DNSSEC

Bohuslav Moučka, Radim Peša,
ÚVT MU

Jednou z klíčových součástí dnešní internetové infrastruktury je systém doménových jmen (DNS – Domain Name System). Jde o hierarchickou databázi umožňující vzájemný převod textových jmen uzlů počítačové sítě a číselných IP adres.

DNS pro překlad adres používají prakticky všechny internetové služby. O to víc zarážející je fakt, že dodnes používaný systém DNS postrádá jakékoli bezpečnostní mechanismy. Uživatel DNS nemá možnost si ověřit pravdivost nebo původ získaných informací, protože protokol neobsahuje mechanismus pro kontrolu přenášených dat.

Bylo již popsáno několik způsobů útoku (např. v [1]) na důvěryhodnost dat poskytovaných systémem DNS. Použité techniky se různí, ale ve výsledku získává klient podvržené údaje. Například když chce klient přistoupit www prohlížečem na stránky svého oblíbeného internetového bankovnictví www.nejakabanka.cz, musí dojit k převodu jména `www.nejakabanka.cz` na příslušnou IP adresu. To zprostředkovává dotazem na přednastavený DNS server DNS klient v operačním systému. Na dotaz odpoví buď přímo předdefinovaný a dotazovaný DNS server nebo pokud odpověď nezná, dotazuje se dalších DNS serverů v DNS infrastruktuře. Jak již bylo řečeno, současný způsob DNS komunikace nenabízí prostředky, které by umožnily ověřit, zda výsledně získaná IP adresa opravdu přísluší původně dotazovanému DNS jménu. Pokud někde v infrastruktuře DNS serverů dojde k úspěšnému podvržení IP adresy internetového bankovnictví `www.nejakabanka.cz` nemá ani předávající DNS server a ani DNS klient žádnou možnost ověřit si, zda je IP adresa, kterou obdržel, správná. Internetový prohlížeč následně může být přesměrován například na počítač útočníka, kde může probíhat další etapa útoku třeba v podobě pokusu o sběr hesel, zneužití chyby v internetovém prohlížeči atd.

Jako příklad úspěšného útoku na DNS je možné uvést mediálně známý případ podvržení DNS údajů, kdy v roce 1997 využil Eugene Kashpureff chybu v DNS serverech k přesměrování stránek registrátora InterNIC na svůj server AlterNIC.

1 Přichází DNSSEC

Jako obrana proti možnému podvržení dat poskytovaných DNS infrastrukturou bylo po řadu let vyvíjeno rozšíření DNS pojmenované DNSSEC (*Domain Name System Security Extensions*). Jeho příprava nebyla jednoduchá, za počátek vývoje se dá považovat RFC 2065 vydané už v roce 1997. Tato původní představa byla dále upravována a rozpracována a v roce 1999 vychází RFC 2535, které již mělo být základem pro funkční implementaci a nasazení DNSSEC v systému DNS. Bohužel specifikace se ukázala jako neživotaschopná, především kvůli problémům se škálovatelností. Proto byla v následujících letech připravena výrazně změněná specifikace. Pro odlišení od předchozí verze byla označována jako DNSSEC-bis. Její vývoj byl v roce 2005 završen standardizací v podobě dokumentů RFC 4033, RFC 4034 a RFC 4035. Ani specifikace DNSSEC-bis však nebyla dokonalá. Je pikantní, že přestože se jedná o protokol definovaný primárně pro zvýšení bezpečnosti, přinesl novou bezpečnostní zranitelnost v podobě možnosti vylistování celého doménového prostoru (zone-walking). Tento problém byl vyřešen v roce 2008 vydáním RFC 5155, které definuje nový druh záznamu pojmenovaný NSEC3.

Vzhledem k popsané historii vývoje specifikace protokolu DNSSEC není velkým překvapením, že používání protokolu DNSSEC není ani dnes zdaleka standardem. Možná se ale blýská na lepší časy. Ke zrychlení šnečího tempa šíření DNESSEC technologie by mohlo výrazně přispět podepsání kořenové domény, ke kterému došlo 15. července 2010. Podepsání kořenové domény výrazně zjednodušuje řešení problémů s údržbou pevných bodů důvěry a vytváření řetězu důvěry (viz dále). Věřme, že spolu s vyřešením dětských nemocí předchozích verzí specifikace se podpis kořenové domény stane akcelerátorem reálného využití DNSSECu.

2 Jak DNSSEC funguje?

DNSSEC zajišťuje kontrolu původu a pravosti dat, ale jeho cílem není zajištění důvěrnosti dat

(přenášená data nejsou šifrována) a ani přímo nechrání před útoky na dostupnost služby. Pro zajištění kontroly integrity přenášených informací využívá DNSSEC nástroje asymetrické kryptografie. Zjednodušeně řečeno je vlastně každý DNS záznam podepsán a autenticitu záznamu je možné zjistit ověřením příslušného podpisu. Samotná realizace je však komplikovanější. Mimo jiné přibylo několik nových typů DNS záznamů:

- RRSIG (Resource Record Signature) – obsahuje digitální podpis příslušné množiny DNS záznamů.
- DNSKEY (DNSSEC public key) – obsahuje veřejný klíč, jehož odpovídajícím privátním klíčem jsou podepsány DNS záznamy této domény.
- DS (Delegation Signer) – je umístěn v nadřazené DNS doméně a obsahuje otisk veřejného klíče uloženého v DNSKEY záznamu podepsané domény. Pomocí DS záznamů se vytváří řetěz důvěry do nadřazených domén.
- NSEC (Next Secure) – využívá se pro informaci o neexistenci dotazovaného záznamu.
- NSEC3 (Next Secure v.3) – využívá se pro informaci o neexistenci dotazovaného záznamu. Na rozdíl od NSEC záznamu neobsahuje jména, ale jen jejich otisky.

Do hlaviček DNS zpráv byly zavedeny nové příznaky:

- AD (Authenticated Data) – indikuje, že všechna data v sekcích odpověď a autorita byla ověřena a jsou správná.
- DO (DNSSEC OK) – v dotazu určuje, že server požaduje validaci dat pomocí DNSSEC.
- CD (Checking Disabled) – určuje, že server má vrátit data, i když validace nebyla úspěšná.

Pro ověření libovolného digitálního podpisu je nezbytné znát z důvěryhodného zdroje veřejný klíč podepisující entity. V případě DNS je samozřejmě nereálné, aby dotazující se klient (případně ověřující DNS server) znal veřejné klíče všech DNS domén, se kterými komunikuje. Proto DNSSEC používá systém pevných bodů důvěry a řetězu důvěry. DNS klient zná veřejné klíče pouze několika vybraných DNS domén – pevných bodů důvěry. Veřejné klíče jejich poddomén může získat zřetězením otisků klíčů z DS záznamů jednotlivých poddomén, které jsou uloženy v podepsané doméně, a příslušných veřejných klíčů jednotlivých poddomén obsažených v jejich DNSKEY záznamech. Tímto zřetězením DS a DNSKEY záznamů vzniká tzv. *řetěz důvěry*, který umožňuje DNS klientu získat důvěryhodným způsobem veřejné klíče libovolné podepsané poddomény. Letošní podpis kořenové domény umožní využít tuto doménu jako nejvyšší pevný bod důvěry a ulehčí DNS serverům, protože si nebudou muset udržovat seznam různých bodů důvěry. Klíč kořenové domény je publikován na serveru `www.iana.org`.

3 Ověřování (validace) DNS záznamů

Ověřování (validace) DNS záznamů se obvykle provádí na úrovni tzv. rekurzního DNS serveru, který dostává dotaz od DNS klienta a zajišťuje veškerou komunikaci s ostatními DNS servery. Na klienta se vrací až výsledek dotazu.

Rekurzivní DNS server si při DNSSEC validaci nejprve ověří pravost DS a DNSKEY záznamů v kořenové doméně pomocí veřejného klíče kořenové domény, který má zapsán ve své konfiguraci. V následujících krocích dostane vždy kromě IP adres autoritativních DNS serverů také DS záznam podřízené domény a pomocí něj si ověří DNSKEY záznam v podřízené doméně. V posledním kroku získá kromě původně hledaného DNS záznamu také RRSIG záznam, kterým ověří původně hledaný záznam. Pokud je vše v pořádku, rekurzivní server v DNS zprávě pro dotazujícího se klienta nastaví příznak AD (Authenticated Data), v opačném případě se zpráva vrátí s příznakem SERVFAIL a klient špatnou odpověď vůbec nedostane. Jestliže dotazovaná doména DNSSEC nepodporuje, server nedostane žádné DS, DNSKEY ani RRSIG záznamy z této domény a vrací obvyklou DNS odpověď, která není ověřena pomocí DNSSEC.

Pokud chceme, aby náš DNS server ověřoval záznamy z cizích domén, musíme na něm mít zapnutou validaci. Server BIND verze 9.5 a vyšší má validaci implicitně zapnutou. Aby server mohl ověřovat pravost záznamů, musí mít k dispozici klíč kořenové domény. Ten zapíšeme do konfiguračního souboru serveru verze BIND-9.6 příkazem:

```
trusted-keys {
. 257 3 8
"AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQb
SEWOO8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RS
tIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9Vn
MVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6CXpoY68Lsv
PVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA
2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ5
7relSQageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1d
fwhYB4N7knNnulqQxA+Uk1ihz0=";
}
```

V případě verze BIND-9.7 můžeme použít příkaz, který zajistí automatickou aktualizaci klíče, bude-li změněn:

```
managed-keys {
"." initial-key 257 3 8
"AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQb
SEWOO8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RS
tIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9Vn
MVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6CXpoY68Lsv
PVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA
2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ5
7relSQageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1d
fwhYB4N7knNnulqQxA+Uk1ihz0=";
};
```

4 Podpis DNS zóny

Majitel domény, která má být zabezpečena, vygeneruje privátní a veřejný klíč. Privátním klíčem podepíše záznamy uložené v DNS a musí jej chránit před zneužitím, veřejný klíč slouží k ověření pravosti těchto podpisů. Je doporučeno pro každou doménu vygenerovat 2 dvojice klíčů. Klíč ZSK (Zone Signing Key) podepisuje jednotlivé záznamy v doméně, je kryptograficky slabší a bývá častěji měněn. Klíč KSK (Key Signing Key) by měl být kryptograficky silnější a slouží k podpisu záznamů obsahujících ZSK. Při použití serveru BIND můžeme klíče vygenerovat například pro doménu muni.cz příkazy:

```
dnssec-keygen -a NSEC3RSASHA1 -b 1024 \
     -r /dev/urandom -f KSK muni.cz

dnssec-keygen -a NSEC3RSASHA1 -b 1024 \
     -r /dev/urandom  muni.cz
```

Oba příkazy vygenerují dva soubory, v souboru s příponou .key je veřejný klíč ve tvaru DNSKEY záznamu a v souboru s příponou .private je soukromý klíč.Veřejné klíče je třeba přidat do zónového souboru domény, kterou podepisujeme. Potom můžeme doménu podepsat příkazem:

```
dnssec-signzone muni.cz
```

Po spuštění tohoto příkazu vznikne nový soubor `muni.cz.signed`, který bude kromě původních informací obsahovat záznamy RRSIG a NSEC3. Záznamy typu RRSIG jsou přidány za každý RRSet, což je skupina záznamů stejného názvu a typu a slouží ke kontrole pravosti předchozích záznamů. Záznam obsahuje také data začátku a konce platnosti podpisu, která můžeme zadat při podpisu domény. Záznam NSEC3 obsahuje informaci o následujícím záznamu v setříděné doméně a informaci o všech existujících typech tohoto záznamu. Pokud se dotážeme na neexistující jméno, vrací DNS server NSEC3 záznam, který je před a za dotazovaným jménem. Záznamy NSEC3 neobsahují jména, ale jen otisky, takže je nelze použít ke získání seznamu všech záznamů v doméně, což je považováno za bezpečnostní problém. Při podpisu domény vznikne také soubor s názvem dsset-muni.cz obsahující DS záznamy, které je třeba umístit do nadřazené domény (cz). V souboru keyset-muni.cz je zapsán KSK klíč, který byl použit pro podpis domény. Tyto dva soubory jsou ekvivalentní v tom smyslu, že DS záznam se vypočítává z klíče a názvu domény. DS záznamy je možné umístit do domény cz prostřednictvím registrátora (pokud podporuje DNSSEC), kterému předáme KSK klíč.Vzhledem k tomu, že kořenová doména je již podepsána a klíč domény cz je v ní zaregistrován, vznikl tak řetěz důvěry. Pokud všechny sekundární DNS servery naší domény podporují DNSSEC, mohou všechny DNS servery, které jsou nakonfigurovány tak, že validují DNSSEC záznamy, ověřovat platnost záznamů z naší domény.

5 DNSSEC na MU

Doména muni.cz byla v návaznosti na podpis kořenové domény a domény .cz podepsána v srpnu 2010. V listopadu byla experimentálně zapnuta validace DNSSECu na serverech `ns.muni.cz` a `ns1.muni.cz`. Během dvou dnů však servery nahlásily chyby při validaci záznamů u 258 domén, z toho 88 v doméně cz. V mnoha případech existuje pro danou doménu DS záznam v nadřazené doméně, ale doména není podepsaná. Tento stav

vede k tomu, že validující DNS server dostane informaci, že doména je podepsaná, ale podpis jejích záznamů není možné ověřit a vrací chybu. Následkem toho se záznamy v těchto doménách jeví jako nedostupné. Vzhledem k možnému dopadu na uživatele byla validace na těchto serverech pozastavena. Věřme, že ne na dlouho.

Literatura

[1] Suranjith Ariyapperuma, Chris J. Mitchell. *ARES '07 Proceedings of the Second International Conference on Availability, Reliability and Security*. ISBN:0-7695-2775-2 □