

DNSSEC

Adam Tkáč, Red Hat, Inc.

<atkac@redhat.com>

1. listopadu 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

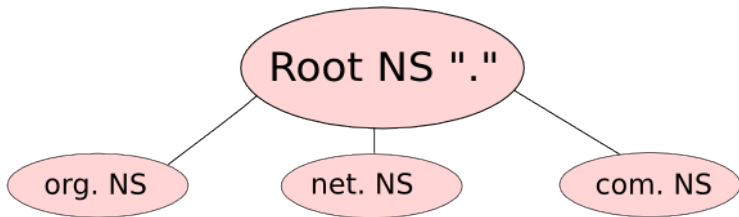
4 Zdroje

Section 1

Úvod

Co je to DNS?

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



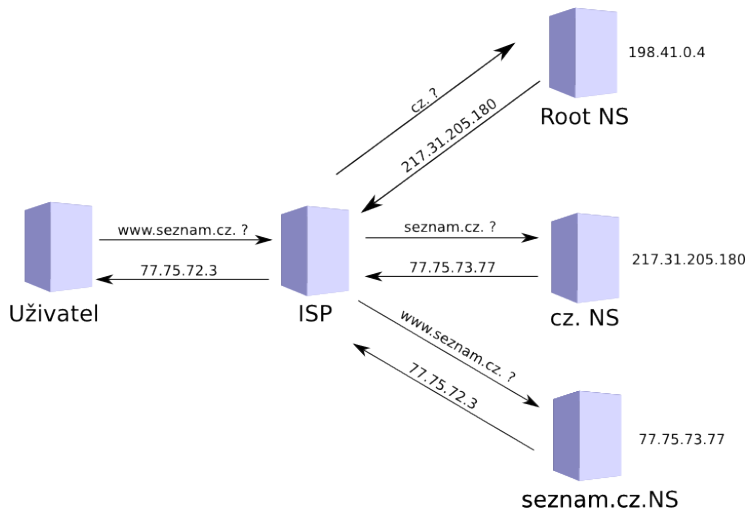
Historie

- distribuce jmen v souboru "hosts"
- základní kameny DNS v roce 1987
- TSIG, autentizace pomocí sdíleného tajemství
- současné DNSSEC v březnu 2005
- další vylepšení (NSEC3) v březnu 2008

Jak DNS pracuje

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

Příklad

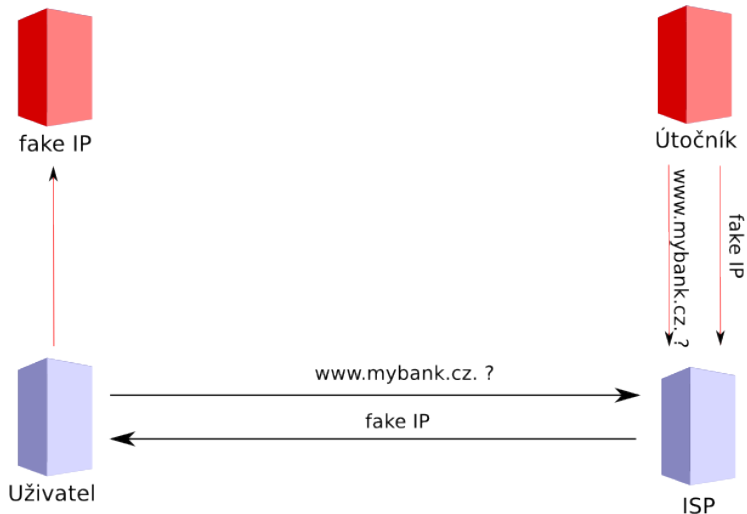


Zranitelnost

- základní problém - jak ověřit autenticitu a integritu příchozích dat
- původní návrh omezené možnosti zabezpečení (zdrojový port + transakční ID)
- mnoho implementací nepoužívá náhodné čísla
- při znalosti ID a portu lze podvrhnout odpověď
- hrubou silou lze náhodná čísla prolomit

Cache poisoning

- vložení podvržených dat do keše rekurzivního serveru



Section 2

DNSSEC

Úvod

- zajišťuje autenticitu a integritu dat
- definice v RFC 4033 - RFC 4035
- využívá asymetrickou kryptografii
- pracuje na principu řetězu důvěry
- zavádí nové typy záznamů
- odkryvá záznamy v zóně

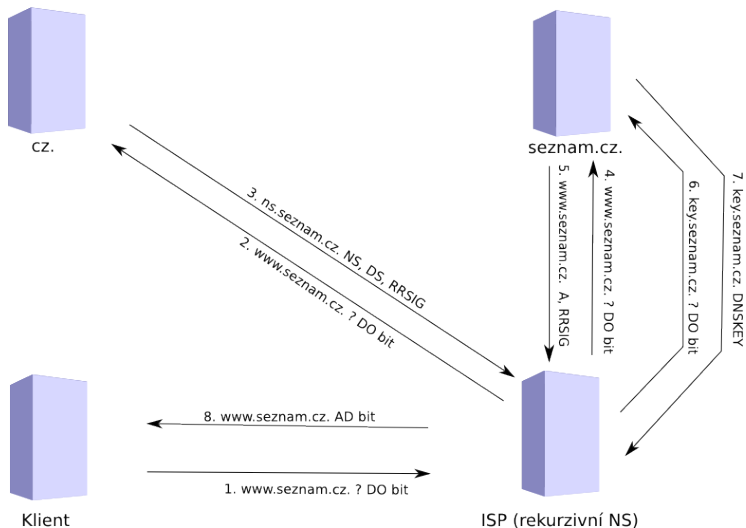
Nové typy záznamů

- DNSKEY
 - veřejný klíč, záznamy jsou podepisovány korespondujícím privátním klíčem
 - specifikuje kryptografický algoritmus, který je používán
- RRSIG (Resource Record SIGnature)
 - digitální podpis, obsahuje používaný kryptografický algoritmus, jméno klíče, kterým byl podepsán a čas uvedení a expirace podpisu
- DS (Delegation Signer)
 - vytváří řetěz důvěry mezi zónou a nadřazenou zónou
 - obsahuje otisk podpisového klíče klíčů (KSK)
 - uložen v nadřazené zóně
- NSEC (Next SECure)
 - autentizované popření existence
 - obsahuje odkaz na další autoritativní záznam v zóně
 - odkrývá všechny záznamy v zóně (zone enumeration, NSEC3)

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

- ZSK (Zone Signing Key)
 - podepsání samotné zóny
 - kryptograficky slabší (3 měsíce, RSA/SHA1, 1024 bitů)
- KSK (Key Signing Key)
 - podepisování ZSK
 - 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" značí, že jde o KSK
- vygenerovány jsou dva soubory - privátní a veřejná část KSK

Podepisování zóny - dnssec-signzone

- přidat veřejnou část ZSK a KSK do zónového souboru
- podepsat pomocí 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, obsahuje DNSKEY, RRSIG a NSEC záznamy
- podepsaná zóna mnohem větší
- v `named.conf` nastavit jméno souboru zóny, nastavit parametr "`dnssec-enable`"
- na rekurzivním serveru nastavit parametr "`dnssec-validation`"
- poslat příslušný DS záznam do nadřazené domény (nachází se v souboru `dsset-example.com.`)

Správa podepsané zóny

- platnost podpisů začíná hodinu před spuštěním `dnssec-signzone`
- platnost končí 30 dnů po podepsání (pozor na TTL!), poté znovu spustit `dnssec-signzone`
- KSK a ZSK musí být periodicky měněny
- utility zjednodušující proces podepisování a správy 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 podpisy je potřeba znát a mít ověřený jejich DNSKEY (KSK)
- 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"
- obvyklé chyby
 - 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

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

Hledání chyb - pokračování

- prošlý (expirovaný) RRSIG záznam

```
dig <záznam> +dnssec +cd
```

- chybí příslušný DNSKEY klíč

```
dig <jméno_klíče> dnskey +multi
```

- chybný DS/DLV záznam

```
dig @<ns_nadřazené_domény> <jméno_klíče> DS
```

Section 4

Zdroje

Zdroje

- RFC 4033 - DNS Security Introduction and Requirements
- RFC 4034 - Resource Records for the DNS Security Extensions
- RFC 4045 - Protocol Modifications for the DNS Security Extensions
- RFC 4641 - DNSSEC Operational Practices
- RFC 5155 - DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
- <http://en.wikipedia.org/wiki/DNSSEC>
- http://www.isc.org/sw/bind/docs/DNSSEC_in_6_minutes.pdf