DNSSEC

CZ.NIC z.s.p.o.
Ondřej Surý / *ondrej.sury@nic.cz*
18. 5. 2009

cz nic
správce domény cz

Vrcholek zóny

- „Nejvyšší“ uzel v hierarchii zóny
- Uzel podřazené zóny v místě delegace
- '@'
- dnssec.cz. IN NS a.ns.nic.cz.
- dnssec.cz. IN NS b.ns.nic.cz.
  - Vrcholek zóny je 'dnssec.cz.'

DNS paket

- Hlavička
  - ID (16 bit)
  - Query/Response (1 bit)
  - Příznaky
- Dotaz
- Odpověď
- Authoritativní sekce
- Další (additional)

Komprese v DNS paketu

- Doménové jméno
- Sekvence labelů
  - Délka labelu
  - Alfanumerické jméno
  - Max 63
- Komprese
  - První dva bity délky 11
  - Odkaz na předchozí použití v paketu

DNS dotaz / query

- Standardní DNS paket
- Nastavený příznak Query v hlavičce
- Vyplněná sekce Dotaz
  - QNAME
  - QTYPE
  - QCLASS

DNS odpověď

- Standardní DNS paket
- Vyplněné sekce:
  - Odpověď
  - Authoritativní
  - Další / Additional
- Nastavený RCODE

Základní principy DNSSEC

- DNSSEC umožňuje autoritativním serverům poskytovat k „standardním“ DNS datům navíc digitální podpisy RRsetů
- Resolvery ověřující DNSSEC podpisy poskytují potvrzené odpovědi
- Klienti, kteří používají validující resolvery, získávají „správná“ data
- Odpovědi, které nejsou validní, jsou klientovi vráceny z nadřazeného resolveru s chybou „SERVFAIL”

Nové RR záznamy

- DNSKEY
- RRSIG
- NSEC/NSEC3
- DS

DNSKEY RR záznam

- DNSSEC klíč
- RDATA obsahují
  - Příznaky (Flags)
  - Protocol (vždy 3)
  - Algoritmus (5 - RSASHA1)
  - Veřejný klíč
- IN DNSKEY 257 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)
  - Tag, Jméno zóny
  - Digitální podpis

NSEC/NSEC3 RR záznam

- Záznam vyznačující neexistenci doménového jména – pomocí vyjmenování dalšího následujícího labelu
- Zóna musí být abecedně setřízena (v každé úrovni hierarchie)
- Obsahuje:
  - Další doménové jméno
  - Bitová maska existujících typů (pro vlastníka)
- IN NSEC udp53.cz. NS RRSIG NSEC DS
- NSEC3 – hash, opt-out

DS RR záznam

- Záznam o bezpečné delegaci
- RDATA obsahují hash DNSKEY klíče, kterým je zóna podepsaná
- Obsahuje:
  - Key Tag
  - Algoritmus
  - Digest Type
  - Digest
- IN DS 17398 5 1 BBDDD[...]3502D

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

Řetěz důvěry

- 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

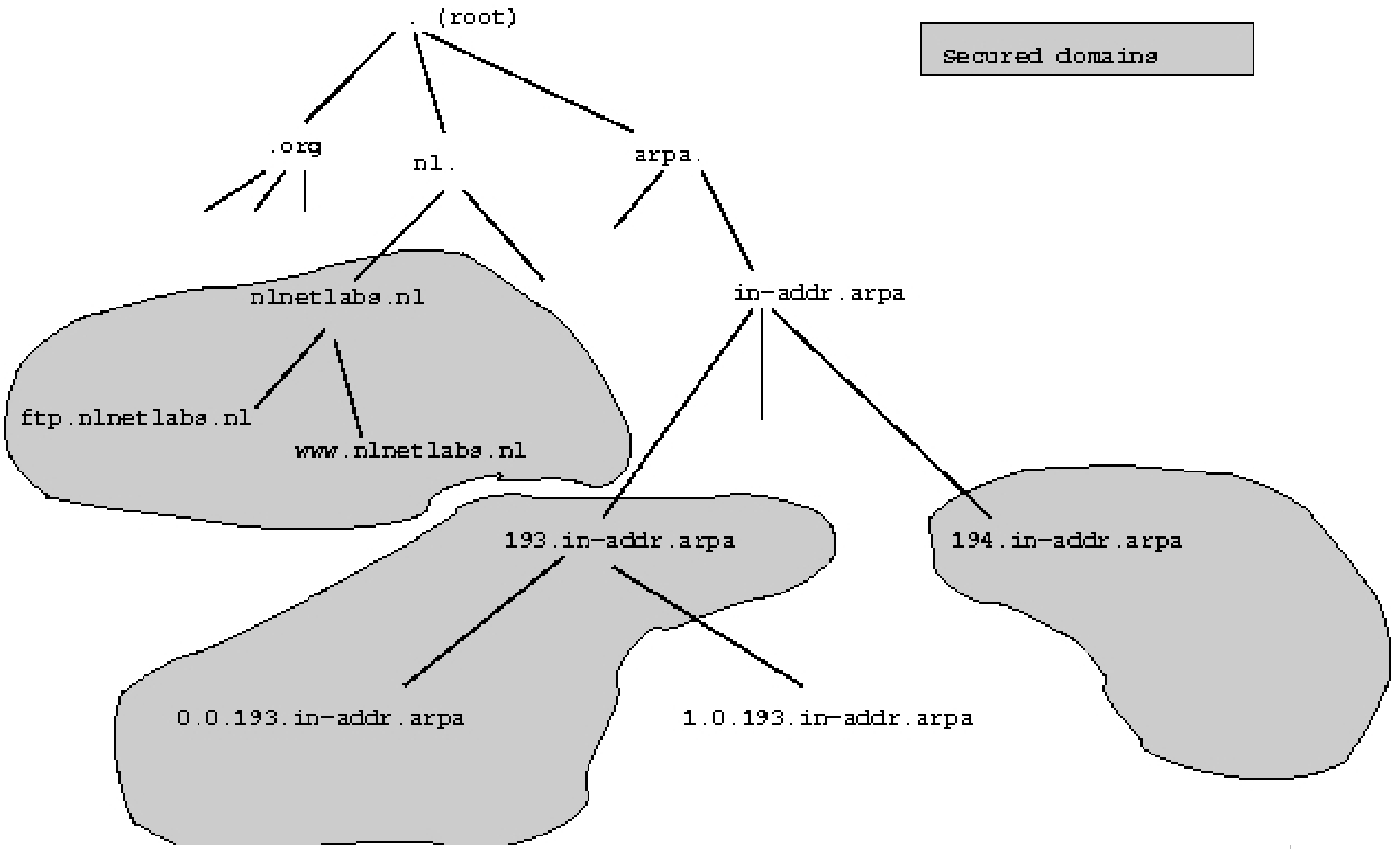
Validující Resolver

- Posílá DNS dotazy s DNSSEC OK
- Ověřuje validitu DNSSEC podpisů v DNS odpovědích
- Má nakonfigurovaný alespoň jeden Pevný bod důvěry

Ostrov důvěry

- 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 RDATA

Zone Signing Key

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

Nasazení DNSSEC

Nasazení DNSSEC

- Jednorázové aktivity:
  - Ujasněte si adresářovou strukturu na autoritativním serveru a pojmenování zónového souboru
  - Povolte DNSSEC na autoritativních serverech
  - Povolte DNSSEC na rekurzivních serverech

Nasazení DNSSECu

- Povolte DNSSEC pro každou zónu
  - Vygenerujte ZSK a KSK
  - Připojte klíče do zónového souboru
  - Podepište zónu
  - Změnte odkaz na zónový soubor v `named.conf` na podepsaný zónový soubor
  - Znovu načtěte zónu

Nasazení DNSSECu

- Umístěte DS záznamy do nadřazené zóny
- V .CZ pomocí svého registrátora
- V případě, že nadřazená zóna nepoužívá DNSSEC, umístěte DLV záznamy do `DLV registru`

Všechny tyto kroky... podrobně!

Připravte adresářovou strukturu

- K dispozici jsou nástroje, jež usnadňují údržbu zóny, ale nejlépe pracují se standardizovanou adresářovou strukturou
- Umístěte všechny soubory zóny do jediného adresáře

Povolte DNSSEC na autoritativních serverech

- BIND >=9.4 má DNSSEC standardně zapnutý
- BIND >=9.6 má podporu NSEC3
- NSD3 má DNSSEC standardně zapnutý
  - Není potřeba nic dělat
  - včetně NSEC3

Zabezpečení zóny

- Pro každou zónu jsou vytvořeny dva typy klíčů

1) Klíč podepisující zóny (ZSK) – používá se k podpisu dat v zóně

2) Klíč podepisující klíče (KSK) – používá se k podpisu klíče podepisujícího zóny a k vytvoření „důvěryhodného vstupního bodu (SEP)“ pro zónu

Vytvoření klíčů

- Vytvoření ZSK

```
dnssec-keygen -a RSASHA1 -b 1024
  -n ZONE zonename
```

  - Využívá algoritmus RSA SHA1
  - o délce 1024 bitů
  - Toto je DNSSEC klíč pro zónu (-n ZONE)

Vytvoření klíčů

- Vytvoření ZSK

```
dnssec-keygen -a RSASHA1 -b 1024
  -n ZONE zonename
```

- Vytvoří 2 soubory

```
Kzonename+<alg>+<fing>.key
```

```
Kzonename+<alg>+<fing>.private
```

  - `.key` je veřejnou částí klíče, `.private` je soukromou částí klíče

Vytvoření klíčů

- Vytvoření KSK

```
dnssec-keygen -a RSASHA1 -b 2048
  -n ZONE -f KSK zonename
```

  - Využívá algoritmus RSA SHA1
  - o délce 2048 bitů
  - Takto velký klíč potřebuje hodně entropie!
  - Toto je DNSSEC klíč pro zónu (-n ZONE)
  - Má nastavení bitu (KSK) důvěryhodného vstupního bodu

Připravte zónu

- Přidejte veřejné části obou KSK a ZSK k zóně, která má být podepsána

  Direktiva `$INCLUDE v zonefile` nebo

  `cat Kzonename+*.key >> zonefile`

  - Dejte si pozor, abyste nepoužili pouze jednu „>“! (přepíše soubor)

Podepsání zóny

- Přidejte `RRSIG, NSEC` a přiřazené záznamy k zóně

```
dnssec-signzone [-o zonename]
  [-N INCREMENT] [-k KSKfile]
  zonefile [ZSKfile]
```

- Název zóny `(zonename)` je implicitně název souboru `(zonefile)`
  - Pojmenujte soubor podle zóny!

Podepsání zóny

```
dnssec-signzone [-o zonename]
  [-N INCREMENT] [-k KSKfile]
  zonefile [ZSKfile]
```

`-N INCREMENT` automaticky inkrementuje sériové číslo během podepisování

- Odstraňuje chybu způsobenou „lidským faktorem“

Podepsání zóny

```
dnssec-signzone [-o zonename]
  [-N INCREMENT] [-k KSKfile]
  zonefile [ZSKfile]
```

- `KSKfile` je implicitně `Kzonefile*`
  - s nastavením bitu `SEP`
- `ZSKfile` je implicitně `Kzonefile*`
  - bez nastavení bitu `SEP`

Podepsání zóny

```
dnssec-signzone [-o zonename]
  [-N INCREMENT] [-k KSKfile]
  zonefile [ZSKfile]
```

Výstupní soubor je `zonefile.signed`

- Seřazený podle abecedy
- včetně `RRSIG, NSEC & DNSKEY` RRs
- Mnohem větší než předtím!

Aktualizujte `named.conf`

Nahraďte

```
zone “udp53.cz” {
type master;
file “/etc/bind/zone/udp53.cz/udp53.cz”;
};
```

Za

```
zone “zonename” {
type master;
file “/etc/bind/zone/udp53.cz/udp53.cz.signed”;
};
```

Začněte poskytovat podepsanou zónu

- Načtěte znovu konfiguraci named

```
rndc reconfig
rndc flush
```

- Nyní poskytujete DNSSEC podepsané zóny

Oznamte nadřazené zóně DNSSEC

- Vaše nadřazená zóna musí nyní vložit “DS” RR pro vytvoření řetězu důvěry
- Postupy se budou lišit podle organizací, ale musí být provedeny bezpečně
  - bude vyžadovat použití dsset- a/nebo keyset- souborů
- Pro .cz kontaktujte svého registrátora

Nadřazená zóna bez podpory DNSSECu

- Ne všechny TLD podporují DNSSEC
  - Ve skutečnosti podporuje v současnosti DNSSEC **VELMI MÁLO** TLD
  - .cz DNSSEC podporuje
- Poskytněte váš `DNSKEY` těm stranám, u kterých chcete, aby ověřovaly vaši zónu.
  - Musí to být provedeno bezpečně, nejen pouze stažením přes DNS protokol ("dig")

Problematika pravidelné údržby

Pravidelná údržba zóny

- Podpisy mají životnost
  - Datum „vzniku“ – 1 hodina před spuštěním `dnssec-signzone`
  - Datum expirace – 30 dní po spuštění `dnssec-signzone`
- Expirované podpisy způsobí, že zóna nepůjde ověřit!

Pravidelná údržba zóny

- Pokaždé, když upravíte zónu – nebo minimálně každých 30 dnů (mínus TTL) musíte znovu spustit `dnssec-signzone`

- Pokud to neuděláte
  1) Podpisy v zóně budou zastaralé
  2) Data zóny budou „NEDOSTUPNÁ“

Pravidelná údržba klíče

- 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 „výměny“ klíče

Pravidelná údržba klíčů

- Klíč o síle 1024b stačí měnit jednou ročně
- Jsou dostupné automatické nástroje
  - RIPE DISI tools (www.ripe.net/disi/)
  - DNSSEC Tools (www.dnssec-tools.org)
  - ZKT (www.hznet.de/dns/zkt/)

Pravidelná údržba klíčů

- Dva způsoby výměny klíčů
- Dvojitý podpis
- Předčasné publikování

Předčasné publikování

- Používá se pro výměnu ZSK
- Do vrcholku zóny se vloží další klíč
- Nutné explicitně specifikovat ZSK klíč používaný k podpisu
- Po uplynutí TTL se může začít podepisovat novým klíčem
- Po uplynutí TTL můžeme starý ZSK odstranit

Dvojitý podpis

- Používá se u KSK
- Všechny klíče jsou podepsány dvěma (či více) KSK klíči
- Nadřazená zóna dostane oba dva klíče

Pevné body důvěry (Trust Anchors)

Pevné body důvěry

- Pro ověření ostatních zón musíte vložit „pevný bod důvěry“ pro každý zónu, kterou budete chtít ověřovat
- Nejvyšší pevný bod důvěry bude pocházet od podepsané root zóny (“ . ”)

Pevné body důvěry

- Až bude podepsána root zóna, bude vyžadován pouze jeden pevný bod důvěry
- Dokonce i poté, co bude podepsána root zóna, je stále možné a pravděpodobné, že bude potřeba mít další pevné body důvěry

Pevné body důvěry

- V současnosti (2009), root zóna (“.”) není podepsána
- Jsou vyžadovány jednotlivé pevné body důvěry
- Pevné body důvěry musí být získány důvěryhodnými prostředky
- DNS není jedním z těchto prostředků, AVŠAK...

Pevné body důvěry

```
dig udp53.cz DNSKEY @localhost
```

```
udp53.cz. 14400 IN  DNSKEY 256 3 5 BE[...]/V1
udp53.cz. 14400 IN   DNSKEY 257 3 5 BE[...]1ylot7
```

- Pomocí digu získáme DNSSEC klíče, které mohou být ověřeny pomocí dalších prostředků (web, telefon, tištěná média, atd.)

Pevné body důvěry

- Klíč pro .cz je na stránkách https://www.nic.cz/dnssec/
- Poštovní konference – informace o změnách:
  - dnssec-announce@lists.nic.cz
  - https://lists.nic.cz/mailman/listinfo/dnssec-announce

Pevné body důvěry (Bind 9)

- bude zapotřebí, aby `named.conf` obsahoval:

```
trusted-keys {
    “udp53.cz.” 257 3 5 “BE[...]1ylot7”;
    “cz.” 257 3 5 “AwEAAdo9[...]MnitkuM=”;
    “se.” 257 3 5 “AwEAAdKc[...]UkNB8Qc=”;
};
```

  - Klíč pro KAŽDOU zónu, kterou chcete ověřovat

Pevné body důvěry (Unbound)

- Unbound umí použít formát trusted-keys, který používá Bind 9
- Direktiva:
  - trusted-keys-file: <soubor>
- Další možnosti:
  - trusted-anchor-file: <soubor>
    - Obsahuje DNSKEY nebo DS v DNS formátu
  - trusted-anchor: "RR záznam"

Pevné body důvěry

- Správa jednotlivých pevných bodů důvěry je složitá
- IANA ITAR
  - Interim Trust Anchor Repository
- ISC DLV
  - Domain Lookaside Validation

IANA ITAR

Interim Trust Anchor Repository

- Dočasné úložiště pevných bodů důvěry
- Pouze do doby než bude podepsán root
- Off-line metoda
- https://itar.iana.org/

Použití ITAR

- Soubor ve formátu trusted-achor-file
  - Přímé použití v Unbound
  - Skript pro konverzi do Bind 9
- Přístup: rsync, http, ftp
- Ověření přes OpenPGP
- Může obsahovat DS nebo DNSKEY
- Pozor na NSEC3 klíče
  - Bind verze 9.5 a menší nepodporuje!

Domain Lookaside Validation

DLV

- Online
  - Musí být dostupný
- Při ověřování hledá resolver v nadřazené zóně záznam `DS` pro zónu, která je ověřována
- Pokud neexistuje, je vytvořen dotaz na záznam `DLV` v zóně registru DLV
- Pokud je úspěšná, je `DLV RR` použito jako `DS` pro danou zónu

Příklad DLV

- `udp53.org` je podepsaná
- Vlastník `udp53.org` se registroval do DLV registru u ISC
- Je vytvořen DNSSEC dotaz na `A RR` jména www.udp53.org
- Není nalezen DS záznam v `.org` pro zónu `udp53.org`

Příklad DLV

- Resolver bez zapnutého DLV nebude v tomto bodě schopen provést ověření
- Resolver se zapnutým DLV bude hledat `udp53.org.dlv.isc.org. DLV RR`
- Tento `DLV RR` pak bude použit jako `DS` pro zónu `udp53.org`.

Povolení DLV

- Použití DLV pro ověření je provedeno na rekurzivním serveru
  - Pro DLV registr musí být nakonfigurován důvěryhodný klíč
  - Konfigurace `dnssec-lookaside` musí být nasměrována na pevný bod důvěry DLV

Povolení DLV

- named.conf:

```
trusted-keys {
        dlv.isc.org. 257 3 5 “BEA[...]uDB”;
};
options {
        dnssec-lookaside "."
       trust-anchor dlv.isc.org.;
};
```

Generování DLV RRs

- Při podepisování zóny pro registrátora DLV přidejte přepínač "-l" (malé L) k dnssec-signzone:

```
dnssec-signzone [-o zonename]
[-N INCREMENT] -l dlvzone
[-k KSKfile] zonefile [ZSKfile]
```

- dlvzone bude závislá na DLV registru

Generování DLV RRs

- Na základě předchozího příkladu:
  `dnssec-signzone -N INCREMENT -l dlv.isc.org. udp53.org`

- V tomto bodě bude vytvořen soubor `dlvkey-udp53.org, který je` rovnou připraven k odeslání správci ISC DLV

Registrace v DLV

- Kontaktujte registrátora DLV pro instrukce jak prokázat vlastnictví zóny a platnost `DLV RR` záznamu
- Vložení vašeho `DLV RR` záznamu do registru DLV musí být provedeno důvěryhodným způsobem

ISC registr DLV

`http://www.isc.org/ops/dlv/`

Testování a ladění DNSSECu

Testování DNSSECu

- Nyní, když distribuujete podepsané DNSSEC RR záznamy, funguje to?
- DNSSEC může být laděn pouze pomocí příkazů “`dig`” a “`date`”

Dotazování na DNSSEC

- Normální DNS dotaz vyžadující ověřená data z jakéhokoliv resolveru dostane v odpovědi RRset

- Dotaz vyžadující nepodepsaná data z jakéhokoliv resolveru také dostane v odpovědi RRset

Dotazování na DNSSEC

- Dotaz, který validujícímu resolveru vrátí upravená nebo neplatná data, skončí s chybou `SERVFAIL`
- Pro aplikace (a uživatele) se bude doména jevit jako „neexistující“
- Příznak CD v hlavičce umožní, aby klient dostal i neplatná data

výstup `dig` – bez DNSSECu

```
dig
;; [..] status: NOERROR
;; flags: qr rd ra;
```

- Správná odpověď; odpověď (qr), požadovaná rekurze (rd), rekurze k dispozici (ra)

výstup `dig` – bez DNSSECu

```
dig www.udp53.cz a
;; [..] status: NOERROR
;; flags: qr rd ra;
```

- Z validujícího resolveru – tohle jsou garantovaná správná data

výstup `dig` – bez DNSSECu

```
dig www.udp53.cz a
;; [..] status: NOERROR
;; flags: qr rd ra;
```

- Ale jak víte, že váš resolver provádí validaci?

výstup `dig -s` DNSSECem

```
dig +dnssec www.udp53.cz a
;; [..] status: NOERROR
;; flags: qr rd ra ad
```

- Jako předtím, ale tentokrát autentizované!

Dotazování na DNSSEC

- Pro vrácení příznaku **`AD`** musí mít resolver provádějící ověření pevný bod důvěry, který může být zpětně vystopován (pomocí `DS` RR záznamů)
- Pokud řetěz důvěry nevede k pevnému bodu důvěry, nebude příznak `AD` nastaven, ale `RRSIG` záznamy budou i tak vráceny

výstup `dig` – DNSSEC

```
dig +dnssec www.udp53.cz a
```

```
www.udp53.cz. 3600 IN A       192.168.154.2
www.udp53.cz. 3600 IN RRSIG   A 5 3 3600 20080627122225 20080617122225
   46704 udp53.org.
    XEkXkv9MCRiGbxO9T0dkNY+3y5EZRB6s6YOk0pFAVUL/y8VDeJphc8yb
      K6E/YLvraItdGvIvpy4P1OuIY09BGQ==
```

- Pokud je `AD` nastaveno, validující resolver má pevný bod důvěry, pokud ne, pořád máme data, která můžeme ověřit sami

Dotazování na DNSSEC

- Pokud víme, že komunikujeme s validujícím resolverem a dostaneme zpět `SERVFAIL`, může se jednat o neověřená podepsaná data
- Pokud je to tak, nastavení bitu `"CD"` v dotazu způsobí, že resolver i tak zašle „nevalidní“ data

výstup `dig` – DNSSEC

```
dig +dnssec +cd www.udp53.cz a
```

```
www.udp53.cz. 3600 IN A       192.168.154.2
www.udp53.cz. 3600 IN RRSIG   A 5 3 3600 20080627122225 20080617122225
   46704 udp53.cz. xxxxxxxxxx
```

- Neplatný záznam `RRSIG` (**xxxxxxxxxx**), ale s příznakem `+cd`, proto dostaneme odpověď

výstup `dig` – DNSSEC

```
dig +dnssec +cd www.udp53.cz a
```

```
www.udp53.cz. 3600 IN A       192.168.154.2
www.udp53.cz. 3600 IN RRSIG   A 5 3 3600 20080627122225 20080617122225
   46704 udp53.org.
   XEkXkv9MCRiGbxO9T0dkNY+3y5EZRB6s6YOk0pFAVUL/y8VDeJphc8yb
   K6E/YLvraItdGvIvpy4P1OuIY09BGQ==
```

výstup `dig` – DNSSEC

```
dig +dnssec +cd www.udp53.cz a
```

```
www.udp53.cz. 3600 IN A       192.168.154.2
www.udp53.cz. 3600 IN RRSIG   A 5 3 3600 20080627122225 20080617122225
   46704 udp53.org.
   XEkXkv9MCRiGbxO9T0dkNY+3y5EZRB6s6YOk0pFAVUL/y8VDeJphc8yb
   K6E/YLvraItdGvIvpy4P1OuIY09BGQ==
```

- Data v podpisu ukazují, že podpis je expirovaný
- Porovnejte s aktuálním datem

Dotazování na DNSSEC

- Všimněte si, že je snadné zkontrolovat datum na podpisech
- Je mnohem těžší (není v lidských silách?) najít chybu v klíči samotném
- Předchozí příklad je krajně nepřirozený (xxx?)

Dotazování na DNSSEC

- Další problém, který může nastat je chybějící nebo jiný hash nebo klíč
  - `DS` v nadřazené zóně
  - `DNSKEY` v aktuální zóně
- Není těžké určit ani tuto chybu!

výstup `dig` – DNSSEC

```
dig +dnssec +cd www.udp53.cz
```

```
www.udp53.cz. 3600 IN A       192.168.154.2
www.udp53.cz. 3600 IN RRSIG   A 5 3 3600 20080627122225 20080617122225
   46704 udp53.org.
   XEkXkv9MCRiGbxO9T0dkNY+3y5EZRB6s6YOk0pFAVUL/y8VDeJphc8yb
   K6E/YLvraItdGvIvpy4P1OuIY09BGQ==
```

- Podpis byl vytvořen s klíčem 46704

výstup `dig` – DNSSEC

```
dig +cd +multi udp53.cz DNSKEY
```

```
udp53.cz.  14400 IN DNSKEY  256 3 5 (
           BEAAAAO2oQi7U9m9i495S/XoAk+j8QxxnBHon6fa7nlN
           7xoqrSr/xzy3+IerFS1KgJz1gJGbTsGV0WI1/bvAzIEK
           Uh+p ) ; key id = 46704
```

`DNSKEY` v zóně existuje

- Pokud ne, nepůjde ověřit!

výstup `dig` – DNSSEC

```
dig +cd +multi udp53.cz DNSKEY
```

```
udp53.cz.  14400 IN DNSKEY 256 3 5 (
   B[...]p ) ; key id = 46704
udp53.cz. 14400 IN DNSKEY 257 3 5 (
   B[...]J ) ; key id = 64249
```

- ZSK `DNSKEY` v zóně existuje
- Připojený KSK je 64249

výstup `dig` – DNSSEC

```
dig +norec @a.ns.nic.cz udp53.cz DS
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29385
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2
```

- `DS` v nadřazené zóně neexistuje
- Pokud neuděláme DLV, tohle je důvod, proč se neautentizuje

výstup `dig` – DNSSEC

```
dig +norec @a.ns.nic.cz udp53.cz DS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29385
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2
```

- Server bude vracet odpovědi, ale bez příznaku „AD“
- Neexistuje řetěz důvěry až k pevnému bodu důvěry
- Není zaregistrovaný DS záznam v doméně .cz

Další možné problémy

- „Chytrý“ firewall/home gateway
  - Neumí EDNS0
  - Zahazuje UDP větší než 512 byte
  - Zahazuje neznámé RR typy
  - Modifikuje obsah RR záznamů
  - Zahazuje neznámé příznaky DNS paketu

Diskuze

Reference

- https://www.nic.cz/dnssec/
- http://www.nlnetlabs.nl/dnssec_howto/
- RFC1034, 1035 (DNS)
- RFC2181 (DNS Clarification)
- RFC2671 (EDNS0)
- RFC4033, RFC4034, RFC3045 (DNSSEC)
- RFC5011 (Trust Anchor Update)
- RFC5155 (NSEC3)