Pour une messagerie instantanée sécurisée et respectueuse de votre vie privée

Daniel ".koolfy" Faucon

RMLL 2014 - Montpellier

July 8, 2014

Intro

- Talk is in French
- Slides are in English

Intro

- Talk is in French
- Slides are in English

DON'T PANIC

Why encrypt?

Why privacy?

Why encrypt?

Why privacy?

- It's also a question of hygene.

Why encrypt?

Why privacy?

- It's also a question of hygene.
- Everything you say will be used against you.

Why encrypt?

Why privacy?

- It's also a question of hygene.
- Everything you say will be used against you.
- The people you talk to might need privacy to stay alive.

What about IM?

Why focus on chat?

What about IM?

Why focus on chat?

- It's the main communication medium between people.

What about IM?

Why focus on chat?

- It's the main communication medium between people.
- It generates (a lot of) "quality" data about you. (low noise/signal ratio)

What about IM?

Why focus on chat?

- It's the main communication medium between people.
- It generates (a lot of) "quality" data about you. (low noise/signal ratio) (contrary to data masturbation)

What about IM?

Why focus on chat?

- It's the main communication medium between people.
- It generates (a lot of) "quality" data about you. (low noise/signal ratio) (contrary to data masturbation)
- Private stuff should remain private.

Quick note

Quick note

- NSA is not your primary threat.

Quick note

- NSA is not your primary threat.
- NSA is NOT your adversary.

Quick note

- NSA is not your primary threat.
- NSA is NOT your adversary.
- (it's everyone's.)

In the beginning...

The Internet arrives in human society.

In the beginning...

The Internet arrives in human society.

- Everything is public.

In the beginning...

The Internet arrives in human society.

- Everything is public.
- Wow! Shit spreads FAST.

In the beginning...

The Internet arrives in human society.

- Everything is public.
- Wow! Shit spreads FAST.
- No passwords, everything is cleartext, THIS IS AWESOME

In the beginning...

Wait, WHAT?!

In the beginning...

Wait, WHAT?!

Err... Maybe this was a bad idea.

In the beginning...

Oh, I know! Let's use symmetric encryption !

In the beginning...

Oh, I know! Let's use symmetric encryption !
It'll be fun!

In the beginning...

Oh, I know! Let's use symmetric encryption !
It'll be fun! I swear.

In the beginning...

Key exchange.

In the beginning...

In 1976, Diffie, Hellman (and Merkle) introduce the world to public (asymmetrical) encryption.

In the beginning...

In 1976, Diffie, Hellman (and Merkle) introduce the world to public (asymmetrical) encryption.

- We can use public crypto for key exchange

In the beginning...

In 1976, Diffie, Hellman (and Merkle) introduce the world to public (asymmetrical) encryption.

- We can use public crypto for key exchange
- And symmetical crypto for encryption.

In the beginning...

In 1976, Diffie, Hellman (and Merkle) introduce the world to public (asymmetrical) encryption.

- We can use public crypto for key exchange
- And symmetical crypto for encryption.
- The best of both worlds! Everything is fine now.

In the beginning...

In 1976, Diffie, Hellman (and Merkle) introduce the world to public (asymmetrical) encryption.

- We can use public crypto for key exchange
- And symmetical crypto for encryption.
- The best of both worlds! Everything is fine now. Right?

In the beginning...

...right?

In the beginning...

To academics, pretty much.

In the beginning...

To academics, pretty much.
In real life, not so much.

The cypherpunk era.

Meanwhile, in real life...

The cypherpunk era.

Meanwhile, in real life...

- up to WWII: Crypto is military only.

The cypherpunk era.

Meanwhile, in real life...

- up to WWII: Crypto is military only.
- 70's: The internet slowly emerges, early hackers start playing with stuff.

The cypherpunk era.

Meanwhile, in real life...

- up to WWII: Crypto is military only.
- 70's: The internet slowly emerges, early hackers start playing with stuff.
- 80's: Cold war. Cold war EVERYWHERE. Academics and hackers join to meet military quality encryption.

The cypherpunk era.

Meanwhile, in real life...

- up to WWII: Crypto is military only.
- 70's: The internet slowly emerges, early hackers start playing with stuff.
- 80's: Cold war. Cold war EVERYWHERE. Academics and hackers join to meet military quality encryption.
- 90's: End of cold war, explosion of the cypherpunk movement. OpenPGP is born.

The PGP case..

PGP as a frame of reference

The PGP case..

PGP as a frame of reference

- Probably our most secure, best reviewed tool out there.

The PGP case..

PGP as a frame of reference

- Probably our most secure, best reviewed tool out there.
- This stuff is built like a tank.

The PGP case..

PGP as a frame of reference

- Probably our most secure, best reviewed tool out there.
- This stuff is built like a tank.
- Very strong encryption.

The PGP case..

PGP as a frame of reference

- Probably our most secure, best reviewed tool out there.
- This stuff is built like a tank.
- Very strong encryption.
- Very strong authentication.

The PGP case..

PGP as a frame of reference

- Probably our most secure, best reviewed tool out there.
- This stuff is built like a tank.
- Very strong encryption.
- Very strong authentication.
- Signatures are forever.

The PGP case..

PGP as a worst case scenario

The PGP case..

PGP as a worst case scenario

- Signatures are forever.

The PGP case..

PGP as a worst case scenario

- Signatures are forever. What happens after a compromize?

The PGP case..

PGP as a worst case scenario

- Signatures are forever. What happens after a compromize?
- It's complicated.

The PGP case..

PGP as a worst case scenario

- Signatures are forever. What happens after a compromize?
- It's complicated.
- It's very complicated.

The PGP case..

PGP as a worst case scenario

- Signatures are forever. What happens after a compromize?
- It's complicated.
- It's very complicated.
- It's really too fucking complicated.

The cypherpunk era.

Meanwhile, in real life... (2.0)

- up to WWII: Crypto is military only.
- 70's: The internet slowly emerges, early hacker start playing with stuff.
- 80's: Cold war. Cold war EVERYWHERE. Academics and hackers join to meet military quality encryption.
- 90's: End of cold war, explosion of the cypherpunk movement. OpenPGP is born.

The cypherpunk era.

Meanwhile, in real life... (2.0)

- up to WWII: Crypto is military only.
- 70's: The internet slowly emerges, early hacker start playing with stuff.
- 80's: Cold war. Cold war EVERYWHERE. Academics and hackers join to meet military quality encryption.
- 90's: End of cold war, explosion of the cypherpunk movement. OpenPGP is born.
- 00's: Hobbyists convince themselves that PGP is the final solution.

The cypherpunk era.

Meanwhile, in real life... (2.0)

- up to WWII: Crypto is military only.
- 70's: The internet slowly emerges, early hacker start playing with stuff.
- 80's: Cold war. Cold war EVERYWHERE. Academics and hackers join to meet military quality encryption.
- 90's: End of cold war, explosion of the cypherpunk movement. OpenPGP is born.
- 00's: Hobbyists convince themselves that PGP is the final solution.
- early 10's: The rest of the world painfully realizes we're far from the truth.

Enters OTR.

OTR is designed for Instant Messaging

Enters OTR.

OTR is designed for Instant Messaging

- Fast and easy to set up.

Enters OTR.

OTR is designed for Instant Messaging

- Fast and easy to set up.
- Encryption key is thrown away forever, ASAP.

Enters OTR.

OTR is designed for Instant Messaging

- Fast and easy to set up.
- Encryption key is thrown away forever, ASAP.

Enters OTR.

OTR is designed for Instant Messaging

- Fast and easy to set up.
- Encryption key is thrown away forever, ASAP.
- "Light" authentication of messages during the conversation.

Enters OTR.

OTR is designed for Instant Messaging

- Fast and easy to set up.
- Encryption key is thrown away forever, ASAP.
- "Light" authentication of messages during the conversation.
- Signatures mean nothing after the conversation is closed.

Enters OTR.

About OTR's "Plausible Deniability"

Enters OTR.

About OTR's "Plausible Deniability"

- Torture is not interrogation, it's a hobby. Nothing you say will stop it.

Enters OTR.

About OTR's "Plausible Deniability"

- Torture is not interrogation, it's a hobby. Nothing you say will stop it.
- Countries violating basic human rights won't give you a fair trial

Enters OTR.

About OTR's "Plausible Deniability"

- Torture is not interrogation, it's a hobby. Nothing you say will stop it.
- Countries violating basic human rights won't give you a fair trial

Enters OTR.

About OTR's "Plausible Deniability"

- Torture is not interrogation, it's a hobby. Nothing you say will stop it.
- Countries violating basic human rights won't give you a fair trial
- Even in fair trials, courts probably won't care.

Enters OTR.

About OTR's "Plausible Deniability"

- Torture is not interrogation, it's a hobby. Nothing you say will stop it.
- Countries violating basic human rights won't give you a fair trial
- Even in fair trials, courts probably won't care.
- Technical "Witnesses" of the chat can un-deny your messages.

Enters OTR.

But OTR is still a great tool.
Despite being young it has become to IM what PGP is to e-mail.

Using OTR.

But OTR is still a great tool.
Despite being young it has become to IM what PGP is to e-mail.

Pidgin

Pidgin

- Main OTR client out there.
- Using the reference C OTR library.
- Supports IRC, XMPP, FBchat, Skype, and a ton of other protocols
- Easy user inteface, multi-platform.

Pidgin

Issues.

- Pidgin is full of bugs, some were quite scary.
- Pidgin was *NOT* created with securiy in mind.
- Current devs are hard to convince that security should be a focus.

Pidgin

Issues.

- Pidgin is full of bugs, some were quite scary.
- Pidgin was *NOT* created with securiy in mind.
- Current devs are hard to convince that security should be a focus.
- (but some security review work has started)

Jitsi

Jitsi

- Easy to use, multi-platform
- Uses thr OTR4J java implementation of OTR (same as mobile cliens)
- OTR is built-in by default.
- Also supports encrypted audio/video chat (but this is offtopic)

Jitsi

Issues with Jitsi

- User experience is... java-ish.
- Some debate in regard to cuting corners in terms of entropy (should be fine)
- No HTTPS when downloading the client (But they fixed it!!)
- Doesn't see as much code review as it should. I have no idea if it's any better than pidgin.

irssi-otr

irssi-otr

- Console IRC client.
- Uses the main C OTR implementation.
- Lightweight.

irssi-otr

Isues with irssi-otr

- Console IRC client. (forget about user experience.)
- Sort of kind of pracically not maintainted anymore. (it's being rebooted)
- Irssi sucks when you want a powerful OTR plug-in.

irssi-otr

Isues with irssi-otr

- Console IRC client. (forget about user experience.)
- Sort of kind of pracically not maintainted anymore. (it's being rebooted)
- Irssi sucks when you want a powerful OTR plug-in.
- (also I hate irssi.)

weechat-otr

Weechat-otr

- Console IRC client.
- Uses a pure python OTR implementation
- Better UX than irssi
- Actively maintained

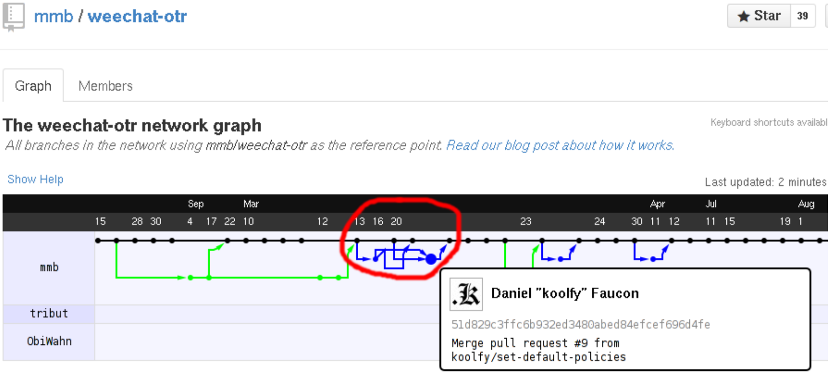
weechat-otr

Weechat-otr

- Console IRC client.
- Uses a pure python OTR implementation
- Better UX than irssi
- Actively maintained
- (HEY LOOK I MAINTAINED IT FOR A YEAR!)

weechat-otr

GUESS WHO DID THIS



mmb / weechat-otr

★ Star 39

Graph Members

The weechat-otr network graph

Keyboard shortcuts availabl

All branches in the network using mmb/weechat-otr as the reference point. Read our blog post about how it works.

Show Help

Last updated: 2 minutes

Daniel "koolfy" Faucon

51d829c3ffc6b932ed3480abed84efcef696d4fe

Merge pull request #9 from koolfy/set-default-policies

weechat-otr

Issues with Weechat-otr

- Console IRC client. (still not for beginners)
- The python implementation needs more review.
- Weechat-otr needs more use/review too.

weechat-otr

Issues with Weechat-otr

- Console IRC client. (still not for beginners)
- The python implementation needs more review.
- Weechat-otr needs more use/review too.
- (also it has my code it in. FEAR THE CONSEQUENCES.)

Mobile Apps

Chatsecure

- For Android and iOS
- Uses the same OTR4J java implementation as Jitsi
- But Apple's iPhone policies make the iOS client not very useful.

Beyond OTR

OTR might still not be enough.

Beyond OTR

OTR might still not be enough.

- OTR only allows 1-1 conversations.

Beyond OTR

OTR might still not be enough.

- OTR only allows 1-1 conversations.
- Like PGP, only a ridiculous minority use it.

Beyond OTR

OTR might still not be enough.

- OTR only allows 1-1 conversations.
- Like PGP, only a ridiculous minority use it.
- Skype and Facebook Chat are so much easier...

crypto.cat and Multiparty OTR

What about crypto.cat?

crypto.cat and Multiparty OTR

What about crypto.cat?

- Can handle encrypted *chatrooms*

crypto.cat and Multiparty OTR

What about crypto.cat?

- Can handle encrypted *chatrooms*
- Full-JS in-browser plugin approach.

crypto.cat and Multiparty OTR

What about crypto.cat?

- Can handle encrypted *chatrooms*
- Full-JS in-browser plugin approach.
- ”Usability as a security feature” doctrine.

crypto.cat and Multiparty OTR

What about crypto.cat?

- Can handle encrypted *chatrooms*
- Full-JS in-browser plugin approach.
- "Usability as a security feature" doctrine.
- It's cute and full of cats!!

crypto.cat and Multiparty OTR

What about crypto.cat?

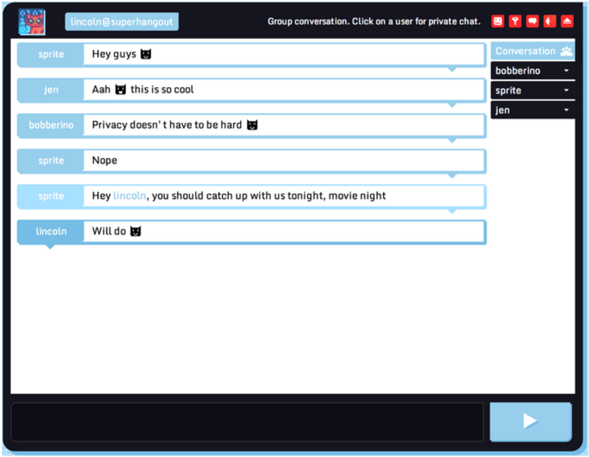
- Can handle encrypted *chatrooms*
- Full-JS in-browser plugin approach.
- "Usability as a security feature" doctrine.
- It's cute and full of cats!!
- oh and by the way

crypto.cat and Multiparty OTR

What about crypto.cat?

- Can handle encrypted *chatrooms*
- Full-JS in-browser plugin approach.
- "Usability as a security feature" doctrine.
- It's cute and full of cats!!
- oh and by the way IT SUPPORTS FACEBOOK CHAT TOO.

crypto.cat and Multiparty OTR



sprite: Hey guys

jen: Aah this is so cool

bobberino: Privacy doesn' t have to be hard

sprite: Nope

sprite: Hey lincoln, you should catch up with us tonight, movie night

lincoln: Will do

crypto.cat and Multiparty OTR

Issues with crypto.cat

- Has seen serious security bugs over the past year
- Full-JS. And let me tell you JS crypto isn't pretty.
- Invented its own multiparty-OTR protocol, which is experimental.

crypto.cat and Multiparty OTR

The future of crypto.cat

- Mobile apps?
- Native W3C browser crypto API offered to JS plugins?
- Whatever happens to crypto.cat, Multiparty-OTR need to happen.
- Whatever happens to crypto.cat, usability must be considered a security feature.

crypto.cat and Multiparty OTR

CRYPTOGRAPHY CANNOT WORK IF IT IS NOT USED.

Reality Check

About that Licence...

- NEVER use anything that is not FREE OPEN-SOURCE SOFTWARE for anything security related.
- Closed-source software or potocol = ZERO expectation of security
- The temptation (or gag order) to put an unnoticed backdoor is too strong.
- Open-source is not enough.

Reality Check

About that Licence...

- NEVER use anything that is not FREE OPEN-SOURCE SOFTWARE for anything security related.
- Closed-source software or potocol = ZERO expectation of security
- The temptation (or gag order) to put an unnoticed backdoor is too strong.
- Open-source is not enough. ...Tryecrypt was Open-source. (lol.)

Reality Check

My advice to users

- Never trust non-free software.
- Chose a client that you understand.
- Don't keep logs. It's stupid and dangerous.
- Get in touch with developpers, they are nice people who want to help you.
- Never underetimate the importance of your feedback or suggestions.

Reality Check

My advice to cypherpunks

- Use an OTR client/implementation that you'd like to play with.
- Using it is the first step to contributions. Even if it's not yours.
- Stick to known secure protocols as much as possible, don't deviate.
- Never underetimate the importance of your feedback or suggestions.