

Jabber-Kurzeinführung

Svenja (Open Source AK)

KISS WS13

1 Warum Jabber?

- Dezentral: Du kannst zwischen vielen kompatiblen Anbietern wählen (wie bei E-Mail)
- Du musst nicht alle Rechte über deine Chatnachrichten abgeben
- Die Nachrichten werden verschlüsselt an den Server geschickt, niemand im Netzwerk kann mitlesen
- Außerdem: Als Studi bekommst du einen RWTH-Jabber-Account

2 Clientsoftware

- Pidgin
 - Mit dem LIP-Installationsskript vorinstalliert
 - Unterstützt Jabber, ICQ, MSN, Google Talk, Facebook Chat und viele mehr
 - Unterstützt Verschlüsselung mit OTR
- Reine Jabberclients, z.B. Psi, Gajim
- Multi-Messenger Clients, z.B. Empathy, Kopete, Jitsi

3 Jabber-Account registrieren

Studentischer Jabber-Server der RWTH

- Für Studenten, Mitarbeiter,... der RWTH
- Anmeldung unter <http://jabber.rwth-aachen.de> mit RWTH-E-Mail-Adresse
- Account in Pidgin einrichten: siehe „Account in Pidgin registrieren“ (natürlich ohne das Häkchen)

Öffentliche Jabber-Server

- z.B. jabber.org oder jabber.ccc.de
- mehr Jabber-Server: <http://www.jabberes.org/servers/>
- Account in Pidgin registrieren:
 - Konten → Konten verwalten
 - Hinzufügen...
 - Protokoll: XMPP
 - Benutzer: gewünschter Nutzernamen
 - Domain: Adresse vom gewünschten Jabberserver, z.B. jabber.ccc.de
 - Ressource: könnt ihr frei lassen
 - Passwort: selbsterklärend
 - Häkchen bei „Dieses neue Konto auf dem Server anlegen“
 - „Hinzufügen“ klicken, nochmal Nutzernamen und Passwort bestätigen

4 Verschlüsseln mit OTR (Off-the-Record Messaging)

Warum OTR?

- Verschlüsselung: Niemand (auch nicht der Serverbetreiber) liest mit
- Authentifizierung: Es ist garantiert, dass sich niemand anders als dein Gesprächspartner ausgibt
- Abstreitbarkeit: Niemand kann dir nachweisen, was du geschrieben hast (das ist bei anderen Verschlüsselungsmethoden anders)
- Folgenlosigkeit: Wenn du oder dein Gesprächspartner den Schlüssel verliert, kann trotzdem niemand vergangene Gespräche entschlüsseln

OTR einrichten

- Paket `pidgin-otr` installieren
- Unter Werkzeuge → Plugins „Off-the-Record Messaging“ aktivieren
- Button Plugin konfigurieren anklicken
- Generieren anklicken (gegebenenfalls weitere Einstellungen)
- Wenn der Schlüssel generiert wurde (kann etwas dauern) wird ein Fingerprint angezeigt. Damit wird dein Schlüssel eindeutig identifiziert.
- Fenster schließen. Du hast nun einen Schlüssel, mit dem du OTR nutzen kannst

Verschlüsselt Chatten

- Im Chatfenster: OTR → Private Unterhaltung starten
- Beim ersten verschlüsselten Gespräch authentifizieren (sicherstellen, dass du mit dem richtigen Gegenüber redest):
 - Rechts unten im Chatfenster Unverified → Authenticate Buddy anklicken
 - Verifizieren über Frage und Antwort: Frage und Antwort eingeben. Die Antwort sollte natürlich nur dein Gegenüber wissen
 - Gemeinsame bekannte Passphrase: Geheimnis eingeben, das vorher mit dem Gegenüber abgesprochen wurde
 - Manueller Fingerprint-Vergleich: Über sicheren Kanal (z.B. persönliches Gespräch) Fingerprint vergleichen
 - Bei allen Methoden darf natürlich das Geheimnis nicht einfach vorher über den verschlüsselten Chat übertragen werden ;-)