Akademie

Lehký úvod do DNSSEC

Zbyněk Michl
<*zbynek.michl@nic.cz*>

Ondřej Surý
<*ondrej.sury@nic.cz*>

10. února 2011

cz nic

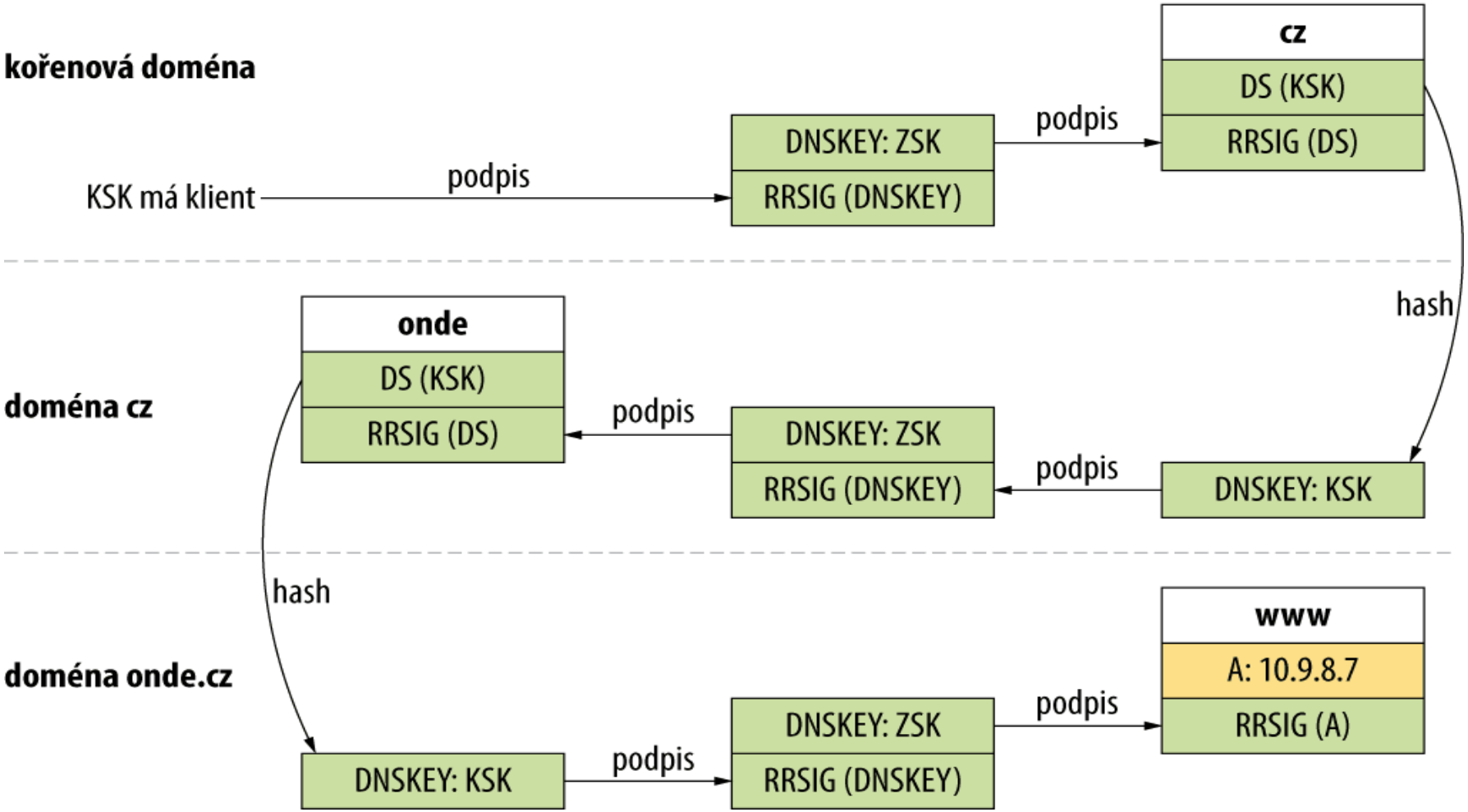
Základní principy DNSSEC

- DNSSEC umožňuje autoritativním serverům poskytovat k „standardním“ DNS datům navíc digitální podpisy RRSetů
- Resolvery ověřující DNSSEC podpisy poskytují potvrzené odpovědi

Základní principy DNSSEC

- Klienti, kteří používají validující resolvery, získávají „správná“ data (podepsaných domén)
- Odpovědi, které nejsou validní, jsou klientovi vráceny z nadřazeného resolveru s chybou „SERVFAIL“

Příklad: doména onde.cz



Základní pojmy DNSSEC

- Pevný bod důvěry
- Řetěz důvěry
- Důvěryhodný klíč
- Ostrov důvěry
- Validující resolver
- Key Signing Key (KSK)
- Zone Signing Key (ZSK)
- Podepsaná vs. nepodepsaná zóna

Pevný bod důvěry (Trust Anchor)

- Nakonfigurovaný klíč (nebo jeho hash), kterému důvěřujeme
- Musíme ho získat nějakou bezpečnou cestou
  - Kořenová zóna
  - ITAR, DLV
  - Stránky doménového registru
    - https://www.nic.cz/dnssec/

Řetěz důvěry (Authentication Chain)

- Sekvence DNSSEC záznamů (DNSKEY a DS) vedoucí od Pevného bodu důvěry k uzlu v DNS stromu
- V každém uzlu/úrovni máme ověřená data

Důvěryhodný klíč

- DNSSEC klíč, který je důvěryhodný
- Pevný bod důvěry
- Klíč získaný přes Řetěz důvěry

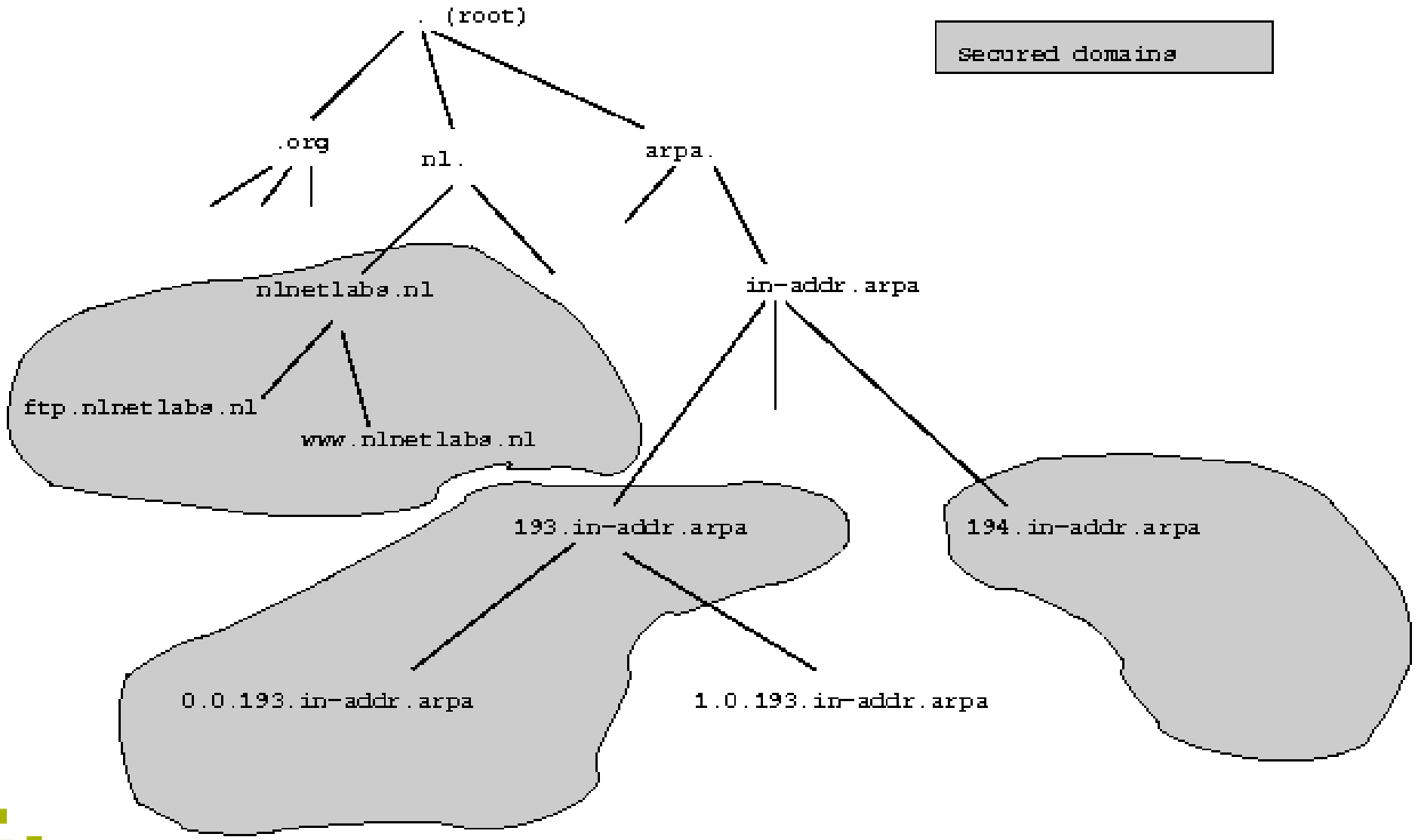
Validující Resolver

- Posílá DNS dotazy s DNSSEC OK příznakem
- Ověřuje validitu DNSSEC podpisů v DNS odpovědích
- Nastavuje **AD** příznak v odpovědích, pro dotazy s nastaveným **DO** nebo **AD** příznakem
- Má nakonfigurovaný alespoň jeden Pevný bod důvěry

Ostrov důvěry (Island of Security)

- Podepsaná důvěryhodná zóna, která není bezpečně delegována z nadřazené zóny
- Může být ověřena pomocí nakonfigurovaného Pevného bodu důvěry
- Obecněji i všechny bezpečně delegované podřazené zóny

Ostrovy důvěry



Key Signing Key

- DNSSEC klíč používaný pro podepsání dalších klíčů
- Silnější
  - Více bitů
  - Výpočetně složitější
  - Více dat
- Speciální bit (SEP) v příznacích DNSSEC klíče

Zone Signing Key

- DNSSEC klíč používaný pro podepsání vlastního obsahu zóny
- Slabší
  - Méně bitů
  - Výpočetně jednodušší
  - Rychlejší podpis i ověřování
  - Méně dat

Nové RR záznamy

DNSKEY RR záznam

- DNSSEC klíč obsahuje (RDATA):
  - Příznaky (Flags)
  - Protocol (vždy 3 – DNSSEC)
  - Algoritmus (5 – RSASHA1)
  - Veřejný klíč
- Key Signing Key

```
IN DNSKEY 257 3 5 AwEAAd[...]kNB8Qc=
```

- Zone Signing Key

```
IN DNSKEY 256 3 5 AwEAAd[...]kNB8Qc=
```

RRSIG RR záznam

- Digitální podpis RRSetu obsahuje:
  - Podepsaný RR typ
  - Algoritmus
  - Počet labelů v podpisovaném jméně (kvůli *)
  - Původní TTL
  - Datum platnosti (začátek a konec)
  - Key Tag, Jméno zóny
  - Digitální podpis

```
IN RRSIG A 5 3 600 20081203010003
20081103010003 58773 dnssec.cz. V0JXuw[...]
```

NSEC RR záznam

- Neexistenci doménového jména – pomocí vyjmenování dalšího následujícího labelu
- Zóna musí být abecedně setřízena (v každé úrovni hierarchie) → NSEC zonewalk
- RDATA:
  - Další doménové jméno
  - Bitová maska existujících typů (pro vlastníka)

```
IN    NSEC udp53.cz. NS RRSIG NSEC DS
```

NSEC3 RR záznam

- Obdoba NSEC (bez zonewalk)
- Každý vlastník → otisk (SHA-1/SHA-2)
- Opt-Out mechanismus
  - Generují se jen „bezpečné“ záznamy
- Setřízené jsou otisky

```
1pc2j02c3bb145tetd4nmtiqo0luvl51.org. 86400 IN
NSEC3 1 1 1 D399EAAB
1PMLFNIO9HCM9JI9DN8VJ9Q1LMA5QIVM A RRSIG
```

NSEC3 RR záznam

- RDATA
  - Algoritmus otisku
  - Příznaky
  - Opt-Out
  - Počet iterací
  - Další doménové jméno
  - Délka salt + salt (hash(owner+salt))
  - Délka otisku
  - Další jméno otisk
  - Bitová maska existujících typů (pro vlastníka/otisk)

DS RR záznam

- Záznam o bezpečné delegaci
  - Key Tag
  - Algoritmus (5 – RSASHA1)
  - Typ otisku (1 – SHA1)
  - Otisk

```
IN   DS 17398 5 1 BBDDD[...]3502D
```

Pravidelná údržba klíčů

- Klíče je zapotřebí střídat
  - Nemají „datum expirace“
- Čím déle je klíč veřejně viditelný, tím větší je pravděpodobnost, že bude prolomen
- Prolomení (zcizení) klíče může vést k potřebě rychlé „výměny“ klíče
  - Komplikované

Pravidelná údržba klíčů

- RFC 4641 – DNSSEC Operational Practices
  - Časy výměny klíčů jsou příliš konzervativní
  - Větší problém může být použitý algoritmus
- Klíč o síle 1024b stačí měnit cca jednou ročně
- Jsou dostupné automatické nástroje
  - OpenDNSSEC (www.opendnssec.net)
  - ZKT (www.hznet.de/dns/zkt/)
  - RIPE DISI tools (www.ripe.net/disi/)
  - DNSSEC Tools (www.dnssec-tools.org)

Hledání chyb

- DNS odpověď, na dotaz koncového klienta, který je podepsán a není validní (tj. data byla změněna, nebo podpis nesedí), vrátí `RCODE=SERVFAIL`
- Pro aplikace (a uživatele) se bude doména jevit jako „neexistující“
- Příznak CD v hlavičce dotazu umožní, aby koncový klient dostal v DNS odpovědi i špatně zvalidovaná data

Hledání chyb: Úkol

- Zeptejte se validujícího resolveru na špatně podepsanou doménu

```
$ dig IN A www.rhybar.cz. @217.31.204.130
```

- Přidejte CD příznak

```
$ dig +cd IN A www.rhybar.cz. @217.31.204.130
```

Kde je chyba?

```
; <<>> DiG 9.6.1-P1 <<>> +multi +cd IN RRSIG www.rhybar.cz @217.31.204.130
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12880
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 6

;; QUESTION SECTION:
;www.rhybar.cz.     IN RRSIG

;; ANSWER SECTION:
www.rhybar.cz.      563 IN RRSIG A 5 3 600 20081030080058 (
                           20080930080058 5172 rhybar.cz.
                           XVkut4l9mw2MhodZFIOD2L57AU2u+I6wGVlK1fr6w5lo
                           cFC5NIe8ukw79jYdOCH3WwFgSMscumIz1sGqRPrN/Crh
                           XiU0ymFGFju9x/k10lv6SGS6lslgnZluet04CyibGQ2H
                           BnwTx7qK3j+bNzxKLvjpn7DY9f+YKB8F2FtwNOc= )
...
```