

# Encrypted IM with Pidgin and OTR



**Tom Ryder**

[tom@sanctum.geek.nz](mailto:tom@sanctum.geek.nz)  
<https://sanctum.geek.nz/>

# IM is insecure

- Chat protocols do often support SSL connections
- But they're third party, and involve trusting the person running the server
  - Google talk
  - Facebook chat
  - Skype chat
  - IRC networks
- Your chat content can still be read by attackers

# Authentication

- Much like PGP email, it's not just about keeping the information secure
- We have to be sure who we're talking to, and IM and email accounts can get stolen
- We want a way not just to **encrypt**, but to **authenticate** a person, and make sure nobody else could be listening to the conversation (**man-in-the-middle**)
- As with email, this is best solved with the use of **public key cryptography**

# What are the options?

- If we want to keep our data completely secure and under control, we have to run our own IM servers:
  - Jabber + SSL
  - IRC + SSL
- The software is free and open source ...
- ... but it's a pain to set up and manage, requires more effort from both parties, and doesn't necessarily have **perfect forward secrecy**
- If your keys are compromised, someone could read your past messages

# Off-The-Record chat

- Works over **third-party systems**; the messages appear garbled to other readers
- **Authenticates** the parties in a conversation, and allows detecting man-in-the-middle attacks
- **Encrypts** the content so it can't be read by the network provider
- Has **perfect forward secrecy**; if any of the keys are stolen, they still can't be used to decrypt past messages (PGP mail does *not* do this)
- Is **deniable**; there's no way to prove you composed any given encrypted message; your keys don't contain identifying information

# How it looks to third parties



**Tom Ryder**

02/11/2013 20:48

?OTR:AAIDAAAAABIAAAATAAAAwAJwGNLLahZ8ivh91pz  
CNQImSpLPfJTKrJSLw/AQOJ6PrzWolgBPkPAC8MmXJO1  
87MkdMT  
/AvB90JIZh89XKP6REq5CraFLxZCPTQMw2dXElaKPBZ4X  
QXNIXJQPrMifl5SLycsp3k00Y  
/Qz9e7WVL6Pe7sRh4E6eT0GCAcGCJ21FmbCtSgPdNoB5n  
iMrhdk5L  
/Jcd9bgudw1peFNSPiizCB0Q+WwqY22TGm1hKQB0unYyn  
uAFOSOuPDYVMErOSIWmwAAAAAAAAAABAAAAE8  
/t0C/RDi0dztbDNN7kd++3UDz6Qew0wtO1AS8F6FQG0k+B  
Hkko6gAAABSd+givbeb+l043QSDrc5UtnAHcmg==.



[Redacted name]

02/11/2013 20:48

?OTR:AAIDAAAAABMAAAATAAAAwIzpn//EsUB0pdONeG5  
umObWtdjRIWhnW  
/4PYPWRQs8lrjoHGslEgDFVq8U4ST2dQUOfztaBB04tDUX  
130mCyAYWk4civQb4wLzo  
/OXyDOmNUjvqLhiWxq0HrmO6F1WzKFjBZ18tmFZcc1fme

---

# What supports it?

Many open source instant messaging clients:

- **Pidgin** – Windows, GNU/Linux, BSD
- Adium – Mac OS X
- Bitlbee (IM to IRC) – GNU/Linux, BSD
- Gibberbot – Android

It won't work in any web interface or proprietary client; you need to install the software on your machine.

# Pidgin

- Multi-IM client: you can chat on many networks:
  - Google Talk
  - Windows Live Messenger/Skype
  - Facebook
  - Jabber
  - Steam
  - IRC
- OTR should work on all of them
- Free software
- Separate, portable library for chat programs: libpurple



# Installation

- Debian, Ubuntu, Mint:

```
# apt-get install pidgin pidgin-otr
```

- Fedora, Red Hat, SUSE:

```
# yum install pidgin pidgin-otr
```

- Can be built from source if necessary

# Demonstration

- Pidgin on Debian XFCE on my laptop
- Talking to my machine at home, running irssi/bitlbee over SSH
- Activating the OTR plugin
- Starting a private conversation with someone else using OTR
- Authentication via some secure channel (e.g. PGP mail)
- Checking fingerprints
- Demonstration of how messages appear to attackers
- Enjoy chatting far more securely!

# How to authenticate?

- You decide what method is good enough for your purposes
  - Meet in person and exchange fingerprints (safest)
  - Sign the fingerprints and send them via PGP mail with a trusted public key
  - Pose them a question only they could answer
  - Phone call
  - Text message the fingerprint to a known trusted number (least secure; don't use this for very sensitive contacts)

# Questions?

- <https://otr.cypherpunks.ca/>
- [https://en.wikipedia.org/wiki/Off-the-Record\\_Messaging](https://en.wikipedia.org/wiki/Off-the-Record_Messaging)
- <https://www.riseup.net/en/otr>