

Off-the-Record (OTR)

Sicheres Instant Messaging

Hinrikus Wolf

RWTH-Aachen, Informatik

15. Januar 2014

Was ist OTR?

Was ist OTR?

- Ein Protokoll zur Verschlüsselung von Nachrichten speziell für Instant Messaging.

Was ist OTR?

- Ein Protokoll zur Verschlüsselung von Nachrichten speziell für Instant Messaging.
- Nachrichten sind signiert, der Empfänger weiß, wer der Absender ist.

Was ist OTR?

- Ein Protokoll zur Verschlüsselung von Nachrichten speziell für Instant Messaging.
- Nachrichten sind signiert, der Empfänger weiß, wer der Absender ist.
- Es kann quasi für jedes IM-Protokoll (Jabber, ICQ, MSN, Facebook-Chat, Google Talk, ...) verwendet werden.

Warum nicht PGP?

Warum nicht PGP?

Theoretisch ließe sich PGP genauso verwenden. Aber:

Warum nicht PGP?

Theoretisch ließe sich PGP genauso verwenden. Aber:

- Angenommen die NSA knackt Euren PGP-Key, kann sie alle Nachrichten, die sie vorher mitgeschnitten hat, entschlüsseln.

Warum nicht PGP?

Theoretisch ließe sich PGP genauso verwenden. Aber:

- Angenommen die NSA knackt Euren PGP-Key, kann sie alle Nachrichten, die sie vorher mitgeschnitten hat, entschlüsseln.
- Wenn Ihr Person X schreibt: „Morgen bringe ich den Weihnachtsmann um!“, kann Person X mit der signierten Nachricht zur Polizei gehen und hat einen Beweis für die Tötungsabsicht.

Warum nicht PGP?

Theoretisch ließe sich PGP genauso verwenden. Aber:

- Angenommen die NSA knackt Euren PGP-Key, kann sie alle Nachrichten, die sie vorher mitgeschnitten hat, entschlüsseln.
- Wenn Ihr Person X schreibt: „Morgen bringe ich den Weihnachtsmann um!“, kann Person X mit der signierten Nachricht zur Polizei gehen und hat einen Beweis für die Tötungsabsicht.

Achtung!

Das wollen wir nicht!

Was macht OTR besser als PGP?

Was macht OTR besser als PGP?

Wir brauchen folgende Eigenschaften:

Was macht OTR besser als PGP?

Wir brauchen folgende Eigenschaften:

- Perfect Forward Secrecy (Folgenlosigkeit)

Was macht OTR besser als PGP?

Wir brauchen folgende Eigenschaften:

- Perfect Forward Secrecy (Folgenlosigkeit)
 - Also selbst wenn unser Private Key kompromittiert wird, soll niemand in der Lage sein alte Nachrichten zu entschlüsseln.

Was macht OTR besser als PGP?

Wir brauchen folgende Eigenschaften:

- Perfect Forward Secrecy (Folgenlosigkeit)
 - Also selbst wenn unser Private Key kompromittiert wird, soll niemand in der Lage sein alte Nachrichten zu entschlüsseln.
- Deniable Signatures (Abstreitbare Signaturen)

Was macht OTR besser als PGP?

Wir brauchen folgende Eigenschaften:

- Perfect Forward Secrecy (Folgenlosigkeit)
 - Also selbst wenn unser Private Key kompromittiert wird, soll niemand in der Lage sein alte Nachrichten zu entschlüsseln.
- Deniable Signatures (Abstreitbare Signaturen)
 - Während der Unterhaltung soll der Gegenüber sich absolut sicher sein, dass er wirklich mit uns kommuniziert.

Was macht OTR besser als PGP?

Wir brauchen folgende Eigenschaften:

- Perfect Forward Secrecy (Folgenlosigkeit)
 - Also selbst wenn unser Private Key kompromittiert wird, soll niemand in der Lage sein alte Nachrichten zu entschlüsseln.
- Deniable Signatures (Abstreitbare Signaturen)
 - Während der Unterhaltung soll der Gegenüber sich absolut sicher sein, dass er wirklich mit uns kommuniziert.
 - Aber nach der Unterhaltung müssen wir behaupten können, dass wir das niemals geschrieben haben.

Was macht OTR besser als PGP?

Wir brauchen folgende Eigenschaften:

- Perfect Forward Secrecy (Folgenlosigkeit)
 - Also selbst wenn unser Private Key kompromittiert wird, soll niemand in der Lage sein alte Nachrichten zu entschlüsseln.
- Deniable Signatures (Abstreitbare Signaturen)
 - Während der Unterhaltung soll der Gegenüber sich absolut sicher sein, dass er wirklich mit uns kommuniziert.
 - Aber nach der Unterhaltung müssen wir behaupten können, dass wir das niemals geschrieben haben.
 - Also brauchen wir eine Art Ablaufdatum.

Wie geht das?

Wie geht das?

Einschub: Message Authentication Code (MAC)

Wie geht das?

Einschub: Message Authentication Code (MAC)

- Ein MAC ist das Ergebnis einer Funktion, die aus einem gemeinsamen Geheimnis und der Nachricht eine „eindeutige Zahl“ bestimmt $f_{MAC}(m, s) = MAC$.

Wie geht das?

Einschub: Message Authentication Code (MAC)

- Ein MAC ist das Ergebnis einer Funktion, die aus einem gemeinsamen Geheimnis und der Nachricht eine „eindeutige Zahl“ bestimmt $f_{MAC}(m, s) = MAC$.
- Der Sender bestimmt den MAC und sendet dann diesen mit der Nachricht an den Empfänger.

Wie geht das?

Einschub: Message Authentication Code (MAC)

- Ein MAC ist das Ergebnis einer Funktion, die aus einem gemeinsamen Geheimnis und der Nachricht eine „eindeutige Zahl“ bestimmt $f_{MAC}(m, s) = MAC$.
- Der Sender bestimmt den MAC und sendet dann diesen mit der Nachricht an den Empfänger.
- Der Empfänger kann bei Erhalt der Nachricht den MAC überprüfen und dabei feststellen, ob der Absender korrekt ist oder die Nachricht verändert wurde.

Wie geht das?

Wie geht das?

Initialisierung

Wie geht das?

Initialisierung

- Alice und Bob brauchen RSA-Keys (z.B. die PGP-Keys).

Wie geht das?

Initialisierung

- Alice und Bob brauchen RSA-Keys (z.B. die PGP-Keys).
- Sie müssen die öffentlichen Schlüssel auf sicherem Wege austauschen.

Wie geht das?

Initialisierung

- Alice und Bob brauchen RSA-Keys (z.B. die PGP-Keys).
- Sie müssen die öffentlichen Schlüssel auf sicherem Wege austauschen.
- Austausch eines Schlüssels für Symmetrische Verschlüsselung (z.B. AES) durch Verwendung der RSA-Schlüssel.

Wie geht das?

Initialisierung

- Alice und Bob brauchen RSA-Keys (z.B. die PGP-Keys).
- Sie müssen die öffentlichen Schlüssel auf sicherem Wege austauschen.
- Austausch eines Schlüssels für Symmetrische Verschlüsselung (z.B. AES) durch Verwendung der RSA-Schlüssel.
- **Austausch eines gemeinsamen Geheimnis**

Wie geht das?

Initialisierung

- Alice und Bob brauchen RSA-Keys (z.B. die PGP-Keys).
- Sie müssen die öffentlichen Schlüssel auf sicherem Wege austauschen.
- Austausch eines Schlüssels für Symmetrische Verschlüsselung (z.B. AES) durch Verwendung der RSA-Schlüssel.
- Austausch eines gemeinsamen Geheimnis

Austausch

Wie geht das?

Initialisierung

- Alice und Bob brauchen RSA-Keys (z.B. die PGP-Keys).
- Sie müssen die öffentlichen Schlüssel auf sicherem Wege austauschen.
- Austausch eines Schlüssels für Symmetrische Verschlüsselung (z.B. AES) durch Verwendung der RSA-Schlüssel.
- Austausch eines gemeinsamen Geheimnis

Austausch

- Alice berechnet den *MAC* und verschlüsselt die Nachricht *m* und den *MAC* und sendet beides an Bob.

Wie geht das?

Initialisierung

- Alice und Bob brauchen RSA-Keys (z.B. die PGP-Keys).
- Sie müssen die öffentlichen Schlüssel auf sicherem Wege austauschen.
- Austausch eines Schlüssels für Symmetrische Verschlüsselung (z.B. AES) durch Verwendung der RSA-Schlüssel.
- Austausch eines gemeinsamen Geheimnis

Austausch

- Alice berechnet den *MAC* und verschlüsselt die Nachricht *m* und den *MAC* und sendet beides an Bob.
- Bob entschlüsselt die Nachricht und überprüft den *MAC*.

Wie geht das?

Initialisierung

- Alice und Bob brauchen RSA-Keys (z.B. die PGP-Keys).
- Sie müssen die öffentlichen Schlüssel auf sicherem Wege austauschen.
- Austausch eines Schlüssels für Symmetrische Verschlüsselung (z.B. AES) durch Verwendung der RSA-Schlüssel.
- Austausch eines gemeinsamen Geheimnis

Austausch

- Alice berechnet den *MAC* und verschlüsselt die Nachricht m und den *MAC* und sendet beides an Bob.
- Bob entschlüsselt die Nachricht und überprüft den *MAC*.
- Bob weiß, dass nur er und Alice diesen *MAC* kennen, er ist sich also sicher, dass die Nachricht von Alice kam.

Wie geht das?

Initialisierung

- Alice und Bob brauchen RSA-Keys (z.B. die PGP-Keys).
- Sie müssen die öffentlichen Schlüssel auf sicherem Wege austauschen.
- Austausch eines Schlüssels für Symmetrische Verschlüsselung (z.B. AES) durch Verwendung der RSA-Schlüssel.
- Austausch eines gemeinsamen Geheimnis

Austausch

- Alice berechnet den *MAC* und verschlüsselt die Nachricht *m* und den *MAC* und sendet beides an Bob.
- Bob entschlüsselt die Nachricht und überprüft den *MAC*.
- Bob weiß, dass nur er und Alice diesen *MAC* kennen, er ist sich also sicher, dass die Nachricht von Alice kam.
- Bob veröffentlicht anschließend den *MAC*.

Ist das sicher?

Ist das sicher?

- Verschlüsselung durch AES ist sicher.

Ist das sicher?

- Verschlüsselung durch AES ist sicher.
- Authentizität:

Ist das sicher?

- Verschlüsselung durch AES ist sicher.
- Authentizität:
 - Alice und Bob haben ihre Schlüssel ausgetauscht, daher können Sie sich sicher sein, dass sie wirklich miteinander kommunizieren.

Ist das sicher?

- Verschlüsselung durch AES ist sicher.
- Authentizität:
 - Alice und Bob haben ihre Schlüssel ausgetauscht, daher können Sie sich sicher sein, dass sie wirklich miteinander kommunizieren.
- **Abstreitbarkeit:**

Ist das sicher?

- Verschlüsselung durch AES ist sicher.
- Authentizität:
 - Alice und Bob haben ihre Schlüssel ausgetauscht, daher können Sie sich sicher sein, dass sie wirklich miteinander kommunizieren.
- Abstreitbarkeit:
 - Alice benutzt nur am Anfang ihre Digitale Signatur.

Ist das sicher?

- Verschlüsselung durch AES ist sicher.
- Authentizität:
 - Alice und Bob haben ihre Schlüssel ausgetauscht, daher können Sie sich sicher sein, dass sie wirklich miteinander kommunizieren.
- Abstreitbarkeit:
 - Alice benutzt nur am Anfang ihre Digitale Signatur.
 - Zum Signieren wird der MAC-Schlüssel gebraucht, die Nachricht könnte genauso gut von Bob kommen.

Ist das sicher?

- Verschlüsselung durch AES ist sicher.
- Authentizität:
 - Alice und Bob haben ihre Schlüssel ausgetauscht, daher können Sie sich sicher sein, dass sie wirklich miteinander kommunizieren.
- Abstreitbarkeit:
 - Alice benutzt nur am Anfang ihre Digitale Signatur.
 - Zum Signieren wird der MAC-Schlüssel gebraucht, die Nachricht könnte genauso gut von Bob kommen.
 - Durch die Veröffentlichung der MAC-Schlüssel, ist es nicht mehr sicher, dass die Nachricht wirklich von Alice kam.

Ist das sicher?

- Verschlüsselung durch AES ist sicher.
- Authentizität:
 - Alice und Bob haben ihre Schlüssel ausgetauscht, daher können Sie sich sicher sein, dass sie wirklich miteinander kommunizieren.
- Abstreitbarkeit:
 - Alice benutzt nur am Anfang ihre Digitale Signatur.
 - Zum Signieren wird der MAC-Schlüssel gebraucht, die Nachricht könnte genauso gut von Bob kommen.
 - Durch die Veröffentlichung der MAC-Schlüssel, ist es nicht mehr sicher, dass die Nachricht wirklich von Alice kam.
- Perfect forward secrecy

Ist das sicher?

- Verschlüsselung durch AES ist sicher.
- Authentizität:
 - Alice und Bob haben ihre Schlüssel ausgetauscht, daher können Sie sich sicher sein, dass sie wirklich miteinander kommunizieren.
- Abstreitbarkeit:
 - Alice benutzt nur am Anfang ihre Digitale Signatur.
 - Zum Signieren wird der MAC-Schlüssel gebraucht, die Nachricht könnte genauso gut von Bob kommen.
 - Durch die Veröffentlichung der MAC-Schlüssel, ist es nicht mehr sicher, dass die Nachricht wirklich von Alice kam.
- Perfect forward secrecy
 - Die Schlüssel für die symmetrische Verschlüsselung werden nicht gespeichert.

Ist das sicher?

- Verschlüsselung durch AES ist sicher.
- Authentizität:
 - Alice und Bob haben ihre Schlüssel ausgetauscht, daher können Sie sich sicher sein, dass sie wirklich miteinander kommunizieren.
- Abstreitbarkeit:
 - Alice benutzt nur am Anfang ihre Digitale Signatur.
 - Zum Signieren wird der MAC-Schlüssel gebraucht, die Nachricht könnte genauso gut von Bob kommen.
 - Durch die Veröffentlichung der MAC-Schlüssel, ist es nicht mehr sicher, dass die Nachricht wirklich von Alice kam.
- Perfect forward secrecy
 - Die Schlüssel für die symmetrische Verschlüsselung werden nicht gespeichert.
 - Damit lässt sich auch nicht mit kompromittierten Schlüsseln die Nachrichten nicht mehr entschlüsseln.

Wie benutzt man OTR?

Wie benutzt man OTR?

- mit dem OTR-Plugin für Pidgin (Windows, Linux)

Wie benutzt man OTR?

- mit dem OTR-Plugin für Pidgin (Windows, Linux)
- mit dem OTR-Plugin für Adium (Mac OS)

Wie benutzt man OTR?

- mit dem OTR-Plugin für Pidgin (Windows, Linux)
- mit dem OTR-Plugin für Adium (Mac OS)
- mit Xabber (Android)

Wie benutzt man OTR?

- mit dem OTR-Plugin für Pidgin (Windows, Linux)
- mit dem OTR-Plugin für Adium (Mac OS)
- mit Xabber (Android)

Zu beachten

Wie benutzt man OTR?

- mit dem OTR-Plugin für Pidgin (Windows, Linux)
- mit dem OTR-Plugin für Adium (Mac OS)
- mit Xabber (Android)

Zu beachten

- Immer an die Schlüsselüberprüfung denken, sonst kann es Man-in-the-Middle Angriffe geben.

Wie benutzt man OTR?

- mit dem OTR-Plugin für Pidgin (Windows, Linux)
- mit dem OTR-Plugin für Adium (Mac OS)
- mit Xabber (Android)

Zu beachten

- Immer an die Schlüsselüberprüfung denken, sonst kann es Man-in-the-Middle Angriffe geben.
- Frage-Antwort- bzw. Gemeinsame-Geheimnis-Authentifikationen sind nicht so sicher wie die Keys manuell zu vergleichen.

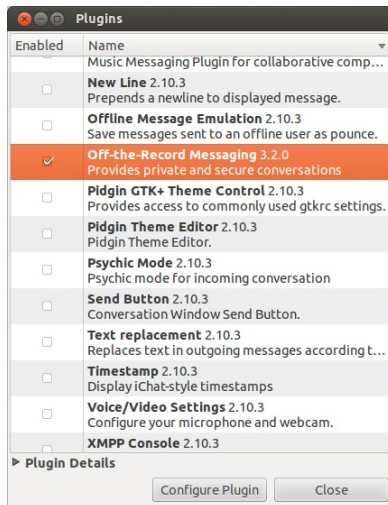
Wie benutzt man OTR?

- mit dem OTR-Plugin für Pidgin (Windows, Linux)
- mit dem OTR-Plugin für Adium (Mac OS)
- mit Xabber (Android)

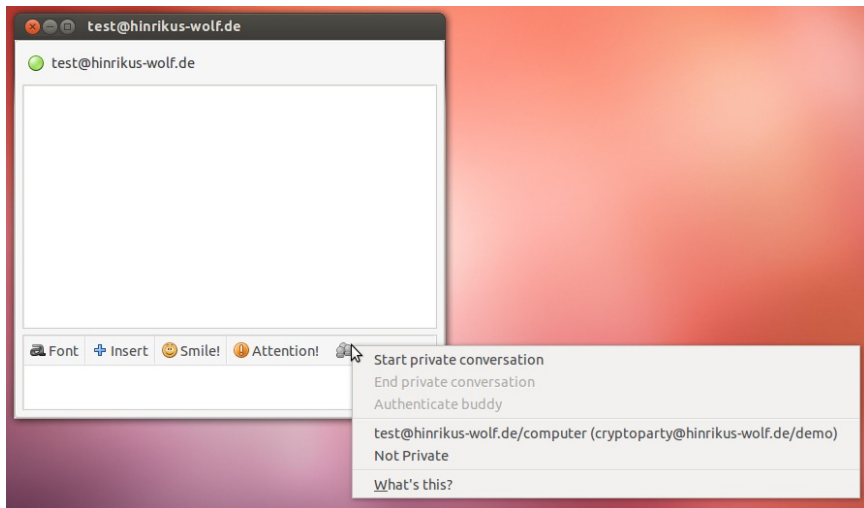
Zu beachten

- Immer an die Schlüsselüberprüfung denken, sonst kann es Man-in-the-Middle Angriffe geben.
- Frage-Antwort- bzw. Gemeinsame-Geheimnis-Authentifikationen sind nicht so sicher wie die Keys manuell zu vergleichen.
- Das Speichern von Chat-Logs ist nicht so sinnvoll, wenn man OTR benutzt.

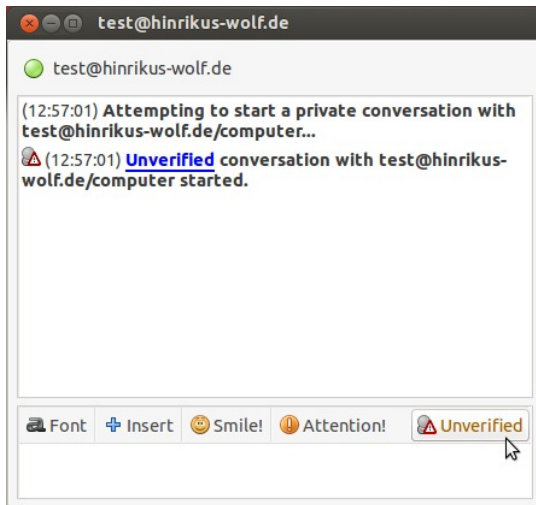
Plugin aktivieren



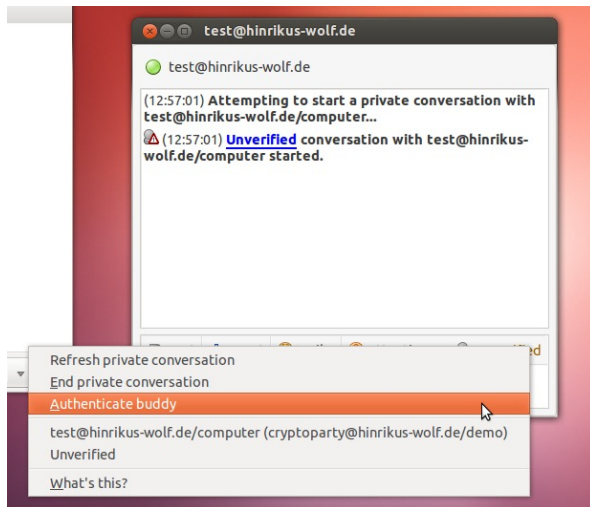
Initialisiere OTR-Verbindung




Unverifizierte Verbindung




Wie verifizieren?



Frage Antwort

 **Authenticate Buddy**

 **Authenticate test@hinrikuswolf.de**

Authenticating a buddy helps ensure that the person you are talking to is who he or she claims to be.

How would you like to authenticate your buddy?

Question and answer

To authenticate using a question, pick a question whose answer is known only to you and your buddy. Enter this question and this answer, then wait for your buddy to enter the answer too. If the answers don't match, then you may be talking to an imposter.

Enter question here:

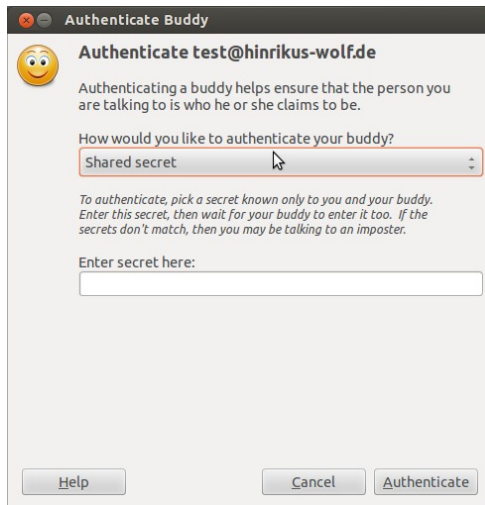
Enter secret answer here (case sensitive):

Help

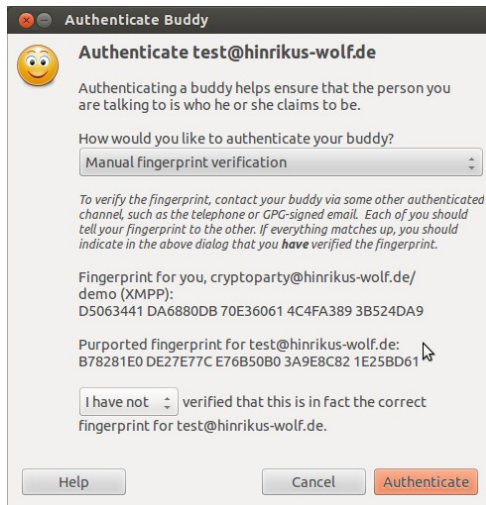
Cancel

Authenticate

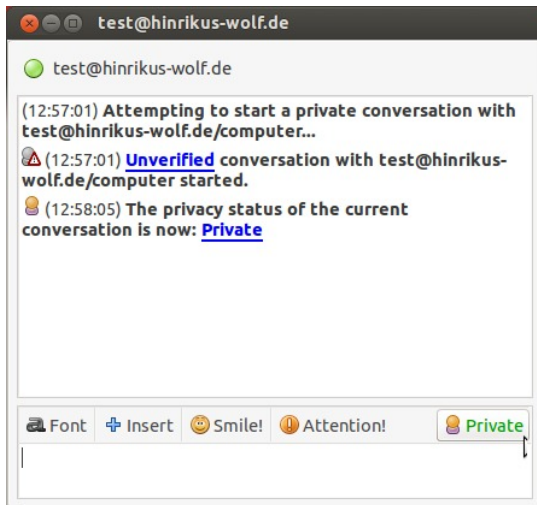
Gemeinsames Geheimnis



Manueller Fingerprintvergleich



Private, gesicherte Unterhaltung



Vielen Dank für Eure
Aufmerksamkeit!