DNSSEC

Martin Stanek

Katedra informatiky
FMFI UK, Bratislava
stanek@dcs.fmph.uniba.sk

2011/12

Obsah

DNS

- hierarchický, distribuovaný, decentralizovaný systém
- klient – server architektúra
- mapovanie doménových mien na IP adresy a naopak
- príklady typov záznamov (RR – resource record):

SOA	start of authority
A	address
AAAA	IPv6 address
NS	name server
MX	mail exchange
CNAME	canonical name (alias)

DNS

- DNS servery:
  - autoritatívne – pre vlastnú zónu alebo odkazy na delegované zóny
  - rekurzívne – postupne dotazujú autoritatívne servery pre zodpovedanie klientských požiadaviek
    . . . + caching – pamätanie odpovedí (efektívnosť)
- DNS klienti (resolvers)
  - v operačnom systéme, lokálna cache (aj v prehliadačoch)
- Protokol (obvykle):
  - UDP, port 53
  - bezstavový protokol (otázka – odpoveď)
  - žiadne mechanizmy na zabezpečenie dôvernosti, integrity a autentickosti

DNS – niektoré bezpečnostné problémy

- DNS spoofing / cache poisoning (klient, mail server a pod. presmerovaný na nesprávnu adresu):
  - útočník odpovie klientovi skôr ako jeho (rekurzívny) DNS server
  - útočník odpovie DNS serveru skôr ako príslušný autoritatívny DNS server
  - útočník upraví odpoveď DNS servera
  - útočník vloží do odpovede svojej zóny dodatočné informácie o inej zóne (napr. o NS), ...
- nedostatky návrhu protokolov, chyby implementácie DNS serverov (napr. zraniteľnosti v bind-e: 2010/9, 2011/6, 2012/doteraz 1)
- ďalšie problémy:
  - DNS amplification (dlhé odpovede + spoofing ... DoS)
  - DNS rebinding (obídenie same-origin politiky v prehliadačoch)
- Threat Analysis of the Domain Name System (DNS), RFC 3833

DNS – niektoré (kryptografické) riešenia problémov

- TSIG
  - Transaction Signatures (RFC 2845)
  - použitie HMAC-MD5 a zdieľaných kľúčov pre zabezpečenie autentickosti komunikácie
  - primárne pre dynamické aktulizácie DNS záznamov, pre zónové transfery a pod.
- SIG(0)
  - digitálne podpisy pre dynamické aktualizácie DNS
  - verejný kľúč súčasťou zóny
- DNSSEC
  - *naša téma . . .*

DNSEC – úvod

- Domain Name System SECurity extensions

  RFC 4033 DNS Security Introduction and Requirements
  RFC 4034 Resource Records for the DNS Security Extensions
  RFC 4035 Protocol Modifications for the DNS Security Extensions
  RFC 5011 Automated Updates of DNSSEC Trust Anchors
  RFC 5155 DNSSEC Hashed Authenticated Denial of Existence
  ...

- Základná myšlienka: digitálne podpísané záznamy DNS serverov

  . . . DNSSEC itself is concerned with object security of DNS data, not channel security of DNS transactions.

- Ciele:
  - zabezpečenie autentickosti a integrity dát
  - zabezpečenie autentickosti pri neexistencii dát

DNSSEC nezabezpečuje

- dôvernosť dát (žiadne šifrovanie)
- ochranu pred DoS útokmi
  - voči DNS serveru
  - voči klientom (DNS amplification)

Aktuálny stav

- júl 2010: podpísaná DNS root zóna
- stav k 4.4.2012 (celkovo 313 TLDs v root zóne)
  - 91 podpísaných
  - SK a okolie:

podpísaná zóna s DS v root zóne	cz., pl., at.
podpísaná zóna bez DS v root zóne	ua.
nič	sk., hu.

- com. zóna podpísaná v marci 2011
  - stav k 4.4.2012 (mizivé rozšírenie DNSSEC v doménach 2. úrovne)
  - nič: google.com, facebook.com, yahoo.com, live.com, youtube.com, ...

Kľuče a algoritmy

- Key Signing Keys (KSK)
  - podpisovanie iných kľúčov v DNSKEY záznamoch
  - potrebné publikovať DS záznam v nadradenej zóne (odtlačok verejného kľúča)
- Zone Signing Keys (ZSK)
  - podpisovanie ostatných záznamov v zóne
  - jednoduchá správa (plne v kompetencii zóny)

- najčastejšie používané algoritmy: RSA (obvykle 2048 bitov) s SHA-256 alebo SHA-1
  - schéma pre digitálne podpisy: RSASSA-PKCS1-v1.5 (PKCS #1)
  - dĺžka RSA modulu max. 4096 bitov (min. 1024 pre RSA/SHA-512)

Nové typy DNS záznamov – DNSKEY a DS

príklady sú uvádzané z root zóny
`http://www.internic.net/zones/root.zone`

- DNSKEY – verejný kľúč

```
. 172800 IN DNSKEY 256 3 8 AwEAAbd0IPTQdvy...Y6YJ
. 172800 IN DNSKEY 257 3 8 AwEAAagAIKlVZrp...hz0=
```

  - 256, 257 – príznaky (256: ZSK; 257: KSK, posledný bit označuje SEP (Secure Entry Point))
  - 3 – protokol (fixné)
  - 8 – algoritmus (RSA/SHA-256)

- DS (Delegation signer) – identifikácia KSK pre delegovanú zónu

```
GR. 86400 IN DS 57519 7 2 89AD46EAD...CF3
```

  - 57519 – key tag (pre urýchlenie výberu správneho DNSKEY záznamu)
  - 7 – algoritmus zodpovedajúci DNSKEY záznamu, ktorý odkazujeme (RSA/SHA1/NSEC3)
  - 2 – typ odtlačku (SHA-256)

Nové typy DNS záznamov – DNSKEY a DS

príklady sú uvádzané z root zóny
`http://www.internic.net/zones/root.zone`

- DNSKEY – verejný kľúč

```
. 172800 IN DNSKEY 256 3 8 AwEAAbd0IPTQdvy...Y6YJ
. 172800 IN DNSKEY 257 3 8 AwEAAagAIKlVZrp...hz0=
```

  - 256, 257 – príznaky (256: ZSK; 257: KSK, posledný bit označuje SEP (Secure Entry Point))
  - 3 – protokol (fixné)
  - 8 – algoritmus (RSA/SHA-256)
- DS (Delegation signer) – identifikácia KSK pre delegovanú zónu

```
GR. 86400 IN DS 57519 7 2 89AD46EAD...CF3
```

  - 57519 – key tag (pre urýchlenie výberu správneho DNSKEY záznamu)
  - 7 – algoritmus zodpovedajúci DNSKEY záznamu, ktorý odkazujeme (RSA/SHA1/NSEC3)
  - 2 – typ odtlačku (SHA-256)

Root zóna

- Správa KSK a ZSK pre root zónu:
  - DNSSEC Root Zone High Level Technical Architecture (Draft)
  - DNSSEC Practice Statement for the Root Zone KSK Operator
  - DNSSEC Practice Statement for the Root Zone ZSK Operator
- Publikovanie KSK
  - DNSSEC Trust Anchor Publication for the Root Zone
  - rôzne formáty (certifikát, CSR, XML, p7s, . . .)
  - prístupné cez HTTP aj HTTPS (`data.iana.org/root-anchors/`)

Nové typy DNS záznamov – RRSIG

- RRSIG – podpis množiny záznamov

```
. 518400 IN RRSIG NS 8 0 518400 20120411000000
20120403230000 56158 . RJ0ceR...8XpzA=
```

  - `. 518400 IN RRSIG` – vlastník, TTL, trieda, typ
  - NS – typy podpísaných záznamov
  - 8 – podpisový algoritmus (RSA/SHA-256)
  - 0 – počet častí mena vlastníka (podstatné pre riešenie $*$)
  - 518400 – pôvodná TTL hodnota
  - 20120411000000, 20120403230000 – platnosť podpisu (do 11.04.2012 0:00 UTC, od 3.4.2012 23:00 UTC)
  - 56158 – key tag kľúča v DNSKEY zázname pre overenie podpisu
  - . – meno podpisujúceho (vlastník v príslušnom DNSKEY zázname)
  - na záver podpis

RRSIG

- podpisuje sa množina záznamov (RRset)
  - RRset určená zhodou záznamov v trojici atribútov: vlastník, trieda, typ
- niektoré záznamy v zóne sú nepodpísané; sú to dáta delegovaných zón (nie ich nadradenej zóny)
  - NS záznamy delegovaných zón
  - A, AAAA záznamy delegovaných zón

Nové typy DNS záznamov – NSEC

- Ako odpovedať, že záznam neexistuje?
- nechceme podpisovať on-line (potrebný súkromný kľúč)
- záznamy sú utriedené (kanonické usporiadanie)
- NSEC – „next secure“ záznam

  `cz. 86400 IN NSEC de. NS DS RRSIG NSEC`

  `cz. 86400 IN RRSIG NSEC ...`
  - pre konkrétne doménové meno (`cz.`)
  - `.de` – nasledujúci vlastník (doménové meno) v súbore
  - NS DS RRSIG NSEC – typy existujúcich záznamov pre aktuálneho vlastníka/meno (`cz.`)
- posledný NSEC odkazuje opäť na začiatok (nasl. vlastník)
- pre každý NSEC záznam existuje zodpovedajúci RRSIG záznam

Neexistujúce záznamy – typy

- NXDOMAIN (neexistujúce doménové meno, napr. `da.`)

```
$dig da. @8.8.8.8
...
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 4649
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ...
```

- NOERROR/0 (prázdna odpoveď, meno existuje ale nie záznam s daným typom)

```
$dig sk-nic.sk. A @8.8.8.8 +short
195.12.159.5
$dig sk-nic.sk. AAAA @8.8.8.8 +short
$
```

Odpovede o neexistencii využívajúce NSEC

- NXDOMAIN: v odpovedi v authority sekcii (o.i.) dostaneme NSEC záznam (aj s príslušným RRSIG), z ktorého je jasné chýbajúce doménové meno:

  `cz. 10574 IN NSEC de. NS DS RRSIG NSEC`

  - žiadne meno medzi `cz.` a `de.`
- NOERROR/0: v odpovedi v authority sekcii (o.i.) dostaneme NSEC záznam (aj s príslušným RRSIG), z ktorého je jasný chýbajúci typ pre doménové meno:

```
$dig @149.20.64.20 sk. DS +dnssec
...
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7087
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ...
...
sk.       7540    IN       NSEC     sl. NS RRSIG NSEC
...
```

NSEC vs. NSEC3

- zone walking (enumerácia doménových mien)
- neexistencia mena (NSDOMAIN) prezradí susedov „nad“ a „pod“
- možnosť enumerovať zónu ($\sim$ transfer zóny cez NSEC)
  - počet otázok cca. lineárny od počtu záznamov
- problém pre nasadenie DNSSEC . . . riešenie NSEC3

NSEC3

- náhrada NSEC záznamov; doménové mená nahradené odtlačkami

```
dig @149.20.64.20 p.bund.de A +dnssec
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38332
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ...
...
EDE5...79LN.bund.de. 10800 IN NSEC3 1 0 10 DDD087
                            EEPT...CS3K A RRSIG
```

- zreťazenie usporiadné podľa hodnoty odtlačku
- resolver vypočíta odtlačok mena a zistí, že hodnota je medzi odtlačkami v NSEC3 zázname (v praxi aj ďalšie NSEC3 záznamy a zodpovedajúce RRSIG)

NSEC3 (2)

- NSEC3 parametre

```
EDE5...79LN.bund.de. 10800 IN NSEC3 1 0 10 DDD087
                                EEPT...CS3K A RRSIG
```

  - 1 – hašovací algoritmus (SHA-1)
  - 0 – príznaky (bez opt-out)
  - 10 – počet iterácií pri výpočte odtlačku
  - `DDD087` – soľ
  - odtlačok ďalšieho mena, typy záznamov pre aktuálneho vlastníka
- off-line útok na odtlačky (priestor doménových mien nie je veľký)

Rozdiely oproti PKI

- bez certifikátov
- kľúče nemajú interval platnosti (podpisy majú)
- správa kľúčov v kompetencii príslušnej zóny
- dôvera vo verejný kľúč
  - dôvera v KSK root zóny (statický import) $\rightarrow$ ZSK (.) $\rightarrow$ DS (v . pre de.) $\rightarrow$ KSK (de.) $\rightarrow$ ZSK (de.) $\rightarrow$ DS (v de. pre .bund.de.) $\rightarrow$ KSK (bund.de.) $\rightarrow$ ZSK (*bund.de*) ... a následne môžeme overiť RRSIG pre záznam typu A pre doménové meno `www.bund.de`
  - samozrejme: ... + caching