

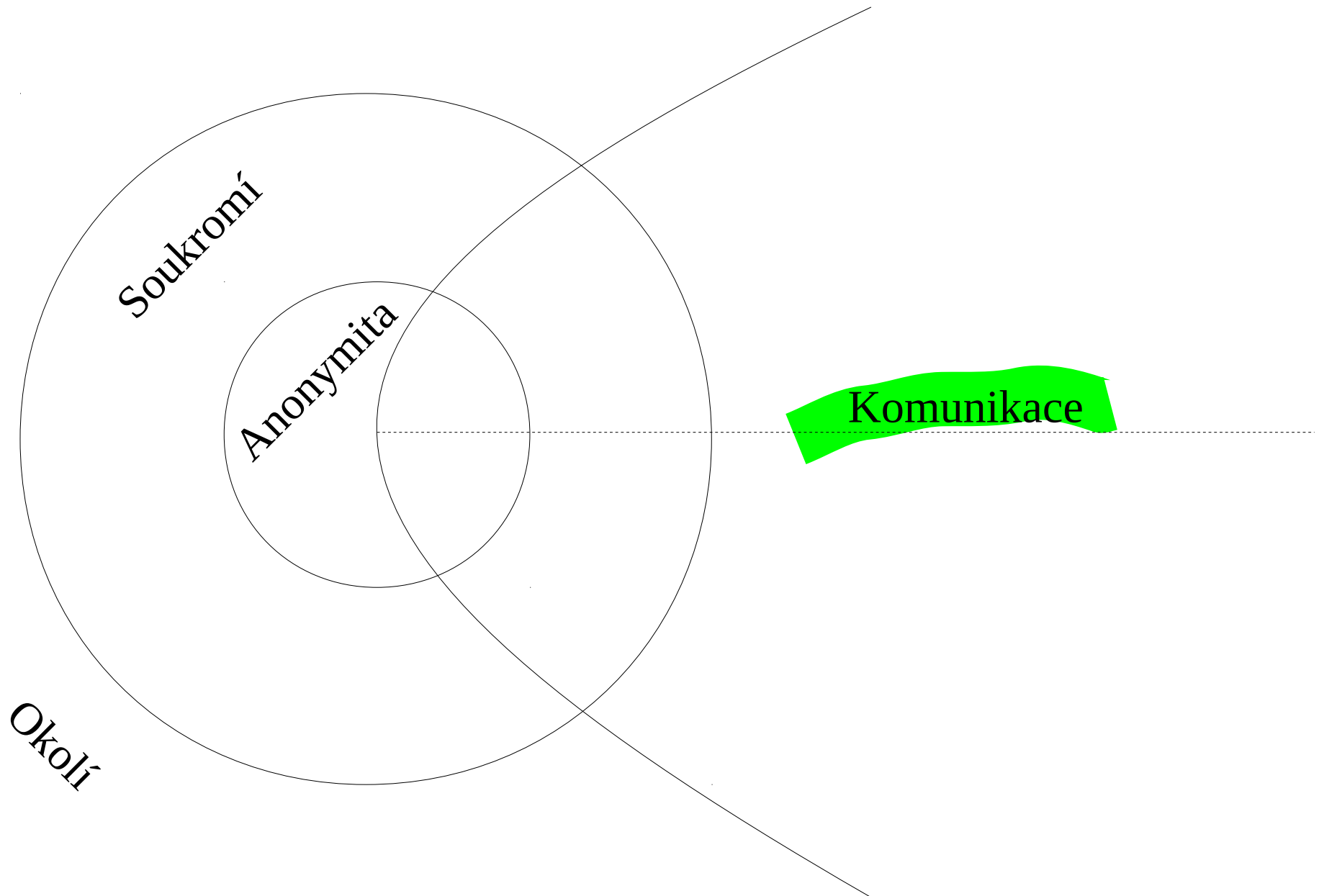


Já, anonym

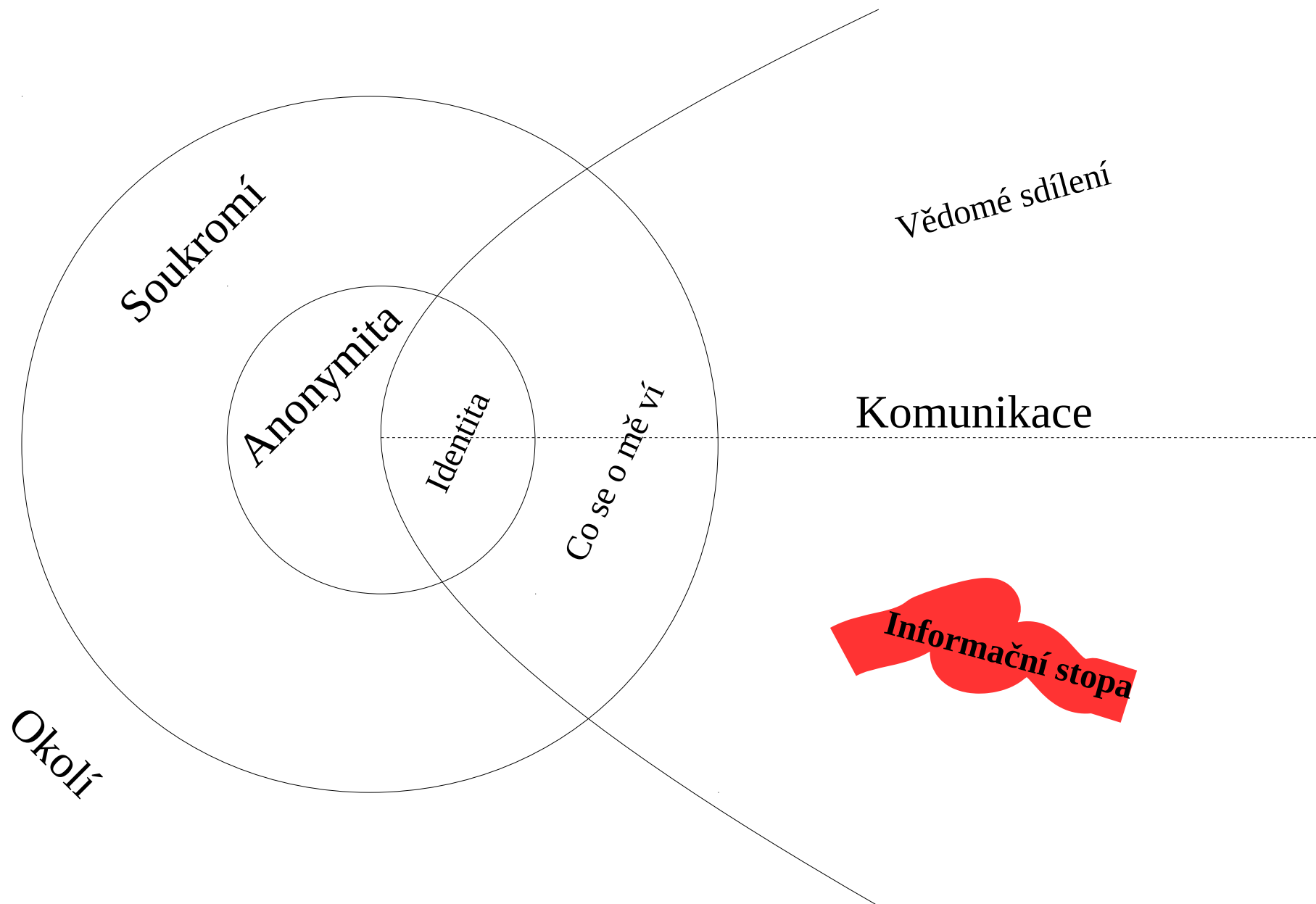
Pavel Kácha
<ph@cesnet.cz>



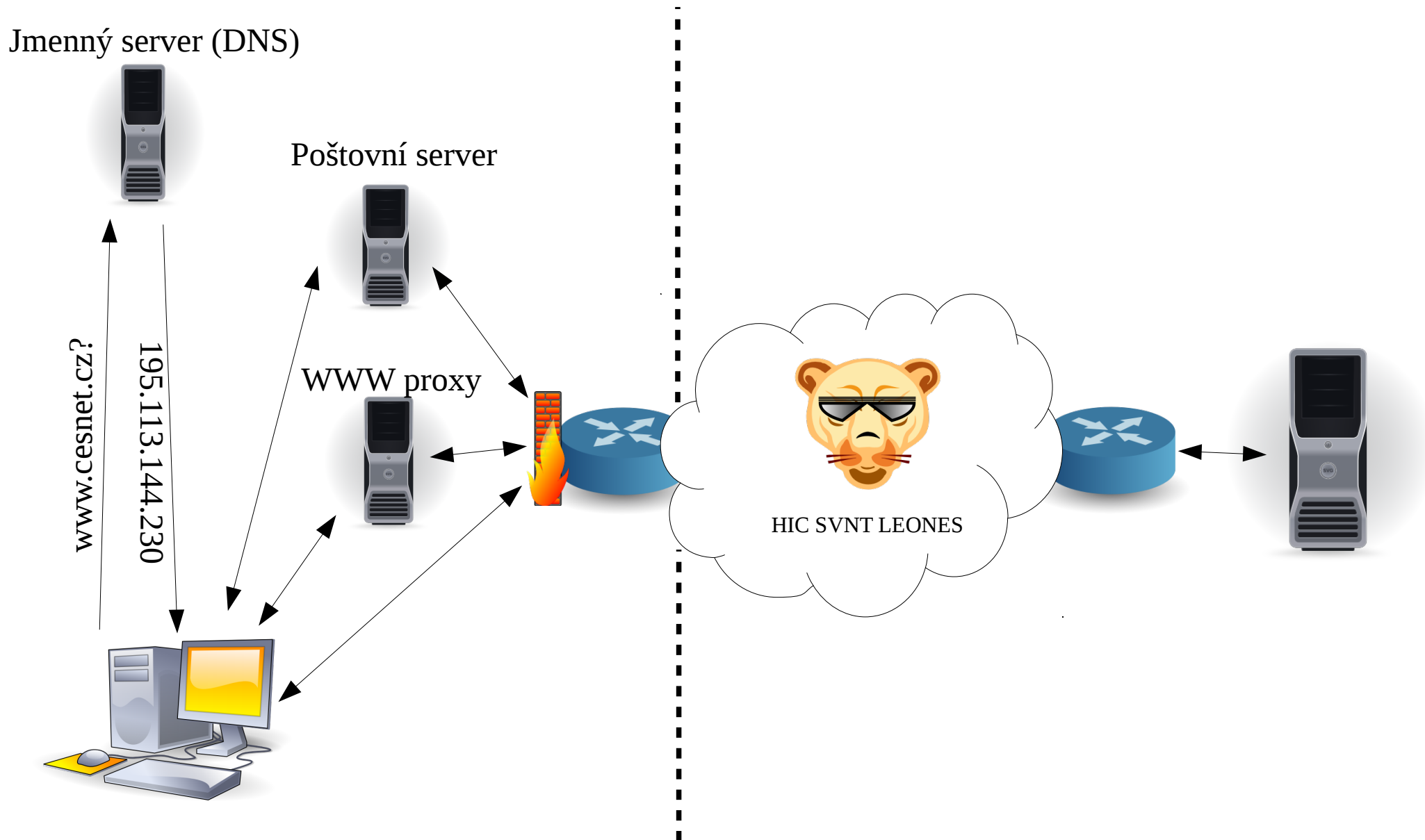
Soukromí? Anonymita?



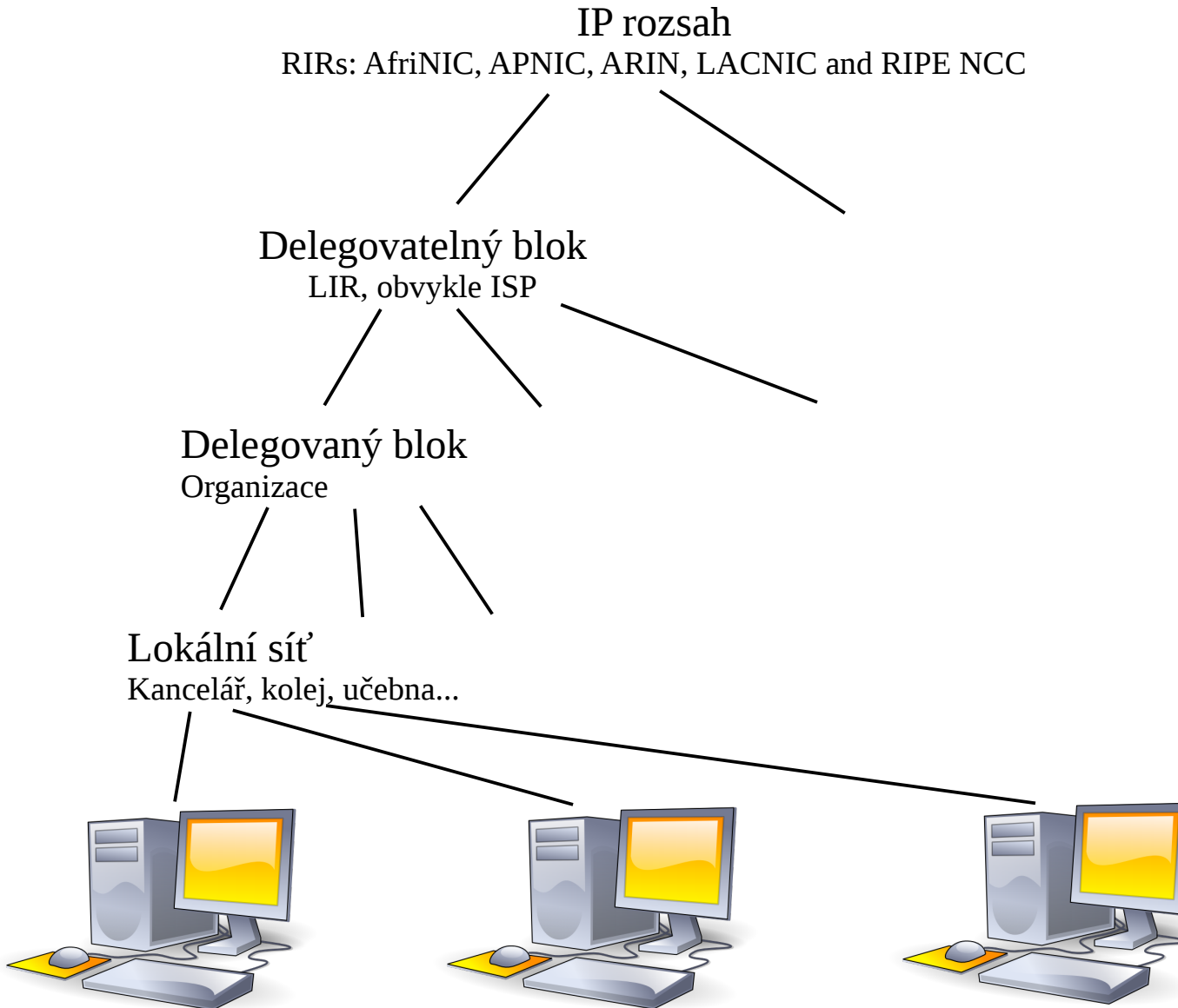
Informační stopa



Cesta informace



IP svět



195.93.216.xx

RIPE

CESNET

ZCU_TCZ

Lokální síť

Uživatel

RIR - RIPE

\$ whois 195.93.216.0

inetnum: 147.228.0.0 - 147.228.255.255
netname: ZCU-TCZ
descr: Zapadoceska univerzita
descr: Plzen
country: CZ
org: ORG-UOWB1-RIPE
admin-c: UOWB1-RIPE
tech-c: UOWB1-RIPE
status: LEGACY
mnt-by: TENCZ-MNT
remarks: Please report network abuse ->
abuse@zcu.cz

route: 147.228.0.0/16
descr: ZCU-TCZ
origin: AS2852
mnt-by: AS2852-MNT

organisation: ORG-UOWB1-RIPE
org-name: Zapadoceska univerzita v Plzni
org-type: OTHER
address: Zapadoceska univerzita v Plzni
address: Univerzitni 8
address: Plzen
address: 306 14
address: The Czech Republic
phone: +420 377 635 700
abuse-mailbox: abuse@zcu.cz
org: ORG-CA9-RIPE
admin-c: UOWB1-RIPE
tech-c: UOWB1-RIPE
abuse-c: UOWB1-RIPE
mnt-ref: TENCZ-MNT
mnt-by: TENCZ-MNT

person: Vladimir Rudolf
address: Zapadoceska univerzita v Plzni
address: Centrum informatizace a
vypocetni techniky
phone: +420 377 632 700
phone: +420 377 632 805
abuse-mailbox: abuse@zcu.cz
nic-hdl: VR3-RIPE
mnt-by: TENCZ-MNT

IP mikrokosmos

- Přidělování IP adres
 - Na základě HW adresy (MAC)
 - Na základě elektronické identity (login + heslo)
- Bezdrátové sítě
 - Možnost určení polohy (triangulace)
 - Pozor na provoz vlastního AP!
- Vazba IP adresa – čas – uživatel
 - Lokální správce ví přesně, komu a kdy bylo IP přiděleno
 - Používaná IP adresa není anonymní!

Auditní záznamy

- WWW

[06/Dec/2010:12:34:37 +0100]

195.113.134.228 grey.cesnet.cz

"GET /search?Gravity+free+download HTTP/1.1" 200 1986 "-"

"Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.14pre)

Gecko/20101204 Ubuntu/9.10 (karmic) Namoroka/3.6.14pre"

- Elektronická pošta

Nov 22 15:05:58 office2 postfix/smtpd[27935]: CAF18ED0073:

client=grey.cesnet.cz[2001:718:1:6::134:228], sasl_method=LOGIN,
sasl_username=pavelk

Nov 22 15:05:58 office2 postfix/cleanup[30693]: CAF18ED0073:

message-id=<20131122140558.GC1700@cesnet.cz>

Nov 22 15:05:59 office2 postfix/qmgr[2599]: CAF18ED0073:

from=<ph@cesnet.cz>, size=7206, nrcpt=1 (queue active)

Nov 22 15:06:00 office2 postfix/smtp[31597]: CAF18ED0073:

to=<oleg@cesnet.cz>, relay=postino.cesnet.cz[195.113.144.242]:25,

delay=2.1, delays=1/0/1/0.11, dsn=2.0.0,

status=sent (250 2.0.0 rAME5x59029798 Message accepted for delivery)

Účel

Řešení problémů

Jaká práva má uživatel?
Byl požadavek předán dál?
S jakou skončil chybou?
Proč?



Ladění služby/sítě

Kolik požadavků v jakých okamžicích služba vyřizuje?

Na jaké cíle?

Kde je vhodné optimalizovat?

Kde jsou úzká místa?

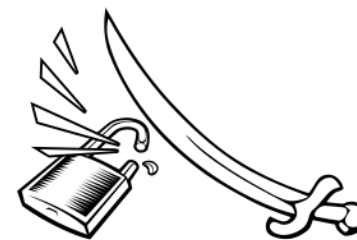
Bezpečnost

Nejsou požadavky na službu neobvyklé?

Na konkrétní stránku? Adresu?

V neobvyklém množství? Formátu?

Nepřístupuje klient na místo, kam přístup mít nemá?



Ochrana provozovatele

„Za dětskou pornografií na serveru neneseme zodpovědnost,
neboť ji tam nahrál uživatel X v čase Y z adresy Z“

Přístup k datům

- Je třeba mít kompletní přístup k datům, se kterými pracuji
- A vždy existují zaměstnanci, kteří musí mít přístup k
 - Logům
 - Administrativním rozhraním
 - Datům uživatelů

GCreep: Google Engineer Stalked Teens, Spied on Chats (Updated)



Adrian Chen

Filed to: EXCLUSIVE 9/14/10 3:26pm

569,687 🔥 3 ★



We entrust Google with our most private communications because we assume the company takes every precaution to safeguard our data. It doesn't. A Google engineer spied on four underage teens for months before the company was notified of the abuses.

David Barksdale, a 27-year-old former Google engineer, repeatedly took advantage of his position as a member of an elite technical group at the company to access users' accounts, violating the privacy of at least four minors during his employment, we've learned. Barksdale met the kids through a technology group in the Seattle area while working as a Site Reliability Engineer at Google's Kirkland, Wash. office. He was fired in July 2010 after his actions were reported to the company. [Update: Google has confirmed the security breach. An update appears below.]

<http://gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats>

Co o nás prozradí SW - WWW

```
connection: keep-alive
accept-language: cs,en;q=0.7,en-us;q=0.3
content-length: 0
accept-encoding: gzip,deflate
referer: http://www.google.com/search?q=cesnet&ie=UTF-8&oe=UTF-8
host: www.cesnet.cz
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
accept-charset: windows-1250,utf-8;q=0.7,*;q=0.7
keep-alive: 300
user-agent: Mozilla/5.0 (X11; U; Linux i686; cs-CZ; rv:1.9.0.4)
           Gecko/2008112309 Icedweasel/3.0.3 (Debian-3.0.3-3)

cookie: UID=ph; SESSION_ID=AF347DC667.33985
```

- Referer – stránka, ze které přicházím
- Prohlížeč, platforma včetně přesné verze
(Kde nechal tesař díru v této verzi..?)
- Cookie – identifikátor sezení nezávislý na IP
(personalizace, sledování)

Příklad: Orbitz – uživatelé Maců si zaslouží férovou cenu

<http://edition.cnn.com/2012/06/26/tech/web/orbitz-mac-users/>



Nevíme, kdo jste, ale vítejte zpátky

- Cookie, Flash Cookie, Silverlight Storage, IE UserData, HTML5 Storage, Cache, historie...

samy.pl/evercookie

- UserAgent, HTTP_ACCEPT, nainstalované pluginy, fonty, časová zóna, rozlišení, cookies, JS vlastnosti

panopticklick.eff.org

- Zkuste si sami

browserspy.dk

- Rozšíření *LightBeam* pro Firefox

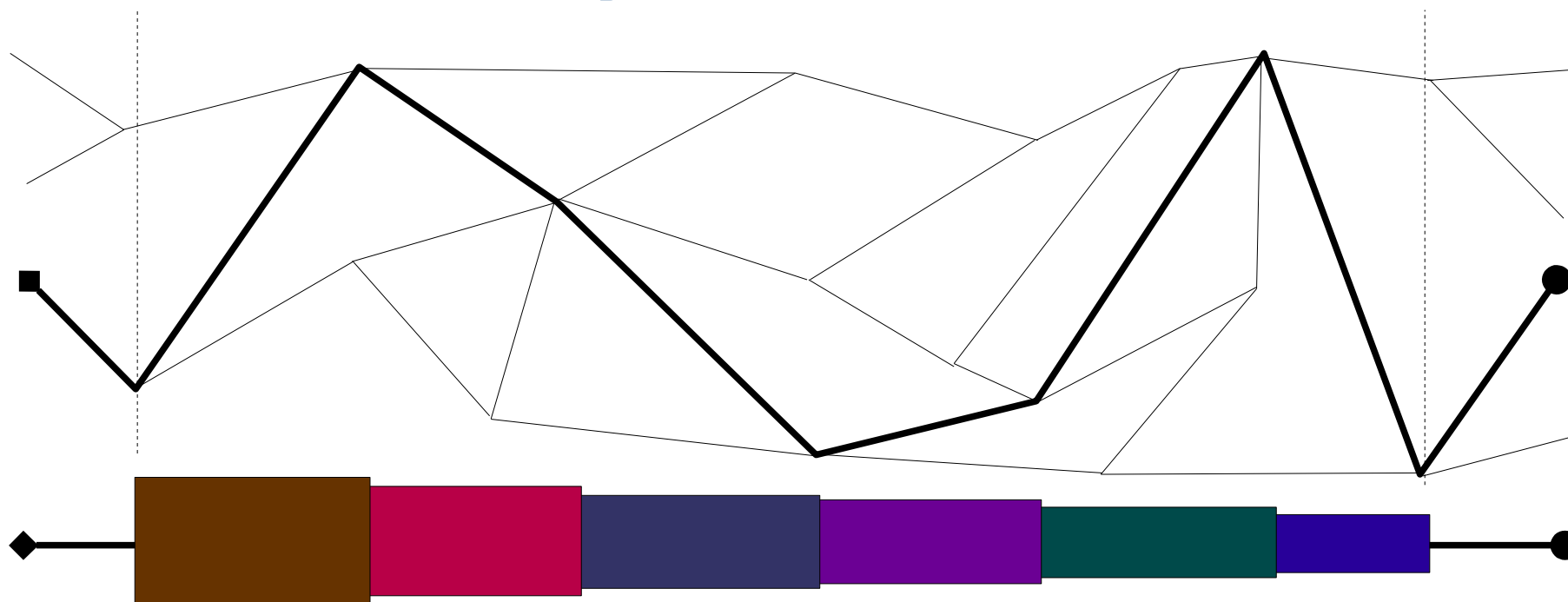
P2P sítě



- Ve většině sítí je stahovaný obsah automaticky nabízen
 - Někdy lze v klientech omezit (pozor na nastavení po instalaci)
 - U některých je to nedílná vlastnost protokolu (BitTorrent)
- Po připojení do P2P sítě
 - Informace o mně (a mé nabídce) se šíří sítí
 - Vidí je každý, kdo o ně má zájem ...
... tedy i vlastníci autorských práv!
 - Velké filmové společnosti jsou velmi aktivní

<https://www.google.com/transparencyreport/>

Anonymizace - Tor

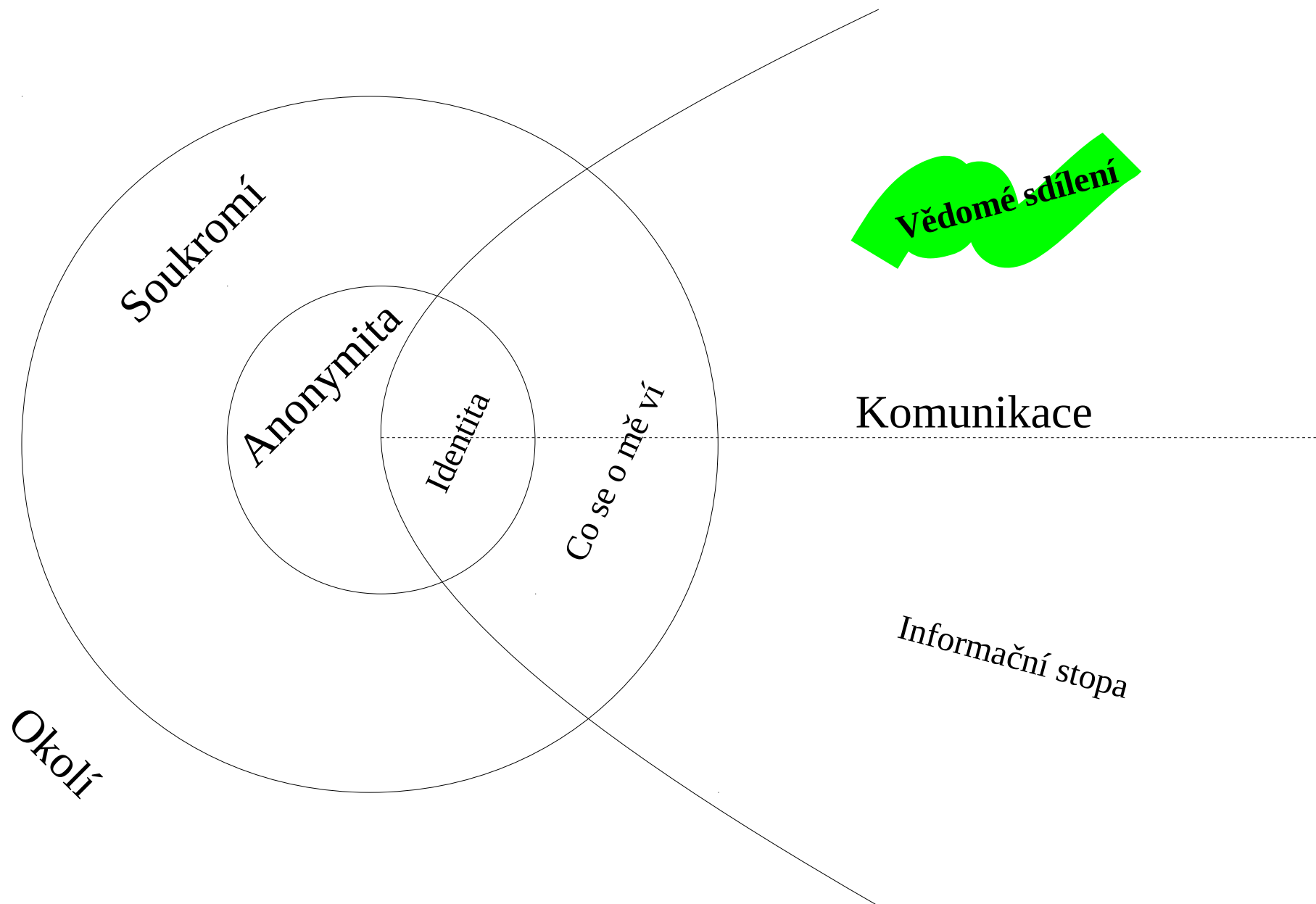


- Žádný uzel nezná kompletní cestu
- Síť je heterogenní
- ! výstupní uzel může nést zodpovědnost
- ! hraniční uzly musí vidět původní data

Tor je síť dobrovolníků

– a s dostatečnou výpočetní silou lze mít pod kontrolou zajímavou část exitů

Vědomé sdílení





Kdo jsme



- Osobní stránky, blog, CV
 - Skryté stránky – zpětné odkazy, webmail
- Cloud   
- Freemail  
- Odkazy, komentáře
- Veřejné databáze: CZ.NIC, RIPE
 - Ale i: Obchodní rejstřík, Katastr nemovitostí
- Co o nás napíše jiní
 - V diskusích, na sociálních sítích
 - Na firemních a školních webech



Na této fotce označen:
[Pavel Kácha](#)

Přidáno 20 leden

- [To se mi líbí](#) 
- [Přidat komentář](#)



... kde se můžeme ocitnout



Hledání vazeb

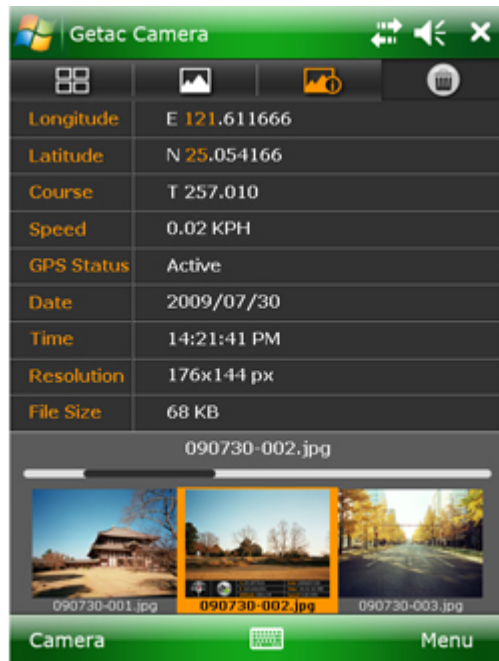
- Přezdívky, neobvyklá jména
- Zpětné odkazy
- Fotografie
 - zpětné hledání – TinEye, Google Images



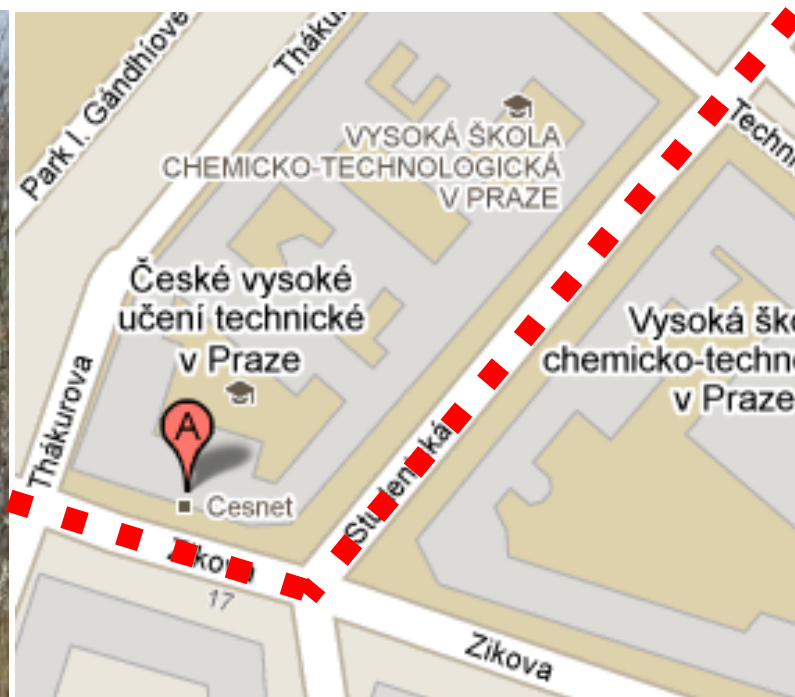
Kde jsme

-  
PLEASE ROB ME

- Fotografie
 - GeoTag -> EXIF
- Wifi síť - SSID



Wifi



Wardriving ve velkém...

Sociální inženýrství

- Průzkum Carnegie Mellon University

<https://www.andrew.cmu.edu/user/nicolasc/publications/CEVG-FC11.pdf>

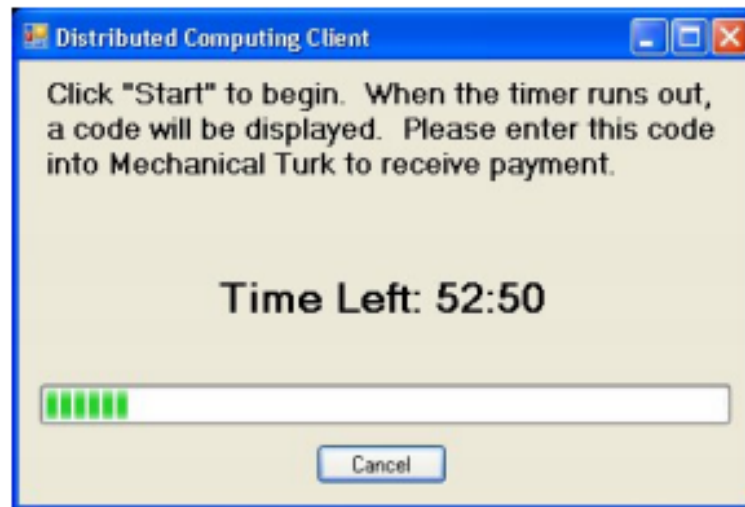


Fig. 1. Screenshot of the “Distributed Computing Client.” After subjects clicked a start button, a timer ran for one hour. Once the timer expired, a completion code was displayed. Subjects entered this completion code into Mechanical Turk in order to receive payment.

Využití dat?



Target – překvapení pro rodiče

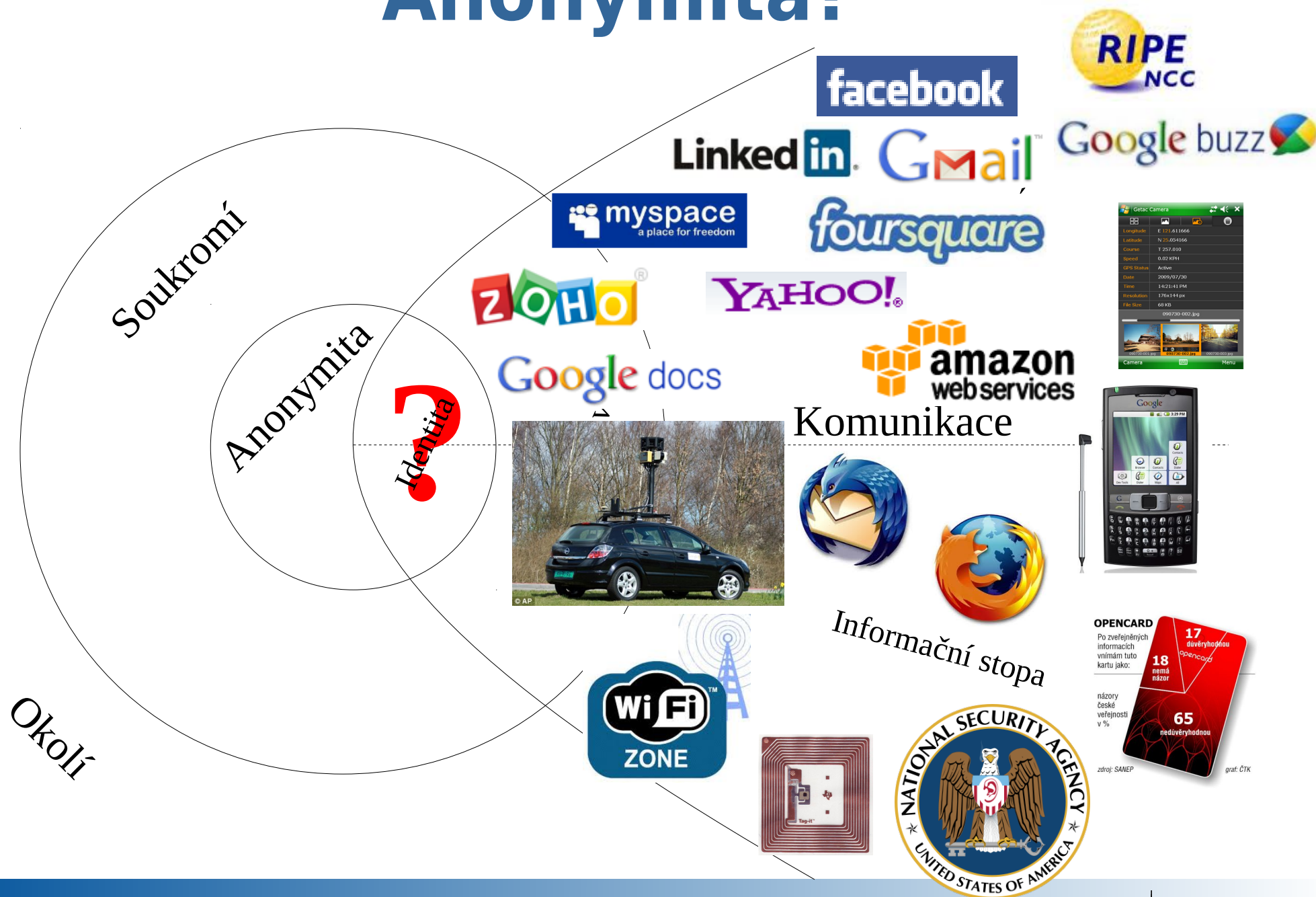
<http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>



Pojišťovny – screening sociálních sítí je levnější, než zdravotní testy

<http://online.wsj.com/news/articles/SB10001424052748704648604575620750998072986?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052748704648604575620750998072986.html>

Anonymita?



Děkuji za pozornost.

The Joy of Tech™



© 2013 Geek Culture

by Nitrozac & Snaggy



joyoftech.com