Správa a zabezpečení DNS

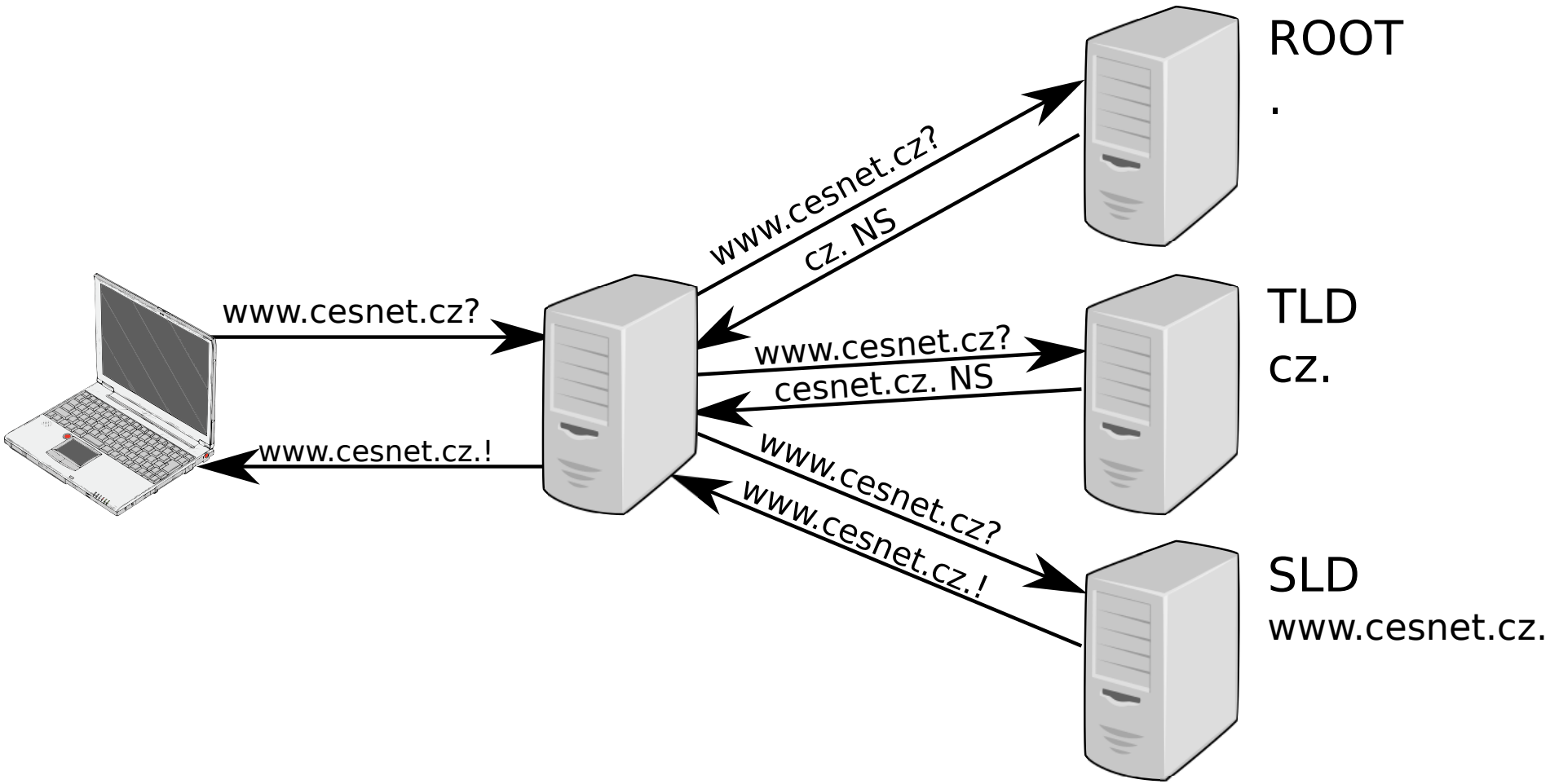
Ondřej Caletka

14. prosince 2015

Obsah

CESNET

O službě DNS


ROOT
.
TLD
cz.
SLD
www.cesnet.cz.
www.cesnet.cz?
cz. NS
www.cesnet.cz?
www.cesnet.cz?
cesnet.cz. NS
www.cesnet.cz?
www.cesnet.cz.!
www.cesnet.cz.!
stub resolver
rekurzivní resolver
autoritativní server

Tři druhy DNS nodů

stub resolver knihovní funkce operačního systému

- s minimální cache
- v GNU C knihovně nepříliš robustní

rekurzivní resolver řeší dotazy a kešuje odpovědi

- agresivní cache řízená TTL hodnotami
- validace DNSSEC dat
- robustní řešení nedostupnosti autoritativních serverů

autoritativní server poskytuje data

- pouze ta, která má v databázi

CESNET

Rekurzivní servery

- malá diverzita v implemetacích:
  - BIND
  - Unbound
  - *PowerDNS recursor* – neumí DNSSEC
  - *Dnsmasq* je ve skutečnosti jen *forwarder*
- nutno zapnout validaci DNSSEC
  dělají to velcí operátoři, není se čeho bát
- ne všechny validátory podporují ECDSA podpisy
- nutno omezit povolené IP adresy pro dotazy
  a implementovat BCP 38 ve své síti

Problém řetězení resolverů s DNSSEC

- problematická validace žolíkových domén
- zejména, je-li forwardováno na zastaralý BIND
- automatizovaný test na `http://wildcarddnssec.jdem.cz/`

	Test	Výsledek testu
1.	Zabezpečení DNSSEC `*.wilda.rhybar.0skar.cz`	Úspěch. Nedostanete se na doménová jména s neplatným podpisem.
2a.	NSEC zóna s A záznamem `*.wilda.nsec.0skar.cz`	Neúspěch. Váš DNS server nedokáže správně validovat *A záznam*, který vznikl expanzí žolíkového znaku na zóně s NSEC.
2b.	NSEC zóna s CNAME záznamem `*.wild.nsec.0skar.cz`	Neúspěch. Váš DNS server nedokáže správně validovat *CNAME záznam*, který vznikl expanzí žolíkového znaku na zóně s NSEC.
3a.	NSEC3 zóna s A záznamem `*.wilda.0skar.cz`	Neúspěch. Váš DNS server nedokáže správně validovat *A záznam*, který vznikl expanzí žolíkového znaku na zóně s NSEC3.
3b.	NSEC3 zóna s CNAME záznamem `*.wild.0skar.cz`	Neúspěch. Váš DNS server nedokáže správně validovat *CNAME záznam*, který vznikl expanzí žolíkového znaku na zóně s NSEC3.
4.	NSEC s extra záznamem uvnitř žolíku `www.wilda.nsec.0skar.cz`	Úspěch. Váš DNS server správně validuje *CNAME záznam*, obklopený žolíkovými *A záznamy* na zóně s NSEC.
5.	NSEC3 s extra záznamem uvnitř žolíku `www.wilda.0skar.cz`	Úspěch. Váš DNS server správně validuje *CNAME záznam*, obklopený žolíkovými *A záznamy* na zóně s NSEC3.

Kompatibilita validátoru s ECDSA

```
$ go run alg_rep.go -r adns1.cesnet.cz
Zone dnssec-test.org.  Qtype DNSKEY Resolver [adns1.cesnet.cz]
 debug=false verbose=false Prime= V
DS     :  1  2  3  4  |  1  2  3  4
ALGS   :    NSEC      |     NSEC3
alg-1  :  -  -  -  -  |  x  x  x  x  => RSA-MD5 OBSOLETE
alg-3  :  V  V  -  -  |  x  x  x  x  => DSA/SHA1
alg-5  :  V  V  -  -  |  x  x  x  x  => RSA/SHA1
alg-6  :  x  x  x  x  |  V  V  -  -  => RSA-NSEC3-SHA1
alg-7  :  x  x  x  x  |  V  V  -  -  => DSA-NSEC3-SHA1
alg-8  :  V  V  -  -  |  V  V  -  -  => RSA-SHA256
alg-10 :  V  V  -  -  |  V  V  -  -  => RSA-SHA512
alg-12 :  -  -  -  -  |  -  -  -  -  => GOST-ECC
alg-13 :  -  -  -  -  |  -  -  -  -  => ECDSAP256SHA256
alg-14 :  -  -  -  -  |  -  -  -  -  => ECDSAP384SHA384
V == Validates  - == Answer  x == Alg Not specified
T == Timeout S == ServFail O == Other Error
DS algs 1=SHA1 2=SHA2-256 3=GOST 4=SHA2-384
```

https://github.com/ogud/DNSSEC_ALG_Check

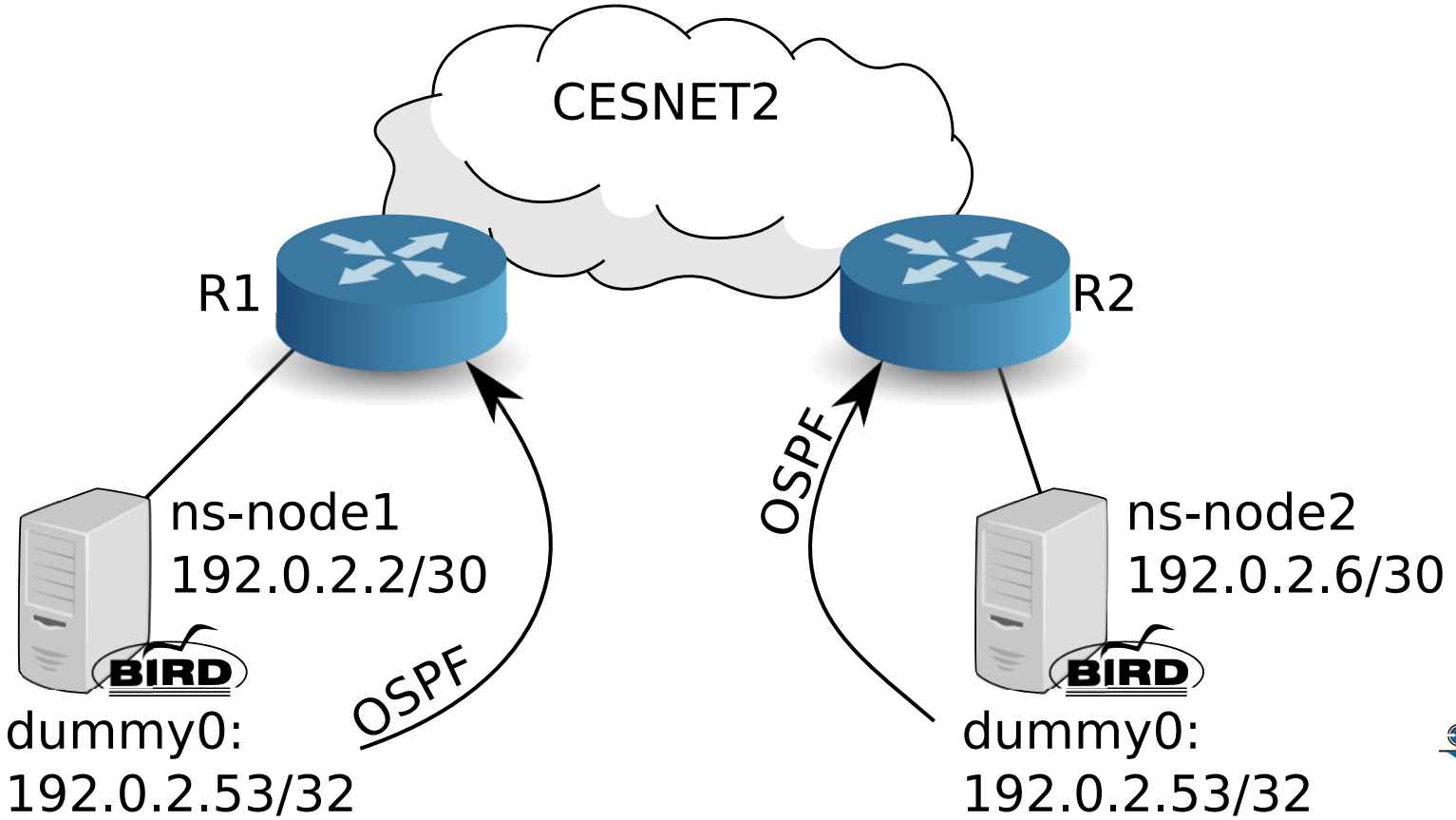
Root DNSSEC KSK rollover

- podpis kořenové zóny před pěti lety – 15. 7. 2010
- rolování kořenového klíče podle potřeby, nebo jednou za pět let
- vyžaduje aktualizaci *trust anchor* ve všech validátorech
- proběhne automaticky ve většině případů (RFC 5011)
- testovací prostředí na `http://keyroll.systems/`
- podrobnosti rolování zatím nejsou stanoveny

Vysoká dostupnost rekurzivních serverů

hodí se zejména v kombinaci s GNU stub resolverem

- tradiční HA pomocí linux-HA, pacemaker…
- anycasting v rámci vlastní sítě
  zabezpečí i proti výpadku routeru



Autoritativní servery

Mnoho slušných implemetací:

- BIND
- NSD
- Knot DNS
- *YADIFA*
- *PowerDNS*

Klíčové vlastnosti:

- podpora DNSSEC včetně NSEC3 a ECDSA
- podpora dynamického DNS
- (ne-)podpora kombinace autoritativního a rekurzivního serveru

DNSSEC na autoritativních serverech

Možné přístupy:

1. online podepisování
   - DNS server drží privátní klíče
   - podepisuje buď po načtení, nebo v reakci na dotaz
   - snadná spolupráce s dynamic DNS
   - možné problémy s přenosem na sekundární servery
2. externí podepisování
   - DNS server má k dispozici zónu včetně předem vytvořených podpisů
   - privátní klíče jsou potřeba pouze při změně dat
   - hotové produkty jako OpenDNSSEC

Dynamické IPv6 záznamy

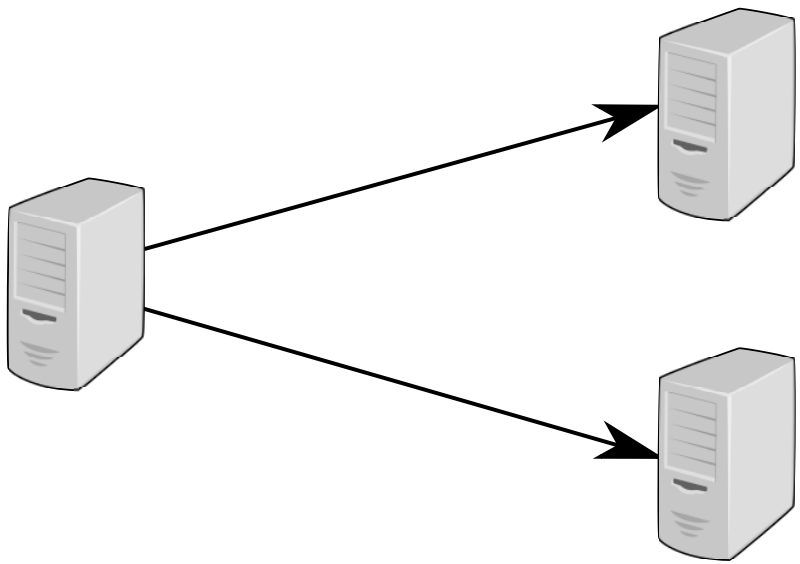
- běžná praxe v IPv4: vygenerování záznamů pro každou IP adresu
- pro IPv6 nemožné, zóna pro /64 zabere stovky EiB (2^{60})
- řešením je dynamické generování, podporované v Knot DNS 1.5+
- vyžaduje podporu ve všech autoritativních serverech zóny

Příklad

```
example.cz {
   file "/etc/knot/empty.zone";
   query_module {
      synth_record "forward dyn- 60 2001:db8:1::/64";
      synth_record "forward dyn- 60 192.0.2.0/24";
   }
}
```

Zónové přenosy

- úplné (AXFR) a inkrementální (IXFR)
- rychlé notifikace zprávami NOTIFY
- ochrana celistvosti zpráv pomocí TSIG
- nutno zvyšovat sériové číslo zóny
- princip skrytý master – veřejný slave



hidden master public slave

Časování a synchronizace

- odpovědi serverů kešovány po TTL daného záznamu
- negativní odpovědi kešovány podle hodnoty `SOA minimum`
- nesynchronnost serverů vede ke *split-brain*:
  o odpovědi rozhoduje náhoda

Za jak dlouho se změna nejpozději projeví?

	s `NOTIFY`	bez `NOTIFY`
nový	`SOA minimum`	`SOA minimum + SOA refresh`
změna	`TTL starého`	`TTL starého + SOA refresh`

Proč nepoužívat obskurní DNS servery

```
$ host www.skvelabanka.cz
www.skvelabanka.cz has address 192.0.2.7
Host www.skvelabanka.cz not found: 3(NXDOMAIN)

$ host www.skvelabanka.cz
Host www.skvelabanka.cz not found: 3(NXDOMAIN)
```

- programátor nepředpokládal, že se někdo zeptá na MX záznam pro `www.skvelabanka.cz`
- jeho implementace na takový dotaz vracela `NXDOMAIN` s TTL = 1 hodina
- BIND takovou odpověd nakešoval a po dobu TTL nevracel žádná data pro `www.skvelabanka.cz`

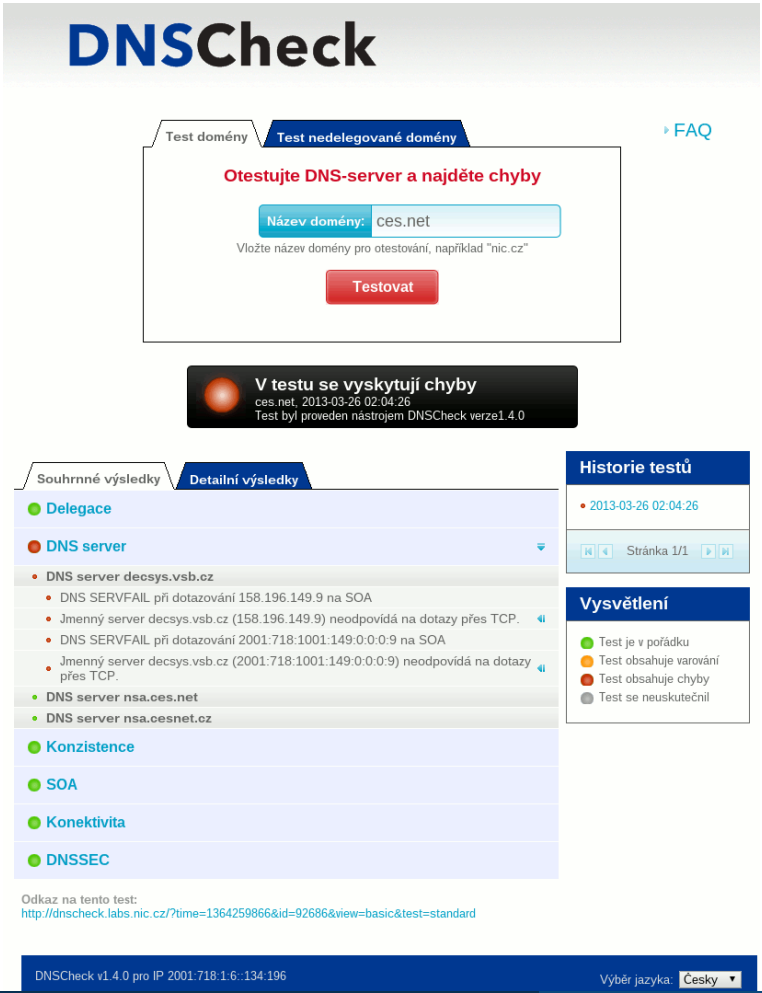
Proč nekombinovat autoritativní a rekurzivní server na jedné IP adrese

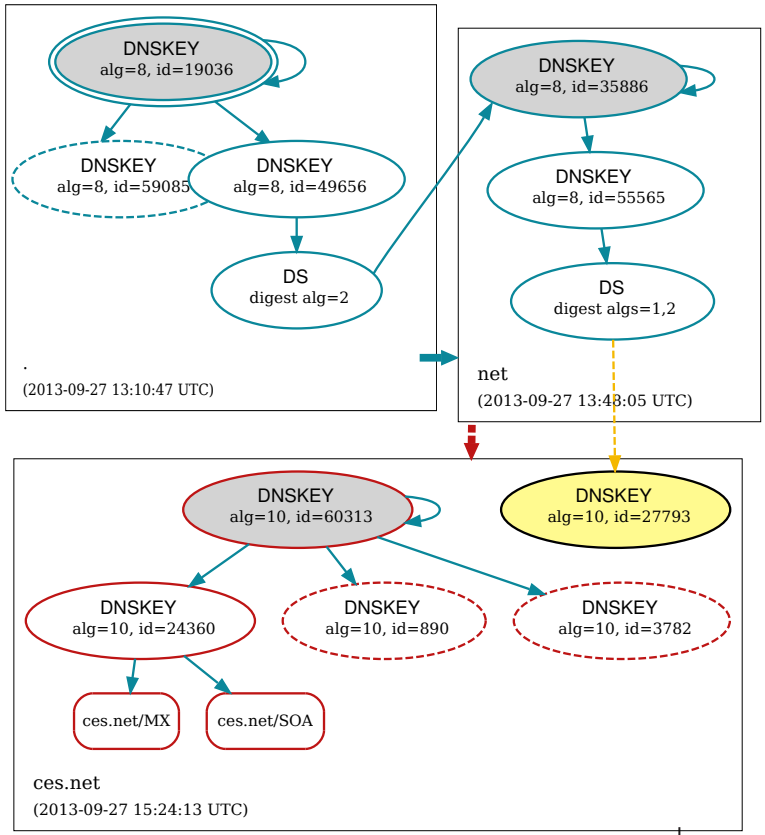
- malá škála dostupného DNS software (BIND a PowerDNS - ale bez DNSSEC)
- nemožnost DNSSEC validace vlastních dat (data z disku se nikdy nevalidují)
- špatná data z oddelegovaných, ale nezrušených zón

„Veškerá pošta nám už chodí na nový server, kromě pošty od našeho bývalého registrátora. Ta chodí stále na starý server.“

On-line kontroly

- http://dnsviz.net
- http://dnscheck.labs.nic.cz





Pravidelné údržby DNS serverů

- kontrola, že jsou zóny stále nadelegovány
- kontrola shody delegace s NS záznamy v zóně

Vlastní řešení `http://ldnshealth.jdem.cz`

```
xargs ./dnsservercheck.py server.example.com < list_of_domains.txt
example.cz: server server.example.com. not in delegation nor zone apex
example.com: server server.example.com. delegated, but not in zone apex
example.net: server server.example.com. not in delegation nor zone apex

List of domains, which should be deleted from server config:
example.cz
example.net
```

Útoky zneužívající DNS

Potírání zesilujících útoků

- implementujte BCP 38 (a nuťte ostatní)
- neotvírejte rekurzivní servery do světa
  a zkontrolujte taky NTP servery a zařízení se SNMP ☺
- na autoritativních serverech zapněte RRL

Response Rate Limiting

Obecná technika limitování odpovědí autoritativních serverů na opakující se dotazů ze stejné adresy. Implementováno nativně v Knot DNS a NSD, existují patche pro BIND 9.

Omezení velikosti UDP odpovědi

- rozšíření EDNS0 zvětšuje délku UDP zpráv nad 512 B *obykle na 4096 B*
- omezením velikosti k ~1 kB snížíme účinnost zesilujícího útoku
- také se tím zlepší situace resolverům s nefunkčním *Path MTU Discovery*
- příliš nízká hodnota může naopak rozbít resolvery bez TCP konektivity
  - obzvláště při použití DNSSEC
  - takto postižených uživatelů je ~2 % (měření Geoffa Hustona)

Útok náhodnými dotazy – princip

- nová forma útoku zneužívající otevřené rekurzivní resolvery
- pro rekurzivní resolver připomíná Slowloris útok
- postihuje zároveň rekurzivní i autoritativní servery
- útočící botnet pokládá dotazy ve stylu `<random string>.www.obet.com`
- dotaz je vždy přeposlán autoritativnímu serveru
- autoritativní server se buď pod náporem zhroutí, nebo zasáhne rate limiting
- rekurzivní server čeká na odpověď a zkouší dotazy opakovat

`http://www.root.cz/clanky/utok-na-dns-nahodnymi-dotazy/`

CESNET

Náhodné dotazy – důsledky a obrana

Důsledky

- zahlcení serverů dotazy
- DoS rekurzivních resolverů, např. BIND:
  - maximum 1000 současně probíhajících rekurzí
  - každá rekurze používá jeden file descriptor
  - pro víc než ~4000 rekurzí přestává být spolehlivý

Obrana

- definování prázdných SLD zón obětí na rekurzoru
  - riziko zablokování významných domén jako `in-addr.arpa`, nebo `co.uk`
- volba `ratelimit` v Unbound, `fetches-per-server` v BIND

DNSSEC jako bezpečné uložiště

Problém důvěryhodnosti PKI modelu

- mnoho *důvěryhodných* certifikačních autorit
- různé úrovně ověření, stejný cílový efekt
  - důkladné ověření (extended validation, €€€)
  - základní oveření (organization validation, €€)
  - bez ověřování identity (Domain control Validation, €)
- kterákoli autorita může kterýkoli certifikát
- na druhou stranu
  - nízký počet vydaných falešných certifikátů
  - velmi účinné útoky bez nutnosti falešných certifikátů (phishing, rom-0,…)

Certificate pinning s DANE

- možnost určit, který certifikát má být pro dané jméno platný
- vyžaduje DNSSEC
- čtyři typy použití (usage) TLSA záznamu
  - 0 kontrola certifikační autority
  - 1 kontrola koncové entity
  - 2 vložení certifikační autority
  - 3 vložení koncové entity

Příklad TLSA záznamu

```
_443._tcp.www IN TLSA 3 1 1 5C4…6099
```

DANE jako zvýšení zabezpečení PKIX

- omezení množiny povolených certifikačních autorit (`Usage: 0`), nebo certifikátů (`Usage: 1`)
- vynucení certifikační autority s přísnou politikou
- PKIX validace je stále nutná

Tip: Umístěte do DNS otisk certifikátu své nejbližší autority. Tu pak pomocí CNAME odkazujte ze všech svých služeb.

```
terenasslca2 IN TLSA 0 0 1 2FF183…BE43
_443._tcp.www  IN CNAME terenasslca2
_443._tcp.www2 IN CNAME terenasslca2
_143._tcp.imap IN CNAME terenasslca2
```

DANE jako alternativa k PKIX

- vynucení konkrétní autority (Usage: 2), nebo certifikátu (Usage: 3), bez vazby na PKI
- možnost ušetřit za DV certifikáty
- v režimu vkládání nové autority je nutné, aby server kořenový certifikát posílal během handshake
- zatím spíše nepoužitelné, málo validujících klientů

DANE pro bezpečné předávání pošty

- PKIX neumožňuje šifrované předávání pošty
  - často nevalidní certifikát
  - nezabezpečená vazba doména $\rightarrow$ MX záznam
  - není k dispozici uživatel, který by odsouhlasil varování
- DNSSEC a DANE dokáží bezpečnost vynutit
  - bezpečená vazba doména $\rightarrow$ MX záznam
  - otisk certifikátu v DNS, nezávislost na PKI
  - zpětně kompatibilní bez možnosti downgrade útoků
    - bez TLSA: oportunistické šifrování bez kontroly
    - s TLSA: šifrování vynuceno
    - selhání DNSSEC: zpráva odložena
- podporováno v Postfixu od verze 2.11

Validace TLSA záznamů

- rozšíření od CZ.NIC pro prohlížeče
- neovlivňuje chování prohlížeče, neumí nahradit PKIX
- odhalí sítě, které rozbíjejí DNSSEC

SSHFP záznamy pro bezpečné SSH

- SSH standardně vede seznam známých serverů
- DNS záznam typu SSHFP umožňuje ukládat otisky serverových klíčů do DNS
- validující klient pak ověří identitu serveru automaticky

Vytvoření záznamu

```
$ ssh-keygen -r server.example.com
```

Zapnutí validace

```
$ echo 'VerifyHostKeyDNS yes' >> ~/.ssh/config
```

http://www.root.cz/clanky/dnssec-jako-bezpecne-uloziste-ssh-klicu/

CESNET

Passive DNS

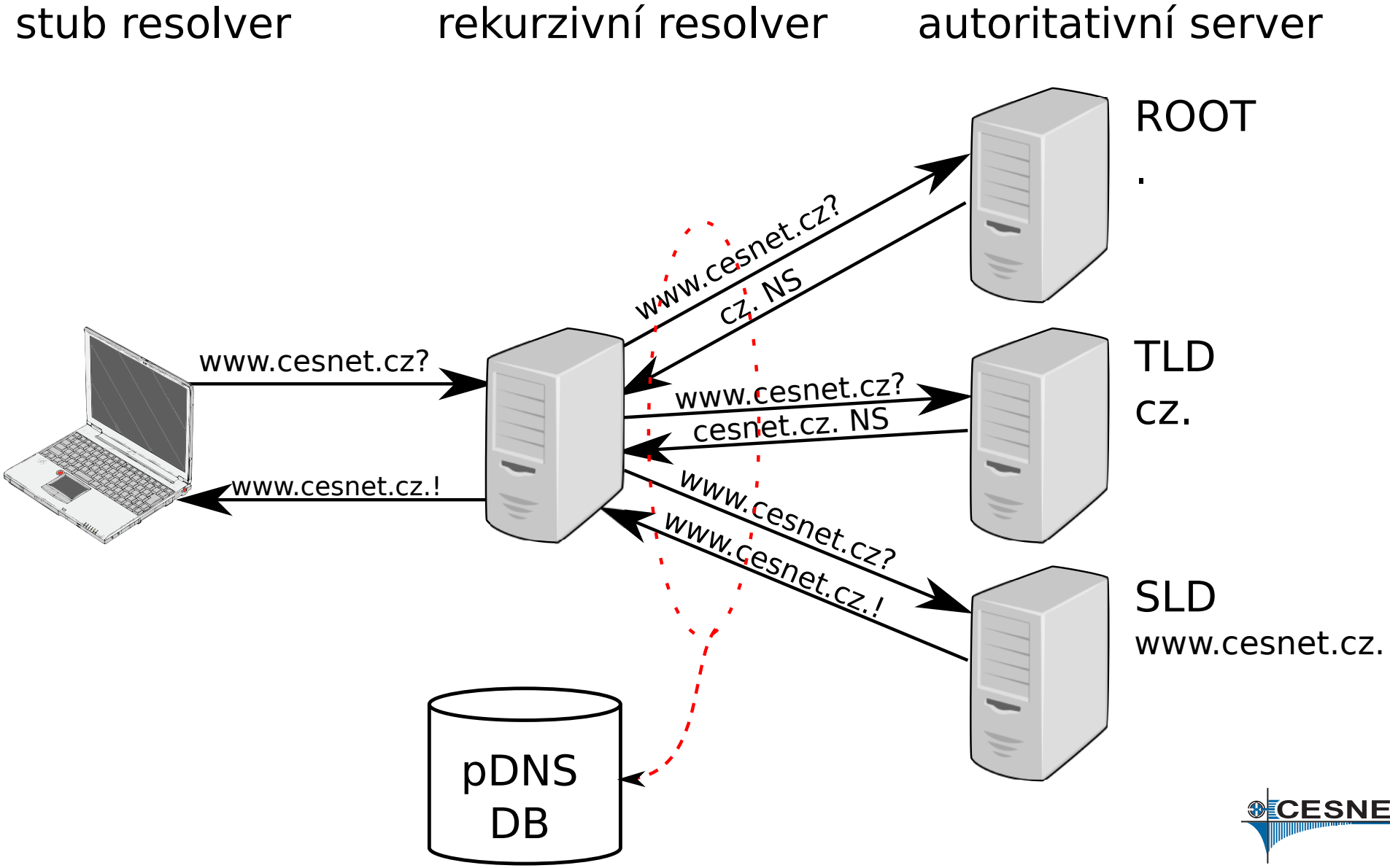
Myšlenka passive DNS

- Sbírat veřejná DNS data na rekurzivních DNS serverech
- Zjišťovat, na co se lidé ptají
- Nezjišťovat, kdo se ptá (ochrana soukromí)
- Ukládat do databáze spolu s časovou značkou
- Získat tak informace o **historii DNS dat**
- Mít možnost pokládat **inverzní DNS dotazy**

Dva přístupy k passive DNS

1. Zachytávání před rekurzivním serverem
   - zaznamenávání každé uživatelské aktivity
   - přesné sledování četnosti dotazů
2. Zachytávání za rekurzivním serverem
   - menší objem dat díky cache
   - implicitní ochrana soukromí

Passive DNS za rekurzivním serverem



Technické provedení

- senzor sbírá DNS provoz pomocí PCAP knihovny v blízkosti DNS serveru
- je možné jej buď spustit na stejném stroji jako DNS server, nebo klonovat data switchi
- data se zapisují do binárních souborů po minutách
- soubory jsou posílány pomocí SCP do databáze

Webové rozhraní pDNS@CERT.at

CERT.at / ACOnet
DNS History

www.google.at | Go | Reset [X]

Format: Whois csv HTML
Options: Sensor info Exact domain
List only: NXDOMAIN A NS CNAME SOA PTR MX TXT AAAA
First seen: >= <=
Last seen: >= <=
Sort: desc , desc , desc

```
% CERT.at / ACOnet DNS replicator WHOIS server, version 2.0.
% (C) 2011 All rights reserved.
% Authors: L. Aaron Kaplan <kaplan AT cert.at>
%          Achim Adam      <achim.adam AT univie.ac.at>
%
% 419 elements, 0.1437s
```

LEFT	RTYPE	RIGHT	FIRST-SEEN	LAST-SEEN	COUNT-SEEN
www.google.at	A	74.125.232.223	2012-09-21 06:05:39	2012-09-21 06:05:39	48
www.google.at	A	74.125.232.215	2012-09-21 06:05:39	2012-09-21 06:05:39	48
www.google.at	A	74.125.232.216	2012-09-21 06:05:39	2012-09-21 06:05:39	48
www.google.at	A	74.125.232.248	2012-09-21 12:39:39	2012-09-21 12:39:39	349
www.google.at	A	74.125.232.247	2012-09-21 12:39:39	2012-09-21 12:39:39	349
www.google.at	A	209.85.148.94	2012-09-11 17:27:31	2012-09-27 11:11:29	5
www.google.at	A	74.125.135.94	2012-09-10 13:06:35	2012-10-17 18:16:55	5
www.google.at	A	74.125.232.56	2012-11-22 18:40:04	2012-11-22 18:40:04	2
www.google.at	A	74.125.232.55	2012-11-22 18:40:04	2012-11-22 18:40:04	2
www.google.at	A	74.125.232.63	2012-11-22 18:40:04	2012-11-22 18:40:04	2
www.google.at	A	74.125.227.56	2012-11-22 18:40:31	2012-11-22 18:40:31	1
www.google.at	A	74.125.227.63	2012-11-22 18:40:31	2012-11-22 18:40:31	1
www.google.at	A	74.125.227.55	2012-11-22 18:40:31	2012-11-22 18:40:31	1
www.google.at	A	74.125.129.94	2012-11-22 18:40:36	2012-11-22 18:40:36	1
www.google.at	A	74.125.224.120	2012-11-22 18:40:41	2012-11-22 18:40:41	1
www.google.at	A	74.125.224.119	2012-11-22 18:40:41	2012-11-22 18:40:41	1
www.google.at	A	74.125.224.127	2012-11-22 18:40:41	2012-11-22 18:40:41	1
www.google.at	A	74.125.230.215	2012-10-23 08:26:04	2012-11-28 11:41:30	3
www.google.at	A	74.125.230.216	2012-10-23 08:26:04	2012-11-28 11:41:30	3
www.google.at	A	74.125.230.223	2012-10-23 08:26:04	2012-11-28 11:41:30	3

CESNET

Příklady použití

- Odhalení řídicích serverů botnetů, ve spolupráci s NetFlow také odhalení infikovaných stanic
- Odpověď na otázky:
  - jde o zneužití legitimní služby, nebo o cílený hosting škodlivého obsahu?
  - jaké další weby jsou hostovány na stejné IP adrese?
- Kontrola neoprávněného využití adresního prostoru (například sítě CESNET2)
- Výzkum nad globálními DNS daty
  - které domény jsou hostovány pouze na území jednoho státu?
  - jak často se mění data v různých doménách?

Přístup k databázi

- přístup k pDNS databázi CERT.at je omezen pro:
  - výzkumníky
  - CERT/CSIRT komunitu
  - provozovatele senzorů
- existuje návrh standardního formátu pro snadnou kombinaci dat z různých Passive DNS systémů
- zapojení dalších českých ISP je vítáno
- ☞ kontaktujte L. A. Kaplana – `kaplan@cert.at`

Závěrem

- DNS není jen UDP/53
- DNS není nejvíce 512 B
- bez DNSSECu nelze bezpečně předávat e-maily

Školení Principy a správa DNS a DNSSEC

- jednodenní školení
- teorie a praxe správy DNS serverů
- princip a implementace DNSSEC

CESNET

Závěr

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://Ondřej.Caletka.cz