.news 07 2008 CZ NIC

Vážení čtenáři,

letošní třetí číslo pravidelného čtvrtletníku .news bude zaměřené možná trochu jednostranně. Poslední zářijový den jsme totiž na tiskové konferenci oznámili spuštění technologie DNSSEC do ostrého provozu a právě jí se budeme v tomto čísle nejvíce věnovat. Jde o záležitost skutečně významnou, CZ.NIC se stal pátým registrem na světě, který DNSSEC pro národní doménu spustil. Nečekejte ale, že zde najdete na každé druhé řádce slovo DNSSEC, prostor dostanou i informace o dalších projektech a aktivitách CZ.NIC.
S novou bezpečnostní technologií souviselo naše setkání s registrátory, s kterými jsme se naposledy viděli na konci srpna. Potěšující pro mě byla informace, že registrátoři deklarovali, že jsou na spuštění DNSSEC připraveni, a že řada z nich spustí tuto technologii ihned po jejím nasazení.
Stále aktuální je pro nás systém ENUM. Loni v září jsme uspořádali první ročník konference ENUM Day, na který tento rok navázal ENUM Day číslo dvě. Mám radost z toho, že si ENUM nachází své místo ve stále více firmách a domácnostech. Druhá polovina konference, prezentace o možnostech konkrétního využití ENUM, toho byla jasným důkazem.
Nemám zde bohužel prostor zmínit všechno, čemu jsme se v uplynulých měsících věnovali. Určitě bych chtěl ale ještě připomenout, že jsme po úspěšném vydání české verze filmu Warriors of the Net spustili projekt, jehož výstupem bude kniha o IPv6. Autorem publikace bude pan Pavel Satrapa a velmi novátorský je způsob, jakým kniha vzniká. Předběžnou verzi jsme umístili na web a nechali jsme čtenáře, aby ke knize posílali své připomínky. Teprve po jejich zapracování bude kniha vydána.
Přeji vám příjemné čtení následujících stránek a co možná nejbarevnější podzim.

Ondřej Filip
Výkonný ředitel sdružení CZ.NIC

Technologie DNSSEC zabezpečuje domény .CZ a ENUM

Sdružení spustilo po půlročním testování do ostrého provozu technologii DNSSEC. Ta dokáže předejít prakticky neodhalitelným útokům, které zneužívají bezpečnostní mezeru v systému DNS. Tyto útoky jsou potencionálním nebezpečím pro téměř všechny služby na internetu, zejména on-line bankovnictví či internetové zpravodajství. Na spuštění technologie spolupracovalo sdružení také se serverem Lidovky.cz, který je prvním českým on-line médiem s takto chráněnou doménou.
Systém DNS je jedním z technologických pilířů internetu. Díky němu si uživatel nemusí pamatovat číselné adresy různých serverů, ale pouze jejich „jména" jako www.nic.cz. Mezera v bezpečnosti systému DNS umožňuje útočníkovi podvrhnout libovolnou číselnou adresu kteréhokoliv doménového jména, a přesměrovat tak jejího uživatele na falešnou internetovou stránku, nebo odposlouchávat jeho e-maily. Nedávno se v internetové komunitě objevily důkazy, že podobný útok je možné provést během několika vteřin. Následná opatření pravděpodobnost takto jednoduchého napadení rapidně snížila, ale s potřebným vybavením v ceně, která nepřekročí několik tisíc korun, je stále v ideálních podmínkách možné provést úspěšný útok v řádu hodin. Zavedení DNSSEC je jednou z mála možností účinné obrany před tímto typem napadení.
Samotné spuštění DNSSEC v registru českých domén ale ještě neznamená stoprocentní ochranu. Nyní je důležité, aby DNSSEC do svých serverů implementovaly všechny relevantní internetové subjekty. Prioritou je zavedení DNSSEC u poskytovatelů internetového připojení. Hned za nimi by měli následovat registrátoři a provozovatelé nejrůznějších webových služeb, například banky či média. Pak bude ochrana skutečně plnohodnotná. Zabezpečit své počítače si však mohou i samotní uživatelé. Návod je k dispozici na stránkách http://podpora.nic.cz/Jak_zprovoznit_DNSSEC.
Česká republika se zařadila mezi pět států světa, které chrání své domény pomocí technologie DNSSEC. Dalšími zeměmi jsou Švédsko, Brazílie, Bulharsko a Portoriko. Řada ostatní států se na zavedení DNSSEC pro své národní domény chystá.

DRUHÝ ROČNÍK KONFERENCE ENUM DAY

Téměř po roce uspořádalo sdružení CZ.NIC druhý ročník konference o technologii ENUM. Do pražského Rock Café přišlo na jednodenní setkání více než 100 zájemců, kteří si mohli poslechnout přednášky věnované především současnému stavu zavádění této technologie v České republice.

VÍCE

ROZHOVORY SE ZÁSTUPCI CZ.NIC V MÉDIÍCH

V odborných médiích si mohli v minulém měsíci přečíst zájemci rozhovory se zástupci CZ.NIC. Server Lupa.cz přinesl rozhovor s Ondřejem Filipem, internetový portál ABC Linuxu otiskl interview v Ondřejem Surým, a na stránkách serveru Živě.cz odpovídal v on-line rozhovoru Pavel Tůma.

NOVÁ PRAVIDLA REGISTRACE DOMÉN .CZ A ENUM

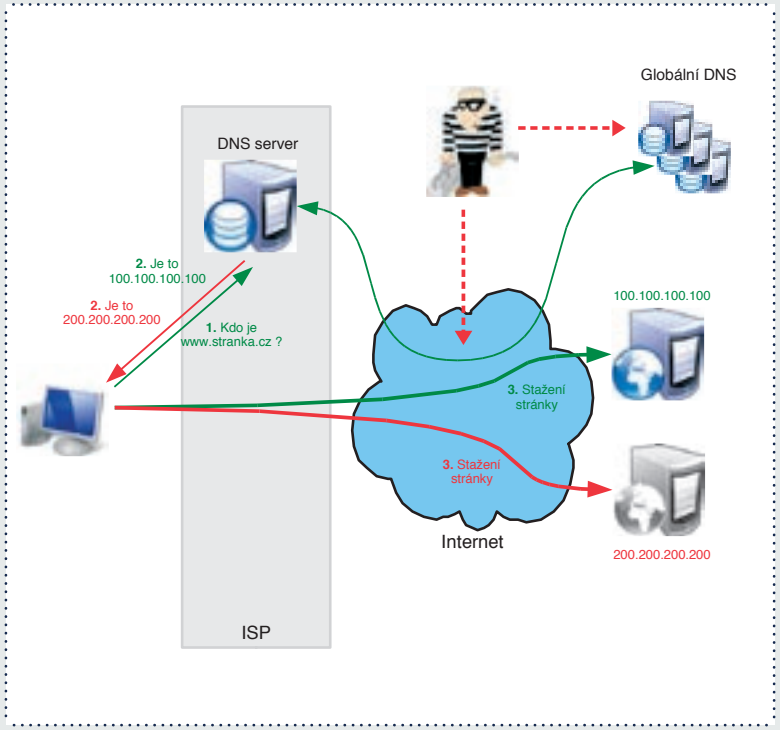
V souvislosti se zavedením technologie DNSSEC do národní domény .CZ a českých ENUM domén došlo také ke změně pravidel registrace. Jejich aktualizované verze najdete jak na domovských stránkách CZ.NIC, tak na internetové adrese technologie ENUM.

VÍTE, ŽE

...na stránce o technologii DNSSEC si můžete otestovat, jestli jste při přístupu na internet chráněni pomocí DNSSEC? Pokud zjistíte, že ne, podívejte se na internetové stránky technické podpory na postup, jak se pomocí DNSSEC ochránit.

Proč potřebujete DNSSEC?

Přestože většina internetových služeb sama o sobě nějaké formy zabezpečení má a uživatelé jsou zvyklí je používat, existuje jedna další hrozba, kterou si málokdo uvědomuje, a kterou dokáže odvrátit pouze DNSSEC.
Všechny internetové služby (e-mail, webové stránky, instant messaging, internetové volání, ...) využívají systém doménových jmen, jehož základním principem je překlad IP adres na doménová jména a obráceně. V případě, že někdo dokáže podvrhnout jmennou adresu, uživatel se, aniž bude cokoliv tušit, dostane na úplně jiné místo, a vůbec se nespojí se službou, kterou očekával. Může to vypadat třeba jako na tomto obrázku.



DNSSEC pro domény .cz a 0.2.4.e164.arpa (ENUM)

Obě domény spravované sdružením CZ.NIC: .CZ a ENUM (0.2.4.e164.arpa) umožňují používat DNSSEC pro ochranu záznamů v DNS. Pokud chcete svou doménu ochránit, musíte vygenerovat své DNSSEC klíče, své záznamy podepsat a prostřednictvím určeného registrátora své domény zveřejnit tzv. DS záznamy do registru domén. Jak na to se dozvíte v průvodci Jak zavést DNSSEC (tento návod je napsán pro domény .CZ, ale postup pro domény ENUM je zcela stejný).

.CZ

Protože dosud není pomocí DNSSEC podepsaná kořenová zóna DNS, je pro správné fungování ověřování DNSSEC podpisů nutná speciální konfigurace rekurzivního serveru - buď manuální umístění klíče do konfiguračního souboru serveru, anebo použití registru DLV. DNSSEC klíč pro doménu .CZ je:

„cz.“ 257 3 5 „AwEAAdo9fGLzCyxz1yTlsHCT7JpHrg0q/yOlvDNg39n/gAUzg6H/5X9p jW6mpecJuZirlcPcRw5E7E8uR8g2ztH4uztoc/7ss01s3rTnEgXfilbd psEdXEuxIfhq+w6zL6PvCcE3qRSzsrc2// x/SXjWp8yeT4YY3W3kvB4Z g5ld0a8bAHBYo4ZY9x7a3qnqOhqunXSG8EfRPD9koUMgWCjdnFNR89L1 5Bkzh+q1J7phTHIY5akKf3YnIB/5BnKmGBC7DimK4uSBLiBA3DLxHnvLffMT5XtKKHuQ/uZ4lxHWqR2cpHz/6e2WaQvOVILwd0gk9lTCiId BGjC7 eNxOMnitkuM=“ ;

Pro stažení klíče použijte tuto stránku zabezpečenou pomocí na SSL.
Konkrétní postup, jak jej manuálně přidat na váš server i jak nastavit používání registru DLV, najdete v návodu Jak zprovoznit DNSSEC. V obou případech se nezapomeňte přihlásit do příslušné e-mailové konference, kam chodí důležité informace o správě klíčů a DNSSEC vůbec! Více informací o tom, jak se přihlásit, najdete také ve zmíněném návodu.

0.2.4.e164.arpa (ENUM)

CZ.NIC jako správce domény 0.2.4.e164.arpa publikuje DS záznamy této domény k nadřazené autoritě, což je doména e164.arpa, kterou spravuje organizace RIPE. Pro správnou konfiguraci ověřování DNSSEC v případě ENUM domén budete tedy potřebovat klíče pro doménu e164.arpa. Najdete je právě u RIPE na stránce projektu DISI, stejně jako další informace o jejich správě. Postup nastavení je obdobný jako pro klíče domény .CZ.

DNSSEC v České republice

V úterý 30. září, v den spuštění DNSSEC do ostrého provozu, ohlásila zavedení této technologie ve svých systémech řada poskytovatelů připojení a také registrátorů.

Poskytovatelé připojení:
- Casablanca INT
- ČD-Telematika
- Dial Telecom
- GTS Novera
- IPEX
- Mobilkom
- STARNET

Registrátoři:
- ACTIVE 24
- GENERAL REGISTRY
- INTERNET CZ
- KRAXNET
- ONE.CZ
- Web4U

Kromě těchto společností řada dalších se zavedením DNSSEC počítá. Podle našich informací se jejich seznam výrazně rozroste do konce roku 2008.

ENUM Day 2 ve znamení praktických zkušeností a mezinárodní spolupráce

Druhý ročník jednodenní konference věnované technologii ENUM nezůstal co do úspěchu svému předchůdci nic dlužen. Setkání, které se uskutečnilo ve středu 17. září v pražském Rock Café, se zúčastnilo více než 100 ICT profesionálů a nadšenců. Ty přilákala především možnost seznámit se s ENUM z praktického hlediska a příležitost vidět, díky přednáškám hostů z Nizozemí a Finska, jaké mají zkušenosti s touto technologií ve světě a jak v těchto zemích probíhá zavádění ENUM do praxe.
ENUM je v České republice od ledna loňského roku a za tu dobu urazil pořádný kus cesty. Letošní ročník ENUM Day ukázal v prezentacích hlavně to, že ENUM už má fázi technologického experimentu za sebou. To bylo nejlépe vidět z přednášek zástupcům firem, které ENUM již využívají. Své zkušenosti s jeho implementací a provozem prezentovali v rámci třetího bloku věnovaného právě praktickému využití této technologie zaměstnanci společností BENETA.cz, PulaSoft, IPEX a Ostravské univerzity. Mezi nejzajímavější momenty patřilo jistě i vystoupení Wilhelma Wimmreutera z německého Mnichova. Ten v prezentaci s názvem Dá se žít bez minutových poplatků ukázal i jiné telekomunikační obchodní modely, než jaké nám řadu let vnucuje naprostá většina operátorů. Prezentace ve formátu PDF, ale i audiovizuální záznamy jednotlivých vystoupení najdete na stránkách konference ENUM Day 2.
Třetí ročník konference o technologii ENUM a VoIP telefonii plánují organizátoři opět na září příštího roku. ■

Nové projekty sdružení CZ.NIC

V srpnu a září spustilo sdružení řadu projektů určených pro širokou veřejnost.

Válečníci sítě

Nejen pro začínající uživatele internetu vydal CZ.NIC v českém překladu film s názvem Válečníci sítě. Z něho se mohou diváci dozvědět, jak vypadají jednotlivé části internetu, jaký je internet "zevnitř". Pokud jste tedy někdy přemýšleli o tom, jak internet vlastně funguje, jaký je router nebo jakou barvu má IP packet, podívejte se na tento zajímavý film. Určitě se dozvíte mnohem více, než jen to.

V.I.P – Vyvíjej, Inovuj, Programuj

Soutěže pro mladé talenty v oblasti ICT se mohou zúčastnit projekty zaměřené na vývoj nového open-source softwaru nebo inovaci softwaru používaného v oblasti internetových technologií, služeb či infrastruktury. Úspěšný projekt může získat až 50.000 Kč.
Soutěž se skládá z několika fází. Soutěžící nejdříve pošlou své návrhy projektů. Z nich odborná hodnotící komise vybere ty, které budou splňovat předepsaná kritéria. Poté začne samotná realizace vybraných projektů, po níž bude následovat vyhodnocení a ocenění výherců.
Cílem projektu je podpořit talentované programátory v tom, aby za svým úsilím viděli konkrétní cíl. Tím je kromě finanční odměny také reálná možnost uplatnění projektu v praxi.
Zájemci o účast v soutěži se mohli přihlásit do 17. října včetně.

Kniha o IPv6

Základem projektu, který je určený odborné veřejnosti se zájmem o problematiku IPv6, je text Pavla Satrapy z Technické univerzity v Liberci. Od 26. září se zájemci o problematiku IP sítí mohou vyjadřovat k jednotlivým částem knihy. Pod jednotlivými kapitolami mají všichni čtenáři možnost připojovat své komentáře, a to až do 31. října. Pavel Satrapa v průběhu listopadu komentáře zpracuje, poté bude konečná podoba knihy volně ke stažení. Od této doby si také budou moci zájemci objednat knihu v tištěné podobě.
Kniha Pavla Satrapy je první publikací, která ve sdružení vyjde. V příštím roce budou pod značkou sdružení následovat další odborné texty z oblasti internetu a internetových médií. CZ.NIC by chtěl proto nabídnout odborníkům, kteří by měli zájem na vydání svých publikací, aby svou nabídku poslali přímo na kontaktní adresu sdružení.

Informační stránky pro školy

Protože je řada projektů zaměřena na studenty a pedagogy středních vysokých škol, vytvořili zaměstnanci CZ.NIC speciální stránky, na kterých bude možné najít aktuální informace o nabídce. Vedle výše představných projektů je na těchto stránkách možné najít nabídku prezentace o DNS a novinách ze světa domén a internetu. Ta je určena především studentům posledních ročníků středních škol a prvních ročníků vysokých škol a univerzit. Vedle toho je zde možné volně stáhnout edukativní letáky nebo se informovat o možnostech absolvování povinné středoškolské nebo vysokoškolské praxe. ■

FRED používá angolský národní registr

Správci angolské národní domény budou pro registraci domén s koncovkou .CO.AO a .IT.AO používat český registrační systém FRED (Free Registry of ENUM and Domains). Tuto informaci oznámili zástupci západoafrické země na červnovém setkání organizace ICANN v Paříži. Registrační systém FRED vyvinuli zaměstnanci sdružení CZ.NIC a od loňského října v něm současně spravují českou národní doménu .CZ a doménu ENUM. Registrační systém FRED byl v říjnu 2007 uvolněn jako open source a Angola je po České republice první zemí, která začne tento registrační systém používat.

Na zavedení nového registračního systému pro domény .CO.AO a .IT.AO spolupracovali správci angolské národní domény s odborníky z České republiky, Portugalska a Francie. Především díky této spolupráci mohli iniciátoři tohoto projektu na posledním setkání ICANN oznámit zavedení systému FRED pro angolský národní registr. Podle všech informací v tuto chvíli systém testují a brzy ho uvedou do plného provozu.

Současně s uvolněním FRED jako open source software sdružení otevřelo diskusi, která by měla navrhnout další úpravy a vylepšení tohoto systému. I angolští správci již ohlásili, že uvolní také jako open source JAVA konektor rozšiřující systém FRED, stejně tak zváží zveřejnění jako open source i další vylepšení nebo rozšíření.

Díky tomu, že se přidávají další uživatelé systému FRED, vzniká komunita, která ho může dále rozvíjet a vylepšovat. Zástupci CZ.NIC věří, že se v blízké budoucnosti přidají i další země, které budou chtít systém pro správu domén zavést. ■

V Praze byla založena ENUM Federation

e.num WEMANAGENUMBERS

Den před konferencí ENUM Day 2, 16. září, se v Praze sešli zástupci národních registrů domén Holandska, Německa, Rakouska a České republiky, aby zde slavnostně podepsali zakládající listinu organizace ENUM Federation. Jejím hlavním cílem je společný postup při šíření povědomí o ENUM.

Přestože se ENUM pomalu dostává do povědomí firem, veřejné povědomí o něm je stále nízké. Zlepšit tuto situaci by mimo jiné mělo právě i založení organizace ENUM Federation, které inicioval CZ.NIC. Členy tohoto sdružení, jež bude mít stálé sídlo v hlavním městě České republiky, jsou zástupci uvedených registrů, tedy zemí, které jsou ve využívání ENUM nejdále. Prvním cílem ENUM Federation je vytvořit značku, kterou by mohly nést všechny produkty a služby podporující ENUM. Smyslem této značky je přiblížit zákazníkům výrobky, které umožňují volání přes ENUM; podobně, jako je to například u technologií Bluetooth nebo Wi-Fi. Od jednotné propagace si všichni zainteresovaní slibují hlavně zvýšení zájmu o ENUM a podporu masovějšího využívání této technologie.

Systém ENUM využívá v současné době z evropských zemí také Rakousko, Německo, Polsko, Finsko, Rumunsko, Holandsko a Irsko; testovací provoz běží v několika dalších státech. Národní doména ENUM je delegována prakticky ve všech evropských zemích. Dá se tedy očekávat, že k čtveřici zakládajících přibudou brzy další zástupci národních registrů domén. ■

Zástupci CZ.NIC se setkali s „otcem internetu“

V pondělí 22. září se výkonný ředitel sdružení Ondřej Filip, předseda představenstva CZ.NIC Tomáš Maršálek a ředitel sdružení CESNET Jan Gruntorád setkali s jedním ze zakladatelů internetu; viceprezident a Chief Internet Evangelist společnosti Google Vint Cerf přijel do Prahy na krátkou návštěvua kromě svých pracovních povinností stihnul i schůzkus významnými představiteli českého internetu.

Ondřej Filip se s Vintem Cerfem nesetkal poprvé. Díky svému aktivnímu působení v radě ccNSO (Country Code Names Supporting Organisation) v rámci organizace ICANN (Internet Corporation for Assigned Names and Numbers) jsou jejich setkání na pravidelných celosvětových fórech poměrně častá.

Vint Cerf byl na začátku sedmdesátých let minulého století jednou z vůdčích postav týmu podílejícím se na vývoji protokolu TCP/IP, který tvoří technologický základ sítě internet. Určuje totiž formát a způsob, jakým data počítačovou sítí putují. Zásadní výhodou protokolu TCP/IP je vysoká efektivnost přenosu dat a také jeho odolnost proti vzniku chyb během jejich cesty. ■

Vybráno z .blogu

DNS útok podle Kaminského

(autor: Ondřej Surý, technický ředitel CZ.NIC, publikováno: 8. srpna 2008)

Útoky typu DNS Cache Poisoning fungují na principu podvržení odpovědi DNS serveru. DNS server, který se ptá na určité doménové jméno, pak dostane falešné informace např. o IP adrese webového serveru. Způsob, jak podvrhnout DNS odpověď, spoléhá na několik vlastností DNS protokolu:

1. DNS dotazy a odpovědi v sobě mají uloženo 2-bytové Transaction ID, tedy počet kombinací je přibližně 65 tisíc.
2. Nezáplatované DNS servery používají pro všechny dotazy stejný zdrojový port.
3. Většina DNS dotazů a odpovědí používá UDP. UDP je bezstavové a v současných sítích je relativně jednoduché podvrhnout zdrojovou IP adresu.

Útočník musí uhodnout správné Transaction ID (nebo vygenerovat všechny možné kombinace) a poslat je ve velmi rychlém sledu za sebou s podvrženou zdrojovou adresou na adresu DNS serveru, na který útočí. Odpověď od útočníka musí přijít v časovém okně na jedné straně vymezeným DNS dotazem a na druhé straně DNS odpovědí od legitimního autoritativního DNS serveru.

Typický útok tohoto typu musel „čekat" na chvíli, kdy dotazující server nemá záznam uložený ve vyrovnávací paměti serveru a musí se zeptat autoritativního serveru. Takový záznam je pak uložen po dobu uvedenou v TTL záznamu ve vyrovnávací paměti serveru a útočník musí čekat, než tato doba vyprší. Časové okno, kdy lze zaútočit na DNS serveru, tohoto útoku je tak díky TTL velmi malé a se vzrůstajícím TTL se pravděpodobnost takového útoku snižuje. Šance podvrhnout správné Transaction ID je 1 ku 65 tisícům a i v případě, že si útočník vygeneruje DNS odpovědi se všemi Transaction ID, je vzhledem k faktu, že lze útočit pouze ve chvíli, kdy záznam není ve vyrovnávací paměti serveru, šance na úspěch takového útoku malá.

Podvržená odpověď bude vypadat nějak takto (Transaction ID je vyznačeno tučně):

```
; <<>> DiG 9.4.2-P1 <<>> www.dnssec.cz
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47457
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 2

;; QUESTION SECTION:
;www.dnssec.cz.          IN    A

;; ANSWER SECTION:
www.dnssec.cz.       86400    IN    A    192.168.1.1

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Aug  8 14:17:41 2008
;; MSG SIZE  rcvd: 139
```

Dan Kaminsky odhalil způsob, jak obejít data uložena ve vyrovnávací paměti a falešnou IP adresu podvrhnout v libovolnou chvíli bez ohledu na TTL. Útočník se při útoku neptá přímo na IP adresu webového serveru, ale na libovolný náhodně zvolený neexistující záznam a IP adresu webového serveru podvrhne pomocí sekce AUTHORITATIVE a ADDITIONAL pomocí mechanismu tzv. GLUE záznamu.

Příklad: Útočník se zeptá DNS serveru, na který útočí, na 007.dnssec.cz a podvrhne odpověď: Odpověď 007.dnssec.cz neznám, ale zná ho server www.dnssec.cz s IP adresou 192.168.1.1.

```
; <<>> DiG 9.4.2-P1 <<>> 007.dnssec.cz
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55309
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 11

;; QUESTION SECTION:
;007.dnssec.cz.          IN    A

;; AUTHORITY SECTION:
dnssec.cz.       86400    IN    NS    www.dnssec.cz.
;; ADDITIONAL SECTION:
www.dnssec.cz.       86400    IN    A    192.168.1.1
;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Aug  8 14:20:58 2008
;; MSG SIZE  rcvd: 139
```

V tu chvíli dojde k přepsání A záznamu pro www.dnssec.cz ve vyrovnávací paměti serveru a další dotazy na www.dnssec.cz, na které bude odpovídat tento DNS serveru, budou obsahovat podvrženou IP adresu.

Šance na uhodnutí správného Transaction ID zůstává stále stejná, ale útočník může volbou dotazů na různé neexistující domény zkoušet podvrhnout IP adresu stokrát až tisíckrát za sekundu. Navíc je schopen lépe řídit čas dotazu (vždy se ptá útočník) a tím pádem lépe načasovat i generování podvržených odpovědí.

Výrobci a autoři DNS serverů vydali aktualizace, které do dotazu vkládají další prvek náhody - náhodný zdrojový port. Před aktualizací byl zdrojový port dotazu zvolen náhodně při startu serveru a po celou dobu běhu serveru byl používaný stejný port. Po aktualizaci se pro každý dotaz používá nové náhodně zvolené číslo zdrojového portu (pokud budeme počítat, že se využije celý rozsah, což většinou nebývá pravdou) a šance na uhodnutí kombinace Transaction ID a čísla zdrojového portu je 1 ku 4 miliardám. Útočník se může pokoušet vygenerovat i takovýto počet podvržených DNS odpovědí, ale šance, že se mu povede trefit správnou odpověď je výrazně menší a provoz, který tímto vygeneruje jen těžko zůstane bez povšimnutí.

Útok, který předvedl Dan Kaminsky, na vyrovnávací pamět DNS serveru je po instalaci opravných aktualizací nepravděpodobný, ale stále možný. Podle kalkulací, které proběhly poštovní konferencí namedroppers, je pravděpodobnost takového útoku po 24 hodinách cca 64%. Takový útok by si ovšem vyžádal generování obrovského množství podvržených DNS odpovědí a u méně výkonných instalací by spíše způsobil zahlcení a přerušení provozu. Než jsem stihl napsat tento příspěvek do blogu, tak se objevil první úspěšný útok v laboratorních podmínkách na DNS server s náhodnými zdrojovými porty, který byl schopný vložit do DNS falešnou adresu během 10 hodin. Jediné řešení, které DNS servery ochrání před tímto stylem DNS útoků je v současné době technologie http://www.dnssec.cz.

Prezentaci Dana Kaminského z konference BlackHat USA 2008 naleznete na jeho stránkách DoxPara. ■