Verschlüsseltes Instant Messaging

CryptoParty Dresden

6. Dezember 2012

Instant Messaging, beispielsweise über ICQ, ist standardmäßig unverschlüsselt. Das heißt, jeder Lauscher auf der Leitung kann im Klartext lesen, welche Nachrichten Du schreibst und bekommst. Mit ein paar kleinen Vorkehrungen lässt sich das aber leicht verhindern

Off-the-Record Messaging (OTR)

OTR ist ein Protokoll, um Instant Messaging zu verschlüsseln. Doch darüberhinaus bietet eine mit OTR verschlüsselte Nachricht auch Abstreitbarkeit, das heißt, dass Nachrichten nur zum Zeitpunkt der Unterhaltung zwischen den Teilnehmern nachweisbar dem Sender zugeordnet werden können. Die Signierung ist nur gegenüber dem Empfänger der Nachricht glaubwürdig, der Empfänger selbst könnte nämlich nach Erhalt der Nachricht die Signatur einfach nachmachen, kann so also gegenüber Dritten nicht glaubhaft machen, dass Du ihm diese Nachricht geschrieben hast und nicht er selbst. Außerdem ist die Kommunikation via OTR auch bei Verlust eines privaten Schlüssels folgenlos, da dieser nur zur Erzeugung der vorübergehenden privaten Schlüssel dient, mit dem die einzelnen Nachrichten dann signiert werden.

Benutzung von OTR

Eine der einfachsten Methoden, OTR zu benutzen, ist besipielsweise mit Pidgin[1]. Pidgin ist ein freier Instant Messaging Client, der eine Vielzahl von Chat-Protokollen unterstützt (ICQ, XMPP, AIM, mit Plugins auch z.B. Skype und Twitter).

[1] https://pidgin.im/

Für Pidgin ist ein OTR-Plugin verwendbar, dass es ermöglicht, jede mit Pidgin geführte Unterhaltung zu verschlüsseln, wenn das Gegenüber auch OTR versteht. Installieren lässt sich das Plugin einfach über das Plugin-Menü[2]. Alternativ kann es über die OTR-Website heruntergeladen und mit dem Installer (unter Windows) installiert werden[3].

[2] Werkzeuge - Plugins

[3] http://www.cypherpunks.ca/otr/

Andere Instant Messaging Clients, die OTR unterstützen sind Adium (Mac OS X), Gajim und Gitterbot (Android-Geräte).

Ein Browser-Plugin, dass es ermöglicht, OTR-verschlüsselte Unterhaltungen mit mehreren Teilnehmern gleichzeitig in einem Chat-Raum zu führen, ist Cryptocat[4]. Nach Installation des Plugins lassen sich einfach Chaträume erstellen, denen jeder ohne Registrierung beitreten kann, um dann sicher zu kommunizieren.

[4] https://crypto.cat

EIN KOMMENTAR ZUM SCHLUSS: All der Aufwand lohnt sich nicht, wenn die Mitschnitte, der via OTR verschlüsselten Gespräche im Klartext auf der Festplatte hinterlegt werden, auf dem eigenen Rechner oder dem des Gesprächspartners. Also Gesprächsmitschnitte ausschalten oder auch verschlüsseln!