# CryptoParty
# Steganografie

Ondřej Profant

Česká pirátská strana

18. května 2013

# Osnova

# Motivace

**Problém**

V mnoha státech je šifrování postaveno mimo zákon (resp. je nám k ničemu).

Např.:

- USA, povinnost osoby dešifrovat, uvažovalo se i o povinnosti výrobce šifry dešifrovat *facepalm*
- Velká Britanie, zákon RIPA
- Francie, donedávna bylo povoleno šifrovat jen za účelem autentifikace (ověření) etc. V roce 2004 zrušeno.
- Pakistán, zákaz VPN
- Jistě mnoho dalších autoritářských režimů

# Motivace

## Problém

V mnoha státech je šifrování postaveno mimo zákon (resp. je nám k ničemu).

Např.:

- USA, povinnost osoby dešifrovat, uvažovalo se i o povinnosti výrobce šifry dešifrovat *facepalm*
- Velká Britanie, zákon RIPA
- Francie, donedávna bylo povoleno šifrovat jen za účelem autentifikace (ověření) etc. V roce 2004 zrušeno.
- Pakistán, zákaz VPN
- Jistě mnoho dalších autoritářských režimů

# Motivace

**Problém**

V mnoha státech je šifrování postaveno mimo zákon (resp. je nám k ničemu).

Např.:

- USA, povinnost osoby dešifrovat, uvažovalo se i o povinnosti výrobce šifry dešifrovat *facepalm*
- Velká Britanie, zákon RIPA
- Francie, donedávna bylo povoleno šifrovat jen za účelem autentifikace (ověření) etc. V roce 2004 zrušeno.
- Pakistán, zákaz VPN
- Jistě mnoho dalších autoritářských režimů

# Motivace

## Problém

V mnoha státech je šifrování postaveno mimo zákon (resp. je nám k ničemu).

Např.:

- USA, povinnost osoby dešifrovat, uvažovalo se i o povinnosti výrobce šifry dešifrovat *facepalm*
- Velká Britanie, zákon RIPA
- Francie, donedávna bylo povoleno šifrovat jen za účelem autentifikace (ověření) etc. V roce 2004 zrušeno.
- Pakistán, zákaz VPN
- Jistě mnoho dalších autoritářských režimů

# Motivace

## Problém

V mnoha státech je šifrování postaveno mimo zákon (resp. je nám k ničemu).

Např.:

- USA, povinnost osoby dešifrovat, uvažovalo se i o povinnosti výrobce šifry dešifrovat *facepalm*
- Velká Britanie, zákon RIPA
- Francie, donedávna bylo povoleno šifrovat jen za účelem autentifikace (ověření) etc. V roce 2004 zrušeno.
- Pakistán, zákaz VPN
- Jistě mnoho dalších autoritářských režimů

# Motivace

## Problém

V mnoha státech je šifrování postaveno mimo zákon (resp. je nám k ničemu).

Např.:

- USA, povinnost osoby dešifrovat, uvažovalo se i o povinnosti výrobce šifry dešifrovat *facepalm*
- Velká Britanie, zákon RIPA
- Francie, donedávna bylo povoleno šifrovat jen za účelem autentifikace (ověření) etc. V roce 2004 zrušeno.
- Pakistán, zákaz VPN
- Jistě mnoho dalších autoritářských režimů

# Co je Steganografie?

- metoda skrytí zprávy
- metoda skrytí toho, že zpráva existuje
- zašifrování zprávy

# Co je Steganografie?

- metoda skrytí zprávy
- metoda skrytí toho, že zpráva existuje
- zašifrování zprávy

# Co je Steganografie?

- metoda skrytí zprávy
- metoda skrytí toho, že zpráva existuje
- zašifrování zprávy

# Co je Steganografie?

- metoda skrytí zprávy
- metoda skrytí toho, že zpráva existuje
- zašifrování zprávy

# Instalace (vybrané OS)

Stránka projektu: http://steghide.sourceforge.net

- Ubuntu:
  1. wget https://launchpad.net/ubuntu/+archive/primary/+files/steghide_0.5.1-9build2_amd64.deb
  2. sudo dpkg -i steghide_0.5.1-9build2_amd64.deb
- Fedora:
  Předpřipravený balík na of. stránkách
- Windows:
  Předpřipravený balík na of. stránkách

# Použití

Připravíme si:

- běžný obrázek: obrazek.jpg
- tajnou zprávu (prostý text): tajna.zprava.txt
- aplikace: steghide

Pro zašifrování použijeme příkaz:

steghide embed\
–embedfile tajna.zprava.txt\
–coverfile obrazek.jpg\
–stegofile obrazek.plus.jpg

Pro dešifrování použijeme:

steghide extract\
–stegofile obrazek.plus.jpg\
–extractfile tajna.zprava.txt

# Stegotools

Homepage: http://sourceforge.net/projects/stegotools
Bohužel podporuje pouze bitmapy (*.bmp), což dnes není příliš běžný formát.

# OutGuess

Homepage: http://www.outguess.org
Obsažen v linuxových distribucích.
Šifrování:
outguess -k heslo -d tajna.zprava.txt obrazek.jpg obrazek.outguess.jpg
Dešifrování:
outguess -k heslo -r obrazek.plus2.jpg out.txt

# Poznámka

Programy jsou vzájemně nekompatibilní!
Což je dobře. Jednotný protokol není z důvodů zachování utajení zprávy.

# Stegdetect

Program pro zjišťování steganogradie.
Od autora OutGuess. Mé pokusy nedopadly příliš dobře - určoval velmi nepřesně.

# StegFS

Steganografický souborový systém!
Bohužel, to již někdy příště.
Homepage: https://albinoloverats.net/projects/stegfs

# Zdroje


1. homepages jednotlivých projektů
2. http://cs.wikipedia.org/wiki/Steganografie
3. http://www.root.cz/clanky/jak-ukryt-tajna-data-do-obrazku-aneb-steganografie-v-praxi
4. http://www.zive.cz/clanky/nejlepsi-program-pro-steganografii/sc-3-a-163982/default.aspx
5. http://en.wikipedia.org/wiki/Cryptography_law

# 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