FH Wedel – University of applied science

Geschütztes Chatten über Jabber Server

Bei Prof. Dr. Michael Anders

Torben Fritsch
1.6.2017

Inhalt

Einleitung

Ein sicheres Gespräch über das Internet führen. Ein einfaches Tool zur Kommunikation weltweit. Gibt es so etwas? Und falls ja: Ist es sicher? An diesen Fragen arbeiten Experten seit Jahrzehnten und haben trotzdem noch keine eindeutige Lösung gefunden. Das liegt zum einen an den unterschiedlichen Sicherheitsbedürfnissen der Nutzer und dem konkreten Anwendungsfall und zum anderen an der rasanten technischen Entwicklung und dem damit verbundenen Wettrüsten der Beteiligten. Prominente Beispiele haben gezeigt, dass es immer wichtiger wird seine persönlichen Daten zu schützen. So machen sich mehr und mehr Menschen Gedanken um ihre Privatsphäre. Der Bedarf an sicheren Kommunikationsmöglichkeiten wird voraussichtlich weiter steigen und es gibt tausende Anwendungen auf dem Markt. Diese Seminararbeit beschäftigt sich mit der sicheren Kommunikation im Sofortnachrichtenbereich über Jabberserver mit OTR Verschlüsselung und die damit verbundenen Vor- und Nachteile gegenüber herkömmlichen „Chat-Apps“.

TOR, XMPP (Jabber), Pidgin und OTR

Um die Thematik verständlich erklären zu können, müssen im Voraus einige Programme und Techniken erklärt werden, die im Folgenden benutzt werden:

TOR (**T**he **O**nion **R**outer)

“The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy.” (Tor - Official Site, 2017)

Das Tor Netzwerk hilft dabei, die eigene Privatsphäre zu schützen, indem es die IP-Adresse des Benutzers verschleiert und die Anfrage verschlüsselt. Das geschieht, indem die zu verschickende Information erst über mehrere sogenannte Knoten geschickt wird, ehe sie beim Empfänger ankommt. Durch diese Dezentralisierung und immer wechselnden Knoten ist es fast unmöglich herauszufinden, wer der ursprüngliche Absender war (siehe Schwachstellen)

XMPP (Jabber)

“Jabber is the original open instant messaging (IM) technology, invented by Jeremie Miller in 1998 and formalized as the Extensible Messaging and Presence Protocol (XMPP) by the IETF as an Internet Standard for IM and presence.” (Jabber.org, 2017)

Das XMP-Protokoll, früher Jabber, ist ein Standard für Sofortnachrichten über das Internet. Grundlage ist dabei eine Freundesliste, in die man Bekannte einträgt. Der große Vorteil von XMPP ist die Plattform- und Anbieterunabhängigkeit. Es gibt hunderte von Clientprogrammen und der Anbieter kann frei ausgesucht werden. Außerdem ist das Protokoll für Jedermann einsehbar (open source). Viele Firmen nutzen XMPP zur Kommunikation, da andere Dienste teilweise fragwürdige AGBs mit sich bringen.

Pidgin

“Pidgin (formerly named Gaim) is a free and open-source multi-platform instant messaging client, based on a library named libpurple that has support for many instant messaging protocols, allowing the user to simultaneously log into various services from one application.” (Wikipedia The Free Encyclopedia, 2017)

Pidgin ist eines der oben erwähnten Clientprogramme und ist mit dem XMPP Netzwerk kompatibel. Das dieses Programm die gleichzeitige Nutzung mehrerer Services erlaubt interessiert in diesem Fall nicht, da sich hier nur mit XMPP beschäftigt wird. Pidgin wird deshalb häufig als Clientprogramm benutzt, da es durch Plug-Ins stark erweitert werden kann. Die Alternative für Mac OS X heißt Adium und funktioniert nach demselben Prinzip.

OTR

“Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing: Encryption […], Authentication […], Deniability […], Perfect forward secrecy […].” (Off-the-Record Messaging - Official Site, 2017)

OTR ist ein Protokoll zur Verschlüsselung von Nachrichten im Instant Messaging Bereich. Über einen Plug-In kann Pidgin eben diese Technik nutzen um eine verschlüsselte Übertragung zu gewährleisten. Der größte Vorteil bei diesem Verfahren ist die so genannte glaubhafte Abstreitbarkeit, bei der nach Beendigung der Unterhaltung (und auch zwischen den Nachrichten) niemand beweisen kann, dass ein Chatpartner eine bestimmte Nachricht geschrieben hat (siehe FunktionsweiseFunktionsweise).

Funktionsweise

Das Herzstück der sicheren Kommunikation bei der Verwendung von Pidgin als Client zum Nachrichtenaustausch über XMPP ist das durch das Plug-In nutzbare OTR Protokoll. Dieses bietet eine **Verschlüsselung/Encryption** (Niemand kann die Nachrichten mitlesen), **Beglaubigung/Authentication** (Man kann sich sicher sein, dass der Empfänger derjenige ist, für den man ihn hält), **Abstreitbarkeit/Deniability** (Es kann nach dem Gespräch nicht bestimmt werden, wer die Nachrichten verfasst hat) und **Folgenlosigkeit/Perfect forward secrecy** (Die Nachrichten können nachträglich nicht entschlüsselt werden), der Kommunikation. (vgl. Borisov, Goldberg, & Brewer, 2004)

Vor allem die letzten beiden Punkte unterscheiden diese Art des Nachrichtenaustausches von vielen anderen Varianten.

Zu Beginn des Gesprächs muss ein sicherer Verbindungskanal geschaffen werden bzw. initiale Schlüssel ausgetauscht werden. Dies geschieht über einen *Authenticated Key Exchange (AKE)* und wird mit dem SIGMA-Protokoll umgesetzt. Über einen Diffie-Hellman-Schlüsselaustausch wird ein sicherer Kanal geschaffen, über den sich jeder Kommunikationsteilnehmer mit Hilfe einer digitalen Signatur identifiziert. Ist diese Authentifikation erfolgreich, werden die weiteren Nachrichten mittels Advance Encryption Standard verschlüsselt und mit einem Message Authentification Code (MAC) authentifiziert.

Hierbei ensteht ein Teil der Abstreitbarkeit dadurch, dass jeder, der einen MAC verifizieren kann, ihn auch produzieren kann. Außerdem liefern die verwendeten Funktionen bei gleichen Initialwerten die gleichen Ergebnisse. Auf ein Beispiel übertragen bedeutet das:

Nimmt man zwei Gesprächspartner Alice und Bob an, so würde Alice ihren Nachrichten mit Hilfe eines Message keys (MK) durch einen Hash-Algorithmus einen MAC-tag hinzufügen, den Bob auf die gleiche Weise mit dem selben MK verifizieren kann. Passen die Werte zusammen, weiß Bob, dass jemand mit dem gleichen MK die Nachricht geschrieben hat. Ist er sich außerdem sicher, dass nur Alice diesen MK besitzt, kann er darauf schließen, dass die Nachricht von ihr stammt. Gegenüber einer dritten Person (Eve) kann Bob aber nicht beweisen, dass er die Nachrichten nicht selbst geschrieben hat. So entsteht eine Abstreitbarkeit für Alice.

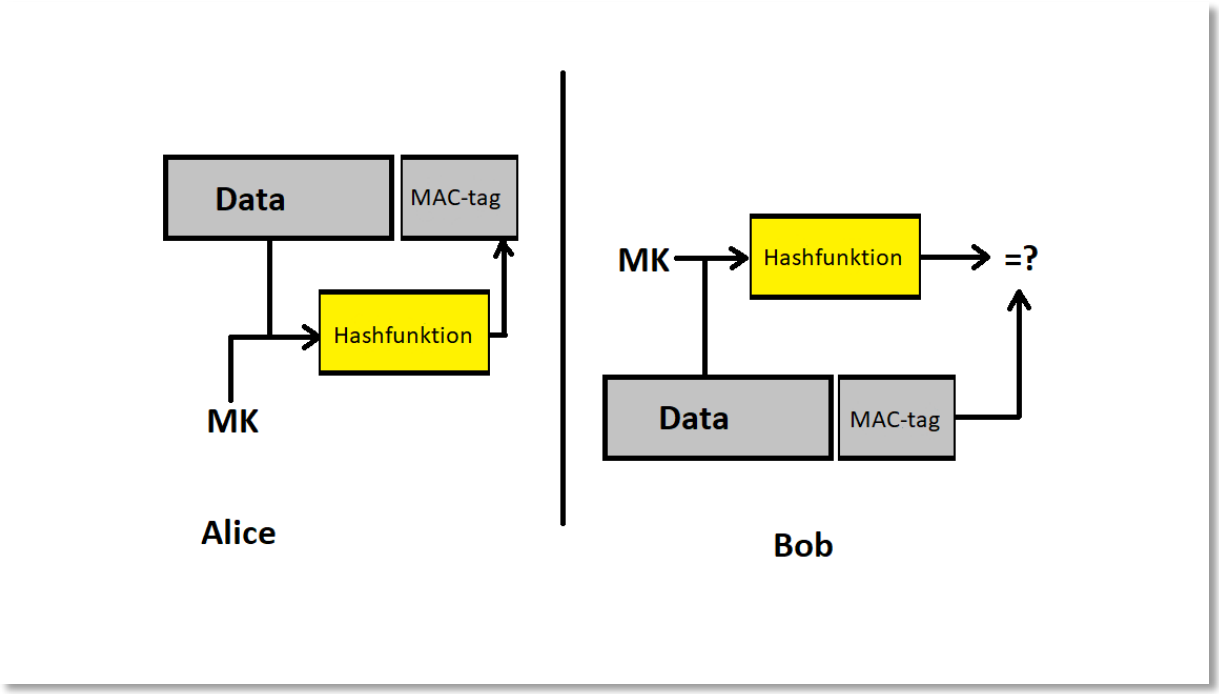

Abbildung 1: MAC Operation, übernommen aus: https://youtu.be/uI1x-z5oafc (YouTube.com, 2008)

Eine weitere, stärkere Abstreitbarkeit entsteht, da die benutzten MKs bei der nächsten Nachricht veröffentlich werden. So kann jeder, der die Unterhaltung liest, diese reproduzieren. Durch ein ständiges Neuwählen von MK (re-keying) durch einen Diffie-Hellman-Schlüsselaustausch und dem Löschen aller anderen Werte, die zur Entschlüsselung der Nachricht notwendig sind, entsteht eine Folgenlosigkeit, weil die Nachrichten von niemandem (auch nicht von Alice oder Bob) wieder gelesen werden können. Dieses Fenster zwischen zwei Schlüsseln sollte möglichst klein gehalten werden. Weil die zum Schlüsselaustausch notwendigen mathematischen Operationen aber relativ simpel sind, ist dies ohne weiteres möglich.

Vor- und Nachteile von OTR

Die größten Vorteile, die OTR von anderen Protokollen unterscheiden, sind die Abstreitbarkeit und die Folgenlosigkeit. Obwohl eine Zuordnung des Autors zu einer Nachricht oft auch gewünscht ist (wie z.B. bei Verträgen), so ist es genau diese Eigenschaft, die man in einem normalen Gespräch auch nicht wiederfindet. Genauso verhält es sich mit der Folgenlosigkeit: Eine vergangene Konversation kann (und soll vielleicht auch) nicht später noch nachvollzogen werden.

Ein weiterer Vorteil des OTR Protokolls ist, dass es einfach über bestehende Protokolle gelegt werden kann. Dafür muss in Pidgin nur ein Plug-In heruntergeladen und aktiviert werden, in anderen Clients wie zum Beispiel Adium (für Mac OS X) ist OTR schon vorinstalliert. Des Weiteren ist OTR sehr einfach zu benutzen und dazu noch effektiv. Lediglich die erste Autorisierung muss sehr sorgfältig durchgeführt werden und kann durch eine out-of-band authentication erfolgen. Dabei wird ein gemeinsames Geheimnis über einen anderen Weg, als den gerade benutzten, mitgeteilt, zum Beispiel durch ein persönliches Treffen. Einmal authentifiziert werden die nötigen Berechnungen im Hintergrund durchgeführt, die dafür sorgen, dass das Gespräch die gleichen Eigenschaften hat, wie eine persönliche Unterhaltung. So gut die Abstreitbarkeit auch ist, muss aber auch klar sein, dass diese nur so gut ist, wie die einer in Klartext geschriebenen Nachricht auch.
Ein Nachteil der Technik ist, dass die Parteien interaktiv miteinander kommunizieren müssen. Es muss ein erster Austausch stattgefunden haben, bevor die Unterhaltung überhaupt beginnen kann, was es unpraktisch für den Gebrauch im E-Mail Bereich macht. Dieses Problem ist im Instant Messaging (IM) Bereich nicht von so großer Bedeutung, da meistens nur mit Partnern kommuniziert wird, die online sind.

Anwendung

Anwendung findet diese Technik vor allem im IM aufgrund der genannten Vor- und Nachteile. Am weitesten verbreitet ist die Kommunikation über XMPP und zusätzlichem OTR Plug-In. Es gibt inzwischen hunderte von XMPP-Servern und ebenso viele Clientprogramme mit unterschiedlichsten Vor- und Nachteilen. Unter Windows und Linux hat sich Pidgin als gute Standartsoftware etabliert, bei Apple Nutzern ist Adium weit verbreitet.
Ziel einer sicheren Unterhaltung ist auch die Anonymität, deshalb reicht es nicht aus das OTR Protokoll über seinen XMPP Chat zu legen. Wichtig ist auch, dass der Account, den die Gesprächspartner erstellt haben keine Verbindung zu ihnen selbst aufweist. Ein Angreifer könnte die Internetaktivität beobachten und würde feststellen, dass die gleiche IP Adresse für die „sichere“ Unterhaltungen und „normale“ Nutzung verwendet wird. Der einfachste und sicherste Weg seine IP Adresse zu verstecken ist TOR zu benutzen (vgl. Lee, 2015). Dabei ist allerdings penibel darauf zu achten, dass TOR nicht nur bei der Erstellung des Accounts, sondern auch bei der Benutzung benutzt wird. Des Weiteren darf auch der Benutzername keine Beziehung zum Benutzer aufweisen.

Schwachstellen

Selbst wenn alle Sicherheitsvorkehrungen getroffen wurden, gibt es immer noch potenzielle Schwachstellen. Eine davon ist das TOR Netzwerk. Ist ein Angreifer in der Lage das gesamte Netzwerk bzw. eine große Zahl an Endknoten zu kontrollieren, könnte er einzelne Benutzer de-anonymisieren. Allerdings ist selbst die gemeinsame Spionagepower der „Five Eyes“ (die USA, Großbritannien, Kanada, Australien und Neuseeland) dazu nicht in der Lage (Stand 2012) (Greenwald, 2013).

Eine weitere Schwachstelle ist der Computer der Gesprächspartner. Wird dieser gehackt, bringt es nichts eine Verschlüsselte Unterhaltung zu führen. Denn wenn der Angreifer jeden Tastenanschlag registrieren und den Bildschirm sehen kann, hilft einem auch die beste Verschlüsselung nicht weiter. Eine Möglichkeit seine Kommunikation zu schützen, ist einen separaten Computer nur für diese Art der Unterhaltung zu benutzen. Eine andere Variante ist die Benutzung des Betriebssystems Tails, welches man von einem USB Stick aus starten kann. Beides verringert die Chance, dass der Computer gehackt wird.

Sicherheitslücken bei verbreiteten „Chat-Apps“

Fast jeder benutzt eine oder mehrere Chat Apps. In Sachen Sicherheit und Datenschutz unterscheiden sich die Programme leider nicht allzu stark und weisen teilweise gravierende Sicherheitslücken auf. Die am weitesten verbreiteten sind: WhatsApp, Facebook Messenger und Snapchat. Wie sicher diese Anwendungen sind, soll im Folgenden betrachtet werden:

WhatsApp

Obwohl WhatsApp eine Ende-zu-Ende Verschlüsselung anbietet gibt es noch viele Punkte, die aus Datenschutzsicht sehr kritisch zu sehen sind. So werden unter anderem die Adressbücher der Nutzer zentral auf einem Server gespeichert und können miteinander abgeglichen werden. Außerdem sind trotz der Verschlüsselung die Metadaten der Unterhaltung weiterhin lesbar und werden unverschlüsselt übertragen (Spiegel.de, 2016).

Auch die Browserversion der Anwendung weist Sicherheitslücken auf. Auf einfachste Art und Weise ist es möglich das Profilbild, den Online-Status und den Profiltext jedes WhatsApp-Nutzers herauszubekommen, obwohl die Telefonnummer nicht im Telefonbuch abgespeichert ist (Spiegel.de, 2016).

WhatsApp-Mutter Facebook behauptet zwar es handle sich um ein gewolltes Feature, überzeugend klingt das allerdings nicht. Die User können sich durch Änderungen in den Einstellungen dagegen schützen, müssen sich allerdings darauf gefasst machen, dass nach jedem Update die Grundeinstellungen zurückgesetzt sind.

Facebook Messenger

Neben vielen weiteren Bedenken ist beim Facebook Messenger auch die Klarnamenpflicht ein Grund, warum die Anwendung nichts für Leute ist, die sich anonym unterhalten wollen. Außerdem ist eine automatische Standortbestimmung bei jeder Nachricht voreingestellt, die erst deaktiviert werden muss. Auch bei dieser Anwendung gibt es (wahrscheinlich auch auf Grund des gleichen Mutterkonzerns) eine Ende-zu-Ende Verschlüsselung. Aber auch hier werden nur der Nachrichtentexte und nicht die eigentlich viel interessanteren Metadaten verschlüsselt. Gerade auch die Tatsache, dass Facebook mit dem Verkauf von Nutzerdaten einen großen Teil seines Umsatzes generiert lässt nicht darauf hoffen, dass sich diese Praxis ändern wird.

Wie auch WhatsApp verlangt der Facebook Messenger bei der Installation sehr viele Zugriffsrechte, über deren Nutzen diskutiert werden sollte. Sicherlich ist für ein angenehmes Chaterlebnis einiges an Rechten erforderlich, allerdings macht ein voller Zugriff den Nutzer auch angreifbar. Auf der einen Seite braucht die App Zugriff auf das Mikrofon, um Sprachnachrichten zu versenden, auf der anderen Seite könnte das aber auch zum Abhören missbraucht werden.

Snapchat

Etwas neuer ist die App Snapchat, bei der sich die User Bilder schicken, die nach wenigen Sekunden nicht mehr aufrufbar sind. Gerade das Versprechen, dass die Bilder nach wenigen Sekunden wieder gelöscht werden veranlasst einige Benutzer zum Versenden unvorteilhafter Bilder. Allerdings können die Bilder ohne viel Aufwand von Dritten wiederhergestellt werden und sind somit nicht wirklich gelöscht (Zeit.de, 2014).

Auch hat Snapchat eingeräumt Bilder an US-Behörden weiterzugeben (Snap.com, 2013) und auch die AGBs lassen auf einen eher lockeren Umgang mit Nutzerdaten schließen (Snap.com, 2017). In jedem Fall ist Snapchat kein sicheres Kommunikationswerkzeug und die Dateien sind nicht so flüchtig, wie es den Anschein haben mag.

Fazit

Wer Wert auf eine sichere, anonyme Kommunikation legt, kann sich nicht auf die heutzutage weit verbreiteten „Chat-Apps“ verlassen, sondern muss andere Wege suchen. Das Chatten über Jabber/XMPP Server und OTR Plug-In ist dabei eine sehr gute und vor allem einfache Möglichkeit ein hohen Grad an Sicherheit zu erreichen. Man muss sich ein wenig mit dem TOR Netzwerk beschäftigen und wissen, wie man Software sicher aus dem Internet herunterladen kann. Die gesamte Berechnung für z.B. den Diffie-Hellman Schlüsselaustausch passiert dann aber im Hintergrund, sodass auch unerfahrene Personen die Technologie nutzen können. In Zeiten der immer stärkeren Überwachung, wird das Sicherheitsbewusstsein weiterwachsen und sichere Kommunikation ein immer größerer Faktor werden. Insofern wird auch die Anzahl der Personen steigen, die Jabber/XMPP Server nutzen. Es ist wichtig zu wissen, dass es Möglichkeiten zur sicheren Kommunikation gibt, sollte man diese nutzen wollen/müssen.

Literaturverzeichnis

Borisov, N., Goldberg, I., & Brewer, E. (09. September 2004). Off-the-Redord Communication, or, Why Not To Use PGP.

Greenwald, G. (2013, Oktober 4). NSA and GCHQ target Tor network that protects anonymity of web users. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption

Jabber.org. (26. Mai 2017). Von https://www.jabber.org/faq.html#jabber abgerufen

Lee, M. (14. Juli 2015). *The Intercept*. Von https://theintercept.com/2015/07/14/communicating-secret-watched/ abgerufen

List of public XMPP servers. (27. Mai 2017). Von https://list.jabber.at/ abgerufen

Off-the-Record Messaging - Official Site. (26. Mai 2017). Von https://otr.cypherpunks.ca/ abgerufen

Snap.com. (14. Oktober 2013). Von https://www.snap.com/en-US/news/post/who-can-view-my-snaps-and-stories/ abgerufen

Snap.com. (10. Januar 2017). Von https://www.snap.com/de-DE/terms/ abgerufen

Spiegel.de. (06. April 2016). Von http://www.spiegel.de/netzwelt/apps/whatsapp-verschluesselung-gut-aber-nicht-komplett-abhoersicher-a-1085726.html abgerufen

Tor - Official Site. (2017, Mai 26). Retrieved from https://tor.eff.org/about/overview.html.en

Welt.de. (13. Mai 2017). Von https://www.welt.de/wirtschaft/webwelt/article164531727/Diese-WhatsApp-Sicherheitsluecke-ist-eine-Einladung-fuer-Kriminelle.html abgerufen

Wikipedia The Free Encyclopedia. (26. Mai 2017). Von https://en.wikipedia.org/wiki/Pidgin_(software) abgerufen

YouTube.com. (13. Mai 2008). Von https://youtu.be/uI1x-z5oafc abgerufen

Zeit.de. (9. Mai 2014). Von http://www.zeit.de/digital/datenschutz/2014-05/snapchat-datenschutz abgerufen