Implementace DNSSEC v CZ.NIC, z.s.p.o.

Úvod

Provoz doménových jmenných serverů v prostředí internetu s sebou v dnešní době přináší různá rizika. Na správném a bezchybném provozu doménového jména závisí mnoho firem a jednotlivců včetně těch, kteří žádné doménové jméno nevlastní. Prostřednictvím internetu probíhá mnoho finančních, obchodních i jinak citlivých transakcí. Nezřídka se objevují případy útoků na internetové bankovnictví a již byly zaznamenány i případy, které byly specificky cíleny na české internetové prostředí.

V případě ochrany před podvržením obsahu webových stránek je používán protokol SSL, který používá certifikáty vydávané certifikačními autoritami. Certifikační autority vydávající certifikáty mají striktní pravidla, která mají za cíl minimalizovat možnost podvrhu důvěryhodnosti, ale již byly zaznamenány i případy, kdy byl certifikát organizace vydán osobě, která neměla s touto konkrétní organizací nic společného (InfoWorld, 2001). Celé toto řešení však trpí jedním zásadním nešvarem. Poslední krok ověření důvěryhodnosti zůstává na koncovém uživateli a je běžné, že uživatelé mají tendenci odkliknout libovolné okno, které jim webový prohlížeč ukáže a to včetně dialogového okna, které oznamuje nedůvěryhodnost certifikátu. Také je vcelku běžné, že společnosti nedbají na řádné obnovení certifikátu a stránky jsou „zabezpečené“ certifikátem, který již není platný. Protokol SSL dnes tedy spíše zabezpečuje komunikaci proti odposlechnutí třetí osobou, a zajištění autenticity je funkce, kterou je nutné přesunout do oblasti, kde ji nemůže ovlivnit koncový uživatel.

Samotný protokol DNS a jeho implementace neobsahuje žádný způsob ověření důvěryhodnosti zdroje získaných informací. Podrobnější popis možných útoků na DNS popisuje Atkins a Austein v dokumentu Threat Analysis of the Domain Name System (2004). Na půdě organizace IETF, která se zabývá návrhy a rozšiřováním internetových protokolů a technologií, vzniklo rozšíření DNSSEC, které problematiku důvěryhodnosti obsahu DNS zóny řeší.

Typy útoků na DNS infrastrukturu

Sledování paketů

Mezi tyto typy útoků spadá např. známý man-in-the-middle útok. Tento druh útoku je závislý na tom, že útočník má přístup k některému z bodů internetové infrastruktury, kudy prochází DNS paket. Je pak schopný pozměnit DNS dotaz nebo DNS odpověď, aby dosáhl určitého cíle. Tento typ útoků není specifický pro DNS, ale struktura DNS provozu (jeden paket, UDP provoz) dělá DNS ideálním cíl takovýchto útoků. Proti tomuto druhu útoku lze DNS chránit pomocí technologie DNSSEC.

Odhadování ID a predikce dotazů

Provedení tohoto útoku je složitější, protože útočník nemá přímý přístup k sítím, kde probíhá DNS provoz cíle útoku. Útok je proveden za pomoci odhadnutí DNS provozu (nebo prostou hrubou silou) a na cíl útoku útočník posílá podvrhnuté DNS pakety, které jsou vytvořeny na základě odhadu chování cíle útoku. Proti tomuto druhu útoku lze DNS chránit pomocí technologie DNSSEC.

Zřetězení jmen

Tento útok patří do skupiny útoků, které se obecně označují jako „otrávení vyrovnávací paměti“ („cache-poisoning“). Obecně se tento útok dá popsat jako vložení nesprávných údajů do vyrovnávací paměti

rekurzivního serveru za pomoci additional sekce v DNS odpovědi. Toto vložení je vcelku jednoduché vyvolat např. pomocí obrázku v emailu nebo ve webové stránce. DNSSEC by měl poskytovat ochranu proti velké většině těchto útoků. Důkladnější popis lze najít v RFC 3833.

Napadení serveru

Tento druh útoků je podobný útoku „Sledování paketů". Rozdíl je v tom, že útočník nenapadne síťovou infrastrukturu, ale přímo server, který uživatel používá pro DNS dotazy (např. server, který dostane pomocí protokolu DHCP při připojení v cizí síti – typicky bezdrátové). Obrana proti tomuto útoku zahrnuje: 1) použití vlastního důvěryhodného serveru, 2) kontrola DNSSECu přímo na straně klienta společně se znalostí důvěryhodného klíče (root zóny).

DNSSEC

Jako odpověď na zmiňované problémy bylo navrženo rozšíření DNS: protokol DNSSEC. Tento protokol by měl poskytovat ochranu proti velké většině těchto útoků. Od své první specifikace z ledna 1997 (RFC2065) byl protokol mnohokrát upravován. Současná podoba popsaná dokumenty RFC 4033/4034/4035 je stabilní a byla implementována v několika registrech domén nejvyšší úrovně.

DNSSEC přidává silné bezpečnostní mechanismy, které zaručují integritu a autenticitu DNS odpovědí. Celý mechanismus pracuje na principu digitálních podpisů. DNSSEC je jakousi přídavnou vrstvou nad protokolem DNS. Přidání DNSEC je zpětně kompatibilní s běžným DNS, to znamená, že implementace DNSEC na straně serverů nevyžaduje změny u klientů, resolverů, pokud uživatel DNS nevyžaduje vyšší stupeň bezpečnosti.

Bezpečnostní hierarchie je postavena zcela analogicky jako je u protokolu DNS běžné. Resolver podporující DNSSEC pracuje stejně jako běžný rekurzivní resolver a získává informace od vyšších úrovní DNS k nižším. Analogicky jako rekurzivní resolver zná kořenové DNS servery, v DNSSEC musí být v resolveru uložena informace o vrcholu bezpečnostní hierarchie (trust anchor), veřejná část klíče nejvyšší podepsané zóny. Z této nejvyšší zóny získává resolver informace pro ověření dat (veřejné části klíčů) nižších zón (záznam DS – delegation signer) a tak postupuje rekurzivně dále až ke koncovým bodům hierarchie[1]. Aby byl řetězec kompletní, musí správce příslušné domény předat správci nadřazené úrovně veřejnou část svého klíče, obdobně jako když jej informuje o nameserverech a glue. Rozdílné je, že platnost klíčů je časově omezena a správce podepsané domény tedy musí mít mechanismus, jak klíče v čase rotovat.

DNSSEC zabezpečuje nejen odpovědi na existující doménová jména v systému DNS, ale je schopen zabezpečit i negativní odpovědi. Obsah podepsané zóny je vždy abecedně seřazen a odpověď na dotaz na neexistující prvek obsahuje odkaz na nejblíže vyšší a nejblíže nižší prvek této posloupnosti. Tímto mechanismem má resolver jistotu, že i negativní odpověď je autentická. Nevýhodou tohoto přístupu je, že je možné vypsat obsah celého zónového souboru (takzvaný zonewalking).

DNSSEC v kořenové zóně

1 Ve skutečnosti je proces trochu složitější. Zveřejněn je klíč (či klíče), který má větší bitovou délku a slouží pouze k podepisování jiných bitově kratších klíčů. Zóna je pak podepsána některým z kratších klíčů. Delší klíč se nazývá KSK – key signing key a má časově delší platnost. Kratší klíče se používají kratší dobu a nazývají se ZKS – zone signing keys.

Ačkoliv správci TLD domén začali implementovat protokol DNSSEC (.se, .pr, .bg, .br) a mnoho dalších na implementaci pracuje, v současném okamžiku není podepsána kořenová zóna. Díky tomu nemá DNSSEC hierarchie jeden vrchol, ale vrcholů několik. To klade zvýšené nároky na správce rekurzivních DNSSEC resolverů, protože by měli sledovat změny klíčů u všech vrcholů.

Bohužel harmonogram podpisu kořenové zóny zatím nebyl stanoven. Tato záležitost je mnohými zúčastněnými stranami v organizaci ICANN vnímána jako vysoce politická a obávají se, že by podpisem jen vzrostl vliv amerických firem a americké vlády na provoz Internetu. Jiní se naopak obávají o provozní zajištění samotného podepisování. V rámci ICANN se tedy neustále řeší, zda-li, kdo, kdy a jak kořenovou zónu podepíše.

K DNSSEC na kořenové úrovni se v současné době vypracovává celá řada materiálů a dokumentů. CZ.NIC se účastní především aktivit ccNSO a to v techwg (DNSSEC @ root level) a IANAwg (DNSSEC briefing and root zone signing).

Alternativa – DLV

Pro zjednodušení konfigurace rekurzivních resolverů byla vyvinuta technologie, která částečně obchází nutnost podepisovat kořenovou zónu. Tato technologie je nazývá DLV – DNSSEC Lookaside Validation. Jejím principem je vytvoření bezpečného úložiště klíčů všech vrcholů DNSEC hierarchie. Tímto de facto vzniká nový a jediný vrchol bez nutnosti podepisování kořenové zóny. Stačí nakonfigurovat resolver, aby jako se v prvním kroku svého ověřování pokusil získat klíč příslušné zóny v tomto úložišti. Problémem je, kdo bude důvěryhodná organizace, která toto úložiště bude spravovat. Problém je tedy vlastně velmi podobný podpisu kořenové zóny s tím rozdílem, že takových úložišť může existovat více.

Problémy DNSSEC

DNSSEC je komplexní technologie a přináší do DNS také některé problémy:

- složitost implementace z důvodů komplexity protokolu
- zvětšení velikosti DNS paketů, zvýšení provozu, atd.
- zpomalení času odpovědi z důvodů validace odpovědi, vypršení času na odpověď
- absence podpisu kořenové zóny
- výměna klíčů v nejvyšší zóně je složitá operace
- požadavek na časovou synchronizaci klientů, DNSSEC záznamy obsahují absolutní časovou značku
- zonewalking

Implementace DNSSEC

Implementace technologie DNSSEC pro centrální registr domény .cz bude znamenat několik důležitých změn. Bude zapotřebí rozšířit datový model centrálního registru o nový objekt KEYSET neboli sada DS (Delegation Signer) záznamů, dále obohatit EPP protokol o funkce na práci s KEYSETy, upravit rozhraní pro veřejnost tak, aby zobrazovalo informaci o novém objektu a v neposlední řadě bude nutné zajistit procesy spojené s vlastním podepisováním vygenerovaného zónového souboru. V důsledku provedených změn a důležitosti správné funkce podepsané zóny budou také rozšířeny technické testy o nový test

s vysokou prioritou, který bude kontrolovat validitu podepsané zóny, která odpovídá doménovému jménu v centrálním registru.

Návrh datové struktury KEYSET

Návrh samostatného objektu v centrálním registru vychází z principů, které stojí za procesy při podepisování zóny. V průběhu návrhu byly zvažovány následující varianty:

1. Umístění DS záznamů v objektu doménového jména
2. Umístění DS záznamů v objektu sady jmenných serverů – NSSET
3. Samostatný objekt KEYSET

Podepsání zónového souboru není proces, který by nutně souvisel s administrativním procesy spojenými s doménovým jménem. Spíše naopak - podepsání zónového souboru budou mít většinou na starosti techničtí správci konkrétního doménového jména. Proto je varianta umístění DS záznamů přímo u doménového jména špatnou variantou.

Nabízí se tedy myšlenka spojení KEYSETu a NSSETu. Takové spojení by ovšem zrušilo hlavní výhodu, která s příchodem NSSETu nastala - pravidlo, kdy v optimálním stavu bude pro každého technického správce a jeho jmenné servery pouze jeden NSSET - protože nemůžeme předpokládat, že všechny domény provozované na stejných jmenných serverech budou mít stejnou sadu klíčů, kterými budou zónové soubory podepsány.

Dá se však předpokládat, že vlastníci většího počtu doménových jmen (tj. více než jednoho doménového jména) budou chtít všechny svá doménové jména podepsat tím samým podepisovacím klíčem. Zároveň budou chtít v případě rotace klíčů provést změnu jednou na jednom místě a nikoliv u každého doménového jména zvlášť. Jedná se tedy o mapování m:n, stejně jako v případě NSSETu. Proto byla v konečné fázi vybrána varianta č. 3, tedy samostatný objekt v centrálním registru.

KEYSET je struktura obdobná NSSETu. KEYSET bude obsahovat následující položky:

- *1*-<*n*> kontaktních osob
- *1*-<*n*> Delegation Signer záznamů
- společné položky pro obecný objekt v centrálním registru

Delegation Signer záznam

DS záznam obsahuje následující seznam atributů, odpovídající příslušnému RFC:

- key tag – hodnota, která usnadňuje zjištění klíče ke kterému se DS záznam odkazuje,
- algorithm – algoritmus vytvoření veřejného klíče ke kterému se záznam váže,
- digest type – typ hashovací funkce která je použita při vytváření hashe veřejného klíče,
- digest – hash veřejného klíče, ke kterému se záznam váže,
- maxTTL(optional) – nastavení TTL pro tento záznam.

Rozšíření funkcí EPP protokolu

Zavedení nového objektu znamená přidání kompletní sady funkcí pro správu tohoto objektu. Tato sada funkcí přesně kopíruje sadu funkcí, které jsou k dispozici pro objekt NSSET. Výchozím dokumentem pro návrh rozšíření funkcí EPP protokolu je RFC standard pro DNSSEC mapování do EPP. Toto RFC odpovídá zavržené variantě 1) z kapitoly o návrhu struktury KEYSET, tzn. DS záznamy jsou uvedené přímo u každé domény. Pro vybranou variantu 3) se z tohoto RFC vybere de facto pouze XML s datovou strukturou DS záznamu. Následuje seznam nově přidaných funkcí do EPP rozhraní registru pro manipulaci s objektem KEYSET:

- CHECK_KEYSET – vstupem je seznam identifikátorů a výstupem seznam odpovědí oznamující možnost registrace uvedeného identifikátoru jako KEYSETu. Pro formát identifikátoru nebudou platit žádná omezení kromě povolených znaků a délky tak, jako je to v případě objektů KONTAKT a NSSET.
- INFO_KEYSET – vstupem je identifikátor KEYSETu jehož detail je požadován. Pokud je objekt zaregistrován, odpověď bude obsahovat dva seznamy. První seznam je seznam kontaktních osob zodpovědných za obsah objektu KEYSET a druhý seznam bude obsahovat jednotlivé DS záznamy. Každý DS záznam bude obsahovat všechny položky uvedené v předchozí kapitole. Kromě těchto údajů bude odpověď obsahovat ještě údaje společné pro všechny objekty registru, tedy heslo pro transfer (authinfo), určeného registrátora (clid), vytvářejícího registrátora (crid), registrátora poslední změny (upid), časové značky vytvoření (crdate), poslední změny (update) a posledního transferu (trdate), a repository identifikátor (roid).
- CREATE_KEYSET – vstupem je identifikátor keysetu a dva seznamy popsané ve funkci INFO_KEYSET. Pokud KEYSET neexistuje a požadované údaje jsou v pořádku, založí se nový s požadovanými vlastnostmi a přiřadí se registrátoru provádějícímu tuto operaci. Jakýkoliv registrátor může vytvořit KEYSET bez dalších omezení. KEYSET bude existovat do té doby, dokud není explicitně smazán nebo nesplňuje podmínky pro automatické smazání (šest měsíců nepoužívání). Standardní odpověď obsahuje časovou značku vytvoření.
- UPDATE_KEYSET – vstupem je identifikátor KEYSETu, který se má aktualizovat, a popis změn formou příkazů add a rem pro kontakty a DS záznamy. DS záznamy je možné kompletně nahradit příkazem chg. Pokud jsou uvedené změny v pořádku, KEYSET existuje a provádějící registrátor je jeho určeným registrátorem, provede se požadovaná změna. Odpověď neobsahuje žádná doplňující data.
- TRANSFER_KEYSET – vstupem je identifikátor KEYSETu, který se má přesunout, a heslo pro transfer. Pokud KEYSET existuje a zadané heslo odpovídá záznamu v registru, provede se transfer objektu k provádějícímu registrátorovi. Původní registrátor je informován poll zprávou. Odpověď neobsahuje žádná doplňující data.
- DELETE_KEYSET - vstupem je identifikátor KEYSETu, který se má smazat. Pokud tento KEYSET existuje, není navázán na žádnou doménu a patří provádějícímu registrátorovi, provede se jeho smazání. Odpověď neobsahuje žádná doplňující data.

O transformačních operacích (CREATE, UPDATE, TRANSFER a DELETE) budou emailem informovány kontaktní osoby ze seznamu kontaktních osob, které mají nastaven notify email, a to i ty, které byly v operaci UPDATE odstraněny.

Vedle těchto základních operací budou přidány další doplňující operace:

- SENDAUTHINFO_KEYSET – vstupem je identifikátor KEYSETU. Tato operace způsobí zaslání hesla pro transfer (authinfo) na emailové adresy všech kontaktních osob z KEYSETu.
- LIST_KEYSEST – připraví k vyzvednutí seznam všech KEYSETů patřících danému registrátorovi. Výsledek je možné vyzvednout funkcí GET_RESULTS.
- KEYSETS_BY_CONTACT – vstupem je identifikátor kontaktu. Připraví k vyzvednutí seznam všech KEYSETů obsahujících zadaný kontakt. Výsledek je možné vyzvednout funkcí GET_RESULTS.
- DOMAINS_BY_KEYSET – vstupem je identifikátor KEYSETu. Připraví k vyzvednutí seznam všech domén, ke kterým je přiřazen zadaný KEYSET. Výsledek je možné vyzvednout funkcí GET_RESULTS.

Pro provázání domén s novým objektem je nutné modifikovat již existující funkce:

- CREATE_DOMAIN – přidá se nový element s identifikátorem KEYSETu,
- UPDATE_DOMAIN – přidá se nový element s identifikátorem KEYSETu do sekce chg. Prázdný identifikátor znamená odstranění vazby,
- INFO_DOMAIN – odpověď je rozšířena o element s identifikátorem KEYSETu.

Rozšíření rozhraní pro veřejnost

Veřejný klíč delegované zóny resp. jemu odpovídající DS záznam je informace užitečná pro veřejnost, která by měla umožnit ověření, zda získaný klíč pro delegovanou zónu je správný. Proto bude do webového rozhraní přidán k detailu domény detail asociovaného KEYSETu. Dále bude možné vyhledat konkrétní KEYSET podle zadaného identifikátoru. Pro podporu transferu budou všechny funkce na webu pro vkládání žádosti o zaslání hesla pro transfer rozšířeny i pro objekt KEYSET.

Stejným způsobem bude rozšířen i unixový whois. V něm navíc přibudou nové indexy pro reversní vyhledávání a to domény podle KEYSETů a KEYSETy podle kontaktů.

Proces podepisování zónového souboru

Proces podepisování zónového souboru vychází ze sady dokumentů RFC (KOLKMAN, 2007; KOLKMAN & GIEBEN, 2006). Pro každou zónu spravovanou centrálním registrem bude udržována vlastní sada klíčů. Klíče budou rozděleny na klíč podepisující klíče – KSK (Key Signing Key) a zónu podepisující klíče – ZSK (Zone Signing Key). Toto rozdělení je vhodné z několika důvodů. KSK klíč je v podobě DS záznamů publikován v nadřazené zóně a jeho výměna v případě kompromitace je proces trvající delší dobu. Proto je vhodné, aby KSK klíč byl zabezpečen tak, aby možnost jeho kompromitace byla minimální. ZSK klíče jsou snáze vyměnitelné, neboť stačí jejich výměna a podepsání pomocí KSK. Pro podrobnější úvod do problematiky doporučuji DNSSEC HOWTO (KOLKMAN, 2007).

Key signing Key

Pro správu KSK bude vyhrazen speciální modul HSM, který běžně nebude připojen k síti internet. Modul HSM a obslužný server bude používán pouze pro potřeby vygenerování nových KSK a ZSK klíčů a podepsání tzv. zone apexu, který obsahuje všechny klíče příslušné zóně podepsané pomocí KSK.

Zone Signing Key

Po vygenerování ZSK a podepsání zone apexu budou ZSK a zone apex přeneseny na server, který bude určen k podepisování zóny. Samotný proces podepisování zóny bude probíhat automaticky. Pro zrychlení podepisování zóny budou pořízeny samostatné moduly HSM s podporou PKCS#11.

Technické parametry klíčů

Při zavádění technologie DNSSEC se budeme držet doporučení z RFC 3766, RFC 4086 a RFC 4641.

KSK klíč bude mít sílu 2048 bitů, algoritmus RSA-SHA1, počet klíčů 2, rotace klíčů jednou ročně pomocí mechanismu dvojitého podpisu (RFC 4641, 4.2.2).

ZSK klíč bude mít sílu 1024 bitů, algoritmus RSA-SHA1, počet klíčů 3, rotace klíčů jednou měsíčně pomocí mechanismu zveřejnění klíče předem (RFC 4641, 4.2.1.1).

Kompromitace klíčů

V případě kompromitace KSK je zapotřebí vygenerování nových KSK klíčů a rychlé nahrazení DS záznamů v nadřazené zóně. Pro případ kompromitace jen jednoho z KSK klíčů stačí jen odstranění z nadřazené zóny a vygenerování nových ZSK.

V případě kompromitace ZSK je zapotřebí vygenerovat novou sadu ZSK, podepsat apex zóny a nahradit sadu ZSK. V případě kompromitace jen jednoho ze ZSK je potřeba jeho vyřazení ze zónového souboru.

Dočasná opatření

Protože stále nedošlo k podepsání root zóny, bude pro publikování DS záznamů využit mechanismus DNSSEC Lookaside Validation (WEILER, S., 2007). Předpokládáme použití služby poskytované sdružením ISC na adrese dlv.isc.org.

Předběžný harmonogram

Skutečný harmonogram se může lišit v závislosti na komentářích k tomuto dokumentu případně na výsledcích jednotlivých kroků, nicméně v současné době předpokládáme tento harmonogram.

- 4.březen 2008 – vydání dokumentu verze 1.0
- 31.březen 2008 – konec posílání komentářů
- 30.duben 2008 – vydání finální revize dokumentu, stanovení přesného harmonogramu
- srpen 2008 – nasazení testovací instance pro registrátory a podpis zón (.cz i enum)
- září 2008 – start DNSSEC v ostrém provozu

Literatura:

1. ATKINS, D. AUSTEIN, R. (2004, duben). *Threat Analysis of the Domain Name System.* Dostupné z http://www.ietf.org/rfc/rfc3833.txt
2. INFOWORLD. (2001, 22. března). *VeriSign issues false Microsoft digital certificates* [online]. Dostupné z http://www.infoworld.com/articles/hn/xml/01/03/22/010322hnmicroversign.html
3. ORMAN, H. HOFFMAN, P. (2004, duben). *RFC 3766: Determining Strengths For Public Keys Used For Exchanging Symmetric Keys.* Dostupné z http://www.ietf.org/rfc/rfc3766.txt
4. EASTLAKE, D. SCHILLER, J. CROCKER, S. (2005, červen). *RFC 4086: Randomness Requirements for Security.* Dostupné z http://www.ietf.org/rfc/rfc4086.txt

5. KOLKMAN, O. GIEBEN, R. (2006, září). *RFC 4641: DNSSEC Operational Practices.* Dostupné z http://www.ietf.org/rfc/rfc4641.txt
6. KOLKMAN, O. (2007, 30. květen). *DNSSEC HOWTO, a tutorial in disguise.* Dostupné z http://www.nlnetlabs.nl/dnssec_howto/
7. WEILER, S. (2007, listopad). *DNSSEC Lookaside Validation.* Dostupné z http://www.ietf.org/rfc/rfc5074.txt
8. ARENS, R. FILIP, O. LISSE, E. (2007). DNSSEC @ root level – pracovní dokument ccNSO techwg
9. GUILLARD, O. (2008). DNSSEC briefing and root zone signing. pracovní dokument ccNSO techwg http://ccnso.icann.org/workinggroups/ccnso-iana-wg-dnssec-paper-04feb08.pdf