Briar Repeater

Schlussbericht

Zuwendungsempfänger:

Julian Dehm Benedikt Wieder GbR

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01IS18S18 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Kurze Darstellung der Aufgabenstellung und Motivation

Als Entwickler und Nutzer des Open-Source Messengers *Briar* war und ist es unsere Motivation *Briar* zu verbessern und interessanter für Nutzer*innen zu machen. Eines der grundlegenden Probleme bei dezentralen Messaging-Apps wie *Briar* ist, dass die kommunizierenden Personen zur gleichen Zeit online sein müssen. Schlechte Netzabdeckung, unterschiedliche Zeitzonen oder abweichende Tag-/ Nachtrhythmen können die Erreichbarkeit beeinflussen oder sogar dazu führen dass Nachrichten gar nicht ausgetauscht werden können.

Mit der *Briar Mailbox*[1] soll dieses Problem gelöst werden ohne dabei das Konzept der Dezentralisierung aufzugeben. DIe Idee der *Mailbox* ist ein Zwischenspeicher für Nachrichten welcher von Nutzer*innen zu Hause betrieben werden kann. Durch den Anschluss an eine zuverlässiges Internetverbindung ist diese dann immer erreichbar. Dabei ist es uns in diesem Kontext wichtig, dass die Daten immer unter der Kontrolle der Nutzer*innen bleiben und nicht auf zentralen Servern gespeichert werden. Außerdem soll die Einrichtung möglichst einfach sein, so dass auch unerfahrene Nutzer*innen von den Funktionen der *Mailbox* profitieren können.

Für den Zeitraum des Projektes war zunächst eine Einarbeitungsphase in die von *Briar* verwendeten Technologien geplant. Darauf aufbauend sollte die Ausarbeitung eines sicheren und robusten Konzeptes, insbesondere in Hinsicht auf die hohen Sicherheitsanforderungen von *Briar*, als erster wichtiger Meilenstein stattfinden. Auf Basis dieses Konzeptes soll dann das Grundgerüst für die *Mailbox* implementiert werden. Anschließend wird die Integration in *Briar* ausgearbeitet und entwickelt, welche uns das Testen des Grundgerüstes, manuell und durch Integrations- und Unittests, erlaubt.

Auf Basis dieses Grundgerüstes sollten die Funktionen der *Mailbox* ausgearbeitet und implementiert werden, wobei ein besonderer Fokus auf Sicherheit und einfacher Bedienung gelegt wird. Nach Abschluss der Implementierungsarbeit soll der Programmcode begutachtet werden um mögliche Fehler und Sicherheitslücken zu entdecken und zu beheben. Abschließend soll eine Dokumentation des Programmcodes ausgearbeitet werden.

[1] Der ursprüngliche Name “*Briar Repeater*” wurde im Laufe des Projekts geändert

Beitrag des Projektes zu den Zielen der Förderinitiative „Software-Sprint“

Im Bezug auf den Software Sprint bietet die *Briar Mailbox* als Teilprojekt von *Briar* Nutzer*innen die Möglichkeit verschlüsselt und direkt (“Peer-to-Peer”) miteinander zu kommunizieren. Dabei werden keine Daten an Dritte weitergegeben oder von Dritten zwischengespeichert. Zusätzlich werden, durch die Nutzung des *Tor*[2]-netzwerks, Metadaten[3] versteckt. Durch die Entwicklung der *Briar Mailbox* wird die Nutzbarkeit von *Briar* im Alltag verbessert und so *Briar* auch interessanter für ein breiteres Spektrum an Nutzer*innen.

Ausführliche Darstellung der Ergebnisse

In der Förderphase wurde sowohl die *Briar Mailbox* als eigenständige Anwendung entwickelt als auch die Funktion der *Briar*-App angepasst um die Kommunikation mit der *Mailbox* zu ermöglichen.

Briar verschlüsselt die Kommunikation zwischen den Nutzer*innen, weshalb es notwendig ist, dass diese einen Schlüssel austauschen. Ebenso ist die Kommunikation zur *Mailbox* verschlüsselt weshalb alle Nutzer*innen, die mit der *Mailbox* kommunizieren, auch hier einen Schlüssel austauschen müssen. Zur Einrichtung der *Mailbox* ist es lediglich erforderlich, dass diese mit einem *Briar*-Account verbunden wird.

Hierfür wurde ein einfacher und sicherer Ablauf, ähnlich dem Kontaktaustausch zwischen zwei *Briar* Nutzer*innen, entworfen und implementiert. Im ersten Schritt wird auf den Geräten ein QR-Code angezeigt, der gegenseitig von der *Mailbox*-App und *Briar*-App mittels der im Mobiltelefon integrierten Kamera ausgelesen wird. Anschließend verbinden sich die Geräte automatisch und sind in der Lage einen sicheren Schlüsselaustausch[4] durchzuführen. Um diesen Prozess möglichst verständlich zu halten und etwaige Fehler der Nutzer*innen zu vermeiden, werden diese über die Benutzeroberfläche interaktiv mit Erklärungen durch die notwendigen Schritte geführt.

Danach werden alle Kontakte der Besitzer*in automatisch über die Existenz der *Mailbox* informiert und ein Schlüsselaustausch mit den Kontakten gestartet. Für diesen Prozess wurde ein eigenes Protokoll[5] implementiert, welches im Hintergrund ausgeführt wird und keine weitere Interaktion erfordert.

Nach dem der Schlüsselaustausch stattgefunden hat können Besitzer*in und Kontakte Nachrichten auf der *Mailbox* zwischenspeichern. Für die sinnvolle Umsetzung dieser Funktion waren Anpassungen und Änderungen an der *Briar*-App notwendig.

---

[2] *https://www.torproject.org/*
[3] Zum Beispiel die Information wer mit wem kommuniziert
[4] Eine detaillierte kryptographische Beschreibung kann hier nachgelesen werden: https://code.briarproject.org/briar/briar-spec/blob/master/protocols/BQP.md
[5] Der detaillierte Ablauf des Protokolls ist hier zu finden: https://code.briarproject.org/goapunk/briar-repeater/wikis/introduction-protocol

Zum einen haben wir ein Kommunikationsprotokoll entwickelt, das die bestehenden Protokolle von *Briar* ergänzt und die Integration der *Mailbox*-Funktionen ermöglicht. Da alle Funktionen der *Mailbox* auf diesem Protokoll basieren, hat dessen Entwicklung einen großen Teil unserer Arbeit ausgemacht.

Zum anderen musste der Umgang mit Verbindungen der *Briar*-App angepasst werden. Die bisher in *Briar* verwendeten Übertragungsmöglichkeiten (*Tor*, *LAN*, Bluetooth) dienen dem direkten Austausch von Nachrichten zwischen den Kommunizierenden. Da die *Mailbox* als Zwischenspeicher eine Ergänzung der bestehenden Verbindungsmöglichkeiten darstellt, werden Nachrichten nach unseren Anpassungen gegebenenfalls über mehrere unterschiedliche Medien übertragen um einen schnellstmöglichen Nachrichtenaustausch zu gewährleisten. Diese Änderungen sind nicht *Mailbox*-spezifisch sondern werden auch für andere geplante Funktionen von *Briar*, wie zum Beispiel eine Übertragung über Funk, benötigt.

All diese Funktionen wurden im Laufe des Projekts in die *Briar*-App integriert und eine eigenständige *Mailbox*-App entwickelt.

Zielgruppe, Nutzen und mögliche Weiterentwicklungen

Als Zielgruppe der *Briar Mailbox* kommen alle bisherigen und zukünftigen *Briar* Nutzer*innen in Frage. Aufgrund der dezentralisierten Kommunikation, welche von Briar genutzt wird, müssen Nutzer*innen bisher gleichzeitig verfügbar sein. Mittels der *Briar Mailbox* können Nutzer*innen in wenigen einfachen Schritten einen privaten Zwischenspeicher für ein- und ausgehende Nachrichten einrichten. Die *Briar Mailbox* ermöglicht somit die Kommunikation zwischen Besitzer*in der *Briar Mailbox* und Kontakten, falls eine der Parteien nicht erreicht werden kann.

Durch die Veröffentlichung des Quellcodes bieten wir interessierten Nutzer*innen die Möglichkeit unsere Arbeit zu verstehen und zu überprüfen. Da wir eine möglichst sichere Implementierung bieten wollen, sind Rückmeldungen und Einblicke in die Entwicklung äußerst wichtig. *Briar*, und damit auch *Briar Mailbox*, richtet sich auch an Nutzer*innen aus Ländern in denen strenge Zensur herrscht. Deshalb sollten Nutzer*innen nachvollziehen können dass *Briar* und *Briar Mailbox* im besten Interesse der Nutzer*innen entwickelt werden.

Das Open-Source Projekt *Briar* besteht seit 2012 und wird auch nach dem Ablauf der Förderphase aktiv weiterentwickelt. Die von uns entwickelte Anwendung *Briar Mailbox* wird ebenfalls als Teil des Projektes weitergeführt und entwickelt. Als nächstes werden wir die in den letzten Monaten entwickelte Software fertigstellen und eine Qualitätskontrolle durchführen, an der auch andere Entwickler*innen von *Briar* beteiligt sind. Anschließend werden wir uns auf die Umsetzung weiterer Funktionen, wie zum Beispiel einer Desktop-Anwendung, konzentrieren.

Durch die Arbeit an der Software konnten wir unsere Erfahrung mit der Android Entwicklung ausbauen und uns tiefgehend mit der Implementierung von *Briar* auseinandersetzen. Von den dadurch gewonnenen Erkenntnisse werden wir bei der weiteren Entwicklung der *Briar Mailbox* und *Briar* auch weiterhin profitieren.

Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

Zu Beginn des Projektes war es geplant mehreren Briar Nutzer*innen zu ermöglichen eine *Briar Mailbox* zu teilen. Damit sollte es der Besitzer*in möglich sein, anderen Nutzer*innen die *Mailbox* als Zwischenspeicher zur Kommunikation mit deren Kontakten zur Verfügung zu stellen. Da *Briar* versteckt wer mit wem kommuniziert, war es wichtig auch bei dieser Funktion keine dieser Informationen Preis zu geben. Da sich aus dem Teilen einer *Briar Mailbox* jedoch eine Beziehung zwischen der Administrator*in und anderen Nutzer*innen derselben *Mailbox* ergibt, müssen zusätzliche Funktionen implementiert werden, um die Geheimhaltung der Beziehungen sicherzustellen. Wir mussten frühzeitig feststellen dass wir diese Funktionen - im zeitlichen Rahmen der Förderung - nicht umsetzen konnten. Dementsprechend haben wir uns vorerst darauf beschränkt, dass eine *Briar Mailbox* nur von ihrer Besitzer*in genutzt werden kann um Nachrichten mit ihren Kontakten auszutauschen.

Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer

Informationen zu *Briar* können unter der Website https://briarproject.org/ gefunden werden. Hier werden auch zukünftig detaillierte Informationen zu der *Briar Mailbox* verfügbar sein. Der Source-Code unseres Projekts ist unter https://code.briarproject.org/goapunk/briar-repeater veröffentlicht. Über die Mailingliste von *Briar* und den offiziellen IRC-Channel können Interessierte auch jederzeit Kontakt zu uns und den anderen *Briar* Entwicklern aufnehmen.

Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Sowohl die Einarbeitungsphase in *Briar* und die vorhandenen Protokolle, als auch die Integration des *Mailbox* Konzeptes in diese hat sich als zeit- und arbeitsintensiver herausgestellt als erwartet. Durch den Mehraufwand bei der Ausarbeitung und Implementierung des Grundgerüsts mussten einige von uns gewünschte zusätzliche Funktionen der *Mailbox* auf die Zeit nach der Förderphase verschoben werden (siehe auch “Zielgruppe, Nutzen und mögliche Weiterentwicklungen”).

Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

Die *Mailbox* ist eine Erweiterung für die bereits existierende Software *Briar*. *Briar* wird aktiv entwickelt und unterlag dadurch fortlaufenden Änderungen. Wir haben während der Entwicklung der *Mailbox* eng mit den Entwickler*innen von *Briar* zusammengearbeitet, um auf dem neuesten Stand zu bleiben und auf für uns relevante Änderungen zu reagieren zu können.