Historie a principy DNSSEC

V roce 1990 byl internet stále místem, kde jeho uživatelé žili v klidu, míru a vzájemné harmonii. Nebo ne? V tom samém roce přichází Steven M. Bellovin na zásadní chybu při používání DNS. Vzájemná důvěra mezi počítači byla v té době většinou řešena pouze na základě správného doménového jména v DNS a útočník, který mohl měnit DNS záznamy, snadno získal přístup na vzdálené servery.

ONDŘEJ SURÝ

V zásadě se nejedná o chybu samotného DNS, ale o chybu přílišné důvěry v systém DNS. Publikace této práce byla odložena z bezpečnostních důvodů o celé čtyři roky, ale jak sám autor poznamenává, nebylo to příliš moudré rozhodnutí, protože informace stejně prosákly na veřejnost a byly zaznamenány útoky, které tento nadbytek důvěry v doménový systém využívaly.

Po zveřejnění tohoto nedostatku se na půdě IETF, což je organizace, která stojí za většinou standardů používaných na internetu, začíná uvažovat nad zabezpečením systému DNS.

Mezitím Eugene Kashpureff objevuje další zranitelnost v současných implementacích DNS serverů (tedy v té době především serveru Bind), která umožňuje v DNS podvrhnout libovolný záznam pomocí sekce „Další“. V roce 1997 pak používá tuto chybu k celosvětovému nebo spíše celointernetovému přesměrování stránek registrátora InterNIC na stránky své firmy AlterNIC.

Jako ochrana proti tomuto typu útoku byl vymyšlen systém správních oblastí (bailiwick), který definuje, jaké DNS záznamy budou v sekci „Další“ akceptovány. Následujícím krokem ještě v témže roce je první dokument popisující kryptografické zabezpečení systému DNS – RFC 2065.

Tento dokument je pak během dvou dalších let rozpracován a v roce 1999 je v RFC 2535 publikována první verze systému DNSSEC. DNSSEC do systému DNS přidává nové záznamy, které kryptograficky zajišťují integritu dat poskytovanou DNS servery.

První implementace DNSSEC podle specifikací RFC 2535 je připravena v DNS serveru Bind, bohužel další dva roky nasazení DNSSEC stagnuje a v roce 2001 je vypracována studie, která konstatuje, že tato první verze systému DNSSEC je nevhodná k nasazení, protože libovolná výměna podepisovacího klíče vyžaduje komplexní komunikaci s nadřazeným DNS serverem, tato změna se ale musí promítnout na všech podřízených DNS serverech.

Tyto požadavky první verzi DNSSEC odsunuly na vedlejší kolej a začíná se pracovat na verzi nové, pracovně nazývané DNSSECbis. DNSSECbis definuje úplně nové záznamy, které nejsou kompatibilní s původní verzí DNSSEC, a rozšiřuje DNS o nový druh záznamu – DS, který má výrazně zjednodušit komunikaci s nadřazeným serverem.

V průběhu let 2002 až 2003 je tato nová verze DNSSEC implementována v DNS serveru Bind a ukazuje se, že je na rozdíl od své předchůdkyně životaschopná. V roce 2004 je podpora DNSSECbis implementována ve dvou nezávislých DNS serverech (Bind a NSD 2.x) a čeká se jen na standardizaci. Ta proběhne až v roce 2005, kdy jsou v březnu vydány dokumenty RFC 4033, RFC 4044 a RFC 4035.

V říjnu 2005, tedy jen o pár měsíců později, implementuje DNSSEC první TLD doména – švédská .se. V září 2008 se jako pátá na světě do exkluzivního klubu podepsaných domén přidává i česká TLD .cz.

Ani DNSSECbis se ovšem neobešel bez problémů. V návrhu protokolu se počítá s tím, že je zapotřebí mít i kryptograficky ověřené odpovědi o neexistenci záznamů. DNSSEC podepisuje DNS záznamy a odpověď o neexistenci doménového jména je standardně realizována nastavením návratového kódu RCODE na hodnotu NXDOMAIN.

Z tohoto důvodu vznikl DNS záznam NSEC, který pro určité doménové jméno říká, jaký záznam jej abecedně následuje. V případě dotazu na neexistující záznam DNS server vrátí jména, která jsou „okolo“, a tato odpověď již může být kryptograficky podepsána.

Tento princip ovšem otevírá jeden nepříjemný důsledek – takto se dá projít celý doménový prostor, jedná se o tzv. zone walk. Návrh řešení existuje v dokumentu RFC 5155, který definuje nový druh záznamu NSEC3, kde je informace o dalším záznamu ukryta pomocí hashovacího algoritmu.

Další zajímavá vlastnost NSEC3 je tzv. Opt-Out, který specifikuje mechanizmus, kdy po přidání nezabezpečené delegace není nutné přepočítávat (a znovu podepsat) celý řetěz NSEC3 záznamů, což zjednodušuje náročnost správy především u velkých domén.

Dnes se píše rok 2011 a pomocí systému DNSSEC již není chráněno pouze pět národních domén: .se, .bg, .pr, .br a .cz, ale také kořenová doména, která byla podepsána v létě 2010, několik velkých TLD, jako jsou .de, .com, .org či .net a také zóna s reverzními záznamy .arpa.

Přehledovou tabulku lze nalézt například na Wikipedii: *en.wikipedia.org/wiki/List_of_Internet_top-level_domains*.

Praktická hlediska DNSSEC

DNSSEC představuje technologii, která rozšiřuje DNS protokol o nové typy RR záznamů a příznaky v DNS zprávě, a pomocí těchto nových typů lze následně ověřit pravost informací, které obsahuje DNS odpověď.

Dnes již klasickým způsobem, jak ověřit pravost informací, je digitální podpis. Každý z nás se s ním v nějaké formě na internetu již setkal, ať už se jednalo o přístup na zabezpečené stránky přes HTTPS, digitální podpis v e-mailu přes X.509 certifikáty nebo OpenPGP. DNSSEC přináší stejný mechanizmus digitálních podpisů do světa DNS.

DNSSEC klíč

Základním DNS záznamem, o který DNSSEC rozšířil protokol DNS, je DNSKEY. Může vypadat například takto:

```
dnssec.cz.   3600 IN   DNSKEY 256 3 5 (
             BQEAAAABtXA40o93iyv96bqSV0aYylb8Z/P1xn9wr4E6
             5N0+Y4SjW6Z2MYTnVY5zyApwx81N4uIg3CB0bvx4ITDx
             fu/Uny3ssEV8lnfC3xzy8pAJ4BNZZrS6cHI5dCtTABel
             LxZdJJ/x7kmCKhsaDIrLli8LE0gRssF+14+jJ8E0vAjK
             Rgs=
             ) ; key id = 55673
```

RDATA záznamu DNSKEY obsahují příznaky klíče (257), typ protokolu (3 = DNSSEC), použitý algoritmus (5 = RSASHA1) a data veřejné části klíče (BQE…). Z DNSKEY klíče se dá získat ještě je-