Internet Survival Kit

CESNET, z. s. p. o.

CESNET

- Provoz a rozvoj páteřní akademické počítačové sítě České republiky
- Založen v roce 1996
- Členové

  25 českých univerzit

  Akademie věd ČR

www.cesnet.cz

My

CESNET-CERTS (csirt.cesnet.cz, certs@cesnet.cz)

- Centrální a důvěryhodný kontaktní bod
- Řešení a koordinace bezpečnostních incidentů v síti CESNET
- Projekty pro podporu bezpečnosti

  (IDS, Audit, Honeypoty, Snort, Mentat, Warden)
- Spolupráce s dalšími projekty a týmy

  (FTAS, WIRT ZČU, CSIRT-MU)

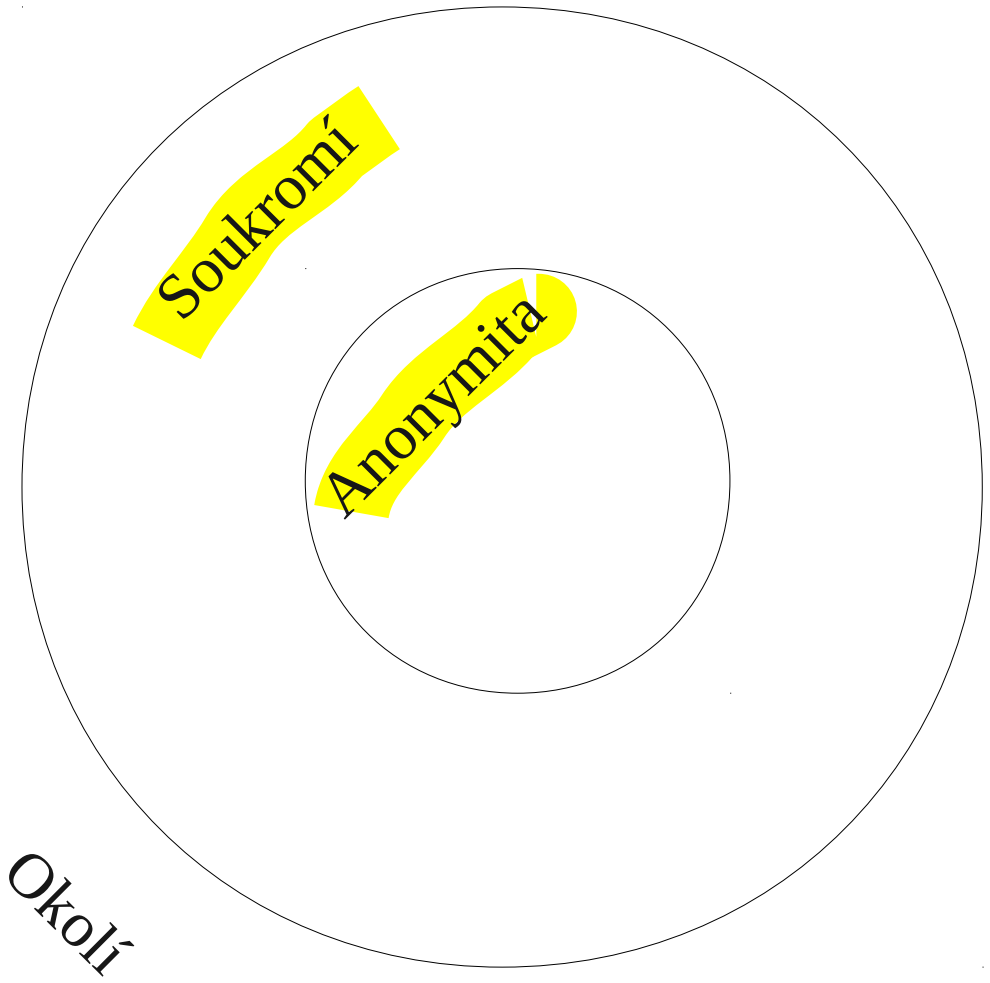
Inspirace pro seminář

- Z reakcí “provinilců” při řešení BI v síti CESNET2:
- Já jsem nenabízel, jenom stahoval!
- Jak by na mě někdo mohl přijít?
- Na síti přece není vidět co dělám.
- Nikdo mi nedokáže, že jsem to byl já!
- Na VŠ si můžu dělat co chci, zaručují mi to akademické svobody!
- Na Internetu je přece všechno free ...
- Licenci na OS/SW? “Půjčil” jsem si ji od kamaráda.
- Já na licence nemám peníze.
- Ale já jsem to napsal jenom na Facebook!

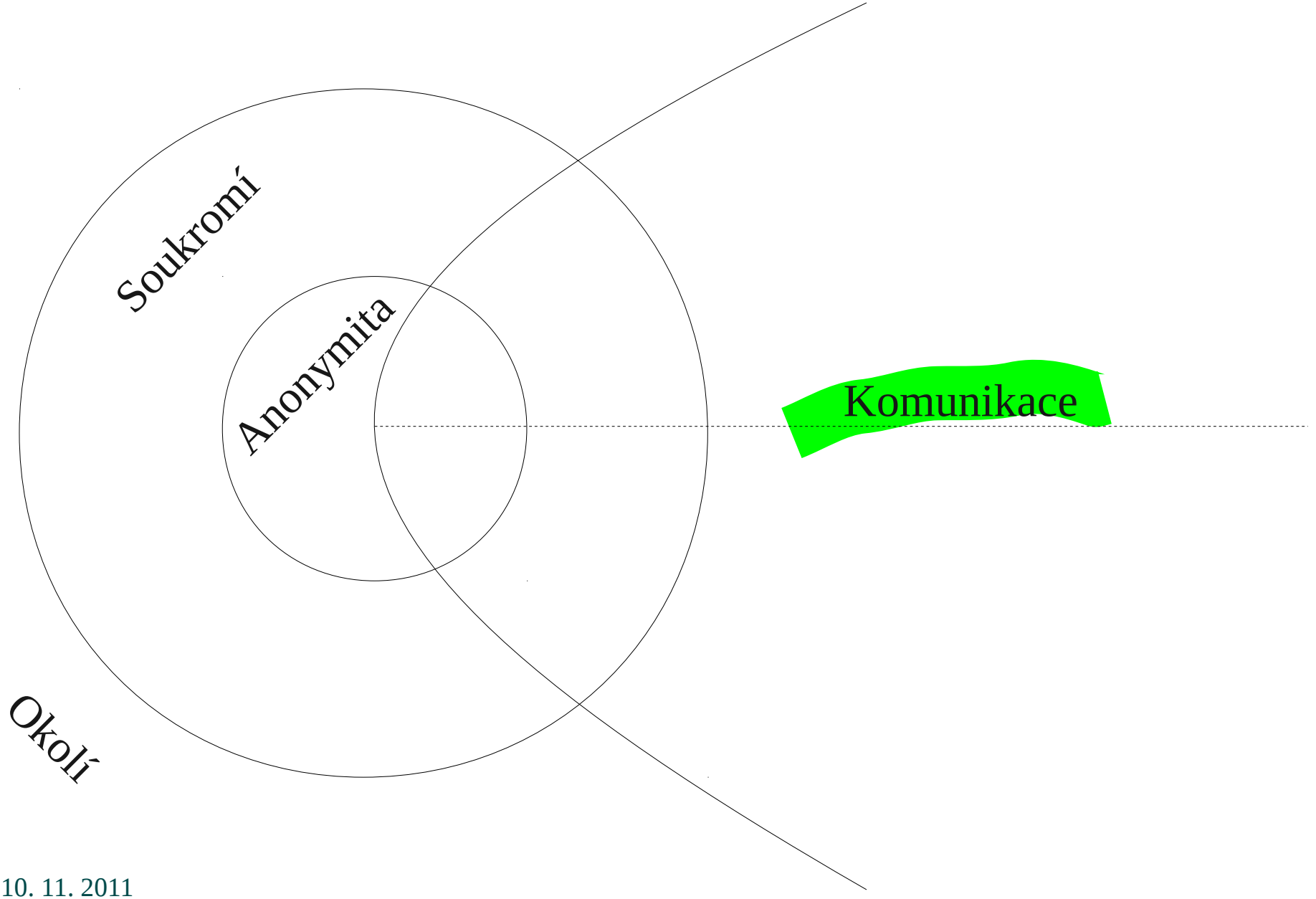
Identita, soukromí, anonymita

Pavel Kácha
CESNET, z. s. p. o.

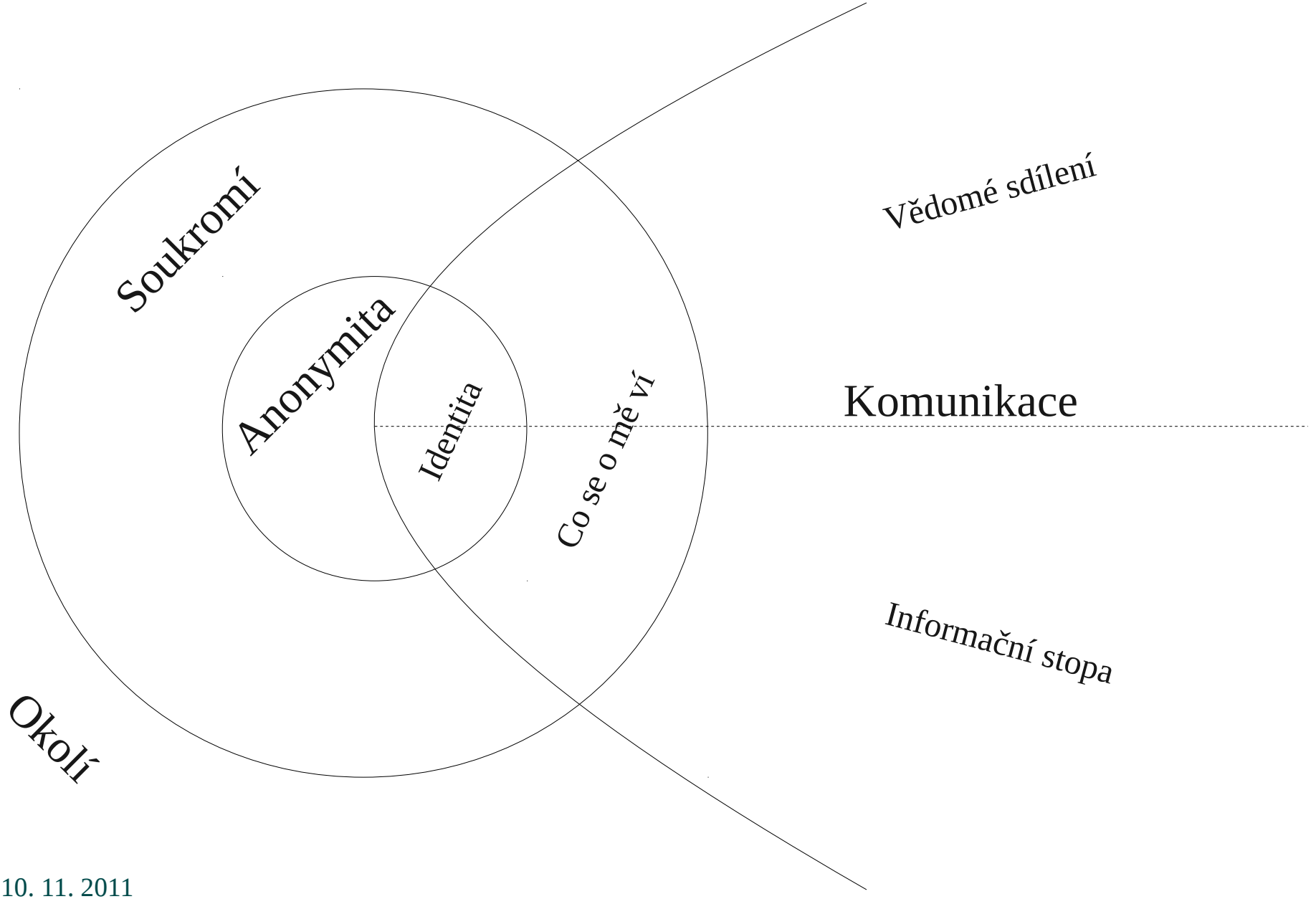
Já



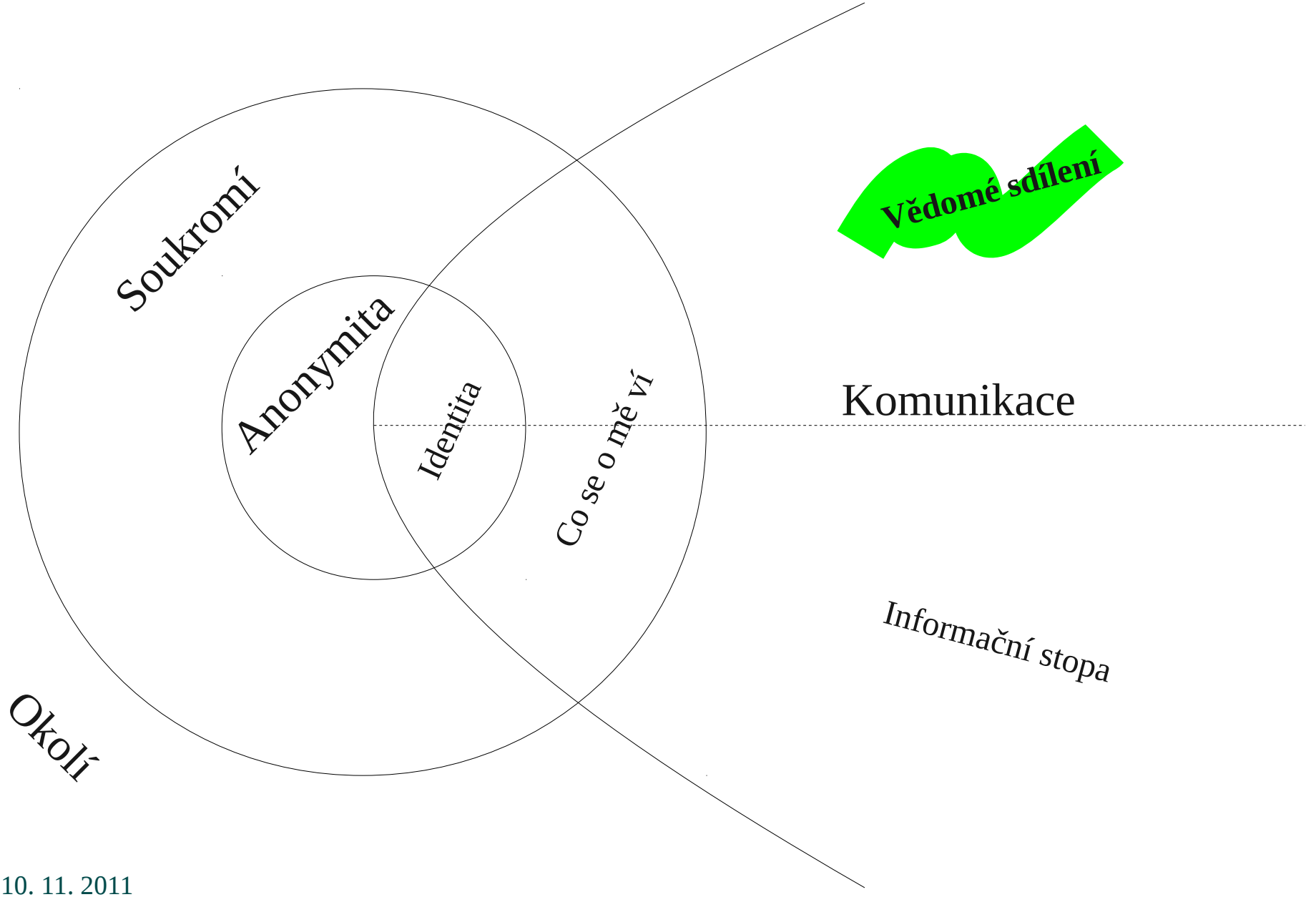
Já



Já


Soukromí
Anonymita
Identita
Co se o mě ví
Okolí
Vědomé sdílení
Komunikace
Informační stopa

Vědomé sdílení



Kdo jsme

- facebook myspace a place for freedom LinkedIn
- Osobní stránky, blog, CV
  - Skryté stránky – robots.txt, zpětné odkazy, webmail
- Cloud ZOHO Google docs amazon web services
- Freemail YAHOO! Gmail
- Odkazy, komentáře
- CZ.NIC, RIPE

```
inetnum:        195.113.134.128 - 195.113.134.255
netname:        CESNET-BB2
descr:          CESNET, z.s.p.o.
descr:          Prague 6
country:        CZ
admin-c:        VN2-RIPE
tech-c:         VN2-RIPE
status:         ASSIGNED PA
mnt-by:         TENCZ-MNT
mnt-lower:      TENCZ-MNT
remarks:        Please report network abuse -> abuse@cesnet.cz
source:         RIPE # Filtered
```

Hledání vazeb

- Přezdívky, neobvyklá jména
- Fotografie (zpětné hledání – TinEye, Google Goggles)

- PGP keystore

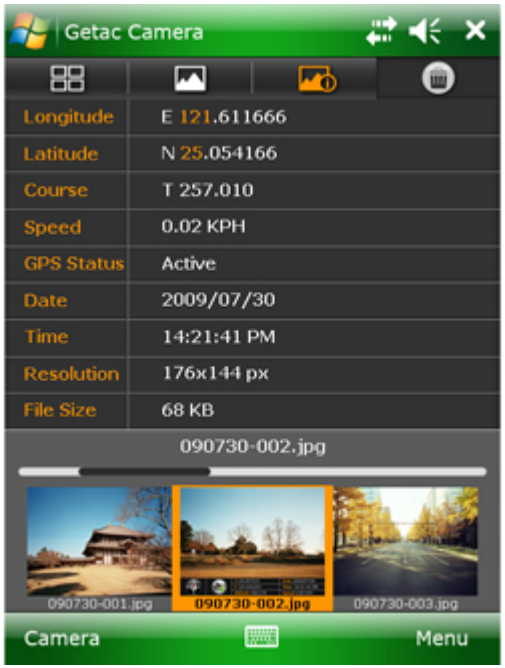
```
uid Pavel Kacha <ph@rook.cz>
sig  sig3  2B2663F8 2002-04-09 __________ __________ [selfsig]
sig  sig   687DA204 2002-04-09 __________ __________ Pavel Kácha (pharook) <ph@cesnet.cz>
sig  sig   163DF9EB 2002-04-09 __________ __________ Pavel K?cha (pharook) <ph@cesnet.cz>
sig  sig   CA57AD7C 2005-06-15 2005-06-29 __________ PGP Global Directory Verification Key
sig  sig   9CAA8579 2008-11-20 __________ __________ CESNET-CERTS <certs@cesnet.cz>
sig  sig   8ECA352E 2008-11-23 __________ __________ CESNET NIC <nic@ces.net>

uid Pavel Kacha <ph@cesnet.cz>
sig  sig3  2B2663F8 2002-04-09 __________ __________ [selfsig]
sig  sig   687DA204 2002-04-09 __________ __________ Pavel Kácha (pharook) <ph@cesnet.cz>
sig  sig   163DF9EB 2002-04-09 __________ __________ Pavel K?cha (pharook) <ph@cesnet.cz>
sig  sig   CA57AD7C 2004-12-30 2005-01-13 __________ PGP Global Directory Verification Key
sig  sig   9CAA8579 2008-11-20 __________ __________ CESNET-CERTS <certs@cesnet.cz>
sig  sig   8ECA352E 2008-11-23 __________ __________ CESNET NIC <nic@ces.net>
```

Kde jsme

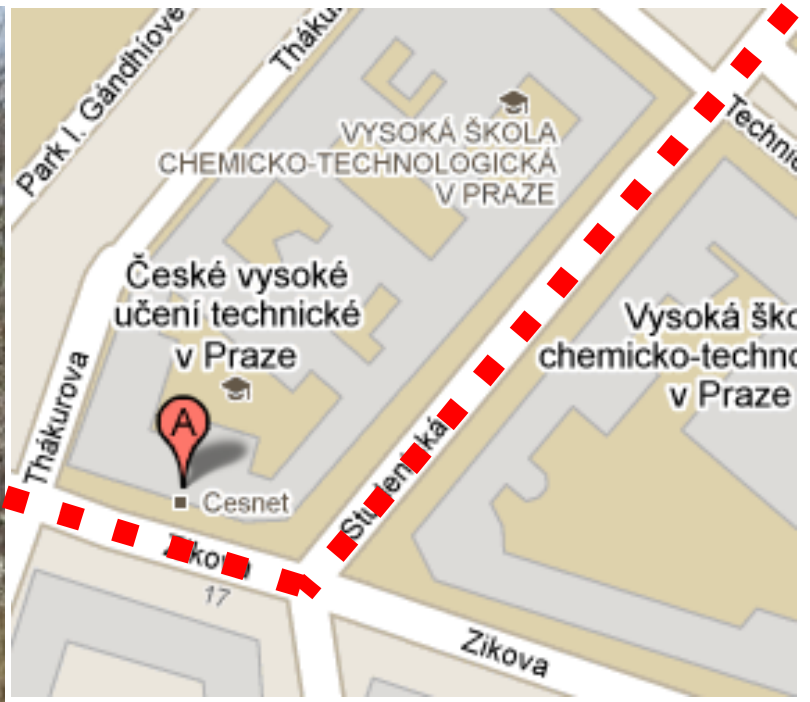
- foursquare Google buzz

  PLEASE ROB ME .com

- Fotografie
  - GeoTag -> EXIF
- Wifi sítě - SSID



Wifi



Wardriving ve velkém...

Wifi

… a v menším

Sociální inženýrství

Robin Sage experiment

- Specialistka na bezpečnost, 25 let
- Stovky přátel během několika měsíců
  Bezpečnostní oddělení firem, vládní a armádní složky...

Robin Sage (you)
N8 at NETWARCOM
Norfolk, Virginia Area | Computer & Network Security

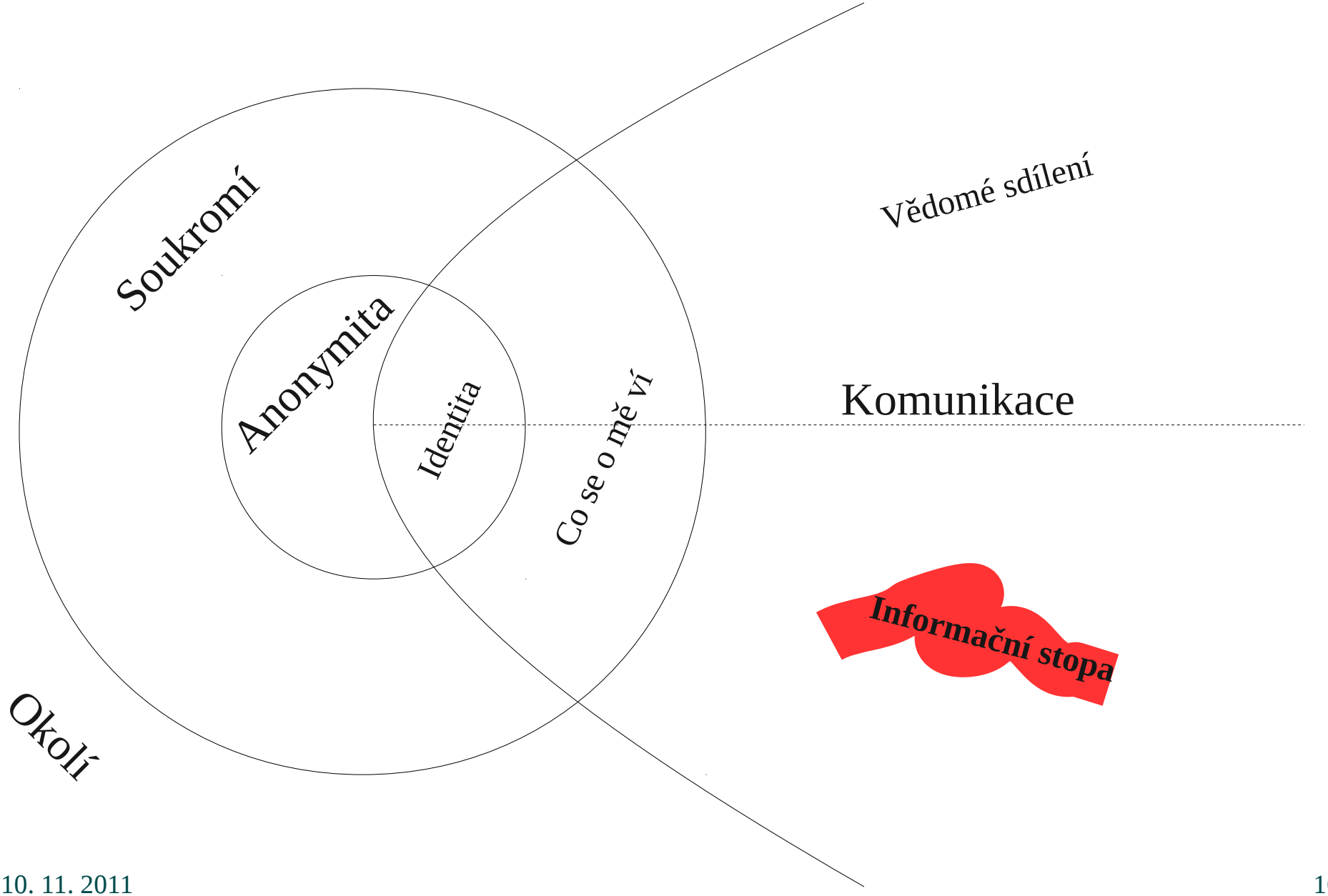
Current	• N8 at Naval Network Warfare Command
Past	• Intern at Government Agency
Education	• Massachusetts Institute of Technology • St. Paul's School
Recommendations	1 person has recommended Robin
Connections	142 connections
Websites	• Where I Work • Dark Side of Security • My Facebook
Twitter	• robinsage
Public Profile	http://www.linkedin.com/in/robinsage

FIKCE

Summary

I have been in the computer hacking scene for over ten years. During this time I have penetrated hundreds of networks as a professionally contracted hacker and was empowered by the adrenaline rush of breaking into secured facilities of Global 500 companies and various governments. Because of my style and diverse areas of expertise, many of my friends refer to me as the real life Abby Scuito of NCIS.

Informační stopa



Informační stopa

- Co o nás napíší jiní
  - V diskusích, na sociálních sítích
  - Na firemních a školních webech
- Zpětné odkazy
- Interview, videa
- Fotografie
  - Označené osoby
  - EXIF
  - Identifikovatelné objekty

Na této fotce označen:
Pavel Kácha

Přidáno 20 leden
· To se mi líbí
· Přidat komentář

Identifikovatelné objekty

Auditní informace – mail

```
Return-Path: johann@cesnet.cz
X-Original-To: ph@cesnet.cz
Delivered-To: ph@office2.cesnet.cz
Received: from [195.113.xxx.yyy] (eduroam-XXX.cesnet.cz [195.113.xxx.yyy])
        by viden.cesnet.cz (Postfix) with ESMTP id 01567D800D1
        for <ph@cesnet.cz>; Mon,  1 Dec 2008 15:58:41 +0100 (CET)
Subject: Re: Pozdravy z Vidne
From: Johann Strauss <johann.strauss@cesnet.cz>
To: Pavel Kácha <ph@cesnet.cz>
In-Reply-To: <20081201142058.GB1602@cesnet.cz>
Date: Mon, 01 Dec 2008 15:58:44 +0100
Message-Id: <1223453524.3834.24.camel@eduroam-221.cesnet.cz>
Mime-Version: 1.0
X-Mailer: Evolution 2.12.3 (2.12.3-5.fc8)
```

- Skutečný odesílatel
- Cesta přes servery
- Zdrojové jméno počítače
- Platforma
- Mailový klient, včetně přesné verze

Auditní informace – 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 Iceweasel/3.0.3 (Debian-3.0.3-3)

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

- Referer – stránka, ze které přicházím
- Prohlížeč včetně přesné verze
- Platforma včetně přesné verze
- Cookie – identifikace uživatele nezávisle na IP adrese (personalizace, sledování)

http://browserspy.dk http://panopticlick.eff.org http://samy.pl/evercookie/

Nevíme, kdo jste, ale vítejte zpátky

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

  samy.pl/evercookie

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

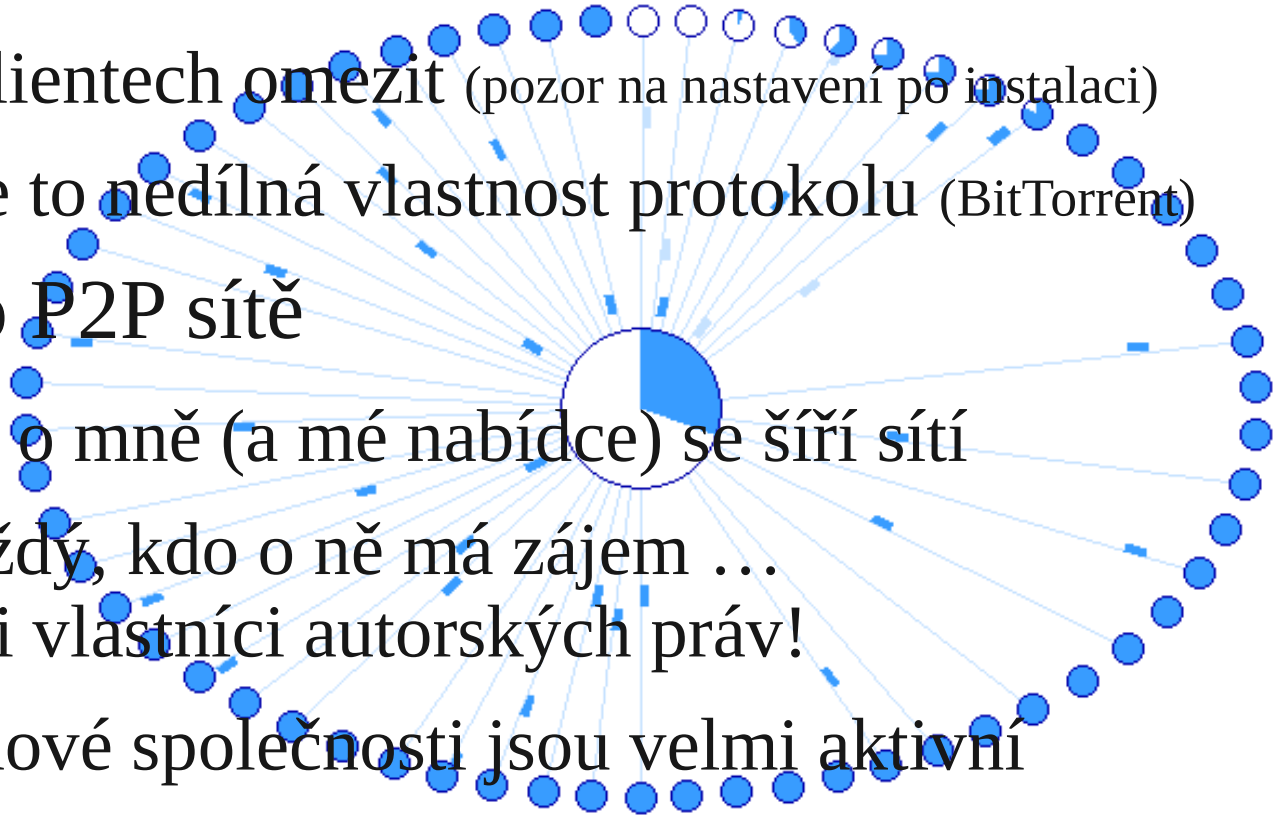
  panopticlick.eff.org

- Zkuste si sami

  browserspy.dk

P2P sítě a autorský zákon

- 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



RFID

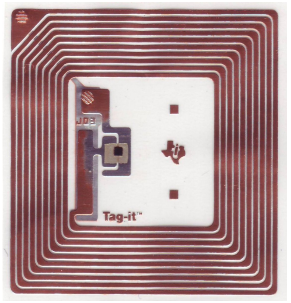
Karty

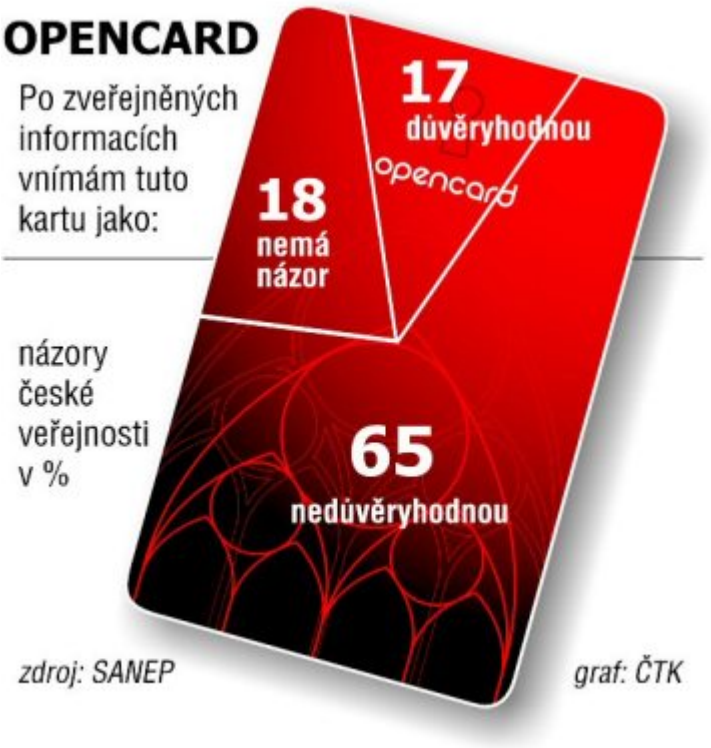
Vstupní tokeny

Auto zámky

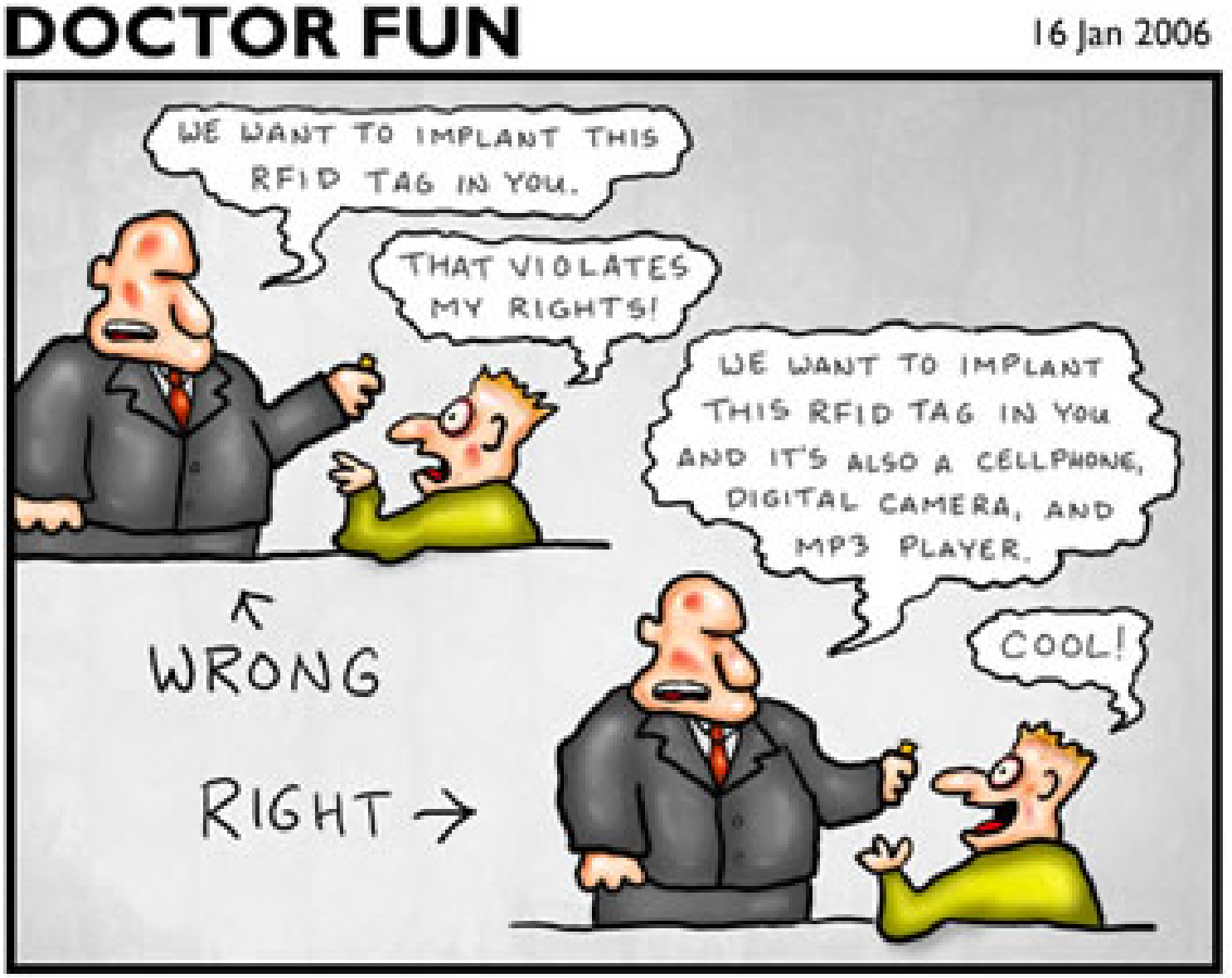
Sledování zboží

Budoucnost USA:
pasy, kreditní karty



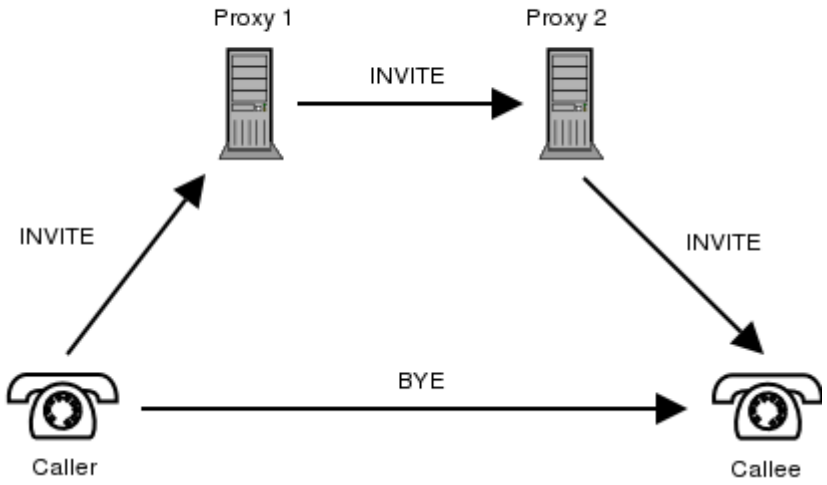


A nemůžeme si za to sami..?



Využití

- Spear phishing
- Krádež identity
- Man-in-the-Middle
- Sociální inženýrství



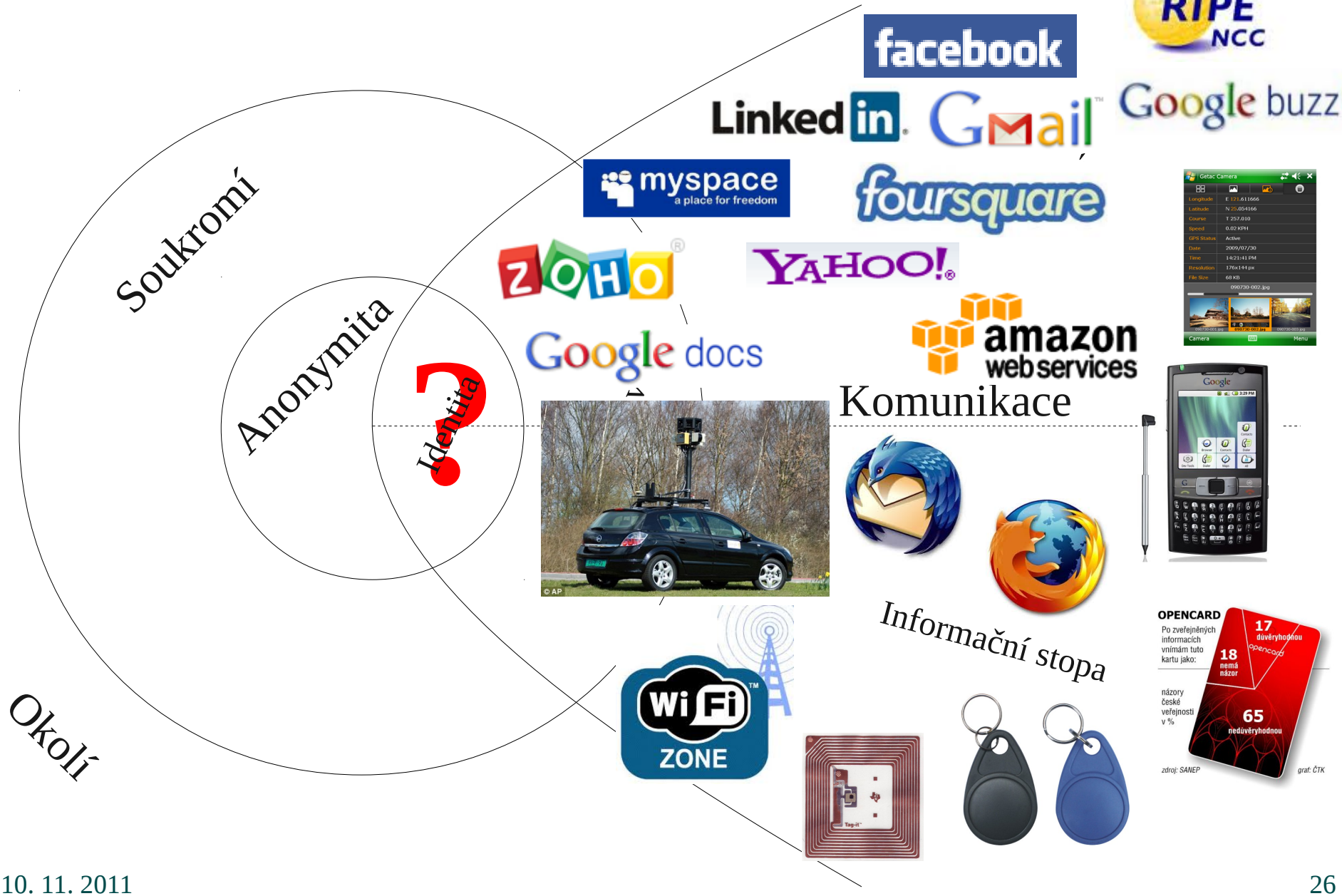
Hello,

I'm sorry for this odd request because it might get to you t
urgent,but due to the situation of things right now, I'm stra
London with my family right now, we came down here on
robbed, worst part is that wallet, cash credit cards and my
was stolen at GUN POINT, It's such a crazy experience fo
help flying back home, the authorities are not being 100%
the good thing is we still have our passport but don't have
money to get my flight ticket back home and some bills se
we need you to loan me some money, will refund you as s
home, I promise.

Thanks

Martha & Thomas Norman-Smith

Já


Soukromí
Anonymita
Identita
?
Okolí
Komunikace
Informační stopa
facebook
RIPE NCC
LinkedIn
Gmail
Google buzz
myspace
a place for freedom
foursquare
ZOHO
YAHOO!
Google docs
amazon web services
Wi Fi ZONE
OPENCARD
Po zveřejněných informacích vnímám tuto kartu jako:
17 důvěryhodnou
18 nemá názor
65 nedůvěryhodnou
názory české veřejnosti v %
zdroj: SANEP
graf: ČTK

Děkuji za pozornost.