeichen, Bilder etc.) auf dem Smartphone des Empfängers und werden dort ggf. gesondert archiviert.

In den letzten Jahren hat die Zahl der Veröffentlichungen zugenommen, bei denen Instant-Messaging-Dienste im Hinblick auf sicherheitsrelevante Eigenschaften untersucht werden. In den meisten Arbeiten konzentrieren sich die Autoren auf die Analyse eines IM-Dienstes oder auf die Diskussion einer spezifischen Schwachstelle. Beispielsweise untersuchen Frosch et al. die

Sicherheit von TextSecure und beschreiben detailliert die verwendeten kryptografischen Verfahren und deren Schwachstellen [FMB+14]. Cattiaux diskutiert Schwachstellen von Apples iMessage und zeigt, wie diese Schwachstellen durch einen Man-in-the-Middle-Angriff ausgenutzt werden können [Catt13]. Schrittwieser et al. beschreiben und testen eine Möglichkeit, mittels eines Man-in-the-Middle-Angriffs die Authentifikation per SMS während der Anmeldung beim IM-Dienstanbieter abzufangen, um somit einen Account zu übernehmen [SFK+12]. Messerer und Eickhoff zeigen, dass beim IM-Dienst Skype Chat-Nachrichten mitgelesen werden können und die eingesetzte Verschlüsselung nicht ausreicht, um sich gegen einen Man-in-the-Middle-Angriff zu schützen [MeEi13]. Kaczmarek und Cattiaux zeigen bei einem ausführlichen Test von ChatSecure, dass Off-the-Record-Messaging nicht wie angegeben automatisch aktiviert ist, sondern dies bei jedem Chat neu gestartet werden muss, da sonst Man-in-the-Middle-Angriffe möglich sind [KaCa15]. Des Weiteren gibt es Arbeiten, in denen mehrere IM-Dienste anhand unterschiedlicher Kriterien miteinander verglichen werden. Ochsenkühn vergleicht z.B. anhand der Kriterien Infrastruktur, Authentizität, Verschlüsselung und Transparenz vier IM-Dienste. Bötner, Pohl und Ulimann führen eine Schutzbedarfsfeststellung für IM-Dienste durch und dokumentieren 17 spezielle Sicherheitsanforderungen, die solche Dienste erfüllen sollen [BöPU15]. Anhand der Anforderungen evaluieren sie den IM-Dienst TextSecure. Die US-amerikanische Bürgerrechtsorganisation Electronic Frontier Foundation (EFF) untersucht mit Hilfe ihrer Secure Messaging Scorecard seit 2014 regelmäßig IM-Dienste [AnBo14]. Anhand von sieben Kriterien hat das EFF bisher 39 IM-Dienste (nicht nur mobile) auf ihre Sicherheit geprüft. Lediglich vier Dienste erfüllen bisher alle sieben Sicherheitskriterien. Die EFF weist jedoch ausdrücklich darauf hin, dass die ausgewählten Kriterien nicht ausreichen, um einen IM-Dienst als sicher oder unsicher einzustufen.

Es fehlt eine Untersuchung von IM-Diensten, welche eine Vergleichbarkeit ihrer Sicherungsmaßnahmen zulässt und zudem dem Anwender einen Überblick gibt, gegen welche Bedrohungen er sich selbst bei der Nutzung eines Dienstes schützen kann bzw. gegen welche keine adäquaten Maßnahmen existieren.

3 Bedrohungen und Sicherungsmaßnahmen

3.1 Literatur-Review

Zur Ermittlung relevanter Bedrohungen bei der Nutzung eines IM-Dienstes und möglicher Sicherungsmaßnahmen haben wir einen Literatur-Review in Anlehnung an die Methodik von Fettke [Fett06] durchgeführt.

Bei der Literaturauswahl konzentrierten wir uns auf alle 22 mit “A” bewerteten Zeitschriften der VHB-Orientierungsliste sowie 40 weitere themenrelevante Zeitschriften der Kategorie B [BBF+08]. Bei unserer Recherche nutzten wir folgende Publikationsverzeichnisse: Gemeinsamer Bibliotheksverbundkatalog (gso.gbv.de), ACM Digital Library (dl.acm.org), Business Source Premier (www.ebscohost.com), ELSEVIER ScienceDirect (www.sciencedirect.com) und Google Scholar (scholar.google.de). Wir beschränkten uns auf englisch- und deutschsprachige Quellen und verwendeten bei der Recherche folgende Suchbegriffe, die wir in Titel, Abstract und den Keywords suchten: Instant Messaging, Instant Message, Instant Messenger. Für deutschsprachige Suchanfragen ergänzten wir die Suchbegriffe Bedrohung und Sicherheit und für englischsprachige Suchanfragen Vulnerability, Threat und Security (jeweils auch die Pluralformen). Bei Google Scholar und Google wurden jeweils nur die ersten fünfzig Treffer

ausgewertet. Aufgrund der Aktualität der Thematik haben wir nur Quellen aus den letzten fünf Jahren in der Untersuchung berücksichtigt.

Insgesamt konnten wir 347 Veröffentlichungen identifizieren, wobei wir nach der ersten inhaltlichen Erschließung nur noch 62 Veröffentlichungen als relevant für die Identifikation von Bedrohungen und Sicherungsmaßnahmen eingestuft und im weiteren Verlauf der Arbeit ausgewertet haben.

3.2 Bedrohungsanalyse

Bei der Bedrohungsanalyse handelt es sich um eine systematische Methode zur Ermittlung von organisatorischen, technischen und benutzerbedingten Bedrohungen[1], welche zu einem Schaden an einem IT-System und damit zur Verletzung von Sicherheitszielen führen können [Ecke14]. Die möglichst vollständige Ermittlung der Bedrohungen eines IT-Systems ist eine schwierige Herausforderung [Schn04]. Die Verwendung von Bedrohungsbäumen (häufig auch als Angriffsbäume bezeichnet) hilft, systematisch relevante Bedrohungen zu ermitteln und darzustellen [Ecke14].

Ein Bedrohungsbaum ist eine aus verschiedenen Knoten bestehende Baumstruktur, wobei der Wurzelknoten ein mögliches Angriffsziel definiert und somit eine mögliche Bedrohung des Systems darstellt [Ecke14, ScRo14, Schn99]. Auf mehreren Detailebenen wird anschließend der Wurzelknoten verfeinert, indem auf den jeweiligen weiteren Ebenen Zwischenziele definiert werden. Eine solche Verfeinerung der Baumstruktur wird solange durchgeführt, bis Elementarereignisse erreicht werden. Dabei ist eine verknüpfende Konjunktion oder Disjunktion mehrerer Zwischenziele durch UND- oder ODER-Verknüpfungen möglich. Abbildung 1 zeigt auszugsweise einen Bedrohungsbaum für einen Lauschangriff auf den Anmeldeprozess bei einem IM-Dienst.

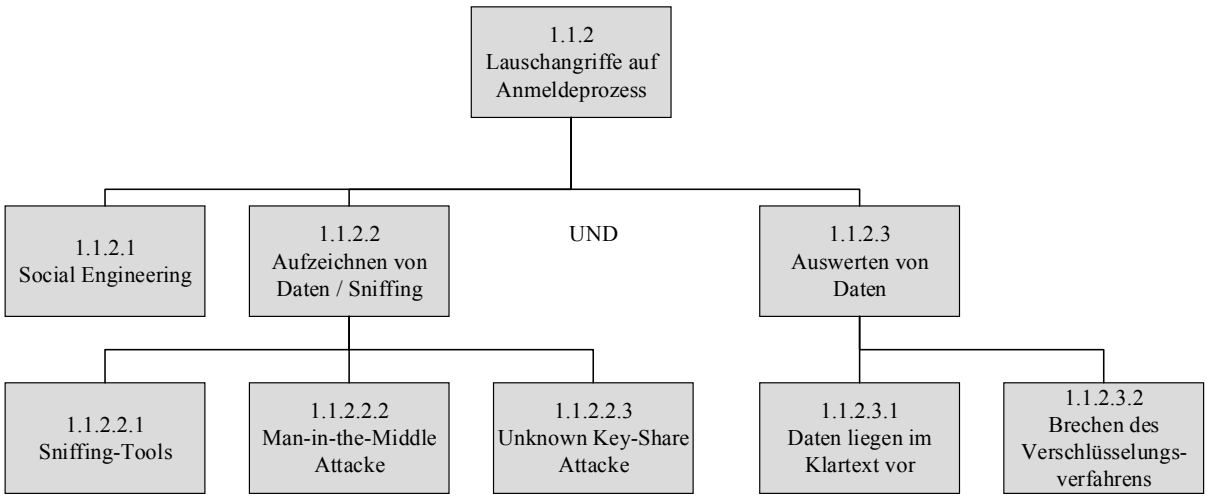

Abb. 1: Bedrohungsbaum für Lauschangriffe beim Anmeldeprozess (beispielhafte Darstellung)

[1] Bedrohungen sind Umstände oder Ereignisse, durch die die Verfügbarkeit, Integrität oder Vertraulichkeit (bzw. andere Sicherheitsziele) eines Systems beeinträchtigt werden und Schäden entstehen können [Ecke14, BSI03].

Bei der Nutzung von IM-Diensten existieren viele Bedrohungen und Schwachstellen, die durch Angriffe gezielt ausgenutzt werden können. Angriffe zielen auf eine Verletzung der Sicherheit. Sie sind eine absichtliche herbeigeführte Form der Gefährdung [BSI11] und nutzen in der Regel gezielt Schwachstellen aus. Es werden aktive und passive Angriffe unterschieden [Ecke14, Schn04, Schw05]. Passive Angriffe bedrohen die Vertraulichkeit, nicht aber die Verfügbarkeit oder die Integrität eines Systems. Aktive Angriffe hingegen bedrohen die Vertraulichkeit, Integrität und/oder Verfügbarkeit. In Tabelle 1 sind typische Angriffstypen zusammengefasst.

Tab. 1: Angriffsformen

Angriffskategorie	Angriffsformen	beeinträchtigte Sicherheitsziele
passiv	Erkundungsangriffe	Vertraulichkeit
	Lauschangriffe	
aktiv	Verfügbarkeitsangriffe	Vertraulichkeit, Integrität und/oder Verfügbarkeit
	Manipulationsangriffe	
	Weitere Angriffe	

Die mit Hilfe des Literatur-Reviews ermittelten Bedrohungen haben wir schrittweise in einen Bedrohungsbaum überführt. Für eine erste Aufteilung des Bedrohungsbaums nutzten wir die in Abschnitt 2 festgelegten drei Nutzungsphasen von IM-Diensten. Abbildung 2 zeigt unseren Hauptbedrohungsbaum.

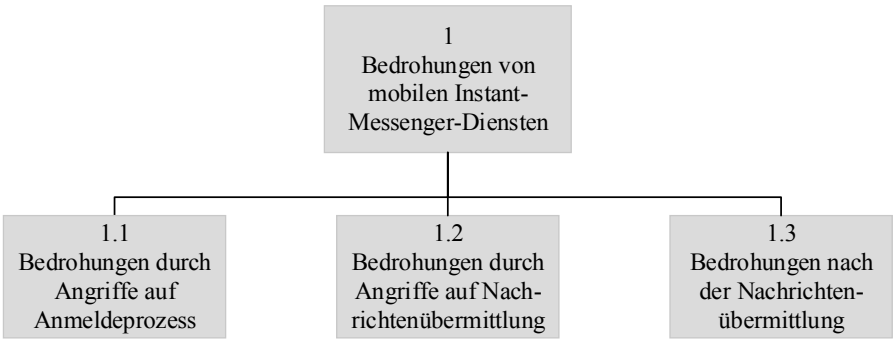

Abb. 2: Bedrohungen mobiler Instant-Messaging-Dienste (Hauptbedrohungsbaum)

Zusätzlich zu dieser Aufteilung haben wir innerhalb der drei Bedrohungsteilbäume 1.1, 1.2 und 1.3 nochmals eine Untergliederung entsprechend der in Tabelle 1 dargestellten Angriffsformen vorgenommen, um eine bessere Übersichtlichkeit zu erhalten. Mit Hilfe dieser systematischen Vorgehensweise konnten wir insgesamt 99 Bedrohungen ermitteln.

Zusätzlich zur grafischen Notation der Bedrohungen haben wir die Bedrohungsteilbäume in einen Bedrohungskatalog überführt, in dem alle Bedrohungen tabellarisch aufgelistet und fortlaufend nummeriert sind. In dem Katalog befinden sich für jede Bedrohung eine kurze Beschreibung und eine Nennung der durch sie beeinträchtigten Sicherheitsziele.[2] Zudem wurde auf Literatur, in welcher die jeweilige Bedrohung genauer beschrieben ist, verwiesen. Beispielhaft ist in Tabelle 2 ein Ausschnitt aus dem Bedrohungskatalog dargestellt.

[2] Zur Ermittlung der bedrohten Sicherheitsziele haben wir eine Wirkungsanalyse durchgeführt [Stel93].

Tab. 2: Auszug aus dem Bedrohungskatalog

Bedro-hungs-Nr.	Knoten-Nr.	Bedrohung	Ver-knüp-fung	Bedrohungs-beschreibung	Beeintr. Sicherheitsziel	Literatur
B 35	1.2.1.1	Foot-printing	ODER	Sammlung und Auswer-tung öffentlich zugängli-cher Informationen	Vertraulichkeit, Anonymität	[Rous07, Bens10, XSL+13]
B 36	1.2.1.2	Enumera-tion	ODER	Gezielte Suche nach IM-Accounts mit regionalen Telefonnummern	Vertraulichkeit, Anonymität	[SFK+12, Müll14, CYJ+13]

3.3 Sicherungsmaßnahmenkatalog

Grundlage der Ermittlung der relevanten Maßnahmen zur Sicherung von mobilen IM-Diensten war das in Abschnitt 3.1 beschriebene Literatur-Review sowie der in Abschnitt 3.2 beschriebene Bedrohungskatalog. Zusätzlich haben wir ergänzend weitere Fachliteratur, Veröffentlichungen des BSI [BSI06, GRT+08] sowie Internetquellen ausgewertet. Wir konnten Maßnahmen ermitteln, die durch den Dienstanbieter durchgeführt bzw. in den jeweiligen IM-Client- und IM-Server-Applikationen zum Einsatz kommen, sowie Maßnahmen, die der Dienstnutzer selbst vornehmen kann. Unser Fokus lag bei der Ermittlung auf den Maßnahmen der IM-Dienstanbieter.

Unser Katalog von Sicherungsmaßnahmen umfasst 25 Maßnahmen für IM-Dienstanbieter und 14 Maßnahmen für Dienstnutzer. In dem Katalog befinden sich für jede Sicherungsmaßnahme eine kurze Beschreibung und eine Nennung der durch sie verfolgten Sicherheitsziele bzw. der Bedrohungen, die durch sie gemindert bzw. abgewendet werden. Auf eine detaillierte Beschreibung jeder einzelnen Sicherungsmaßnahme haben wir in dem Katalog verzichtet. Stattdessen haben wir dort auf Publikationen verwiesen, die genauere Erläuterungen zu den einzelnen Maßnahmen enthalten. Tabelle 3 zeigt einen Auszug aus dem Sicherungsmaßnahmenkatalog. AM steht für Maßnahmen des Dienstanbieters und NM für Maßnahmen des Dienstnutzers.

Tab. 3: Auszug aus dem Sicherungsmaßnahmenkatalog

ID	Maßnahme	Beschreibung	Verfolgte Sicherheits-ziele	Bedrohungs-ID	Literatur
Maßnahmen des Dienstanbieters					
AM 4	Einsatz einer digitalen Signatur	dient der Bestimmung einer zweifelsfreien Urheberschaft einer Nachricht im juristischen Sinn	Authentizität, Verbindlichkeit	B 14, B 15, B 43, B 44, B 63,	[Ecke14]
AM 5	Einsatz von Zertifikaten	stellt eine digitale Bescheinigung über die Zuordnung eines öffentlichen Schlüssels zu einer natürlichen oder juristischen Person dar	Authentizität, Anonymität	B 14, B 15, B 43, B 44, B 63, B 68	[Ecke14]
Maßnahmen des Dienstnutzers					
NM 11	Regelmäßiges Löschen von Nachrichten	verhindert, dass sich sensible Daten auf dem Smartphone befinden, falls ein Angreifer Zugriff auf den internen Speicher bekommt	Vertraulichkeit, Anonymität	B 84, B 85, B 86	[Mayb09]
NM 12	Identität von Kontakten überprüfen	neuen Kontakt erst in die Kontaktliste aufgenommen, wenn überprüft ist, ob es sich tatsächlich um die jeweilige Person handelt	Authentizität	B 6, B 8, B 9, B 11, B 35, B 37, B 38, B 40, B 63, B 68, B 69, B 77, B 79, B 80, B 82	[Mayb09]

Um beschreiben zu können, welche Sicherungsmaßnahmen welche Bedrohungen mindern bzw. abwenden können, haben wir eine Kreuzreferenztabelle erstellt [Tern05]. Sie ermöglicht eine bessere Übersicht der bereits im Maßnahmenkatalog vorgenommenen Zuordnung der 39 Sicherungsmaßnahmen zu den 99 Bedrohungen. Die Zuordnung erfolgte einerseits auf Grundlage von Plausibilitätsüberlegungen und andererseits objektiv anhand der jeweils beeinträchtigten bzw. verfolgten Sicherheitsziele der Bedrohungen bzw. Maßnahmen.

Viele der ermittelten Bedrohungen entstehen durch Lauschangriffe, womit Verletzungen der Vertraulichkeit und Anonymität einhergehen. Jedoch zeigt die Kreuzreferenztabelle, dass 63 Bedrohungen mit Hilfe einer oder sogar mehrerer Sicherungsmaßnahmen verhindert bzw. abgeschwächt werden können. Nutzer können sich selbst z.B. bereits durch ein selbstständiges Informieren und Sensibilisieren zu den Sicherheitsaspekten bei der Verwendung von IM-Diensten, das regelmäßige Updaten der IM-Software sowie das Blockieren unbekannter und unerwünschter Kontakte schützen. Für 36 Bedrohungen konnten wir jedoch keine adäquaten Sicherungsmaßnahmen finden.

In Tabelle 4 ist ein Ausschnitt der erstellten Kreuzreferenztabelle zu sehen, in der abgelesen werden kann, welche Sicherungsmaßnahme gegen welche Bedrohung schützen kann.

Tab. 4: Auszug aus der Kreuzreferenztabelle

Maßnahme (ID: Bezeichnung) / Bedrohung (ID: Bezeichnung)	…	AM 12: Sichere Protokolle auf der Transportebene	AM 13: Ende-zu-Ende-Verschlüsselung	…	AM 21: Blockierung unbekannter Nutzer	…
...						
B 14: Man-in-the-Middle-Attacke		x	x			
B 63: Spoofing					x	
...						

Es sei erwähnt, dass einzelne Sicherungsmaßnahmen nicht zwingend dazu führen, dass die Bedrohung vollständig abgewendet wird. Oft ist erst eine Kombination mehrerer Maßnahmen nötigt, um das zu erreichen. So kann eine Applikation beispielsweise durch regelmäßig durchgeführte Kontrollen des Quellcodes vor Angriffen auf Schwachstellen besser geschützt werden, doch müssen die notwendigen Änderungen auch über Softwareupdates dem Endkunden zur Verfügung gestellt und dort eingespielt werden [BSI15].

4 Analyse ausgewählter Instant-Messaging-Dienste

Auf der Grundlage des von uns erstellten Sicherungsmaßnahmenkatalogs haben wir im 4. Quartal 2015 zehn verbreitete und als sicher beworbene IM-Dienste auf deren implementierte Sicherungsmaßnahmen hin überprüft. Zunächst haben wir dazu die von den jeweiligen IM-Dienstanbietern veröffentlichten technischen Dokumentationen und Beschreibungen ausgewertet. Zur Überprüfung und Vervollständigung unserer Ergebnisse kontaktierten wir anschließend die IM-Dienstanbieter und baten sie, selbst Auskunft über die von ihnen genutzten Sicherungsmaßnahmen zu geben. Auf diese Weise konnten wir einerseits unseren Maßnahmenkatalog evaluieren und andererseits die von uns ermittelten Informationen über die IM-Dienste überprüfen und ggf. vervollständigen lassen.

Aus Platzgründen stellen wir hier nur exemplarisch einige Ergebnisse zu den beiden Diensten Telegram und Threema vor.

Der werbefreie und kostenlose IM-Dienst Telegram wird seit 2013 von der Telegram Messenger LLP mit Sitz in Berlin betrieben und hat nach eigenen Angaben bereits 100 Mio. monatliche aktive Nutzer (Stand Februar 2016) [oV15a, oV16]. Unterstützt wird neben dem Versenden von Textnachrichten auch das Versenden von Daten jeglicher Art an verschiedene Endgeräte (einschließlich PCs, Tablets, Smartphones und Webbrowser). Da Telegram nach eigenen Aussagen eine Ende-zu-Ende-Verschlüsselung nur bei der Aktivierung des sogenannten geheimen Chats anbietet, haben wir diesen Modus in der Programmversion 3.2.6 für unseren Test gewählt [oV16].

Der 2012 erstmals veröffentlichte IM-Dienst Threema wird von der schweizerischen Threema GmbH entwickelt und betrieben. Threema ist im vollen Funktionsumfang nur auf Android-, iOS- und Windows-Phone-Smartphones und nur nach Zahlung einer einmaligen Lizenzgebühr einsetzbar. Threema nutzt eine Ende-zu-Ende-Verschlüsselung und ermöglicht zudem die Identitäten von Kontakten durch das Scannen persönlicher QR-Codes zu verifizieren. Trotz der proprietären Software dokumentiert Threema sehr detailliert die eingesetzten Verschlüsselungsmechanismen und zeigte auch in unserer Befragung in Bezug auf die Programmversion 2.4 eine sehr offene Kommunikation zu den verwendeten Sicherungsmaßnahmen [oV15b].

In Tabelle 3 ist ein Auszug aus dem von uns erstellten Vergleich der beiden IM-Dienste zu sehen. Es ist z.B. erkennbar, welche Verschlüsselungsmechanismen bei den beiden Diensten für die Absicherung der Nachrichten und Medieninhalte eingesetzt werden. Zwar unterscheiden sich die konkreten Verfahren teilweise, jedoch gibt es viele Ähnlichkeiten bei den grundsätzlich eingesetzten Prinzipen. Unterschiede sind aber z.B. bei der Speicherung von Medieninhalten nach dem Empfang von Nachrichten zu erkennen (AM 15.2). Threema sichert die Medieninhalte in einer verschlüsselten Datei und erlaubt den Nutzern den Zugriff nur über die eigene App. Bei Telegram werden diese Daten stattdessen unverschlüsselt gespeichert, was zu einem Verlust verschiedener Sicherheitsziele führen kann.

Tab. 5: Auszug aus dem Sicherungsmaßnahmenkatalog der IM-Dienste Telegram und Threema

Anbieter Maßnahmen (ID: Bezeichnung)	Telegram (geheimer Chat), Version 3.2.6	Threema, Version 2.4
AM 1: Einsatz kryptograf. Verfahren	ja	ja
AM 1.1: Verschlüsselung vom Sitzungsschlüssel	asymmetrisch, RSA	asymmetrisch, ECDH über Curve25519 mit HSalsa20 Hash
AM 1.2: Verschlüsselung der Nachricht	symmetrisch, AES	symmetrisch, XSalsa20
AM 1.3: Verschlüsselung der Medieninhalte	symmetrisch, AES	symmetrisch, XSalsa20
AM 2: Einsatz von Hashfunktion	ja, SHA-1	ja, HSalsa20
AM 3: Einsatz des Message Authentication Code	nein	ja, 128 Bit
AM 4: Einsatz einer digitalen Signatur	nicht ermittelbar	nein
AM 5: Einsatz von Zertifikaten	nicht ermittelbar	ja
AM 6: Sichere Schlüsselerzeugung	nicht ermittelbar	Elliptic Curve (Curve25519)
AM 6.1: Länge des Sitzungsschlüssels	2048 Bit	ECC 255 Bit entspricht RSA 2048-3072 Bit
AM 6.2: Schlüssellänge für Nachrichten	256 Bit	256 Bit
AM 6.3: Schlüssellänge für Medieninhalte	256 Bit	256 Bit
...		
AM 15.1: Sichere Speicherung der Nachricht	in verschlüsselter Datei	in verschlüsselter Datei
AM 15.2: Speicherung von Medieninhalten	nicht verschlüsselt	in verschlüsselter Datei
...		

5 Schlussbemerkung

Durch die zunehmende Verbreitung internetfähiger mobiler Endgeräte sowie der Vielzahl und Einfachheit von Instant-Messaging-Diensten nimmt das Instant Messaging sowohl im privaten als auch im geschäftlichen Bereich stetig zu. Ein sicherer Umgang der über diese Dienste ausgetauschten Daten wird immer wichtiger. Die Entwicklung der letzten Jahre zeigt, dass die Dienstanbieter den Spagat zwischen Nutzerfreundlichkeit und Sicherheit kontinuierlich zu verbessern versuchen, um sich im starken Konkurrenzkampf beweisen zu können.

Mit Hilfe einer Bedrohungsanalyse konnten wir typische Bedrohungen beim Einsatz mobiler Instant-Messaging-Dienste ermitteln und diese in Form von Bedrohungsbäumen dokumentieren. Für jede Bedrohung haben wir untersucht, zu welchen Konsequenzen/Folgen diese führen kann und welche Sicherheitsziele dadurch gefährdet werden. Für die sichere Gestaltung mobiler Instant-Messaging-Dienste haben wir einen Katalog von Sicherungsmaßnahmen entwickelt. Diese können Bedrohungen verhindern bzw. zumindest abschwächen. Mit Hilfe des Sicherungsmaßnahmenkatalogs konnten wir anschließend die zwei Dienste Telegram und Threema

in Bezug auf Gemeinsamkeiten und Unterschiede bei den eingesetzten Sicherungsmaßnahmen analysieren.

Unsere Arbeit ermöglicht einen ersten Überblick über die im Bereich des Instant-Messagings vorhandenen Bedrohungen und Sicherungsmaßnahmen. Eine vollständige Erfassung aller möglichen Bedrohungen eines IT-Systems ist durch den Einsatz einer Bedrohungsanalyse jedoch nicht garantiert [ScRo14] und soll hier auch nicht unterstellt werden. Beispielsweise haben wir uns bei den schutzwürdigen Datenelementen auf die Nachrichteninhalte, die Kontakt- und Nutzerdaten konzentriert und auf eine detaillierte Betrachtung der auf den Servern der Dienstanbieter befindlichen Verkehrs- und Logdaten verzichtet. Auch haben wir aus Vereinfachungsgründen mögliche Wechselwirkungen bzw. Abhängigkeiten zwischen Sicherungsmaßnahmen nicht weiter betrachtet, obwohl diese die Wirksamkeit der Maßnahmen entscheidend beeinflussen können.

Aktuell steht die Sicherung der Vertraulichkeit bei der Nachrichtenübertragung im Fokus der Diskussion. Viele Instant-Messaging-Anbieter reagieren darauf mit der Einführung einer permanenten und möglichst transparenten Ende-zu-Ende-Verschlüsselung, wie zuletzt auch beim meistgenutzten Instant-Messaging-Dienst WhatsApp [Eike16]. Doch auch wenn mit diesen Maßnahmen die Vertraulichkeit der versendeten Nachricht durchaus verbessert werden kann, bleiben noch viele Angriffslücken offen. Angreifer können weiterhin z.B. durch eine ungesicherte Speicherung der Nachrichten und Medieninhalte auf dem Smartphone die Vertraulichkeit, Integrität und Verfügbarkeit beeinträchtigen. Problematisch ist des Weiteren z.B. auch ein adäquater Schutz der auf den Servern der IM-Dienstanbieter befindlichen Verkehrs- und Logdaten. Hierzu sollten kurz- und mittelfristig weitere Untersuchungen durchgeführt werden.

Literatur

[AnBo14] J. Angwin, J. Bonneau: Secure Messaging Scorecard - Which apps and tools actually keep your messages safe? https://www.eff.org/de/secure-messaging-scorecard, San Francisco (2014), Abruf: 2015-04-14.

[BBF+08] J. Becker, M. Bichler, U. Frank, A. Heinzl, T. Hess, M. Jarke, D. Karagiannis, W. König, H. Kremar, D. Schoder, C. Weinhardt: WI-Orientierungslisten - WI-Journalliste 2008 sowie WI-Liste der Konferenzen, Proceedings und Lecture Notes (2008). http://gcc.uni-paderborn.de/WWW/WI/WI2/wi2_lit.nsf/ac81c1a6a57ffce8c1256f3c003fea01/549991b84925b9d5c12573d200360077/$FILE/Orientierungslisten_WKWI_GIFB5_ds41.pdf, Karlsruhe (2007), Abruf: 2015-10-24.

[Bens10] J. P. Benson: Cyber Threats - An Emerging Concern. o. O. (2010), S. 215–234.

[BöPU15] T. Bötner, H. Pohl, M. Ulimann: Sicherheitsanforderung an Messenger Apps. In: Peter Schartner (Hrsg.): D-A-CH Security Bestandsaufnahme - Konzepte - Anwendungen - Perspektiven. St. Augustin bei Bonn, 08.-09. September 2015, syssec, Frechen (2015).

[BSI03] BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Kommunikations- und Informationstechnik 2010+3: Neue Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Trend2010/IT-Sicherheit_pdf.pdf?__blob=publicationFile, Bonn (2003), Abruf: 2015-08-25.

[BSI06] BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Mobile Endgeräte und mobile Applikationen. http://www.rz.uni-greifswald.de/fileadmin/mediapool/1_Dienste/Formulare/mobile_endgeraete_pdf.pdf, Bonn (2006), Abruf: 2015-11-17.

[BSI11] BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutzkataloge. 12. Aufl., Bundesanzeiger, Köln (2011).

[BSI15] BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Regelmäßige Updates für mehr Sicherheit. https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Tipp_Patchmanagement_13112015.html, Bonn (2015), Abruf: 2015-11-18.

[Catt13] C. Cattiaux: iMessage Privacy. http://blog.quarkslab.com/imessage-privacy.html, o. O. (2013), Abruf: 2015-04-29.

[CYJ+13] Y. Cheng, L. Ying, S. Jiao, P. Su, D. Feng: Bind your phone number with caution - automated user profiling through address book matching on smartphone. In: ASIA CCS '13 (2013), S. 335–340.

[DaRS00] M. Day, J. Rosenberg, H. Sugano (Hrsg.): RFC 2778: A Model for Presence and Instant Messaging. https://www.ietf.org/rfc/rfc2778.txt, o. O. (2000), Abruf: 2015-10-06.

[Ecke14] C. Eckert: IT-Sicherheit - Konzepte - Verfahren - Protokolle. 9., aktualisierte und korrigierte Auflage, De Gruyter Oldenbourg, München (2014).

[Eike16] R. Eikenberg: WhatsApp: Verschlüsselung für alle freigeschaltet. http://www.heise.de/security/meldung/WhatsApp-Verschluesselung-fuer-alle-freigeschaltet-3163009.html, Hannover (2016), Abruf: 2016-05-20.

[Far10] S. M. Far: Social Software in Unternehmen - Nutzenpotentiale und Adoption in der innerbetrieblichen Zusammenarbeit. 1. Aufl., Eul, Lohmar [u.a.] (2010).

[FePR14] S. Feierabend, T. Plankenhorn, T. Rathgeb: JIM 2014 Jugend, Information, (Multi-) Media - Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland. Stuttgart (2014).

[Fett06] P. Fettke: State-of-the-Art des State-of-the-Art - Eine Untersuchung der Forschungsmethode "Review" innerhalb der Wirtschaftsinformatik. In: Wirtschaftsinformatik. Nr. 48, (2006), S. 257–266.

[FMB+14] T. Frosch, C. Mainka, C. Bader, F. Bergsma, J. Schwenk, T. Holz, H. Götz: How Secure is TextSecure? Bochum (2014).

[GRT+08] H. Gerwing, G. Reckhaus, B. Ternes, D. Ferrest, S. Hoff, D. Hübner, F. Imhoff, M. v. Laak, B. Moayeri, N. Schirmer, M. Wallbaum, J. Wetzlar, D. Zöller: Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte. Bonn (2008), Abruf: 2015-11-17.

[Jend14] K. Jendrian: Sicheres Instant Messaging - Alternativen zu WhatsApp und iMessage. In: Datenschutz und Datensicherheit - DuD. Nr. 5, (2014), S. 301–304.

[KaCa15] S. Kaczmarek, C. Cattiaux: Security assessment of instant messaging app ChatSecure: when privacy matters. http://blog.quarkslab.com/security-assessment-of-instant-messaging-app-chatsecure-when-privacy-matters.html, o. O. (2015), Abruf: 2015-10-11.

[Khal15] S. Khalaf: Messaging Apps: The New Face of Retail Banking. http://www.flurry.com/blog/flurry-insights/messaging-apps-new-face-retail-banking#.VSuACpMgASE, San Francisco (2015), Abruf: 2015-04-14.

[Koll15] T. Kollmann: Instant Messaging - Gabler Wirtschaftslexikon. http://wirtschaftslexikon.gabler.de/Archiv/81864/instant-messaging-v8.html, o. O. (2015), Abruf: 2015-08-26.

[Mayb09] M. Maybaum: Erstellung eines Bausteins "Instant Messaging" für die IT-Grundschutz-Kataloge. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Diplomarbeiten/Instant_Messaging_pdf.pdf?__blob=publicationFile, Hagen (2009), Abruf: 2015-09-04.

[Medi15] M. Medicus: WhatsApp-Alternative - Die 10 besten Messenger für Android, iPhone, iPad & Co. http://www.pc-magazin.de/ratgeber/whatsapp-alternative-ersatz-kostenlos-messenger-android-iphone-pc-2921707.html, München (2015), Abruf: 2015-04-26.

[MeEi13] T. Messerer, B. Eickhoff: Einsatz von Skype im Unternehmen - Chancen, Risiken und Policy-Empfehlungen. http://www.esk.fraunhofer.de/content/dam/esk/dokumente/Skype_im-Unternehmen.pdf, o. O. (2013), Abruf: 2015-10-10.

[Müll14] R. Müller: Re-evaluating Smartphone Messaging Application Security. https://www.sba-research.org/pubs/reevaluating_smartphone_app_security.pdf, Wien (2014), Abruf: 2015-04-29.

[oV14a] o. V. (Hrsg.): Chaos im Messenger-Dschungel - Die PSW GROUP testet ausführlich. Fulda (2014).

[oV14b] o. V. (Hrsg.): Facebook übernimmt WhatsApp - Was bedeutet das für die Nutzer? http://www.welt.de/newsticker/dpa_nt/infoline_nt/computer_nt/article125041000/Facebook-uebernimmt-WhatsApp-Was-bedeutet-das-fuer-die-Nutzer.html, Berlin (2014), Abruf: 2015-04-14.

[oV14c] o. V. (Hrsg.): WhatsApp und Alternativen - Datenschutz im Test. https://www.test.de/WhatsApp-und-Alternativen-Datenschutz-im-Test-4675013-0/, Berlin (2014), Abruf: 2015-04-14.

[oV15a] o. V. (Hrsg.): Telegram FAQ. https://telegram.org/faq, Berlin (2015), Abruf: 2015-11-18.

[oV15b] o. V. (Hrsg.): Threema Cryptography Whitepaper. https://threema.ch/press-files/cryptography_whitepaper.pdf, Pfäffikon (2015), Abruf: 2015-11-17.

[oV16] o. V. (Hrsg.): 100,000,000 Monthly Active Users. https://telegram.org/blog/100-million, Berlin (2016), Abruf: 2016-04-03.

[Ochs14] C. Ochsenkühn: Mobile Instant Messenger und deren Sicherheitsstand. http://www.herr-yeah.de/wp-content/uploads/2014/03/IWS_Ochsenkuehn_

Mobile-Instant-Messenger-und-deren-Sicherheitsstand.pdf, Hof (2014), Abruf: 2015-04-29.

[Rous07] M. Rouse: footprinting definition. http://searchsecurity.techtarget.com/definition/footprinting, Newton (2007), Abruf: 2015-09-11.

[ScRo14] G. Schäfer, M. Roßberg: Netzsicherheit - Grundlagen & Protokolle ; mobile & drahtlose Kommunikation ; Schutz von Kommunikationsinfrastrukturen. 2., aktualisierte und erw. Aufl., dpunkt-Verlag, Heidelberg (2014).

[Schn99] B. Schneier: Attack Trees - Modeling security threats. https://www.schneier.com/paper-attacktrees-ddj-ft.html, New Orleans (1999), Abruf: 2015-08-28.

[Schn04] B. Schneier: Secrets & Lies: IT-Sicherheit in einer vernetzten Welt. dpunkt-Verlag, Heidelberg (2004).

[Schw05] J. Schwenk: Sicherheit und Kryptographie im Internet - Von sicherer EMail bis zu IP-Verschlüsselung. 2. Aufl., Vieweg Verlag, Braunschweig (2005).

[SFK+12] S. Schrittwieser, P. Frühwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, E. Weippl: Guess Who´s Texting You? - Evaluating the Security of Smartphone Messaging Applications. http://www.internetsociety.org/sites/default/files/07_1.pdf, o. O. (2012), Abruf: 2015-04-29.

[Stel93] D. Stelzer: Sicherheitsstrategien in der Informationsverarbeitung - Ein wissensbasiertes, objektorientiertes System für die Risikoanalyse. Deutscher Universitätsverlag, Wiesbaden (1993).

[Tern05] B. Ternes; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Technische Richtlinie Sicheres WLAN. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03103/TRS_WLAN_Praesentation_pdf.pdf?_blob=publicationFile, München (2005), Abruf: 2011-05-08.

[Trep13] S. Trepesch: WhatsApp: Bedeutet die Jahresgebühr das Ende des Chat-Dienstes für iPhone und Android? http://www.giga.de/apps/whatsapp-fur-android/news/whatsapp-bedeutet-die-jahresgebuhr-das-ende-des-chat-dienstes-fur-iphone-und-android/, Berlin (2013), Abruf: 2015-06-23.

[WaLL13] C.-J. Wang, W.-L. Lin, H.-T. Lin: Design of An Instant Messaging System Using Identity Based Cryptosystems. In: Fourth International Conference on Emerging Intelligent Data and Web Technologies (2013), S. 277–281.

[XSL+13] N. Xia, H. H. Song, Y. Liao, M. Iliofotou, A. Nucci, Z.-L. Zhang, A. Kuzmanovic: Mosaic - quantifying privacy leakage in mobile networks. In: ACM SIGCOMM 2013 Conference (2013), S. 279–290.