CryptoParty
OTR

Ondřej Profant

Česká pirátská strana

18. května 2013

Osnova

Co je IM?

- instant messaging
- okamžitá komunikace
- např. ICQ, Facebook chat, Google talk
- svobodný prokol jabber

Co je OTR?

- Off-the-Record Messaging
- šifrovací protokol
- šifrování probíhá na klientech (koncových uzlech komunikace)

Co potřebujeme

IM klienta podporujícího OTR.
V našem případě:

- Pidgin - www.pidgin.im
- OTR plugin
- Ubuntu 12.10

Instalace v Ubuntu:
sudo apt-get install pidgin pidgin-otr

Šifrování a autentizace

Šifrování:

zpráva je šifrovaná. To znamená, že si jí lze přečíst pouze se správným klíčem.

Autentizace:

ověření identity. Pokud jen šifrujeme, tak víme pouze to, že na druhé straně je někdo, kdo umí naše zprávy dešifrovat.

Více: http://www.cypherpunks.ca/otr/help/3.2.1/levels.php

Autentizace

3 možnosti ověření identity:

- Question and answer (otázka a odpověď)
- Shared secret (sdílené heslo)
- Manual fingerprint verification (ověření otisku)

Autentizace

3 možnosti ověření identity:

- Question and answer (otázka a odpověď)
- Shared secret (sdílené heslo)
- Manual fingerprint verification (ověření otisku)

Autentizace

3 možnosti ověření identity:

- Question and answer (otázka a odpověď)
- Shared secret (sdílené heslo)
- Manual fingerprint verification (ověření otisku)

Ukázka 1 - Pidgin

Screencast na youtube:
http://youtu.be/4d3pqkelsrU

Ukázka 2 - Xabber

Potřebujeme: Android, Xabber
http://www.xabber.com

Užití velmi podobné jako v Pidginu.

Závěr

Děkuji za pozornost.

Doplňující otázky?

Prezentace v úplné formě[1] na:
https://www.github.com/kedrigern/prezentace-cs, screencast tvořen v programu Kazam.

Mail: ondrej.profant -at- pirati.cz

[1] i se zdrojovými kódy