DNSSEC

Proč je důležité chránit internetové domény?

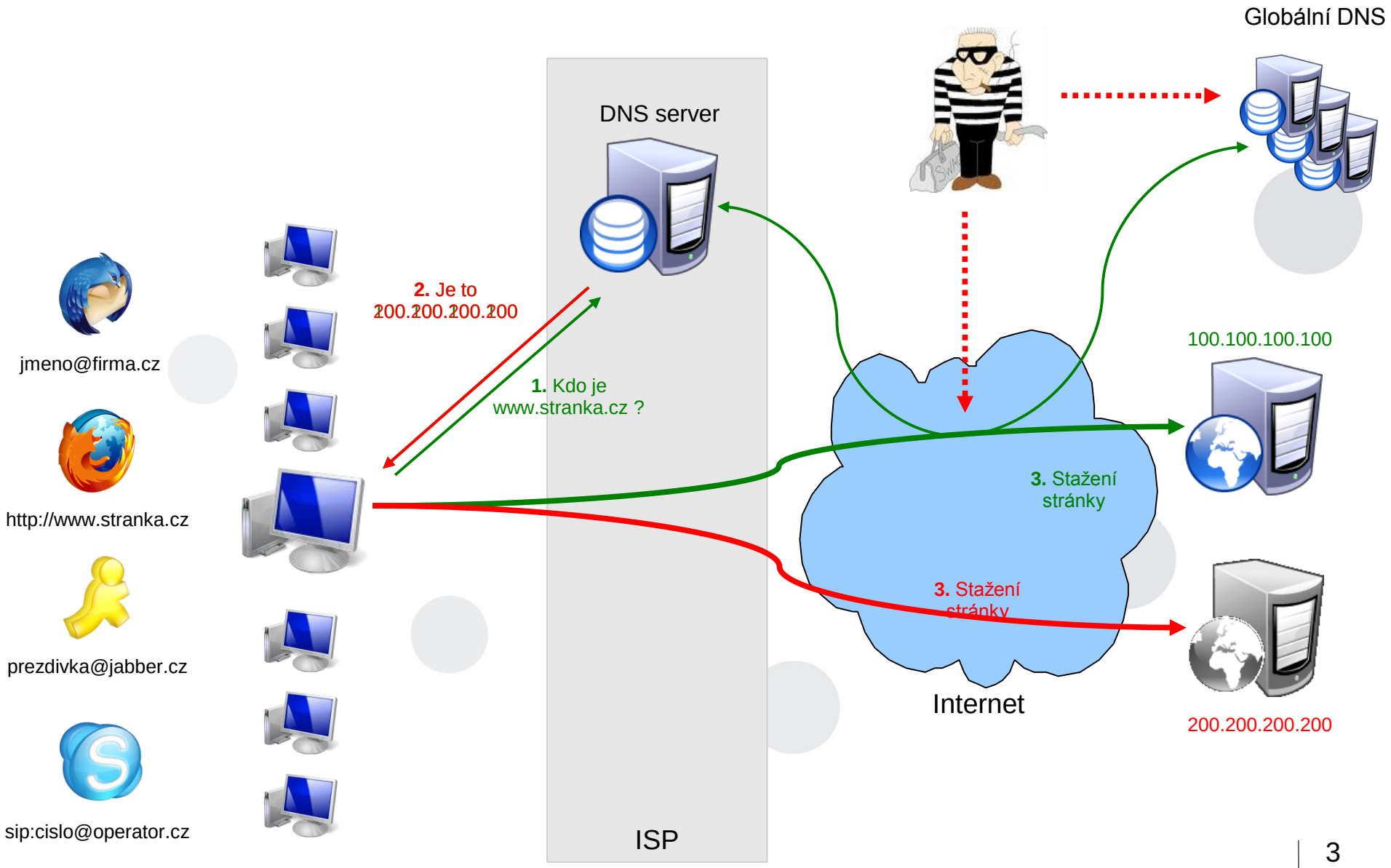
CZ.NIC z.s.p.o.
Pavel Tůma
pavel.tuma@nic.cz
18. 2. 2009

správce domény cz

Systém doménových jmen

- Proč vlastně doménová jména?
  - IP adresa
  - 124.45.10.231
  - 2001:1488:800:200:217:a4ff:fea7:49fe
  - Problém: čísla jsou špatně zapamatovatelná
  - Řešení: používání jmen místo čísel = systém DNS
- Adresy internetových služeb
- DNS ovlivňuje všechny internetové služby!
- … **a to ještě dříve než uživatelé použijí službu samotnou**

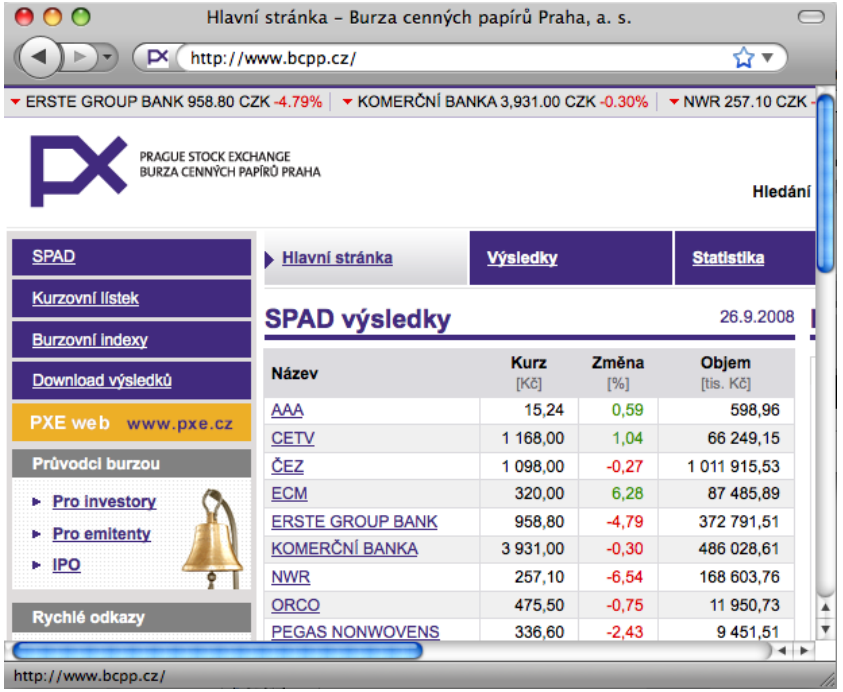
Jak DNS funguje?

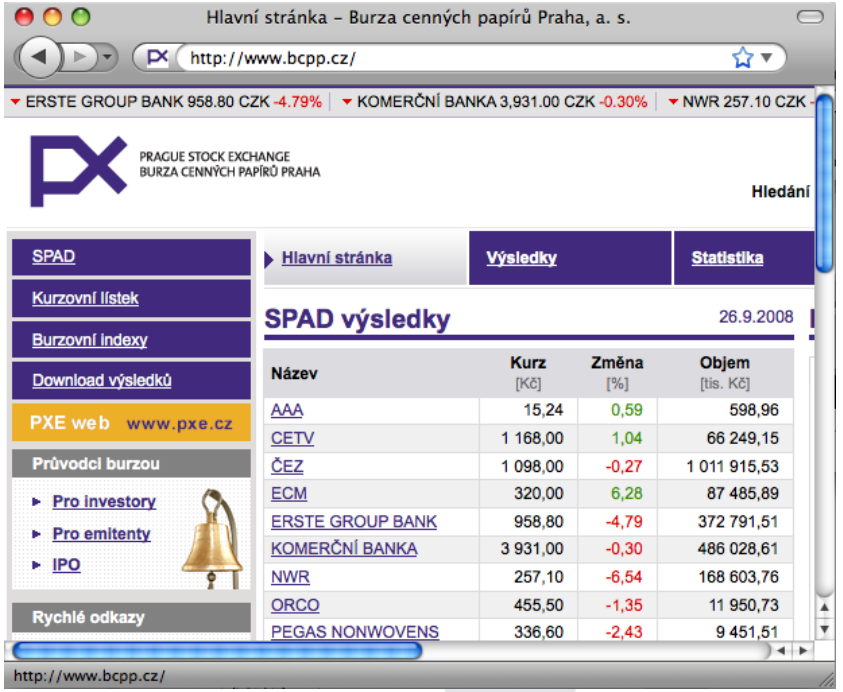


Poznáte rozdíl?

- Phishing / pharming
- Bez nutnosti „akce“ uživatele
- … naštěstí bývá i další zabezpečení (SSL certifikáty?)

Poznáte rozdíl?





- Obecný podvrh informací
- … řádově větší dosah s Web 2.0 nástroji např. RSS

Poznáte rozdíl?

From: Jana Nevěrná <"jana.neverna"@firma.cz>
Subject: **Ahoj Pavliku**
Date: September 29, 2008 8:23:30 PM GMT+02:00
To: Pavel Tuma <pavel.tuma@nic.cz>

Ahoj Pavle,
dekuju ti za vcerejsi den.
Jsem moc rada, ze je ted tvoje manzelka pryc, ze se muzeme vidat casteji nez obvykle. Vcera vecer bylo prijemne sedet spolu pri svickach, divat se do tvych oci, snit o dalsi takove chvili.
Dnes rano jsem se citila tak krasne. Vecer byl proste nadherny, bezchybny, stejne, jako ta noc, co po nem prisla. Prala bych si probouzet se vedle tebe kazde rano.
Krasny novy den bez mracku a tesim se na dalsi schvile s tebou, na tve polibky.
Tvoje Janicka

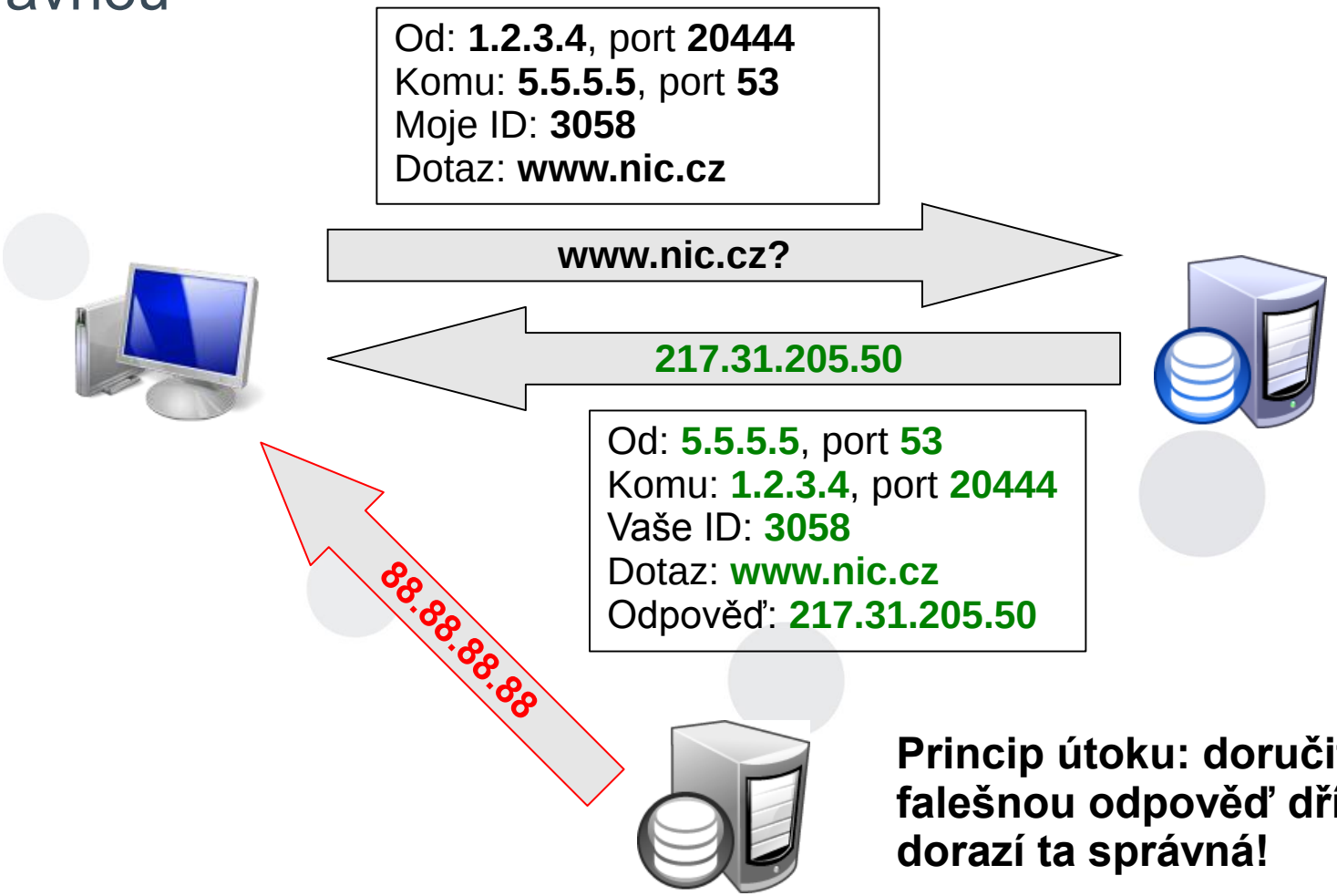
From: Jana Nevěrná <"jana.neverna"@firma.cz>
Subject: **Ahoj Pavliku**
Date: September 29, 2008 8:23:30 PM GMT+02:00
To: Pavel Tuma <pavel.tuma@nic.cz>
Return-Path: <jana.neverna@firma.cz>
Received: from mail.nic.cz ([unix socket]) by mail (Cyrus v2.2.13-Debian-2.2.13-10ubuntu2) with LMTPA; Mon, 29 Sep 2008 20:23:34 +0200
Received: from [10.0.0.3] (prg1-v-7-3.static.adsl.vol.cz [62.177.80.3]) by mail.nic.cz (Postfix) with ESMTPSA id 99D8473400A for <pavel.tuma@nic.cz>; Mon, 29 Sep 2008 20:23:34 +0200 (CEST)
X-Sieve: CMU Sieve 2.2
Organization: CZ.NIC
User-Agent: Thunderbird 2.0.0.17 (Windows/20080914)
Mime-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-2; format=flowed
Content-Transfer-Encoding: 7bit
Message-Id: <20080929182334.99D8473400A@mail.nic.cz>

Ahoj Pavle,
dekuju ti za vcerejsi den.

- Odposlech komunikace
- Nejen emaily – VoIP, Instant messaging, ...

Útok na DNS

- Pokud příchozí odpověď odpovídá dotazu, považuje se správnou



Princip útoku: doručit falešnou odpověď dříve než dorazí ta správná!

Útok na DNS

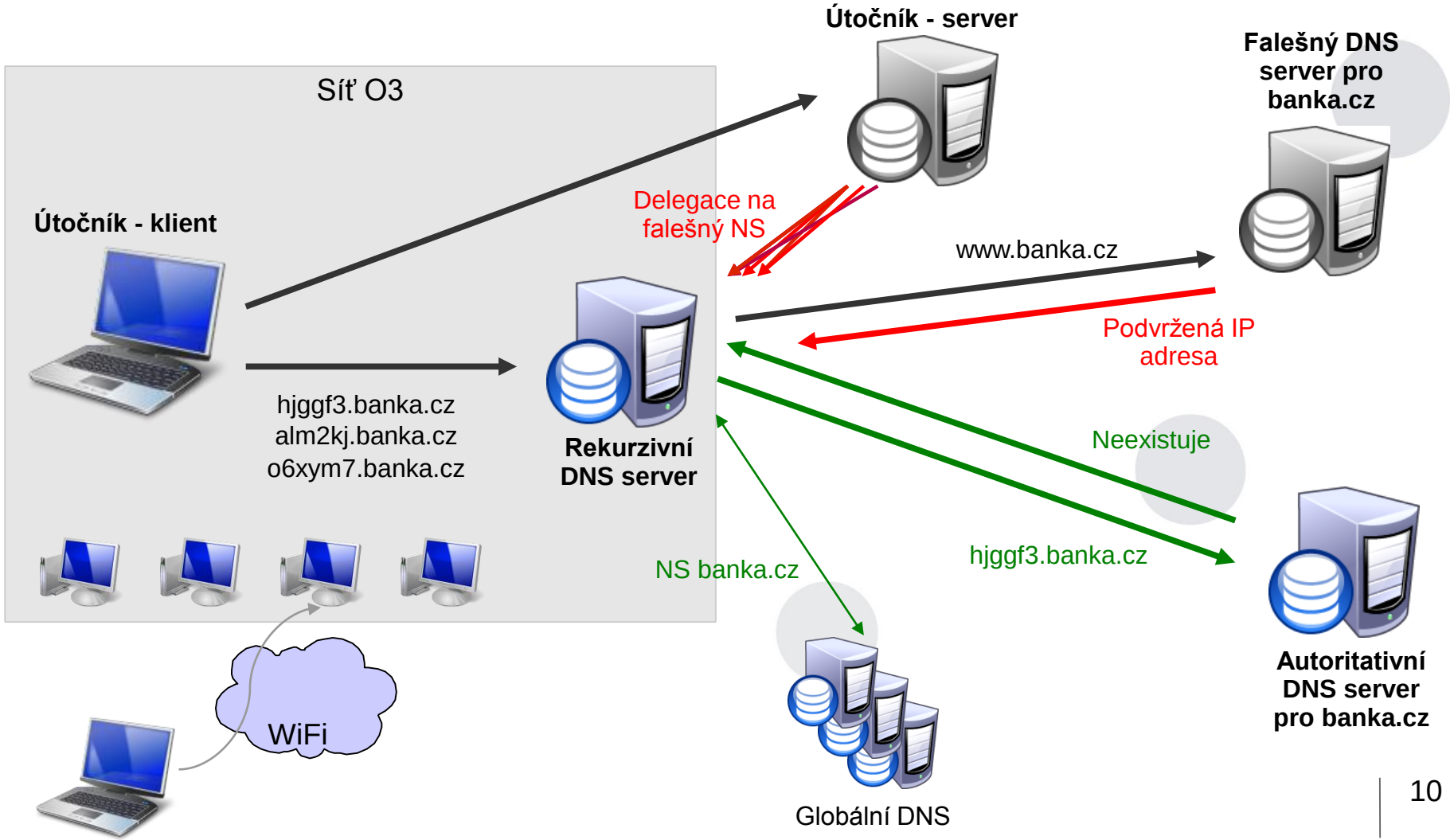
- Prvky ochrany: Port + Transaction ID
- Kauza zranitelnosti DNS (Kaminski)
  - Léto 2008
  - Predikovatelnost portu i transaction ID
  - Time-to-live (TTL) nehraje roli (dotazování na náhodné domény)
  - Útok na takový server trvá v řádu vteřin
  - Řešení: plná randomizace
  - Patch pro všechny implementace – DNS servery zabezpečeny
- **… ale přesto jsou všechny zranitelné!**

Útok na DNS

- Port: cca 64 000 možností
- Transaction ID: cca 65 000 možností
- Průměrná délka DNS paketu: 120 bytů
- Útok hrubou silou!
  - 4,2 miliardy kombinací teoreticky
  - Rychlost 1 Gbps = 1,1 milionu kombinací za sekundu
  - Dotazy na náhodnou doménu … opakujeme stále dokola
- Pokus v laboratorních podmínkách
  - Ze třech míst v lokální síti
  - **1:01 až 10:40!**

Jak útok na DNS provést

Útočíme na doménu www.banka.cz u pokytovatele O3 ...



Jak útok na DNS provést – ukázka

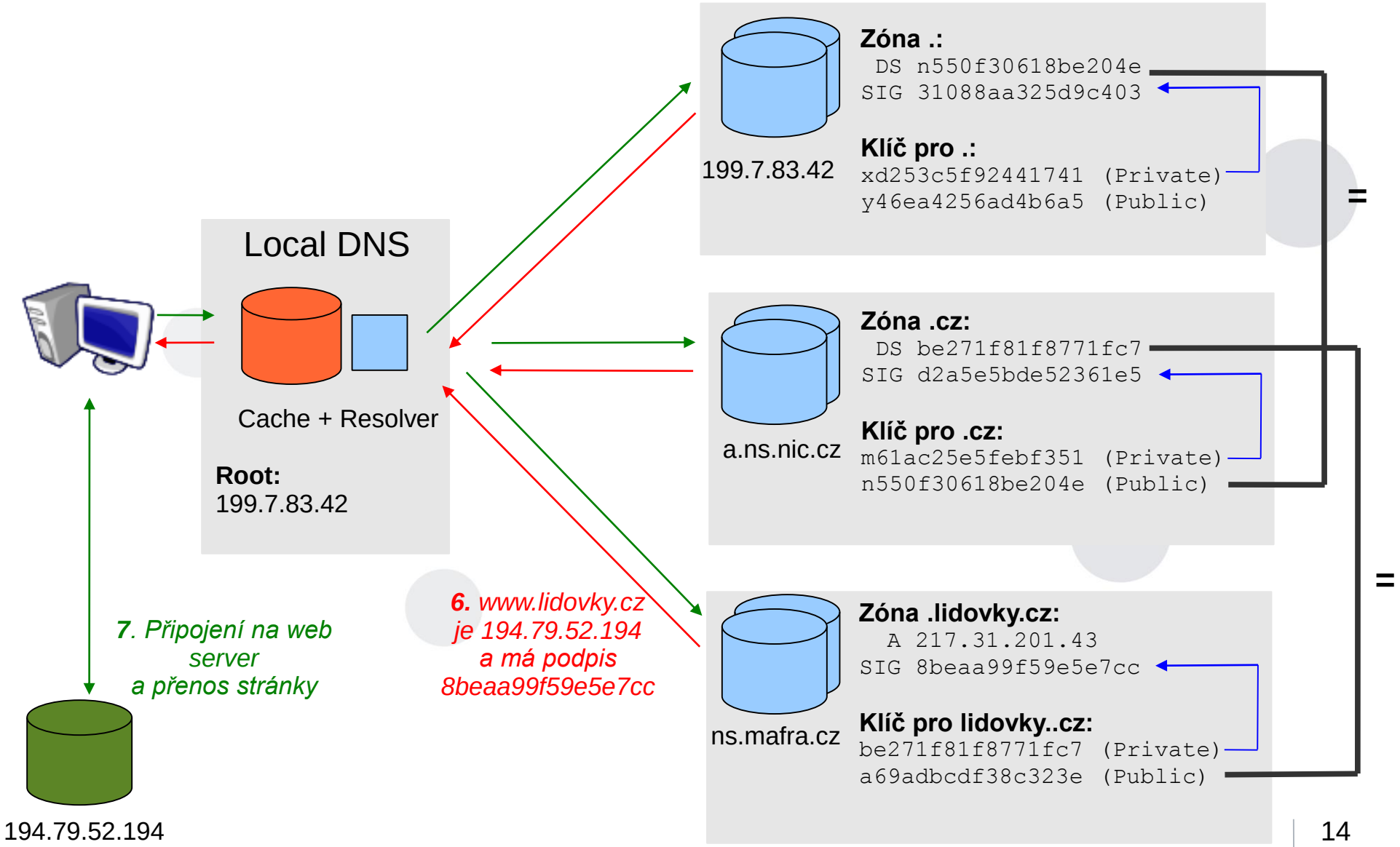
Co je DNSSEC

- Rozšíření zabezpečující DNS protokol
- Přináší
  - Ověření zdroje DNS údajů
  - Ověření integrity získaných údajů
  - Důvěryhodnou informaci o neexistenci údaje
- DNSSEC zajistí, že získané odpovědi můžeme důvěřovat
- DNSSEC nezajistí
  - Důvěrnost komunikačního kanálu při přenášení dat
  - Ochranu před Denial-Of-Service útoky

Jak DNSSEC funguje

- Zavádí do DNS asymetrickou kryptografii
- Data v DNS jsou digitálně podepsána soukromým klíčem
- DNS server obsahuje
  - Data samotná
  - Podpis dat
  - Veřejný klíč
- Zavádí se řetěz důvěry – podobně jako u SSL
  - Hash veřejného klíče se ukládá u nadřazené autority
  - Nadřazená autorita = doména nižšího řádu
  - nejakadomena.cz -> .cz

Jak DNSSEC funguje



DNSSEC u poskytovatelů služeb

1) Vygeneruji dvojici klíčů
2) Podepíšu své zóny
3) Publikuji veřejnou část do registru .cz
4 … X) Spravuji své klíče
   - Pravidelná rotace
   - Bezpečnostní pravidla
   - Obdobně jako SSL certifikáty / elektronické podpisy

DNSSEC u poskytovatelů služeb

- Lze vidět v WHOIS
- www.nic.cz/whois

Domain name	lidovky.cz
Registered since	18.11.1998
Last update date	01.10.2008 11:20:46
Expiration	20.10.2009
Holder	SB:JC607LN-RIPE Lidové noviny, a.s.
Administrative contact	JC607-RIPE Jaroslav Cerveny
Temporary contact	
Sponsoring registrar	REG-INTERNET-CZ INTERNET CZ, a.s. since 02.11.2004 21:25:00
DNSSEC secured	✔
Status	Domain is paid and in zone

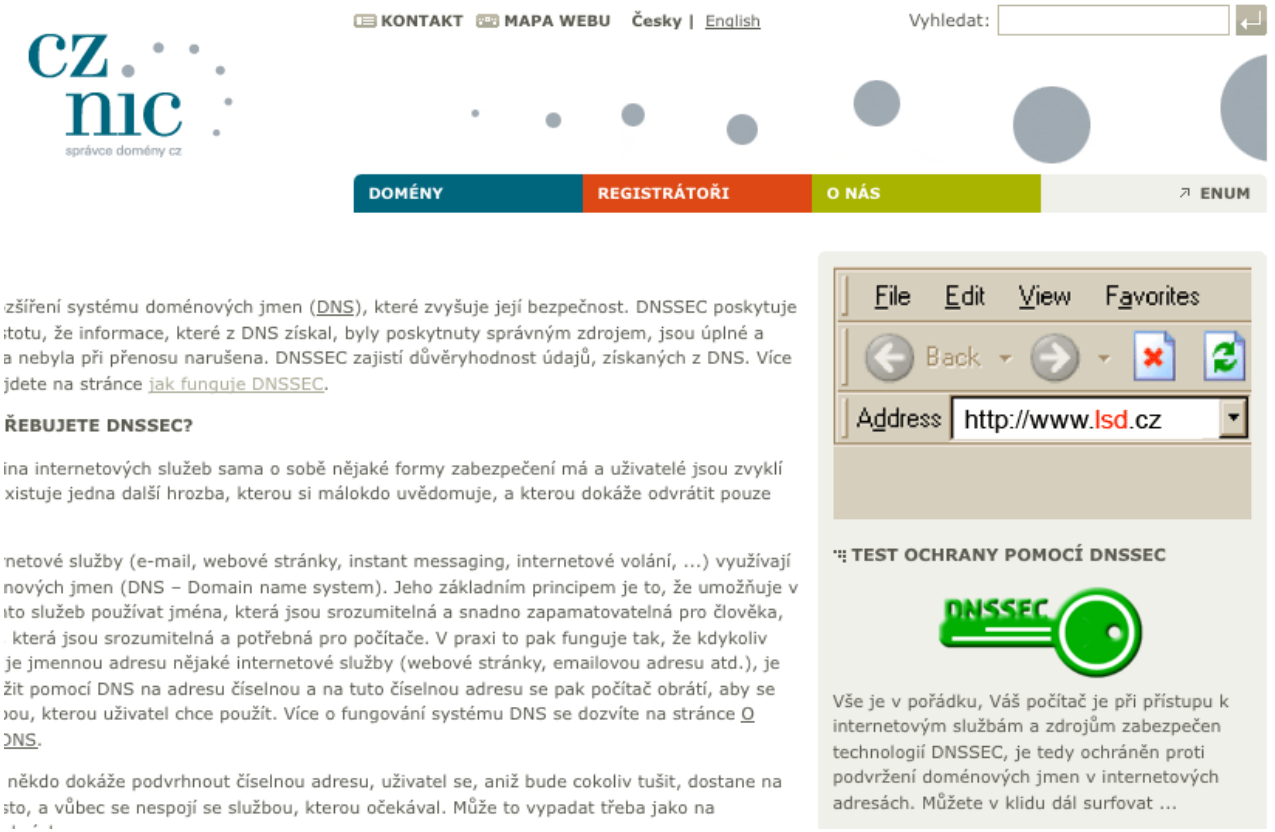
Key set	KS:LIDOVKY.CZ
DS record	Keytag: 52357 Algorithm: 5 [RSA/SHA-1] Digest type: 1 [SHA-1] Digest: 892d2a8c244bf5cfa90721cb30d6754d022d57e2 Max sig. life: 0
Technical contact	SB:JC607-RIPE_XX MAFRA, a.s. JC607-RIPE Jaroslav Cerveny
Sponsoring registrar	REG-CZNIC CZ.NIC, z.s.p.o. since 30.09.2008 08:11:10
Status	Has relation to other records in registry

DNSSEC u koncových uživatelů

- Podle používaného rekurzivního DNS serveru
  - Vlastní (geeks)
  - Firemní (větší organizace)
  - ISP (domácnosti)
- Pouze změna konfigurace příslušného serveru

DNSSEC u koncových uživatelů

- Možnost otestovat na www.dnssec.cz
- Vyžadujte zabezpečení!



Děkuji za pozornost

Otázky?

Pavel Tůma

pavel.tuma@nic.cz