Já, anonym

Existuje anonymita v prostředí internetu?

Aleš Padrta
CESNET, z. s. p. o.

Obsah

- Úvodní slovo
- Připojení k internetu
  - Přidělování IP adres
  - Anonymita v organizaci
  - Vnější anonymita
- Anonymita e-mailu
- Anonymita WWW
- Anonymita P2P
- Dobrovolně zveřejněné informace
- Shrnutí

Nikdo neví kdo jsem

"On the Internet, nobody knows you're a dog."

Úvodní slovo

- Anonymita = utajení totožnosti
  - Postupné odhalování informací
  - Postupné zanechávání stop
    - ⇨ Časem méně pravděpodobná
- Specifika internetu
  - Složitější situace
  - Dlouhodobé přetrvání elektronických stop
  - Snadno dostupné velkému množství lidí
  - Jednoduché spojení jednotlivých stop

Připojení k internetu

- Komunikace v síti
  - Na základě IP adres (147.228.aaa.bbb)
- Hierarchické přidělování IP adres
  - RIR (Region Internet Registry)
    - AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC
  - LIR (Local Internet Registry)
    - Obvykle ISP (Internet Service Provider)
  - Organizace
    - Západočeská univerzita v Plzni
  - Část organizace
    - Koleje, katedra, učebna, ...

Anonymita v organizaci

- Přidělování IP adres
  - Na základě HW adresy (MAC) – žádost uživatele
    - Katedry, ...
  - Na základě elektronické identity (login +heslo)
    - Eduroam, učebny, ...
- Známá vazba IP adresa – čas – uživatel
  - ⇨ Lokální správce ví přesně, komu přidělil IP
  - ⇨ Používaná IP adresa není anonymní
- Bezdrátové sítě
  - Možnost určení polohy (triangulace)

Anonymita v organizaci

- Statistiky provozu a provozní informace
  - Datové toky (Netflow)
    - Komunikace mezi IP adresami
    - Množství přenesených dat
    - Čas, porty, ...
  - IDS
    - Abnormální aktivity
    - Zakázané aktivity
  - Přístupy k zajímavým nebo důležitým službám
- Uchovávání provozních informací
  - Několik měsíců
  - Využito při řešení problémů (incidenty, PČR, ...)

Vnější anonymita

- Z hierachické struktury
  - RIR-LIR-Organizace-...
  - Každá IP adresa někomu patří
  - Všeobecně dostupné (např. www.db.ripe.net/whois)
  - Hlášení incidentů patřičné organizaci
- Vnější komunikace
  - Infrastruktura vlastněná třetími subjekty
    - Přístup z ČR do USA přes Francii apod.
  - Obdobná dostupnost provozních informací (!)
    - CESNET: univerzita ⇔ zbytek světa

Anonymita e-mailu

- Hlavička e-mailu = cenný zdroj informací

```
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: Thunderbird 2.0.0.23 (Windows/20070812)
```

- Skutečný odesílatel (cesta pro odpověď)
- Cesta přes servery
  - Jednotlivé uzly, včetně zdrojového počítače
- Mailový klient, včetně přesné verze
  - Často lze zjistit/odvodit platformu

Anonymita WWW

- Hlavička http požadavku = cenný zdroj informací

```
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

Anonymita P2P

- Kazaa, eMule, DirectConnect, BitTorrent, Overnet, ...
- Většinou je stahovaný obsah automaticky nabízen
  - Někdy lze v klientech omezit (DC, ...)
  - U některých součást protokolu (BitTorrent, eMule, …)
- Po připojení do P2P sítě
  - Informace o mně (a mé nabídce) se šíří sítí
  - Každý zájemce tyto informace vidí
  - Také vlastníci autorských práv
  - Farmy P2P serverů ⇨ reakce na nelegální činnost

Ukázka stížnosti

Dear University of West Bohemia Network Abuse:

We are writing this letter ....

.....

.... Please include the Case ID 1005217498, also noted above, in the subject line of all future correspondence regarding this matter.

We appreciate your assistance and thank you for your cooperation in this matter.

Your prompt response is requested.

Respectfully,

XXXXXX

Enforcement Coordinator

MediaSentry

INFRINGEMENT DETAIL

Infringing Work: 90210

First Found: 25 Nov 2009 12:34:56 EST (GMT -0500)

Last Found: 25 Nov 2009 12:34:56 EST (GMT -0500)

IP Address: 147.228.xxx.yyy

IP Port: 49223

Protocol: BitTorrent

Torrent InfoHash: B143BA878D68AA38AA5C7362A39E76E3FCA80EE2

Containing file(s):

90210.S02E10.HDTV.XviD-2HD.avi.torrent (367,141,156 bytes)

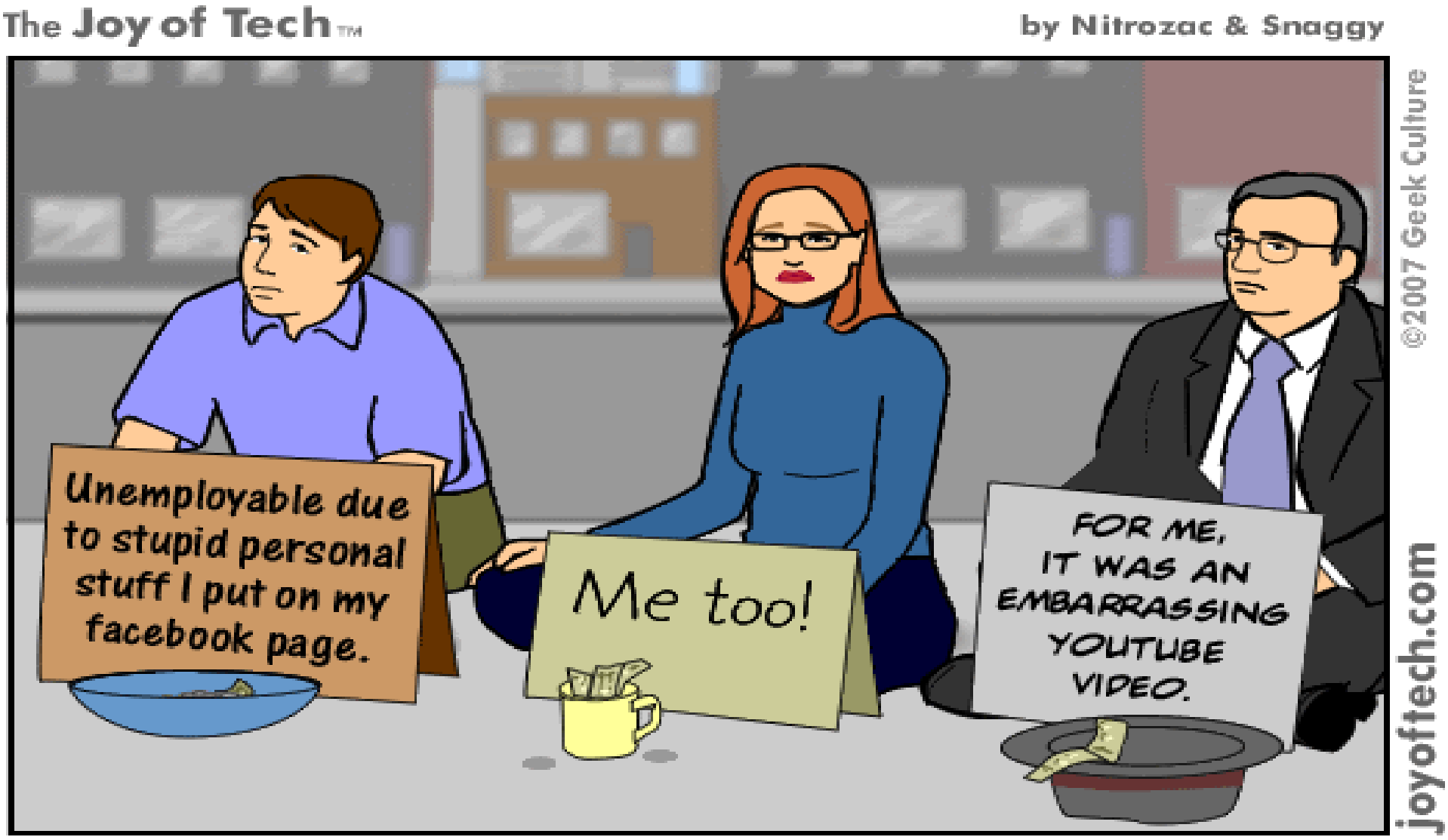
Anonymizéry

- Tor, Freenet, I2P...
- Síť tvořena dobrovolníky
  - Komunikace přes několik uzlů
  - Každý zná jen předchozí a následující
- Úskalí
  - Každý zájemce může být součástí
    - Zajímavé i s malým počtem uzlů
    - Vstup/výstup ze sítě – sledování dat
  - Problém výstupního uzlu
    - Cizí problémy na mou hlavu

Dobrovolně zveřejněné informace

- Uživatelé jsou exhibicionisté
  - Rádi o sobě zveřejňují informace
  - Facebook, Twitter, Flicker, LinkedIn, …
  - Blogy, chaty, seznamky, diskuse, …
- Zásadní otázky
  - Co o sobě zveřejňuji (fotky, adresy, kontakty, ...)
  - Kdo si to může přečíst (všichni, omezená skupina, ...)
- Vyhledání informací, skládání střípků …
  - Sociální inženýrství – viz „přítel“ na Facebooku
- Provozovatelé služby znají přístupovou IP adresu ...

Dobrovolně zveřejněné informace



Signs of the social networking times.

Shrnutí

- Anonymní internet?
  - Záleží na poskytovateli připojení
    - Potřebné údaje má k dispozici
  - Záleží na poskytovateli služeb
    - Potřebné údaje má k dispozici
  - Záleží na uživateli
    - Potřebné údaje rád vyzradí
- Na anonymitu nelze spoléhat
  - Internet je příliš komplexní
  - Nutno přizpůsobit své chování

Dotazy

???