BRIAR Messenger

Einführung	Warum Smartphones?	Aktuelle Projekte	✔ Briar Messenger

Vorwort

Folgende Zusammenfassung ist das Ergebnis eigener Beobachtungen aus dem Einsatz der Briar-App für Android sowie der Analyse folgender Quellen:

- https://briarproject.org/how-it-works/
- https://briarproject.org/manual/
- https://nico.dorfbrunnen.eu/de/posts/2021/diving-at-xmpp/

Der Schwerpunkt dieser Zusammenfassung wurde auf die für den Notfunkeinsatz relevanten Features und Eigenschaften gelegt. Auch wenn sie mit viel Sorgfalt und Zeit erarbeitet wurde, können Fehler nicht ausgeschlossen werden.

Briar

Es ist ein Messenger für Smartphones und Computer mit einer schlichten Benutzeroberfläche, der neben üblichem Nachrichtenaustausch auch interessante Dienste wie Foren und Blogs bietet.

Schwerpunkte

Die App wurde primär für eine Zielgruppe wie Journalisten und Aktivisten entwickelt. Dabei war bei der Konzeption ein besonderer Wert auf abhörsichere und robuste Kommunikation gelegt. Die Abhörsicherheit steht aber kompromisslos an erster Stelle.

- Abhörsicherheit
  - Schutz der Benutzer-Identität und -Beziehungen vor Dritten
  - Schutz von Metadaten
- Robuste Kommunikation durch mehrere Peer-to-Peer Datentransportwege
  - Internet, über das Tor-Netzwerk
  - WLAN, innerhalb eines lokalen Netzwerks
  - Bluetooth, direkt innerhalb der Reichweite
  - Export/Import von Dateien

Transportwege

Generell findet Datenaustausch nur zwischen bekannten Kontakten statt und nur dann, wenn sich beide gegenseitig kennen. Während der Übertragung müssen beide erreichbar sein, da hier keine Infrastruktur für spätere Zustellung eingesetzt wird. Die Kommunikation basiert auf einer Synchronisation der noch ausstehenden Datenpakete zwischen Kontakten. Kontakte können entweder direkt per QR-Code ausgetauscht oder von gemeinsamen Bekannten vermittelt werden. Die App selbst kann von Einstellungen aus mittels WLAN-Hotspot direkt verteilt werden.

Einige der im Nachfolgenden verwendeten Begriffe sollten an dieser Stelle erklärt werden.

- Mit „Daten“ werden generell Daten jeglicher Art gemeint, die zwischen Briar-Instanzen ausgetauscht werden.
- Unter dem Begriff „Nachricht“ wird in der Regel eine personenbezogene Nachricht verstanden, die als Text oder Bild verfasst und als „Daten“-Pakete übertragen wird.
- Mit „Briar-Konto“ wird ein lokal angelegtes, verschlüsseltes Profil gemeint.

Derzeit werden folgende Transportwege unterstützt, die jederzeit vom Benutzer ein- und ausgeschaltet werden können.

- Internet
    - Um eine weltweite Kommunikation zu ermöglichen, aber auch die Identität der Benutzer zu schützen, wird hier über das Tor-Netzwerk ausgetauscht. Dieser Transportweg verbraucht recht viel Energie, da die App immer erreichbar sein muss.
- WLAN
    - Sollte das Internet nicht verfügbar sein, können Daten innerhalb eines lokalen Netzwerks direkt ausgetauscht werden, wenn sich beide Kontakte z. B. im selben WLAN-Netz befinden.
- Bluetooth
    - Sind beide Kontakte in Reichweite, so wird auch über Bluetooth ausgetauscht.
- Externe Datenträger
    - Manueller Export/Import als Datei für alle anderen Transportwege
        - USB-Stick, Packet Radio, …

Briar versucht alle verfügbaren Kommunikationswege parallel zu nutzen, um eine möglichst hohe Verfügbarkeit zu erreichen. Durch den modularen Aufbau der Anwendung können weitere Transportwege hinzugefügt werden. Die App ist quelloffen.

Private Chats

Privatnachrichten, so wie wir sie von anderen Messengern kennen. Die Kommunikation unterliegt folgenden Regeln:

- Nachrichtenaustausch immer nur direkt zwischen Absender und Empfänger
- Es wird nicht über dritte vermittelt, auch wenn es die Erreichbarkeit sehr einschränkt
- Derzeit der einzige Dienst, der einen Versand von (komprimierten) Bildern ermöglicht

Private Groups

Private Gruppen sind auf den ersten Blick auch so realisiert, wie wir sie von anderen Messengern kennen. Da der Datenaustausch aber generell nur unter bekannten Kontakten stattfindet und deswegen nicht alle Mitglieder untereinander kommunizieren können, müssen Gruppeninhaber Nachrichten von jedem Mitglied an alle anderen vermitteln. Hier wird primär ein zentralisierter Ansatz verfolgt. Der Gruppeninhaber bildet das Zentrum des Kommunikationsnetzwerks.

Die Ausbreitung der Nachrichten unterliegt folgenden Regeln:

- Gruppeninhaber
    - ... ist die einzige Person, die neue Mitglieder hinzufügen kann
    - ... ist die einzige Person, die alle Mitglieder direkt kennt
    - ... ist die einzige Person, die mit allen Mitgliedern Daten austauschen kann
    - ... ist generell eine Vermittlungsstelle für jede Kommunikation
    - ... ist der einzig mögliche Kommunikationsweg zwischen unbekannten Mitgliedern
- Bekannte Kontakte können direkten Austausch untereinander einwilligen
    - Ermöglicht eine bessere Erreichbarkeit durch alternative Kommunikationswege
- Inselnetzwerke möglich
    - Zeitweise mehrere Darstellungen bzw. Zustände der Gruppe möglich
    - Nachrichten können beim Zusammenführen in beliebiger Reihenfolge ankommen
    - Der Bezug wird durch die Thread-Darstellung gesichert

Foren

Die Foren sehen auf den ersten Blick wie private Gruppen aus. Der eigentliche Unterschied besteht in der Ausbreitung der Nachrichten und der Sichtbarkeit der Foren selbst. Hier wird ein dezentraler Ansatz verfolgt. Alle Forenmitglieder bilden ein Kommunikationsnetzwerk, das wie ein Baum aussieht, aber mehrfache Kommunikationswege ermöglicht.

Die Ausbreitung der Nachrichten unterliegt folgenden Regeln:

- Der Inhaber kann das Forum an eigene Kontakte selektiv freigeben
- Jedes Mitglied kann das Forum an eigene Kontakte selektiv weiter freigeben
- Mehrere Mitglieder können das Forum an dasselbe Mitglied freigeben
    - Ermöglicht eine bessere Erreichbarkeit durch alternative Kommunikationswege
- Die Ausbreitung der Nachrichten folgt den Freigabeketten in beide Richtungen

Blogs und RSS-Feeds

Jedes Briar-Konto verfügt über ein eigenes Blog, in dem Neuigkeiten veröffentlicht werden können. In diesem Bereich werden eigene, sowie auch Blogs anderer Kontakte in einem Feed angezeigt. Hier ist auch ein RSS-Feed-Reader eingebaut. Es wird ein dezentraler Ansatz verfolgt. Alle Blogmitglieder bilden ein Baumartiges Kommunikationsnetzwerk.

Die Ausbreitung der Nachrichten unterliegt folgenden Regeln:

- Das eigene Blog wird an eigene Kontakte automatisch freigegeben
- Blogs anderer Kontakte können an eigene Kontakte selektiv weiter freigegeben werden
- Jeder Blogeintrag kann im eigenen Blog beantwortet oder weitergeleitet werden
- Die RSS-Feeds verhalten sich wie Blogs anderer Kontakte
- Die Ausbreitung der Nachrichten folgt den Freigabeketten in eine Richtung

Mailbox

Mithilfe einer zusätzlichen App auf einem Zweitgerät, das ständig verfügbar sein muss, können Briar-Benutzer eine Mailbox einrichten, die eine bessere Erreichbarkeit von und für eigene Kontakte ermöglichen kann. Diese kann sowohl eingehende als auch ausgehende Nachrichten

zwischenspeichern und später zustellen, sobald der Empfänger wieder verfügbar ist. Dazu kann z. B. ein weiteres Smartphone mit WLAN-Hotspot verwendet werden, welches an einer externen Stromquelle stationär betrieben wird.

Einsatzmöglichkeiten in Krisen

Da Briar aufgrund der Zielsetzung ausschließlich nur mit bekannten Kontakten kommuniziert, eignet es sich nicht für eine globale, nicht-organisierte Nachrichtenausbreitung, wie wir sie von den Mesh-Netzwerken kennen. Allerdings hat es mit Foren und Blogs das Potential, schon mithilfe eines einzigen Smartphones als WLAN-Hotspots, ein lokales soziales Netzwerk zu werden, welches eine oder (mit etwas mehr Organisation) sogar mehrere Kommunen umfassen kann.

Beispielkonzept:

An einer zentralen Stelle wird ein Smartphone mit einem WLAN-Hotspot autonom betrieben, auf dem ein Briar-Konto der Kommune eingerichtet ist, welches zentrale Auftritte wie offizielle Foren und Blogs verwaltet. Alle Bewohner lassen sich mit dem Kommunenkonto verknüpfen. Vertrauenswürdige Personen können die Briar-Installationsdatei bereitstellen und beim Kontaktaustausch mit dem Kommunenkonto vermitteln. Selbst wenn sich nicht alle Bewohner in WLAN-Reichweite befinden, können ggf. regelmäßig wandernde Bekannte für Datenaustausch sorgen, wenn sie die Foren und Blogs an isolierte Mitglieder direkt freigeben. Sollte es gelingen, weitere Linkstrecken einzurichten, so lassen sich weiter entfernte Inseln oder andere Kommunen anschließen. Hier benötigt man lediglich eine Hierarchie von Kontakten, die Zentren der jeweiligen Kommunen oder Inselgruppen bilden.

Ausblick

Da Briar immer weiterentwickelt wird, könnten in der Zukunft auch andere Transportwege und Features implementiert werden.

Aktuell wird u. A. nach der Einsatzmöglichkeit eines öffentlichen Mesh-Netzwerkes geforscht, bei dem auch Datenaustausch zwischen Unbekannten ermöglicht werden soll:

- https://code.briarproject.org/briar/public-mesh-research/-/wikis/public-mesh-research-report#packet-radio-and-lora

Darüber hinaus gibt es bereits ein Feature Request, einen Rattlegram-ähnlichen akustischen Transportweg zu implementieren, bei dem u. A. auch Funkgeräte zum Einsatz kämen:

- https://code.briarproject.org/briar/briar/-/issues/2441

Forschung und Dokumentation: DO1EG/JO53

Einführung	Warum Smartphones?	Aktuelle Projekte	✘ Briar Messenger

From:
https://notfunkwiki.de/ - **Das NOTFUNK-WIKI**

Permanent link:
https://notfunkwiki.de/doku.php?id=allgemeines:notfunk:smartphone:projekte:briar

Last update: **2023/11/10 14:23**