CESNET

SLU v Karviné, 13. dubna 2011

CESNET

- http://www.cesnet.cz/
- Provoz a rozvoj páteřní akademické počítačové sítě České republiky - **CESNET2**
- Založen v roce 1996
- Členové sdružení
  - 25 českých univerzit
  - Akademie věd České republiky
- Cca 130 zaměstnanců, řada z nich z prostředí VŠ a AV ČR

CESNET

- Hlavní cíle:
  1. Provoz a rozvoj sítě CESNET2
  2. Podpora vědy a výzkumu v oblasti pokročilých síťových technologií a aplikací
  3. Podpora a šíření vzdělanosti, kultury a poznání
- Připojit do sítě CESNET2 se může každý, kdo vyhoví bodům 2. a 3.
- Připojené organizace:
  - Univerzity, Akademie věd ČR
  - Střední školy, knihovny, muzea apod.

CESNET

- **2004 – 2010: Výzkumný záměr "Optická síť národního výzkumu a její nové aplikace"**
- **2011 – 2015: Projekt "Velká Infrastruktura", zaměřen na vývoj v následujících oblastech:**
  - Sítě
  - Programovatelný HW
  - Sledování provozu sítí
  - Bezpečnost (AAI, PKI, CSIRT)
  - Datová úložiště
  - Gridy
  - Multimédia

CESNET

- http://csirt.cesnet.cz/, certs@cesnet.cz
- CSIRT (Computer Security Incident Response Team)
- Ustanoven v roce 2003
- Základní služby:
  - **Řešení a koordinace řešení bezpečnostních incidentů v síti CESNET2**
  - Rozvoj a provoz IDS a Audit systém
  - Organizace seminářů a školení pro uživatele a administrátory CESNET2

CESNET

- **Z reakcí “provinilců” při řešení BI v síti CESNET2:**
  - Já jsem ty filmy 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!

Já, anonym

Jan Mach
CESNET, z. s. p. o.

Obsah

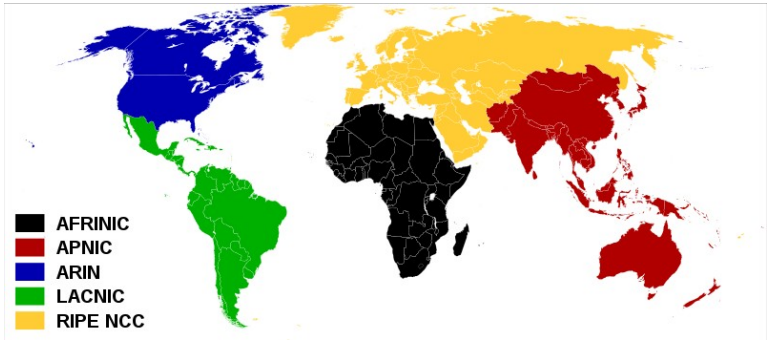
- Anonymita připojení k internetu?
  - Přidělování IP adres
  - Anonymita v organizaci
- Anonymita síťových služeb?
  - Sledování provozu sítě a služeb
  - E-mail, WWW, P2P
- Dobrovolné vystupování z anonymity
  - Komunitní sítě a s nimi spojená úskalí
  - Social engineering
  - Obecná doporučení

Anonymita připojení k internetu?

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

Anonymita připojení k internetu?

- Komunikace v síti
  - Identifikace = v TCP/IP síti IP adresa (195.113.144.194)
- Hierarchické přidělování IP adres
  - ICANN (http://www.icann.org)
  - RIR (Regional Internet Registry)
    - AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC
  - LIR (Local Internet Registry)
    - Obvykle ISP (Internet Service Provider)
  - Organizace
  - Část organizace (fakulta, kolej, katedra, učebna)
- **Informace o alokacích veřejně dostupné ve w*hois* databázích**



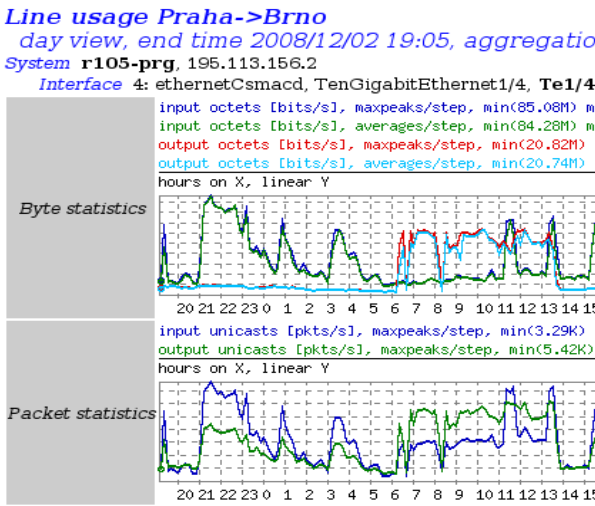
Anonymita připojení k internetu?

- V rámci organizace přidělování IP adres nejčastěji:
  - Na základě HW adresy (MAC) – žádost uživatele
  - Na základě elektronické identity (login +heslo)
- Bezdrátové sítě
  - Navíc možnost přesného určení polohy (triangulace)
- Informace ***IP adresa – čas – uživatel*** se uchovávají řádově měsíce – roky, lokální správce ví přesně, komu a kdy bylo IP přiděleno
- **Používaná IP adresa tedy NENÍ anonymní!**

  (IP adresa (+ čas) => whois => síť => správce => uživatel)

Anonymita síťových služeb?

- Sledování provozu služeb (logování)
  - Přidělování síťových zdrojů, přístupy k zajímavým nebo důležitým službám, e-mailová komunikace, WWW, DNS
  - Z administračních a bezpečnostních důvodů, pouze provozní informace (nikoliv data)
- Provozovatelé služby znají vaši IP adresu...
- Sledování provozu sítě
  - Analýza datových toků (Netflow)
  - Analýza logů, IDS, LaBrea, Snort
  - Abnormální, zakázané, podezřelé aktivity
- Provozní informace (logy) se uchovávají
- **Jakoukoliv aktivitou v síti za sebou zanecháváte elektronické stopy**



Anonymita e-mailu?

```
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
- Mailový klient, včetně přesné verze, často lze odvodit platformu

Anonymita WWW? (1)

```
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, sledování pohybu uživatelů, personalizace

Anonymita WWW? (2)

- Technologie na straně klienta (JavaScript, Flash) poskytují další možnosti pro:
  - Získávání informací o uživateli

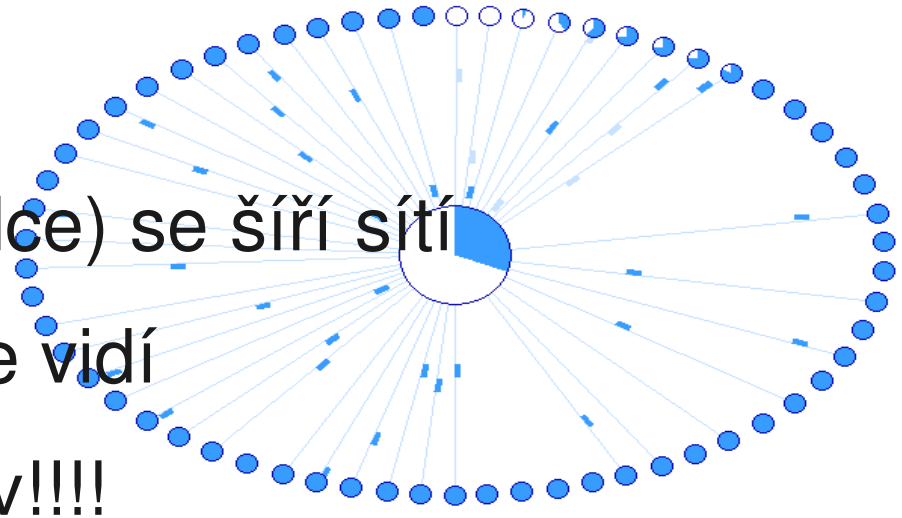
    (http://browserspy.dk/)
  - Identifikaci uživatele – nesmazatelné cookies (zombie cookies)

    (http://samy.pl/evercookie/)
  - Identifikaci uživatele – otisk vlastností prostředí (prohlížeče a počítače)

    (http://panopticlick.eff.org/)

Anonymita Peer-to-peer sítí?

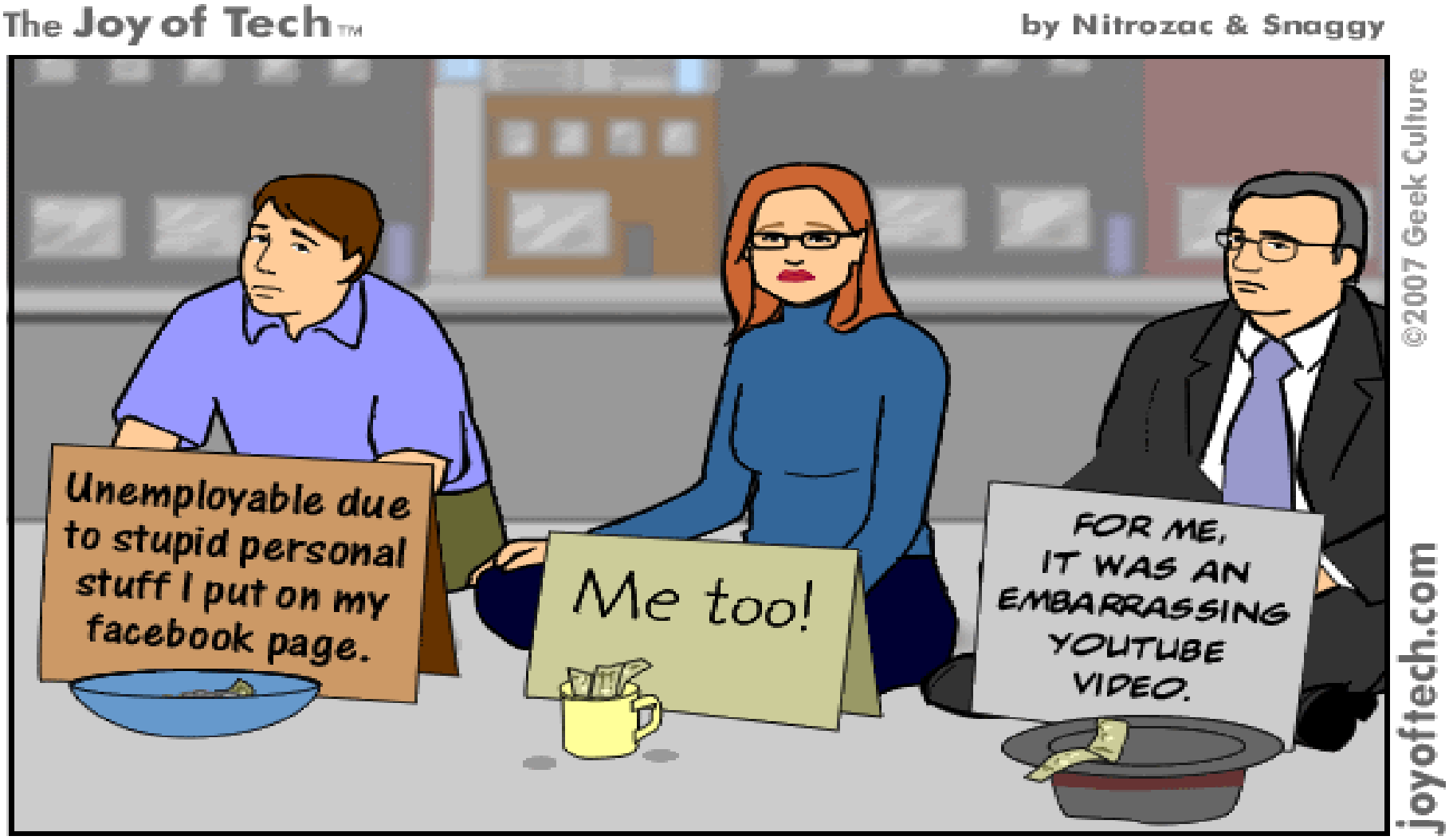
- Většinou je stahovaný obsah automaticky nabízen
  - Někdy lze v klientech omezit (DC, ...)
  - U některých součást protokolu (BitTorrent, eMule, …)
- Po připojení do P2P sítě
  - Informace o mně (a mé nabídce) se šíří sítí
  - Každý zájemce tyto informace vidí
  - Také vlastníci autorských práv!!!!



- Nejaktivnější jsou velké filmové společnosti!!!

Dobrovolné vystupování z anonymity

- Seznamky, chaty, BBS, blogy, komunitní sítě



Signs of the social networking times.

Dobrovolné vystupování z anonymity

- Provozovatelé služby znají vaši IP adresu...
- Komunitní sítě
  - Jednoduché, cool, jednodušší komunikace s přáteli, sdílení fotografií, … ALE
  - Velké množství nezkušených uživatelů => ideální prostředí pro šíření klasických hrozeb (viry, spam, podvodné odkazy, miniaplikace)
  - Zdání přátelského prostředí => nižší obezřetnost
  - **Zbytečné zveřejňování citlivých informací =>**

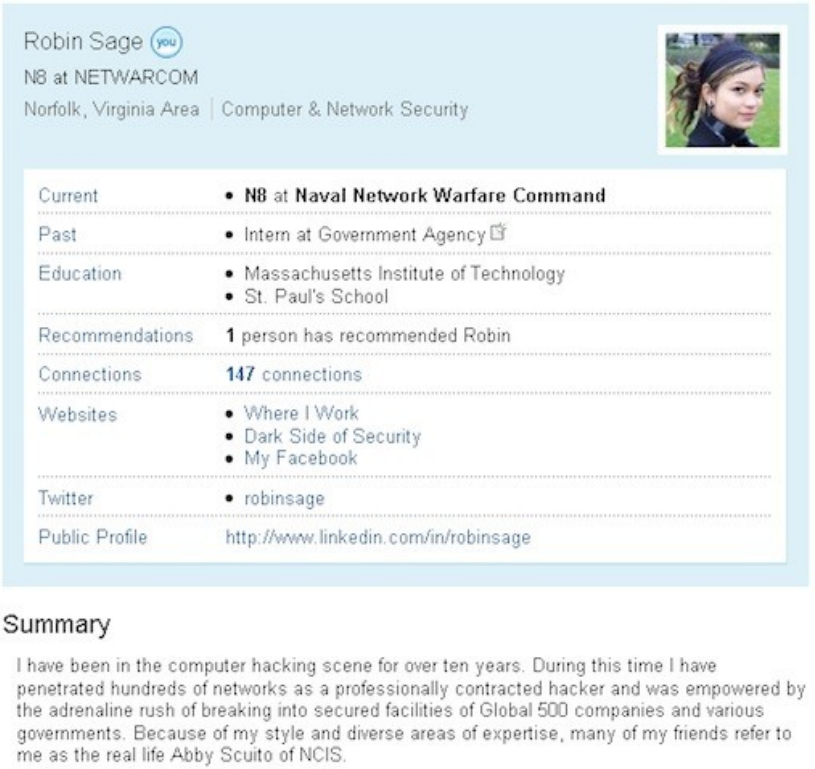
Nebezpečí komunitních sítí

- Uživatelé jsou mnohem otevřenější (řeší intimní osobní problémy, pracovní záležitosti)
- Špatně nastavená oprávnění + výběr “přátel” = sdílení s každým na síti
- Jednou zveřejněné informace nelze “smazat” (ohrožení osobní reputace), pozor na licenční ujednání při zakládání účtu, kešování, zálohování a mirroring webu
- Krádež identity – je tím snazší vás napodobit, čím více informací o sobě zveřejňujete
- Na první pohled nevinné informace mohou být zneužity

  (PleaseRobMe.com, kontrolní otázky)
- Nikdy není jisté, kdo je na druhém konci (Robin Sage)

Experiment Robin Sage

- Falešná identita vytvořená Thomasem Ryanem
- Během 2 měsíců ~ 100 přátel na FB, Twitteru a dalších z oblastí bezpečnostních odborníků, armády
- Pracovní nabídky, nabídky na schůzku, přístup k interním informacím, žádosti o odbornou korekturu prací



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	**147** connections
Websites	• Where I Work • Dark Side of Security • My Facebook
Twitter	• robinsage
Public Profile	http://www.linkedin.com/in/robinsage

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.

Social Engineering

- Data z KS jsou levná, aktuální, snadno přístupná, v elektronické formě (zpracovatelná automaticky)
- Screening zaměstnanců
  - známky problémového chování (alkohol, nezákonné chování, pochybné skupiny)
  - schopnosti (gramatika, vyjadřovací schopnosti, logická argumentace)
  - pracovní záležitosti (názory ke kolegům a na zaměstnavatele, aktivity v pracovní době)
  - zdravotní stav, volnočasové aktivity, …
- Scouting (hackeři), falešné sbírky a žádosti o pomoc, průzkum trhu, reklama, analýzy, …

Obecná doporučení

Ztráta popularity KS by byla překvapivá, uživatelé se musí naučit v novém prostředí chovat

- Jistota identity protistrany (ověření jiným kanálem – telefon, podepsaný email, …)
- Zvažte všechny důsledky svého jednání – Co píšete, ke komu se to může donést, jak to může být hodnoceno v budoucnu. Nikdy nepřispívejte ve vzteku nebo v opilosti!
- Oddělujte práci a volný čas – různé skupiny, různá oprávnění
- Buďte obezřetní

Já, anonym?

Internet je anonymní jen do té míry, do jaké vám to dovolí poskytovatel připojení a služeb.

Chraňte svoje soukromí,
nespoléhejte na anonymitu,
chraňte svou identitu,
své zdroje a nástroje
a chovejte se podle pravidel.

Nikdy nepište na internet nic, co byste nemohli říct každému kolemjdoucímu na ulici.

CESNET

Děkuji za pozornost.

Jan Mach
jan.mach@cesnet.cz