Off-the-Record Messaging

Agenda

1. Wozu OTR?
2. Funktionsweise
    1. Einführung
    2. Verschlüsselung
    3. Authentifizierung
    4. Abstreitbarkeit
    5. Folgenlosigkeit
3. Verwendung im Alltag
4. Aussichten
5. Quellen und Verweise

Wozu OTR?

- „Sicheres“ Chatten dank Verschlüsselung
- Authentifizierung des Gesprächpartners

Wachsende Datenschutzsensibilität

(Vorratsdatenspeicherung, …)

Funktionsweise - Übersicht

- Nicht an Protokolle sondern Clients gebunden
- Protokoll muss nur kodierten Text austauschen
- OTR-Sessions
  1. Authentifizierung
  2. Verschlüsselung

Verschlüsselung

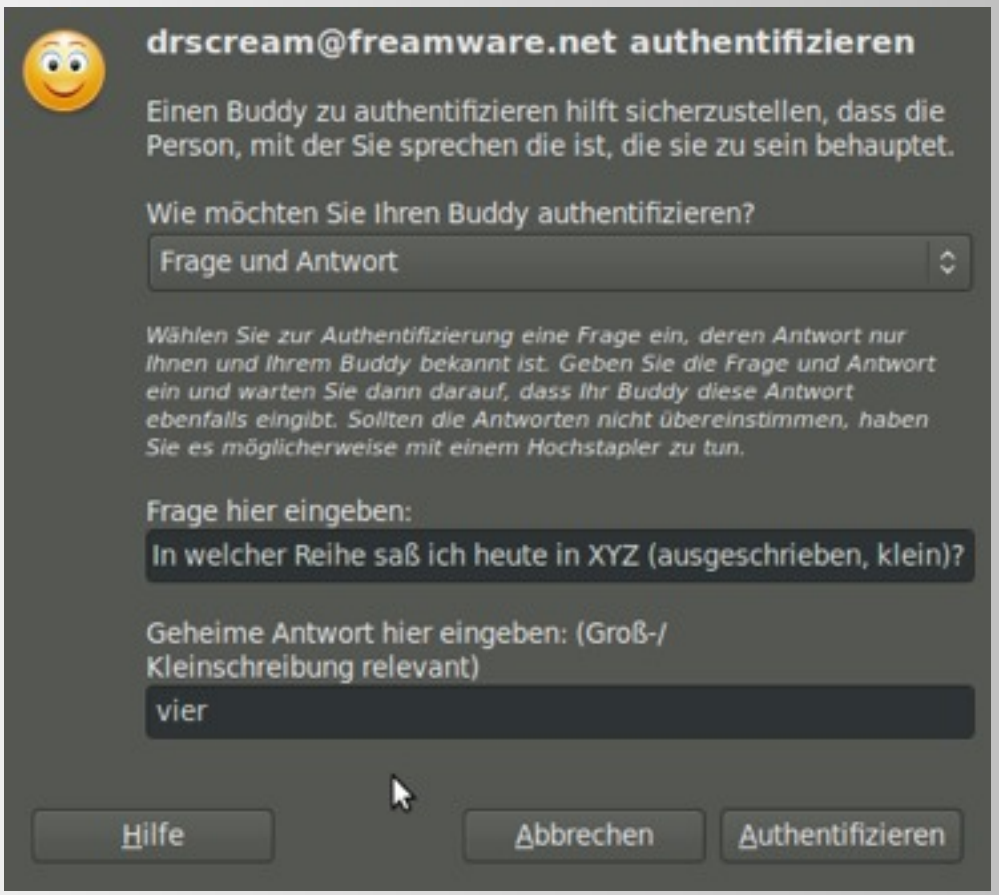
- Nur beide Gesprächspartner sollen die Nachrichten lesen können
- Nachrichten müssen manipuliert werden können (**Abstreitbarkeit** u. **Folgenlosigkeit**)
- **Ein** Manipuliertes, verschlüsseltes Bit wirkt sich auf **ein** manipuliertes Bit im Klartext aus

Authentifizierung

- Authentifizierung ist **notwendig**
- Öffentliche Schlüssel u. Fingerprints
- Erfolgt jeweils am Anfang eines Gesprächs
- Je nach Implementierung auch durch Fragen

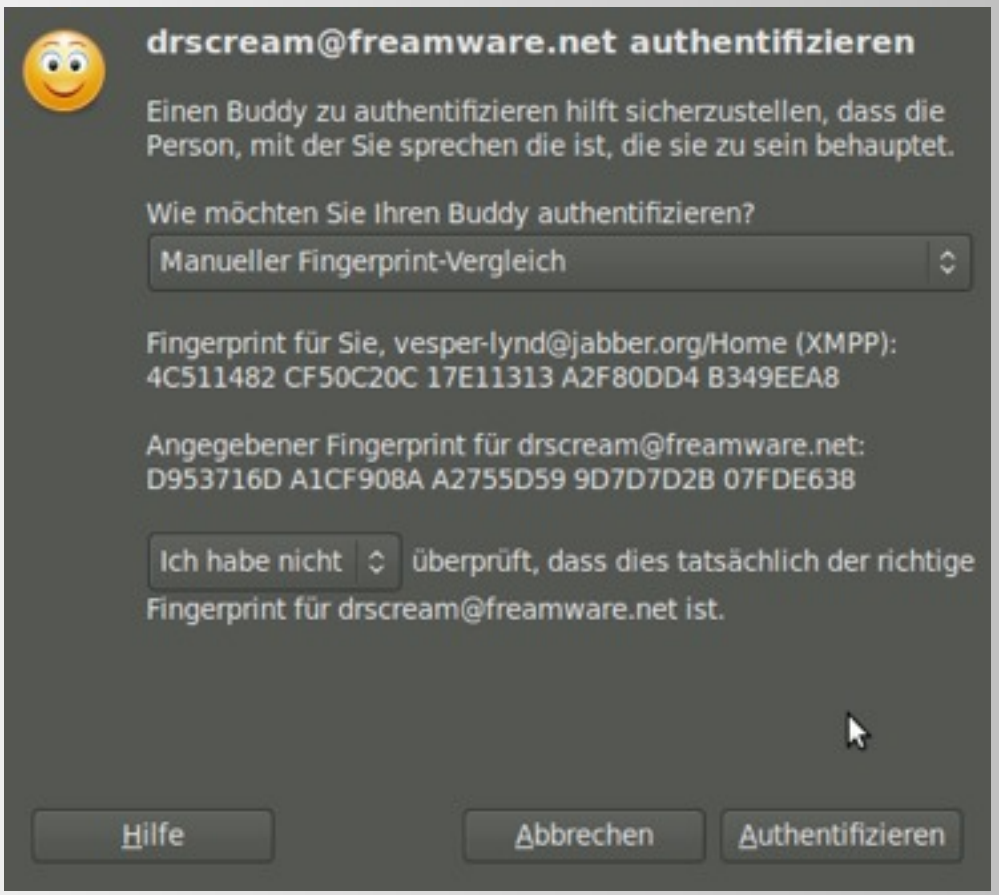
Authentifizierung in Pidgin

Authentifizierung in Pidgin



Authentifizierung in Pidgin

Authentifizierung in Pidgin



Abstreitbarkeit

- Nur Inhalt ist abstreitbar
- Existenz eines Gesprächs lässt sich nicht verschleiern – nur Inhalt
- Nachrichten könnten von jedem sein, der den geheimen Schlüssel des Partners kennt

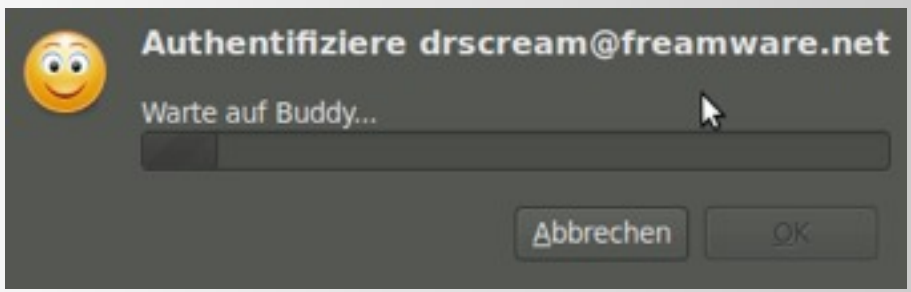
Folgenlosigkeit

- Verlust des priv. Schlüssel ist ohne Folgen
- Keine Nachrichten können damit dekodiert werden
- Gefahr: Identitätsfälschung

Verwendung im Alltag

(15:56:51) drscream@freamware.net wurde noch nicht authentifiziert. Sie sollten diesen Buddy authentifizieren.

(15:56:51) Nicht verifizierte Unterhaltung mit drscream@freamware.net begonnen.



(16:06:03) Der Status der aktuellen

Verwendung im Alltag (2)

- Folgende Clients unterstützen OTR nativ:
  - Adium
  - Climm
  - Mcabber
  - CenterIM
- Via plug-in:
  - Pidgin
  - Kopete
  - Miranda
  - Trillian

Aussichten

- Geplante Funktionen
  - Gruppenchat mit mehreren Personen
  - Dateiübertragung

Quellen und Verweise

- http://www.cypherpunks.ca/otr/

  Projektseite
- http://public.tfh-berlin.de/~s30935/off-the-record-messaging.pdf

  Diplomarbeit zu OTR-Verschlüsselung