


Off-the-Record Messaging

Rainer Hihn - Off-The-Record

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 Gesprächspartners
- 

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



 **drscream@freamware.net authentifizieren**

Einen Buddy zu authentifizieren hilft sicherzustellen, dass die Person, mit der Sie sprechen die ist, die sie zu sein behauptet.

Wie möchten Sie Ihren Buddy authentifizieren?

Frage und Antwort

Wählen Sie zur Authentifizierung eine Frage ein, deren Antwort nur Ihnen und Ihrem Buddy bekannt ist. Geben Sie die Frage und Antwort ein und warten Sie dann darauf, dass Ihr Buddy diese Antwort ebenfalls eingibt. Sollten die Antworten nicht übereinstimmen, haben Sie es möglicherweise mit einem Hochstapler zu tun.

Frage hier eingeben:

Geheime Antwort hier eingeben: (Groß-/ Kleinschreibung relevant)

Hilfe Abbrechen Authentifizieren

Rainer Hihn - Off-The-Record

Authentifizierung in Pidgin



 **drscream@freamware.net authentifizieren**

Einen Buddy zu authentifizieren hilft sicherzustellen, dass die Person, mit der Sie sprechen die ist, die sie zu sein behauptet.

Wie möchten Sie Ihren Buddy authentifizieren?

Frage und Antwort

Wählen Sie zur Authentifizierung eine Frage ein, deren Antwort nur Ihnen und Ihrem Buddy bekannt ist. Geben Sie die Frage und Antwort ein und warten Sie dann darauf, dass Ihr Buddy diese Antwort ebenfalls eingibt. Sollten die Antworten nicht übereinstimmen, haben Sie es möglicherweise mit einem Hochstapler zu tun.

Frage hier eingeben:

In welcher Reihe saß ich heute in XYZ (ausgeschrieben, klein)?

Geheime Antwort hier eingeben: (Groß-/ Kleinschreibung relevant)

vier

Hilfe Abbrechen Authentifizieren

Rainer Hihn - Off-The-Record

Authentifizierung in Pidgin



 **drscream@freamware.net authentifizieren**

Einen Buddy zu authentifizieren hilft sicherzustellen, dass die Person, mit der Sie sprechen die ist, die sie zu sein behauptet.

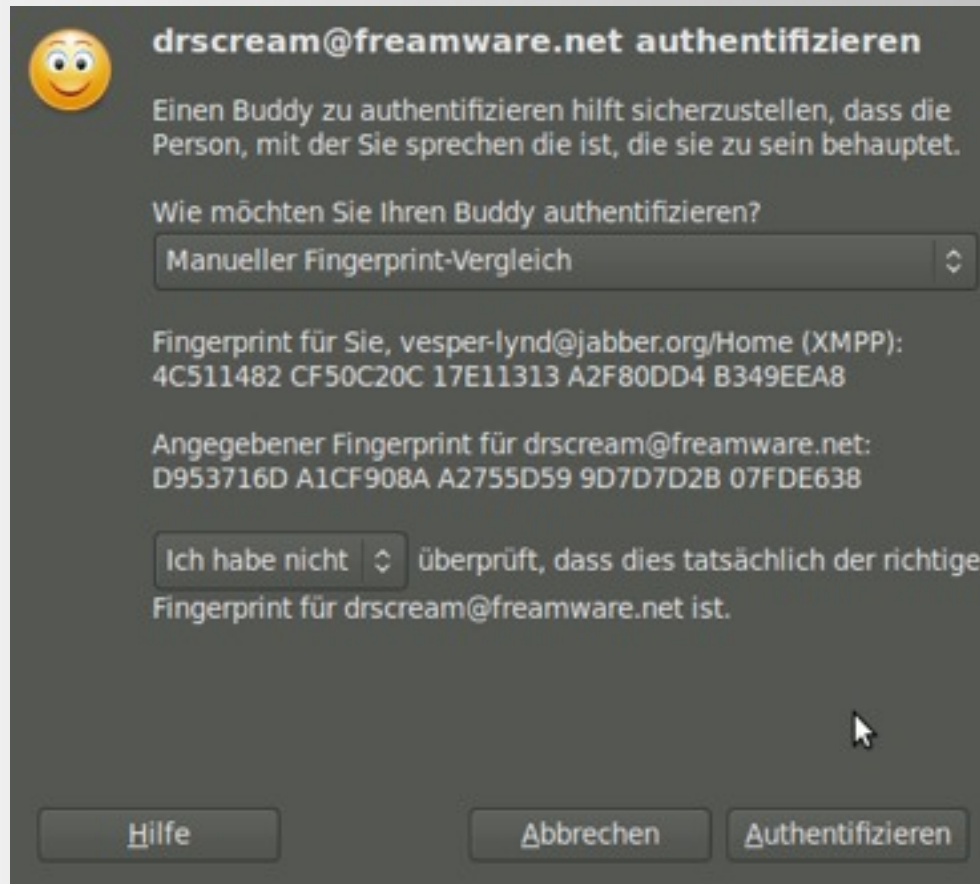
Wie möchten Sie Ihren Buddy authentifizieren?

Wählen Sie zur Authentifizierung eine Passphrase, die nur Ihnen und Ihrem Buddy bekannt ist. Geben Sie diese Passphrase ein, warten Sie dann darauf, dass Ihr Buddy diese Passphrase ebenfalls eingibt. Wenn die Passphrasen nicht übereinstimmen, haben Sie es möglicherweise mit einem Hochstapler zu tun.

Geheime Passphrase hier eingeben

Rainer Hihn - Off-The-Record

Authentifizierung in Pidgin



Rainer Hihn - Off-The-Record

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

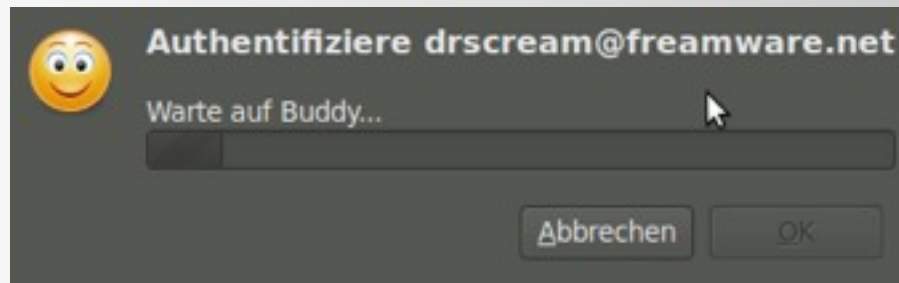
Folgenlosigkeit

- 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