# Ephemeral Communication

Alexander Biro
Betreuer: Marcel von Maltitz
Seminar Future Internet SS2015
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: alexander.biro@tum.de

## KURZFASSUNG

Im Zusammenhang mit digitaler Kommunikation und Datenverarbeitung ist der Schutz von Daten und privaten Informationen von allergrößter Wichtigkeit. Daten stellen ein wichtiges wirtschaftliches Gut dar: Nutzerdaten können für personalisierte Werbung genutzt werden und detaillierte Informationen über die Produkte anderer Unternehmen, um die Qualität eigener Produkte zu steigern. In dieser Arbeit wird der relativ neue Ansatz selbstlöschender Nachrichten zum Schutz von Daten anhand von bestehenden Diensten vorgestellt und kritisch bewertet. Ziel dieses neuen Ansatzes ist die Nachricht neben bekannten Angreifermodellen (externe Angreifer, Dienstanbieter) nun auch gegen den legitimen Empfänger der Nachricht zu schützen.

Ephemeral Communication stellt durch kurze Lebensdauern der Nachrichten einen sehr interessanten Ansatz zum Schutz der Nachrichten vor dem Empfänger dar. Jedoch ist dieser Ansatz praktisch nur sehr begrenzt umsetzbar, da die sensiblen Inhalte der Nachrichten mit Hilfe von Aufnahmen des Bildschirms, entweder durch Screenshots oder externe Kameras, permanent gespeichert werden können.

## Schlüsselworte

Ephemeral Communication, Vergängliche Kommunikation, Selbstzerstörende Nachrichten, Datenschutz, Security, Privacy

## 1. MOTIVATION

Seit den Enthüllungen von Edward Snowden im Juni 2013 über die Spionage-Aktionen der amerikanischen National Security Agency (NSA) wurde in vielen Staaten vermehrt über Datenschutz diskutiert. [1] Der Schutz von Informationen und Daten beschränkt sich nicht nur auf Ärzte oder Banken, sondern ist für jede Organisation und auch besonders für jede Privatperson von allergrößter Bedeutung.

Beispielsweise ist Datenschutz für ein Softwareunternehmen zum Schutz der eigenen Produkte sehr wichtig. Falls z.B. der Quellcode dieser Produkte frei zur Verfügung stehen würde, wäre die gewinnbringende Vermarktung dieser Produkte schwierig.

Für Automobilhersteller ist auch der Schutz ihrer Konzepte und Ideen wichtig, anderenfalls könnte ein Konkurrent die Autos günstiger nachbauen und das ursprüngliche Unternehmen würde einen großen wirtschaftlichen Schaden davontragen.

Privatpersonen werden auf sozialen Internetplattformen wie Facebook, dazu angehalten möglichst viele persönliche Informationen in das private Profil einzupflegen. Ein Nutzerprofil wird dabei erst als vollständig betrachtet, sobald Informationen zum Wohnort, Beruf, Bildung und weiteres vorhanden sind. Auf Facebook werden täglich mehrere Milliarden Inhalte geteilt [2]. Wenn ein Nutzer hier ein ungünstiges Foto von sich selbst teilt, können sehr viele verschiedene Personen dies sehen. Auch dritte Personen, wie z.B. Arbeitgeber, können unter Umständen die persönlichen Bilder sehen und dadurch negativ beeinflusst werden. Es kann viele Situationen geben, bei denen geteilte Inhalte einer Person schaden können. Aus diesem Grund ist es ratsam nicht nur auf sozialen Plattformen, sondern generell sehr vorsichtig mit seinen privaten Daten und Informationen umgehen.

Dienste wie verschlüsselte E-Mails [3] oder Off-The-Record Messenger [5] bieten Funktionen an, um möglichst sicher miteinander zu kommunizieren. Allerdings können diese beiden Ansätze nicht vor dem Missbrauch der Nachricht durch den Empfänger schützen. Diese Arbeit beschreibt den neuen Ansatz “Ephemeral Communication” zum Schutz von privaten Daten und gibt Beispiele für bestehende Dienste. Anschließend werden die Grenzen und Schwierigkeiten dieser Technik genauer betrachtet sowie eine mögliche Umsetzung am Beispiel von Vanish [30] vorgestellt.

## 2. ANGREIFERMODELLE

Die möglichen Bedrohungen lassen sich in zwei Kategorien einteilen:

- Anbieter des Ephemeral Messaging Dienstes und externe Angreifer

  Versendete Nachrichten werden über die Server des Dienstes zum Empfänger transportiert. Oft erstellen die Server ein Protokoll und archivieren die Nachrichten. Die Anbieter des Dienstes können aus wirtschaftlichen Gründen ein hohes Interesse an den Inhalten versendeter Nachrichten besitzen. Durch die Inhalte der Nachrichten können diese auf die Vorlieben und Gewohnheiten ihrer Nutzer schließen und ihnen personalisierte Werbung und Angebote bieten. Die Anbieter haben oft viele Mitarbeiter aber kein Interesse daran, einem Nutzer direkt zu schaden.

  Externe Angreifer sind Personen, welche sich für die Inhalte der Nachrichten aus persönlichen oder krim-


doi: 10.2313/NET-2015-09-1_01

inellen Gründen interessieren. Diese Angreifer können beispielsweise den Netzwerkverkehr ihrer Opfer mitschneiden (wenn beide sich im selben Netzwerk befinden) um die Nachrichten abzufangen. Diese Personen nutzen die erhaltenen Informationen um ihrem Opfer aktiv zu schaden.

- Empfänger der Nachricht

  Selbst der legitime Empfänger der Nachricht könnte zu einer potentiellen Bedrohung werden. Ein Beispiel-Szenario dazu: Nutzer A schickt eine Nachricht mit einer Aussage, welche ihm zu einem späteren Zeitpunkt schaden könnte, an einen Nutzer B. Somit hat nun B einen Beweis für die Aussage von A und könnte diese später nutzen um A zu schaden. Hätte A seine Aussage in einem natürlichen Gespräch zu B geäußert, hätte B keinen Beweis gegen A.

  Zu dem Zeitpunkt, an welchem eine Nachricht verschickt wird, hat der Empfänger vielleicht noch kein Interesse daran dem Sender damit zu schaden. Der Empfänger hat allerdings die Möglichkeit die Nachricht solange zu speichern und aufzubewahren bis die Nachricht dem Sender schaden kann. Der Sender hat keinen Einfluss darauf und kann die dauerhafte Speicherung der Nachricht nicht verhindern.

  Im folgenden wird nun hauptsächlich der zweite Typus Angreifer (Empfänger) behandelt. Der Schutz vor dem ersten Typus Angreifer lässt sich bereits mit etablierten Methoden (z.B. PGP und Off-The-Record Messaging) bereitstellen.

# 3. WARUM WIRD EPHEMERAL MESSAGING BENÖTIGT?

In diesem Kapitel werden, anhand des im Kapitel 2 bestimmten Angreifermodells, die Grenzen von verschlüsselten E-Mails und Off-The-Record (OTR) Messengern zum Schutz der Privatsphähre dargestellt. Anschließend wird der neue Ansatz “Ephemeral Communication” zum besseren Schutz persönlicher Daten vor dem Empfänger vorgestellt.

Verschlüsselte E-Mails werden oft mit dem freien Pretty-Good-Privacy (OpenPGP) [4] Standard verschlüsselt. PGP verwendet eine asymmetrische Verlüsselung, deswegen muss der Sender dem Empfänger kein Passwort zum Öffnen der Nachricht mitteilen. Die Nachrichten werden mit der digitalen Signatur des Senders authentifiziert und mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Die Nachricht wird direkt am Gerät des Absenders verschlüsselt und in diesem Zustand über die Server des Mail-Anbieters zum Empfänger transportiert. Nur der Besitzer des privaten Schlüssels des Empfängers ist in der Lage die Nachricht zu entschlüsseln. Durch die digitale Signatur kann sich der Empfänger sicher sein, dass die Nachricht nicht gefälscht wurde und tatsächlich vom richtigen Sender stammt. [3]

Niemand bis auf den legitimen Empfänger, kann den Inhalt Nachricht der Nachricht lesen. Der Inhalt der Nachricht ist vor den Anbietern des E-Mail-Dienstes und weiteren Angreifern geschützt. Einer Nachricht werden aus technischen Gründen zum Versand unverschlüsselte Meta-Daten angehängt. In den Meta-Daten einer Nachricht stehen beispielsweise der Absender, der Empfänger, die Zeit des Versands und der Betreff der Nachricht. Anbieter und Angreifer können sehen, dass es zu einer Kommunikation gekommen ist, wissen wer die beiden beteiligten Kommunikationspartner sind, aber nicht über was sie schreiben.

Dieser Ansatz schützt gut gegen Anbieter und Angreifer, aber nicht vor dem Empfänger. Der Empfänger könnte die Nachricht, bewusst oder unbewusst durch einen Mail-Client in entschlüsselter Form auf seinem Computer speichern. Die Nachricht könnte anschließend in falsche Hände gelangen, wenn jemand Zugriff auf den Computer besitzt. Mit Hilfe von Schadsoftware (z.B. Computerviren) könnte diese Nachricht auch automatisch an einen Angreifer weitergeleitet werden. Da der Absender einer verschlüsselten Nachricht durch seine digitale Signatur bekannt ist, kann die Information direkt einer Person zugeordnet werden und er kann den Versand der Nachricht nicht abstreiten. Allerdings besteht auch die Möglichkeit, dass der Empfänger direkt zum Angreifer wird. Er kann die Informationen aus der Nachricht speichern und zu einem späteren Zeitpunkt gegen den Sender einsetzen.

OTR-Messaging wurde entwickelt um vertrauliche und verschlüsselte Kommunikation bei Instant Messaging bereitzustellen. Zusätzlich kann nach einem Gespräch nicht bewiesen werden, dass ein Nutzer eine gewisse Nachricht gesendet hat oder nicht. Das heißt, dass der Versand einer Nachricht bei OTR-Messaging im Nachhinein immer abgestritten werden kann. OTR baut dabei auf die folgenden vier großen Prinzipien: [5]

- Verschlüsselung: Während eines Gespräch kann niemand den Inhalt der Nachrichten mitlesen, denn die Nachrichten werden Ende-zu-Ende verschlüsselt.
- Authentifizierung: Zu Beginn von jedem Gespräch wird mit Hilfe des Digital-Signature-Algorithm (DSA) sichergestellt, dass die Person mit der kommuniziert wird, tatsächlich die ist, für die sie gehalten wird. Die Authentifizierung findet nur am Beginn des Gesprächs mit digitalen Signaturen statt und verwendet den Diffie-Hellman (DH) Schlüssel-Aus-tausch zur Berechnung eines gemeinsamen Schlüssels.
- Abstreitbarkeit: Die beiden Kommunikationspartner besitzen jeweils einen langlebigen, öffentlichen DSA-Schlüssel zur gegenseitigen Verifizierung. Nach der anfänglichen Authentifizierung durch digitale Signaturen, werden folgende Nachrichten, aufgrund der Abstreitbarkeit, mit Message Authentication Codes (MAC's) authentifiziert. Gesendeten Nachrichten wird immer die MAC des Senders beigefügt. Nach dem Versand einer Nachricht berechnet der Sender einen neuen privaten Schlüssel, so dass beide Kommunikationspartner sich gegenseitig immer nur ”alte” Schlüssel veröffentlichen. Der Empfänger der Nachricht kann sicher sein, dass die Nachricht vom richtigen Sender stammt, da für die Berechnung der MAC-Schlüssel der gemeinsame Schlüssel aus dem DH-Schlüssel-Austausch benötigt wird. Gegenüber Fremden kann nicht bewiesen werden, ob eine Nachricht von einem bestimmten Absender stammt, da beide Kommunikationspartner in der Lage waren die MAC's mit Hilfe des gemeinsamen Schlüssels zu errechnen.


doi: 10.2313/NET-2015-09-1_01

- Folgenlosigkeit: Falls es einem Angreifer gelingen sollte den privaten Schlüssel eines Nutzers herauszufinden, kann dieser damit nicht die Nachrichten vergangener Gespräche entschlüsseln. Versendete Nachrichten werden bei OTR nicht mit dem privaten Schlüssel eines Nutzers authentifiziert oder verschlüsselt. Allerdings ist der Angreifer nun in der Lage gefälschte Nachrichten unter dem Namen des Nutzers zu verbreiten. Sobald der Nutzer den Verlust seines privaten Schlüssels mitteilt, verliert die digitale Signatur ihre Gültigkeit und der Angreifer kann keine Nachrichten mehr fälschen.

Durch die Funktionen von OTR lässt es sich bereits sehr sicher im Internet kommunizieren, jedoch gibt es auch Informationen, welche auch ohne die Zuordnung zu einer Person oder einer Sache wertvoll sind. Ein Beispiel dazu wäre folgendes Szenario: Eine Person versteckt sehr viel Geld an einem geheimen Ort für eine zweite Person und verschickt diese Information mit einem OTR-Messenger. Wenn jemand drittes den Inhalt der Nachricht herausfindet, kann dieser die Information auch ohne Bezug zu den Gesprächspartnern nutzen.

Um versendete Nachrichten besser gegen den Empfänger zu schützen wurde der Ansatz "Ephemeral Communication" entwickelt. Mit diesem Ansatz versendete Nachrichten besitzen eine begrenzte, vom Sender bestimmte Lebensdauer. Mit Ablauf dieser Lebensdauer wird die Nachricht dauerhaft gelöscht. Selbst der Empfänger der Nachricht, die Anbieter des Dienstes oder dritte Angreifer haben nach dieser Zeit keine Möglichkeit mehr die Nachricht zu lesen.

Ephemeral Messaging ist das digitale Pendant zu natürlichen, analogen Gesprächen. Alle Sicherheitseigenschaften natürlicher Gespräche sollen bei dem digitalen Gegenstück auch umgesetzt werden. Zu diesen Eigenschaften zählt, dass kein Gesprächsprotokoll erstellt wird. Weiterhin soll es nicht möglich sein im Nachhinein zu beweisen, dass eine Person eine bestimmte Aussage gemacht hat. Darüber hinaus kann, im Gegensatz zu natürlichen Gesprächen, bei Ephemeral Messaging mit Hilfe einer sicheren Ende-zu-Ende Verschlüsselung sichergestellt werden, dass niemand fremdes mitlesen kann. [6]

Ziel von Ephemeral Communication ist der Schutz privater Daten und Nachrichten durch Inexistenz nach einer gewissen Zeit. "Private Daten und Informationen können am besten geschützt werden, wenn keine zu schützenden Daten existieren" [6].

Das folgende Beispiel soll eine mögliche Anwendung von Ephemeral Messaging darstellen. Die Ehefrau A möchte sich von ihrem Ehemann B scheiden lassen und kommuniziert via E-Mail deswegen mit ihrem Scheidungsanwalt C. A und B nutzen Zuhause gemeinsam einen Computer. B könnte sich auf verschiedenen Wegen (z.B. A meldet sich im Postfach an und verlässt später eventuell das Zimmer) Zugang zu dem E-Mail Postfach von A verschaffen. A möchte sicher sein, dass ihr Nachrichtenverlauf mit C sicher ist und B auf keinen Fall mitlesen kann. Mit verschlüsselten E-Mails könnten die Nachrichten nicht geschützt werden, denn diese sind nach der Anmeldung am Postfach, frei zugänglich. Mit Hilfe von OTR-Messengern kann der Versand einer Nachricht abgestritten werden, jedoch aber nicht, dass eine Kommunikation stattgefunden hat. B könnte hier die Nachrichten lesen, aber nicht beweisen, dass A eine gewisse Nachricht gesendet hat. Durch Ephemeral Messaging könnte die Lebensdauer der Nachrichten auf beispielsweise 15 Minuten nach Abruf festgelegt werden. Diese Zeitspanne reicht aus, damit A ihre Nachrichten lesen und antworten kann. Nach dem Ablauf dieser Zeit vernichten sich alle Spuren dieser Kommunikation von selbst und B hat keine Möglichkeit die Nachrichten mitzulesen und etwas über das Vorhaben von A in Erfahrung zu bringen.

# 4. ÜBERBLICK ÜBER BESTEHENDE EPHEMERAL MESSAGING DIENSTE

In diesem Kapitel werden bekannte Ephemeral Messaging Dienste mit ihren wichtigsten Funktionen vorgestellt und kritisch beleuchet:

## 4.1 Snapchat

2011 wurde mit Snapchat die erste Anwendung für mobile Geräte veröffentlicht, welche es dem Nutzer erlaubt, selbstzerstörende Nachrichten zu versenden. Die Anwendung wurde von zwei Informatikstudenten (Evan Spiegel und Bobby Murphy) der Universität Stanford aus den USA programmiert. [9] Vor dem Versenden einer Nachricht entscheidet der Sender, wie lange sie auf dem Gerät des Empfängers angezeigt werden darf. Als Lebensdauer sind nur Werte von einer bis zehn Sekunden möglich. Nach Ablauf der festgelegten Zeit werden die Nachrichten selbstständig von beiden Geräten gelöscht und sind von nun an nicht mehr abrufbar. Snapchat hat dabei den Fokus nicht auf das Versenden von Textnachrichten, sondern von Bildern und kurzen Videos ("Snaps") gelegt. Die App ist für die beiden beliebtesten Betriebssysteme mobiler Geräte (Android und iOS) verfügbar. Heute ist Snapchat mit insgesamt über 100 Millionen Nutzern [10] und 350 Millionen versendeten Snaps pro Tag [11] die beliebteste Anwendung im Ephemeral Messaging Bereich. Bei Snapchat werden alle Nachrichten unverschlüsselt versendet und die Meta-Daten bleiben auch nach dem Ablauf der Lebensdauer erhalten und werden auf den Servern des Anbieters gespeichert. Des Weiteren gibt es die sogenannte "Story"-Funktion, welche es den Nutzern erlaubt persönliche Informationen wie Bilder für 24 Stunden im eigenen Profil zu veröffentlichen, die "Replay"-Funktion um einen Snap pro Tag nach Timeout nochmal sehen zu können und "Discover" um aktuelle Nachrichten zu lesen oder neue Nutzer zu finden. Wenn ein Nutzer einen Screenshot von einer empfangenen Nachricht erstellt, wird dies dem Sender umgehend mitgeteilt. [7] Bei der Anmeldung muss die E-Mail Adresse sowie die Telefonnummer angegeben werden. Beide Informationen werden genutzt um weitere Kommunikationspartner zu finden. [8]

Die fehlende Ende-zu-Ende Verschlüsselung von Snapchat lässt jeden Angreifer und den Anbieter ungehindert bei jeder Nachricht mitlesen und bietet deswegen keinen Schutz gegenüber diesem Angreifermodell. Durch die Replay- und Story-Funktion verliert Snapchat größtenteils die Vergänglichkeit der Nachrichten. Aufgrund der Verletzung der Vergänglichkeit liefert Snapchat nur einen sehr geringen Schutz gegen den Empfänger. Wegen diesen Tatsachen ist Snapchat nicht zum Versand sensibler Botschaften geeignet.


doi: 10.2313/NET-2015-09-1_01

## 4.2 Ansa

Ansa bietet im Gegensatz zu Snapchat eine vollständige Ende-zu-Ende Verschlüsselung, so dass selbst die Anbieter des Dienstes nicht den Inhalt der Nachrichten sehen können. Bei Ansa können Nachrichten entweder im normalen Modus oder im "Off-The-Record"-Modus mit Selbstzerstörung versendet werden. [14] Das Timeout kann hier nicht frei eingestellt werden und liegt immer bei 60 Sekunden. Versehentlich versendete Nachrichten können im Nachhinein durch "Remote Deletion" wieder vom Gerät des Empfängers gelöscht werden. Diese Funktion heißt bei Ansa "Synced Deletion" [12]. Diese Funktion ermöglicht es Nutzern versendete Nachrichten direkt nach dem Versand zu löschen, so dass der Empfänger keine Chance hat diese zu lesen. Nachrichten können aber auch erst nach einigen Minuten oder Stunden gelöscht werden, solange die Nachricht noch nicht durch den Empfänger geöffnet wurde und wegen ihrer begrenzten Lebensdauer bereits gelöscht wurde. Weiterhin wird der Sender einer Nachricht auch bei Ansa benachrichtigt, wenn der Empfänger davon einen Screenshot erstellt hat. Ansa ist bisher, nur für Android und iOS verfügbar. Der Ansa Account wird, wie bei Snapchat, an die E-Mail Adresse sowie an die Telefonnummer gekoppelt. [13]

Ansa bietet seinen Nutzern durch eine sichere Ende-zu-Ende Verschlüsselung und Synced Deletion ein hohes Maß an Sicherheit an. Die Anwendung besitzt alle wichtigen Funktionen um die Privatsphähre möglichst gut zu wahren. Screenshots und Bildschirmaufnahmen sind allerdings auch bei Ansa ein großes Sicherheitsproblem. Darüber hinaus können Nutzer auch Nachrichten verschicken, welche sich nicht automatisch löschen.

## 4.3 Wickr

Wie auch Ansa, bietet Wickr seinen Nutzern eine verlässliche Ende-zu-Ende Verschlüsselung an. [17] Bei Wickr können Nach-richten nur mit einer begrenzten Lebensdauer versendet werden, aber diese ist frei wählbar und lässt sich maximal auf sechs Tage nach dem ersten Öffnen beim Empfänger einstellen. [16] Die Anbieter des Dienstes versprechen, dass keine Meta-Daten der versendeten Nachrichten gespeichert werden. Dieses Versprechen kann jedoch nicht überprüft werden und stellt keine Garantie für die Löschung der Meta-Daten dar. [15] Wickr speichert auch keine Passwörter auf ihren Servern, deswegen kann dieses bei Verlust auch nicht wieder zurückgesetzt werden und das Konto ist nicht mehr zugänglich. Zum Nutzen der Anwendung muss der Nutzer ein Passwort vergeben, dieses wird allerdings nur zum lokalen Starten von Wickr benötigt. [15] Eine weitere Funktion ist, die Remote Deletion wie bei Ansa. Weiterhin besitzt auch Wickr wie Ansa und Snapchat, die Benachrichtigungsfunktion bei Screenshots. Die Messaging Anwendung ist bereits für fast alle Plattformen verfügbar: Windows Desktop, OS X, Linux (32 und 64 Bit), Android und iOS. Bei der Anmeldung fÃijr Wickr, wird weder die E-Mail Adresse noch die Telefonnummer mit dem Account gekoppelt. Diese Einstellung lässt sich später optional vornehmen. [18]

Wickr verspricht seinen Nutzern keine persönlichen Informationen wie echte Namen, Passwörter der Meta-Daten zu speichern. Ob dieses Versprechen wirklich eingehalten wird, lässt sich nicht überprüfen. Nutzer können standardmäßig nur durch ihren Wickr-Benutzernamen gefunden werden und sind so relativ sicher. Da Wickr auf so vielen Plattformen verfügbar ist, besteht das Risiko, dass Nachrichten am Computer geöffnet werden und dort gespeichert werden. Am Computer gibt es einfachere Möglichkeiten den Inhalt des Bildschirms zu speichern, so kann z.B. ein Video der Bildschirmausgabe gespeichert werden.

## 4.4 Frankly Messenger

Der Frankly Messenger bietet keine Ende-zu-Ende Verschlüsselung an, besitzt aber eine Vielzahl an sozialen Funktionen. Zu diesen sozialen Funktionen zählen die Gruppen-Chat-Funktion, Kopplung der App mit Facebook und die Möglichkeit an Kontakte, welche die Anwendung nicht besitzen zu schreiben. Wenn ein Nutzer von Frankly Messenger eine Nachricht mit einer begrenzten Lebensdauer an einen Kontakt, außerhalb von Frankly Messenger (z.B. via E-Mail) schickt, soll sich diese auch automatisch löschen. [21] Wie die Löschung der Nachricht bei dem Versand einer Nachricht zwischen mehreren Diensten funktioniert, wird allerdings nicht von Seiten der Anbieter von Frankly Messenger beschrieben. Aus diesem Grund wird diese Funktion nicht weiter behandelt.

Versendete Nachrichten löschen sich selbst innerhalb von 10 Sekunden nach Abruf, diese Zeitspanne kann nicht verkürzt oder verlängert werden. Zudem ist es auch möglich einzelne, versendete Nachrichten vor der Löschung zu bewahren, indem man den Button mit der Stecknadel beim Erstellen einer Nachricht antippt. Frankly Messenger besitzt zusätzlich auch die Remote Deletion um nachträglich die Nachrichten zu löschen, welche zuvor von der Löschung ausgenommen wurden. Der Gruppenchat innerhalb von Frankly Messenger bietet zusätzlich die Funktion nur die Inhalte der Nachrichten und nicht die Sender anzuzeigen. Das heißt, dass kein Teilnehmer des Gruppenchats genau sagen kann welcher Teilnehmer welche Nachricht gesendet hat. [20] Die App ist für Android und IOS verfügbar. Beim Registrierungsprozess wird der Account mit der Telefonnummer verbunden und jeder Nutzer erhält eine eigene und einzigartige PIN. Die Kopplung mit der E-Mail-Adresse ist optional. Neue Kontakte werden mit Hilfe ihrer PIN hinzugefügt. [19]

Die fehlende Ende-zu-Ende Verschlüsselung schadet der Privatssphähre der Nutzern sehr und ermöglicht Nachrichten im Rahmen des ersten Angreifermodells mitzulesen. In Gruppen-Chats geteilte Informationen sind stärker gefährdet als normale Chats, da hier mehrere Personen theoretisch Screenshots erstellen könnten. Durch die Anonyme Gruppenchat-Funktion kann der Versand einer Nachricht nicht einem gewissen Nutzer zugeschrieben werden. Diese Funktion ähnelt der Funktion von OTR-Messengern.

## 4.5 Privatext

Privatext ist eine minimalistische Ephermeral Messaging Anwendung mit Ende-zu-Ende Verschlüsselung für Android und IOS. Die App kann mit einem Passwort versehen werden, so dass niemand sonst Zugriff auf die privaten Nachrichten erhält. [23] Die Lebensdauer der Nachrichten kann zwischen 30 Sekunden und 24 Stunden frei eingestellt werden. Weiterhin kann eingestellt werden, ob die Zeit ab dem Versand der Nachricht anfängt zu laufen oder erst sobald der Empfänger

diese geöffnet hat. Bei den anderen vorgestellten Diensten beginnt die Zeit erst ab dem öffnen der Nachricht zu laufen. Eine weitere Funktion von Privatext ist "Confirmation Texting", vor dem Absenden einer Nachricht fragt die Anwendung den Nutzer, ob dieser auch sicher den richtigen Kontakt für die Nachricht gewählt hat. Damit soll verhindert werden, dass private Nachrichten versehentlich an die falsche Person gesendet werden. [22, 24] Zudem besitzt auch Privatext eine Remote Deletion Funktion und die Benachrichtigung des Senders bei Screenshots seiner Nachrichten. Der Privatext Account wird nur mit der E-Mail Adresse und einem beliebigen Nickname gekoppelt.

Privatext bietet die Möglichkeit, die Lebenszeit der Nachricht gleich nach dem Absenden zu starten. Außerdem kann die kleine Funktion "Confirmation Texting" verhindern, dass private Informationen aus versehen an falsche Personen gesendet werden. Weiterhin können Nutzer auch den Start der Anwendung mit einem Passwort schützen, sodass wirklich nur der legitime Empfänger in der Lage ist die Nachrichten zu lesen.

Alle vorgestellten Apps sind kostenlos erhältlich und bieten im Kern dieselbe Funktionalität an. Große Unterschiede gibt es hinsichtlich der Frage, ob Verschlüsselung verwendet wird und bei der Länge der Lebensdauer der Nachrichten. Im Augenblick gibt es lediglich für Snapchat aufgrund der großen Beliebtheit Fake-Clients. Wahrscheinlich ist es theoretisch möglich für viele Dienste Fake-Clients zu programmieren um damit die Selbstzerstörung der Nachrichten zu umgehen. Die genaue Funktionsweise der vorgestellten Dienste ist nicht bekannt und aus diesem Grund ist der Nutzer der Anwendungen gezwungen dem Anbieter zu vertrauen.

# 5. GRENZEN UND SCHWIERIGKEITEN

Ephemeral-Messaging-Dienste unterscheiden sich durch die begrenzte Lebensdauer der Nachrichten am deutlichsten von herkömmlichen Messaging-Anwendungen. Hauptziel des Ephemeral Communication Ansatzes ist, dass die Nachrichten unwiederbringlich nach dem Timeout gelöscht werden und die Informationen nicht gespeichert und anschließend weitergegeben oder missbraucht werden können. Dieses Ziel zu erreichen ist überaus kompliziert, denn es existieren mehrere Sicherheits-Probleme welche eine permanente Speicherung ermöglichen.

Beispielsweise können Nachrichten von Snapchat auf verschiedene Wege dauerhaft gespeichert werden. Mit Hilfe einer veränderten Snapchat App (z.B. SaveMySnaps), einem Fake Client können noch ungelesene Nachrichten aus der originalen Snapchat App, ohne Zeitlimit betrachtet und anschließend gespeichert werden. Das funktioniert wie folgt: Der "Angreifer" meldet sich im Fake Client mit den gleichen Log-In Daten, wie in der originalen Anwendung an und findet dort ein ähnliches Interface. Der Sender der Nachricht wird bei einer Speicherung durch SaveMySnaps [25] standardmäßig nicht benachrichtigt und erhält nicht einmal eine Lesebestätigung. SaveMySnaps bietet aber den Versand von Lesebestätigungen an, damit der Absender keinen Verdacht schöpft. [26, 27] Alternativ lassen sich auch bereits geöffnete und durch Snapchat gelöschte Snaps durch Datenwiederherstellungstools sichern. Eine App mit dieser Funktion unter Android heißt Dumpster. [28]

Da es bei Snapchat so viele Möglichkeiten gibt die automatische Selbstzerstörung der Nachrichten zu umgehen, sollten sicherheitsbewusste User zu alternativen Anwendungen greifen. In anderen Anwendungen wie z.B. Wickr, Ansa oder Frankly Messenger wurden noch keine Sicherheitslücken gefunden, welche eine ähnlich einfache Speicherung erlauben. Die versendeten Nachrichten sind allerdings auch hier nicht vollkommen sicher, da der Empfänger sie jederzeit durch Screenshots aufzeichnen kann. Screenshots werden bei vielen Herstellen durch das Drücken einer bestimmten Tastenkombination (z.B. Home-Taste + Ein/Ausschalter bei Samsung) erstellt. Um die Nutzer daran zu hindern Screenshots zu erstellen, müssen diese beim Betrachten von Bildern, mit einem Finger auf den Bildschirm tippen. Das Bild verschwindet entweder nach Ablauf der Zeit oder sobald der Bildschirm nicht mehr berührt wird.

Diese Methode zum verhindern von Screenshots wird "tap-to-view" genannt. Tap-to-view schützt selbstverständlich nicht gänzlich vor Screenshots, aber dadurch werden eventuell weniger Screenshots gemacht. Auf "gerooteten" Android Geräten ist es mit der App "Screenshot HD" [29] möglich Screenshots zeitgesteuert oder durch das Schütteln des Geräts zu erzeugen. "Gerootet" bedeutet, dass der Nutzer Admin-Rechte auf seinem System besitzt. Im Auslieferungszustand haben Android Nutzer keinen administrativen Zugriff auf das System.

Noch einfacher als durch Screenshots, kann man sich durch das Anfertigen einer Fotografie oder eines Films vom Bildschirminhalt des Geräts, während die Nachricht geöffnet ist, gegen über die Selbstlöschung hinwegsetzen. Bei dieser Art des Angriffs wird das sogenannte "analog hole" ausgenutzt. Vor der Ausnutzung des analog hole können sich die Anbieter der Dienste nur sehr schwer schützen. Da der Bildschirm angetippt werden muss, ist wenigstens nicht der gesamte Bildschirm auf dem Foto oder Film erkennbar.

Schwierigkeiten gibt es zusätzlich, wenn die Anwendung auf einer Vielzahl an unterschiedlichen Plattformen funktionieren soll. Die Anwendung Wickr kann beispielsweise auf Windows Phone, Windows Desktop, Mac OS X, Linux, Android und IOS genutzt werden. Auf Android kann die Screenshot-Funktion für die Anwendung deaktiviert werden, bei allen anderen Plattformen aber (noch) nicht. Bei Desktop Systemen gibt es sehr viele Methoden die Bildschirmausgabe zu speichern. Jede Plattform besitzt eigene Besonderheiten und Funktionen und macht es den Entwicklern sehr schwer Probleme einheitlich zu lösen.

# 6. FUNKTIONSWEISE SELBSTLÖSCHENDER NACHRICHTEN AM BEISPIEL VON VANISH

Die meisten Anwendungen veröffentlichen aus sicherheitstechnischen oder wirtschaftlichen Gründen ihren Programmcode nicht. Aus diesem Grund ist es für Außenstehende nicht einfach herauszufinden wie eine Applikation funktioniert. Die genaue Funktionsweise von Closed-Source Software bleibt so geheim.

Im folgenden wird Vanish [30], eine quelloffene Software der University of Washington, vorgestellt. Da bei Vanish der Quellcode der Anwendung frei zugänglich ist, kann die genaue Funktionsweise der Anwendung nachvollzogen werden. Vanisch erlaubt mit Hilfe von verteilten Hash-Tabellen, Nachrichten mit einer festgelegten Lebensdauer zu verschicken. Verteilte Hash-Tabellen (Englisch: Distributed Hash-Table, DHT) werden genutzt, um den Ablageknoten einer Datei in einem Peer-to-Peer Netzwerk zu speichern. Nach Ablauf der festgelegten Lebensdauer der Nachrichten wird die Hash-Tabelle die entsprechenden Einträge entfernen und die Knoten werden die Daten unwiderruflich löschen.

Bei Vanish besteht ein anderes Angreifermodell. Hier halten sich die Empfänger der Nachrichten an das Protokoll und haben kein Interesse an der dauerhaften Speicherung von Nachrichten. Bei Vanish ist das Ziel sich gegen einen externen Angreifer zu verteidigen, welcher sich Zugriff zum Endgerät des legitimen Empfängers verschafft um Nachrichten mitzulesen und zu speichern. (Vergleiche Beispiel zur Scheidung des Ehepaares am Ende des 3. Abschnitts)

Im Folgenden wird das Vorgehen bei der Ver- und Entschlüsselung von Vanish erklärt:

Als erstes wird ein zufälliger Schlüssel K erzeugt, um die zu versendenden Daten D zu verschlüsseln. Hierfür wird eine symmetrische Verschlüsselung genutzt, damit das Verschlüsselte Datenobjekt (Ciphertext) C mit dem gleichen Schlüssel K wieder entschlüsselt werden kann. Dem Nutzer wird dieser Schlüssel nicht mitgeteilt und bleibt geheim.

Dieser geheime Schlüssel K wird nun durch die Anwendung des Secret Sharing Algorithmus von Adi Shamir [32] in N Teile bzw. Shares $(K_1, K_2, \ldots, K_N)$ geteilt. Bei Vanish liegt der Schwellwert standardmäßig bei 90%, das heißt, dass mindestens 90% aller Shares benötigt werden um den ursprünglichen Schlüssel K zu errechnen. Falls mehr als 90% der Shares verloren gehen, kann der Schlüssel nicht mehr errechnet werden und die Daten können nicht entschlüsselt werden. Der Schwellwert kann auch frei eingestellt werden. Je höher dieser Wert eingestellt ist, umso schneller kann der ursprüngliche Schlüßel nicht mehr berechnet werden und die Information ist dauerhaft verloren.

Die errechneten N Shares sollen nun auf die Knoten eines weltweiten Peer-to-Peer (P2P) Netzwerkes verteilt werden. Zur Bestimmung welcher Share des Schlüssels K auf welchen Knoten des P2P-Netzwerks gespeichert wird, generiert Vanish einen zufälligen "Zugriffsschlüssel" L. Aus dem Zugriffsschlüssel werden die Adressen der Knoten, auf denen die Shares gespeichert werden, bestimmt. Die Schlüsselteile (Shares) $(K_1, \ldots, K_N)$ werden an den Positionen, welche durch die Zugriffsschlüssel $(L_1, \ldots, L_N)$ bestimmt werden, in eine verteilte Hash-Tabelle geschrieben. Die Zugriffsschlüssel L werden anschließend alle im Vanishing Data Object (VDO) gespeichert, um später dem Empfänger mitzuteilen wo die Shares gefunden werden können. Beispielsweise wird das Schlüsselteil $K_1$ an der Adresse $L_1$ bzw. $K_N$ an der Stelle $L_N$ des P2P-Netzwerks gespeichert.

Abbildung 1 [30] veranschaulicht wie die Schlüsselteile $K_{1,\ldots,N}$ ent-sprechend dem Zugriffsschlüssel L innerhalb der DHT

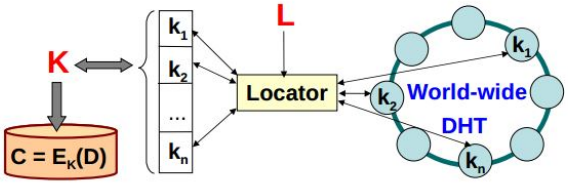


**Abbildung 1: Schematischer Ablauf**

abgespeichert werden. Die Schlüsselteile $K_{1,\ldots,N}$ werden benötigt um den symmetrischen Schlüssel K zur Entschlüsselung der verschlüsselten Daten C zu errechnen.

Die verschlüsselten Daten C werden mit der Anzahl der Schlüsselteile N, den Zugriffsschlüsseln $(L_1, \ldots, L_N)$ und dem Schwellwert zu einem VDO-Object zusammengefasst. Dieses VDO kann anschließend via Mail oder Messenger verschickt werden und ist bis zu einem festgelegten Timeout (beginnend ab Versand der Nachricht) lesbar. Das VDO besteht folglich aus (L, C, N, Schwellwert). Nach dem Time-out wird die DHT die Shares verwerfen und die Datei kann nicht mehr entschlüsselt werden. In die DHT werden immer Tupel bestehend aus den Shares des Schlüssels und einem Wert für ihr Time-out eingefügt. Die DHT durchsucht permanent alle ihre Einträge auf abgelaufene Time-outs und entfernt diese.

Um die Daten D eines VDOs vor dem Ablauf der Lebensdauer lesen zu können müssen als erstes die Zugriffsschlüssel $(L_1, \ldots, L_N)$ aus dem VDO extrahiert werden. Anschließend werden die Shares $(K_1, \ldots, K_N)$ an den Stellen, welche durch die Zugriffsschlüssel angegeben sind, zu dem Schlüssel K zusammengesetzt. Der Schwellwert gibt hier genau an wie viele Shares benötigt werden um K zu errechnen. Mit diesem Schlüssel können nun die verschlüsselten Daten C entschlüsselt und gelesen werden. [30]

Vanish nutzt OpenDHT als P2P-Netzwerk. OpenDHT ist eine öffentliche, verteilte Hashtabelle, das heißt, dass jeder dem Netzwerk beitreten kann. Wenn nun ein Angreifer sehr viele Knoten in dieses Netzwerk einbringt, besteht die Gefahr, dass die Shares beim Verteilen auch auf diese Knoten gespeichert werden. Der Angreifer kann so eventuell alle Shares sammeln und die Daten längerfristig speichern. Durch ein Erhöhen des Schwellwerts zur Rekonstruktion des Schlüssels K kann man dieser Art des Angriffs entgegen wirken. Zusätzlich kann auch die Anzahl N der Shares erhöht werden um die Kosten dieses Angriffs weiter zu steigern. Es besteht jedoch weiter die Gefahr, dass zufällig die benötigte Anzahl an Shares auf den Knoten des Angreifers gespeichert werden. Die genannten Maßnahmen können die dauerhafte Selbstzerstörung der Daten zwar nicht garantieren, aber sie steigern drastisch den Aufwand und die Kosten für den Angreifer. [31]

## 7. SCHLUSSFOLGERUNGEN

Von allen vorgestellten Anwendungen ist Wickr die einzige, welche die Aufnahme des Bildschirminhalts mittels Screenshots auf Android blockiert. Weiterhin gibt der Anbieter des Dienstes das Versprechen, alle Meta-Daten der versendeten

Nachrichten zu löschen und das alle gelöschten Informationen nicht mehr wiederhergestellt werden können. Es kann allerdings nicht überprüft werden, ob tatsächlich alle Spuren des Nachrichtenaustauschs gelöscht werden. Aufgrund der Ende-zu-Ende-Verschlüsselung aller Nachrichten ist Wickr trotzdem mein persönlicher Favorit unter den vorgestellten Anwendungen. Die Anwendung Privatext kann ich ebenso empfehlen, da sie viele sinnvolle Funktionen zum Schutz der Nachrichten bietet, wie z.B. Confirmation Texting und die Passwortsperre für das Starten der Applikation. Die Nutzung von Snapchat kann ich, aufgrund der vielen Möglichkeiten (z.B. Fake-Clients) empfangene Nachrichten zu speichern, nicht empfehlen. Vermutlich kann bei vielen Diensten beispielsweise durch Reverse Engineering ein Fake-Client implementiert werden, welcher eine permanente Speicherung der Nach-richten ermöglicht. Für Snapchat gibt es bereits mehrere Fake-Clients, dies liegt wahrscheinlich an der Tatsache, dass Snapchat der Ephemeral Messaging Dienst mit der größten Nutzerzahl ist.

Wenn in Zukunft auf allen Plattformen ein Weg gefunden wird, die Nutzung von Fake-Clients zu unterbinden, würde dies die Sicherheit der Anwendungen enorm steigern. Zusätzlich müssten möglichst viele Möglichkeiten der Bildschirmaufnahme innerhalb der Ephemeral Messaging Anwendung blockiert werden, um dem Empfänger die Speicherung der Nachricht möglichst schwer zu machen. Darüber hinaus wären Bildschirme, welche aufgrund ihrer Konstruktion oder Oberfläche das Fotografieren der Anzeige erschweren, in diesem Kontext sehr wünschenswert.

Ephemeral Communication ist meiner Meinung nach ein sehr interessanter Ansatz um persönliche Nachrichten und Daten im Internet zu schützen. Diese Lösung schränkt die Nutzung nur wenig ein und liefert kann ein hohes Maß an Sicherheit liefern. Aufgrund von Fake-Clients und der Möglichkeit von Bildschirmaufnahmen aufgrund des “analog hole” bleibt allerdings ein wesentliches Risiko der Datenspeicherung bestehen. Das Konzept wirkt im ersten Moment sehr ansprechend, ist aber aus diesem Grund praktisch nicht umsetzbar.

Besonders schützenswerte und private Nachrichten und Daten sollten trotz selbstlöschender Nachrichten und Ende-zu-Ende-Verschlüsselung nicht über das freie Internet geschickt werden. Es gibt keinen Weg die Sicherheit einer Nachricht in jedem Fall zu garantieren. Aus diesem Grund sollten geheime Informationen am besten von Angesicht zu Angesicht an einem geschützten Ort ausgetauscht werden.

# 8. LITERATUR


[1] *The Guardian: Edward Snowden and the NSA files* http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline, letzter Aufruf: 02.04.2015

[2] *FutureBiz: Facebook Statistiken* http://www.futurebiz.de/artikel/facebook-statistiken-475-mrd-inhalte-werden-taeglich-auf-facebook-geteilt, letzter Aufruf: 05.05.2015

[3] *eMail-Verschlüsselung mit PGP* http://www.elektronikinfo.de/pc/pgp.htm, letzter Aufruf: 05.05.2015

[4] *PGP - Pretty Good Privacy* http://tools.ietf.org/html/rfc2440, letzter Aufruf: 02.04.2015

[5] T. Engel, R. Weis, C. Kordecki *Sichere Nachrichtenübermittlung mit Off-the-Record-Messaging*, Doktorarbeit, 2007, Technische Fachhochschule Berlin

[6] *Apptimate* https://apptimate.io/2014/01/ephemeral-messaging-for-privacy-protection/, letzter Aufruf: 02.04.2015

[7] *Snapchat* https://www.snapchat.com/, letzter Aufruf: 02.04.2015

[8] *Snapchat bei Google Play* https://play.google.com/store/apps/details?id=com.snapchat.android&hl=de, letzter Aufruf: 05.05.2015

[9] *Snapchat Review* http://www.1mtb.com/snapchat-review-and-features-of-the-ephemeral-messaging-app/, letzter Aufruf: 02.04.2015

[10] *Snapchat Nutzerzahlen* http://www.golem.de/news/sexting-dienst-snapchat-hat-100-millionen-nutzer-1408-108835.html, letzter Aufruf: 05.05.2015

[11] *Snapchat Anzahl versendeter Snaps pro Tag* http://www.netzpiloten.de/snapchat-geplatzter-traum-von-loschbaren-daten/, letzter Aufruf: 05.05.2015

[12] *Ansa* http://www.ansa.com, letzter Aufruf: 02.04.2015

[13] *Ansa bei Google Play* https://play.google.com/store/apps/details?id=com.ansa.messenger, letzter Aufruf: 02.04.2015

[14] *Ansa bei TechCrunch* http://techcrunch.com/2013/09/09/ansa-is-a-messaging-app-that-let-you-talk-off-the-record/, letzter Aufruf: 02.04.2015

[15] *Wickr* https://www.wickr.com/, letzter Aufruf: 02.04.2015

[16] *Wickr Review* http://www.1mtb.com/wickr-review-and-features-of-the-ephemeral-messaging-app/, letzter Aufruf: 02.04.2015

[17] *Wickr bei Mashable* http://mashable.com/2013/03/04/wickr/, letzter Aufruf: 02.04.2015

[18] *Wickr bei Google Play* https://play.google.com/store/apps/details?id=com.mywickr.wickr2&hl=de, letzter Aufruf: 02.04.2015

[19] *Frankly Messenger* http://franklyinc.com/, letzter Aufruf: 02.04.2015

[20] *Frankly Messenger Review* http://www.1mtb.com/frankly-messenger-review-and-features-of-the-ephemeral-messaging-app/, letzter Aufruf: 02.04.2015

[21] *Frankly Messenger bei Google Play* https://play.google.com/store/apps/details?id=com.chatfrankly.android&hl=de, letzter Aufruf:

02.04.2015

[22] *Privatext* http://www.privatext.co/, letzter Aufruf: 02.04.2015

[23] *Privatext bei Google Play* https://play.google.com/store/apps/details?id=com.privatext.droid&hl=de, letzter Aufruf: 02.04.2015

[24] *Privatext bei Gigaom* https://gigaom.com/2013/06/24/burn-after-reading-privatext-messaging-app-allows-secure-texts-pictures-to-self-destruct/, letzter Aufruf: 02.04.2015

[25] *SaveMySnaps* http://www.savemysnaps.com/, letzter Aufruf: 02.04.2015

[26] *5 Ways To Save Snapchat Snaps Permanently Without The Senders Knowledge* http://www.1mtb.com/5-ways-to-save-snapchat-snaps-permanently-without-the-senders-knowledge/, letzter Aufruf: 02.04.2015

[27] *Top 5 Apps To Save Snapchat Photos/Videos/Stories On iOS And Android* http://www.1mtb.com/top-5-best-apps-to-save-download-snapchat-photos-videos-stories-ios-android/, letzter Aufruf: 02.04.2015

[28] *Dumpster* http://dumpsterapp.mobi/index.html, letzter Aufruf: 02.04.2015

[29] *ScreenShot HD bei Google Play* https://play.google.com/store/apps/details?id=com.acr.screenshothd, letzter Aufruf: 02.04.2015

[30] R. Geambasu, T. Kohno, A. Levy, H. M. Levy *Vanish: Increasing Data Privacy with Self-Destructing Data*, Proc. of the 18th USENIX Security Symposium, 2009, University of Washington

[31] L. Zeng, Z. Shi, S. Xu, D. Feng *SafeVanish: An Improved Data Self-Destruction for Protecting Data Privacy*, Cloud Computing, Second International Conference, 2010, Huazhong University of Science and Technology

[32] A. Shamir *How to Share a Secret*, Communications of the ACM, Volume 22 Issue 11, 1979, Masssachusetts Institute of Technology



doi: 10.2313/NET-2015-09-1_01