

DNSSEC

Adam Tkáč, Red Hat, Inc.

21. října 2008

Copyright © 2008 Adam Tkáč, Red Hat, Inc.

Copyright © 2008 Tomáš Janoušek (beamer template)

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.

Obsah

1 Úvod

- DNS
- Zranitelnost DNS

2 DNSSEC

- Úvod
- Nové typy záznamů
- Jak DNSSEC pracuje

3 Praktické nasazení, server BIND

- Podepisování zóny
- Současný stav
- Testování a hledání chyb

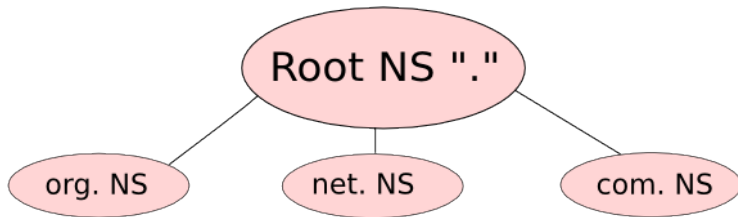
4 Literatura

Section 1

Úvod

Co to je?

- hierarchické pojmenování počítačů a služeb na Internetu
- distribuovaná databáze
- sdružuje počítače do logických celků, tzv. domén



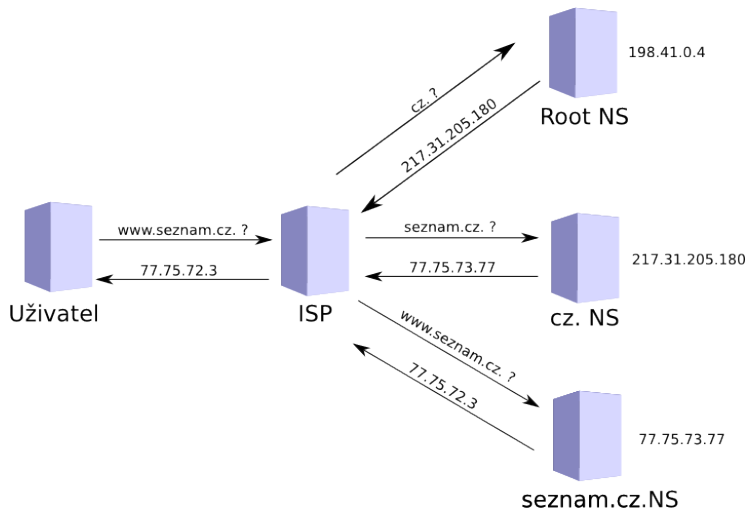
Historie

- distribuce jmen v souboru "hosts"
- RFC 1033, 1034 a 1035 (rok 1987), základní kameny DNS
- první pokusy o DNSSEC v roce 1997, poté revize v roce 1999 (RFC 2535), nedostatečná škálovatelnost
- TSIG (RFC 2845, rok 2000), autentizace pomocí sdíleného tajemství
- současná definice DNSSEC v RFC 4033, 4034 a 4035, tzv. DNSSEC-bis
- NSEC3 (RFC 5155, březen 2008), další vylepšení DNSSEC

Jak DNS pracuje

- resolver (= uživatel) se ptá serveru, který obvykle provozuje jeho Internetový provider (ISP)
- ISP server rekurzivně vyřeší dotaz a vrátí odpověď uživateli

Příklad



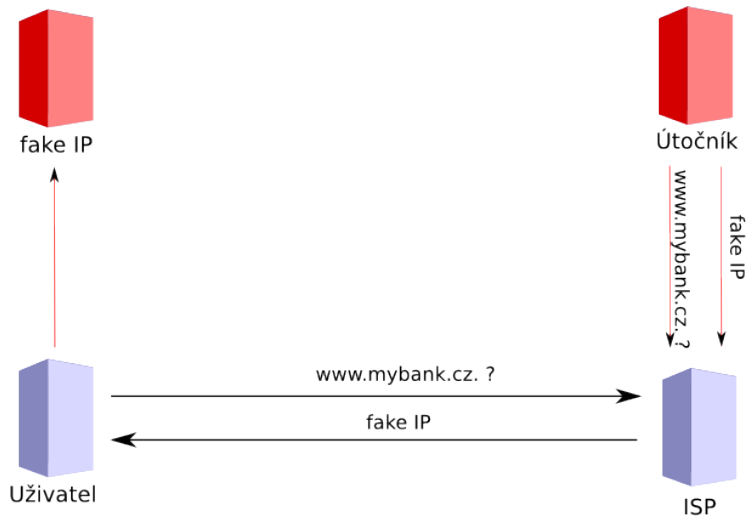
Zranitelnost

- základní problém - jak ověřit autenticitu a integritu příchozích dat
- DNS bylo původně navrženo s omezenými možnostmi zabezpečení - dvě šestnáctibitové náhodné hodnoty, zdrojový port a transakční ID
- mnoho implementací nepoužívá náhodné čísla
- pokud útočník uhodne port a transakční ID může podvrhnout odpověď
- hrubou silou lze prolomit i náhodné čísla

Základní typy útoků

- podvržení dat koncovému uživateli (endpoint spoofing)
- vložení podvržených dat do keše rekurzivního serveru (cache poisoning)

Příklad



Section 2
DNSSEC

Úvod

- zajišťuje autenticitu a integritu dat
- první návrhy (rok 1997 a 1999) se nerozšířily, nedostatečná škálovatelnost
- současná definice v RFC 4033 - RFC 4035
- využívá asymetrickou kryptografii
- pracuje na principu řetězu důvěry
- vyžaduje rozšíření protokolu, tzv. EDNS0 (RFC 2671)
- zavádí nové typy záznamů
- odkrývá záznamy v zóně

EDNS0

- definován v RFC 2671 (rok 1999)
- prodlužuje délku DNS packetu až na 4 KB
- EDNS0 packet je nekompatibilní s původním DNS packetem
- starší (a chybně navržený) software nebo hardware může způsobovat problémy

DNSKEY

- obsahuje veřejný klíč, záznamy jsou podepisovány korespondujícím privátním klíčem
- specifikuje kryptografický algoritmus, který je používán

DNSKEY záznam

```
example.com. 86400 IN DNSKEY 256 3 5 (
AQPSKmynfzW4kyBv015MUG2DeIQ3
Cbl+BBZH4b/OPY1kxkmvHjcZc8no
kfzj31GajIQKY+5CptLr3buXA10h
WqTkF7H6RfoRqXQeogmMHfpftf6z
Mv1LyBUgia7za6ZEz0JB0ztyvhjL
742iU/TpPSEDhm2SNKLiJfUppn1U
aNvv4w== )
```

RRSIG - Resource Record SIGNature

- obsahuje digitální podpis a používaný kryptografický algoritmus a ID klíče, kterým byl podepsán
- obsahuje čas uvedení a expirace podpisu

RRSIG záznam

```
host.example.com. 86400 IN RRSIG A 5 3 86400
20030322173103 (
20030220173103 2642 example.com.
oJB1W6WNGv+ldvQ3WDGOMQkg5IEhjRip8WTr
PYGv07h108dUKGMeDPKijVCHX3DDKdfb+v6o
B9wfuh3DTJXUafI/M0zm0/zz8bW0Rznl803t
GNazPwQKkRN20XPXV6nwwfoXmJQbsLNRlFkG
J5D6fwFm8nN+6pBzeDQfsS3Ap3o= )
```

DS - Delegation Signer

- slouží k vytvoření řetězu důvěry mezi zónou a nadřazenou zónou
- obsahuje otisk klíče, který slouží jako podpisový klíč (KSK)
- uložen v nadřazené zóně

DS záznam

```
dnskey.example.com. 86400 IN DS 60485 5 1 (
2BB183AF5F22588179A53B0A98631FAD1A292118 )
```

NSEC - Next SECure

- slouží k autentizovanému popření existence
- obsahuje odkaz na další existující autoritativní záznam v zóně
- spojuje záznamy v zóně do "kruhu"
- odkrývá všechny záznamy v zóně - tzv. "zone enumeration" problém

NSEC záznam

```
alfa.example.com. 86400 IN NSEC host.example.com. (
A MX RRSIG NSEC TYPE1234 )
```

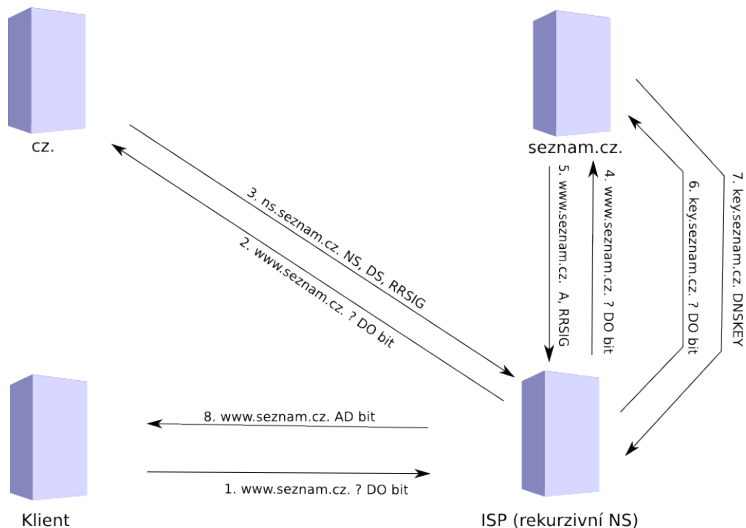
NSEC3 - Next SECure 3

- RFC 5155 (březen 2008)
- podobně jako NSEC slouží k autentizovanému popření existence
- místo jmen používá jejich hash
- řeší "zone enumeration" problém

AD, CD a DO bity

- DO bit (DNSSEC OK) nastavuje rekurzivní server v dotazu. Značí, že autoritativní server má vrátet DNSSEC data (DNSKEY, RRSIG ...)
- AD bit (Authentic Data) nastavuje rekurzivní server v odpovědi u záznamů, u kterých ověřil podpis
- CD bit (Checking Disabled) nastavuje klient. Rekurzivní server poté neověřuje podpis záznamů

Příklad "bezpečného" DNS



Section 3

Praktické nasazení, server BIND

Klíče - KSK a ZSK

- používání pouze jednoho klíče k podepisování záznamů a jako vstupního bodu do zóny (SEP - Secure Entry Point) je nevhodné
- ZSK (Zone Signing Key) se používá k podepsání samotné zóny, kratší doba platnosti, kratší délka (3 měsíce, RSA/SHA1, 1024 bitů)
- KSK (Key Signing Key) slouží k podepisování ZSK a slouží jako SEP, příslušný DS záznam uložen v nadřazené zóně, kryptograficky silnější (platnost 1 rok, RSA/SHA1, 4096 bitů)

Generování klíčů - dnssec-keygen

- součást populárního serveru BIND

Generování ZSK

```
$ dnssec-keygen -a RSASHA1 -b 1024 -n ZONE example.com  
Kexample.com.+005+23070
```

- vygenerovány jsou dva soubory - privátní a veřejná část ZSK

Generování KSK

```
$ dnssec-keygen -a RSASHA1 -b 4096 -f KSK \  
-n ZONE example.com  
Kexample.com.+005+40132
```

- parametr "-f KSK" nastaví SEP bit
- vygenerovány jsou dva soubory - privátní a veřejná část KSK

Podepisování zóny - dnssec-signzone

- nejdříve je nutné přidat veřejnou část ZSK a KSK do zónového souboru

Přidání klíčů

```
$ cat Kexample.com.+005+23070.key >> example.com
$ cat Kexample.com.+005+40132.key >> example.com
```

- k podepisování (generování RRSIG a NSEC záznamů) se používá dnssec-signzone (součást serveru BIND)

Podepsání zóny

```
$ dnssec-signzone -o example.com -N increment example.com
example.com.signed
```

Podpisování zóny - pokračování

- podepsaná zóna je v souboru `example.com.signed`
- `example.com.signed` je abecedně seřazen a obsahuje DNSKEY, RRSIG a NSEC záznamy
- výstupní soubor je mnohem větší
- v konfiguračním souboru `named.conf` se musí změnit jméno souboru, ve kterém je zóna uložena a nastavit parametr "dnssec-enabled" (na rekurzivním serveru je nutné nastavit i "dnssec-validation")
- nakonec je nutné poslat příslušný DS záznam do nadřazené domény (nachází se v souboru `dsset-example.com.`)

Správa podepsané zóny

- platnost podepsané zóny začíná hodinu před spuštěním `dnssec-signzone`
- platnost končí 30 dnů po podepsání (pozor na TTL!), poté je nutné znovu spustit `dnssec-signzone`
- KSK a ZSK musí být periodicky měněny
- utility zjednodušující proces podepisování a správy lze nalézt na <http://www.dnssec-tools.org/>

Doporučení

- je vhodné používat "standardní" adresářovou strukturu
- zóny ukládat ve stejně pojmenovaných souborech
- podepsané zóny ukládat v .signed souborech
- ukládat všechny zónové soubory ve stejném adresáři

Trusted keys - "Důvěryhodné klíče"

- aby bylo možné ověřit záznamy v zóně je potřeba znát a mít ověřený její SEP (KSK, DNSKEY)
- pokud není DS záznam v nadřazené zóně musí se DNSKEY ověřit "ručně" a poté musí být vložen do souboru named.conf (trusted-keys)
- v ideálním případě bude pouze jeden - klíč "." zóny

”Lookaside validation”

- v současné době není podepsána kořenová doména
- správa klíčů pro všechny podepsané domény je velmi náročná
- pokud neexistuje DS záznam v nadřazené zóně, hledá se v DLV registru, pokud je nalezen, použije se
- nejznámější DLV registr spravuje ISC
(<https://secure.isc.org/ops/dlv/>)

DNSSEC v doméně cz.

- zaveden 30.09.2008
- její klíč lze autentizovat přes ISC DLV registr
- více informací na
http://podpora.nic.cz/Jak_zprovoznit_DNSSEC

Hledání chyb

- velmi užitečný nástroj je "dig"
- mezi obvyklé chyby patří
 - cílový server neodpovídá na EDNS0 dotazy
 - RRSIG záznam je "prošlý"
 - k záznamu chybí příslušný DNSKEY klíč
 - KSK nejde ověřit z nadřazené zóny (nebo DLV registru)

Cílový server neodpovídá

- server nepodporuje EDNS0
- chybně nastavený firewall nebo router

Ověření komunikace přes EDNS0

```
$ dig @<server> +edns=0 <autoritativní_záznam>
```

```
;; connection timed out; no servers could be reached
```

- pokud se nevrátí odpověď na EDNS0 packet a na DNS ano, je chyba "na cestě"

Prošlý RRSIG záznam

- obvykle pokud administrátor zapomene znovu spustit dnsssec-signzone a záznam expiruje
- `dig @<server> <autoritativní_záznam> +dnssec`

```
$ dig @ns1.example.com ns1.example.com +dnssec
```

```
;; ANSWER SECTION:
```

```
ns1.example.com. 86400 IN A 1.1.1.1
```

```
ns1.example.com. 86400 IN RRSIG A 5 3 86400  
20051120103744 ...
```

- je vidět, že RRSIG záznam již expiroval

Kontrola příslušného DNSKEY klíče

```
$ dig @ns1.example.com ns1.example.com +dnssec

;; ANSWER SECTION:
...
ns1.example.com. 86400 IN RRSIG A 5 3 86400
                20081120103744 20081021103744 23070 example.com.

$ dig @ns1.example.com example.com. dnskey +multi
...
;; ANSWER SECTION:
example.com. 86400 IN DNSKEY 256 3 5
                ( ... ) ; key id = 23071
```

- v zóně neexistuje klíč s příslušným ID

chybný DS záznam

```
$ dig @com example.com DS
```

- pokud se nevrátí žádný DS záznam (nebo záznam s chybným ID klíče) nelze autentizovat DNSKEY
- pokud používáme DLV můžeme ještě zjistit, zda není příslušný DS záznam v DLV registru

```
$ dig @<dlv.isc.org> example.com DLV
```

Section 4

Literatura

Literatura

- RFC 1033, RFC 1034, RFC 1035, RFC 2535, RFC 2671, RFC 2845, RFC 4033, RFC 4034, RFC 4035, RFC 5155
- <http://en.wikipedia.org/wiki/DNSSEC>
- http://www.isc.org/sw/bind/docs/DNSSEC_in_6_minutes.pdf