Belfast CryptoParty

Welcome

Pete Maynard
@pgmaynard

October 14, 2014

What is a CryptoParty?

> *A CryptoParty is free, public and fun. It's a decentralized, global initiative to introduce the most basic cryptography software and the fundamental concepts of their operation to the general public.*

`https://cryptoparty.in`

Future Topics

- PGP (Data encryption and authentication)
- Tor (Anonymity Online)
- Disk Encryption
- Securely Downloading applications
- Whatever you want :)

Disclaimer

"The only secure computer is one that's unplugged, locked in a safe, and buried 20 feet under the ground in a secret location. . . and I'm not even too sure about that one" – Dennis Huges, FBI.

What is OTR?
Encrypted Instant Messaging

- **Encryption** - No one else can read your instant messages.
- **Authentication** - You are assured the correspondent is who you think it is.
- **Deniability** - The messages you send do not have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, during a conversation, your correspondent is assured the messages he sees are authentic and unmodified.
- **Perfect forward secrecy** - If you lose control of your private keys, no previous conversation is compromised.

What OTR is not

- Some applications will allow "Off the record"
  Normally disables logging - **Does not mean it's encrypted!**
- SSL, the padlock on websites (HTTPS), is not the same
- OTR is not secure if you log the conversation
- OTR does not allow more than two people in a conversation

What you will need

- **Windows/Linux** - Pidgin with the OTR plug-in
  - https://pidgin.im
  - https://otr.cypherpunks.ca
- **Mac OS** - Adium (built in support for OTR)
  - https://adium.im
- **Android/iOS** - Chat Secure
  - https://chatsecure.org

Connect and Go

1. Download your client
2. Setup account
3. Accounts, Manage Account, Add
4. Enter connection details (right)
5. Enable OTR

- **Protocol**: Facebook (XMPP)
- **Username**: [think]
- **Domain** : chat.facebook.com
- **Resource**: none
- **Password**: [think]
- **Proxy** : Port 443