Maciej Andziński

Bezpieczeństwo z DNSSEC

Pod koniec grudnia ubiegłego roku NASK udostępnił domenę .pl w formie zabezpieczonej rozwiązaniem DNSSEC *(ang. DNS Security Extensions)*. Był to początek polskiego wdrożenia rozwiązania, które ma podnieść poziom bezpieczeństwa kluczowej dla działania internetu usługi jaką jest DNS. Zwieńczenie całego procesu wdrożenia nastąpiło 4 czerwca 2012 r., wówczas to NASK rozpoczął przyjmowanie od abonentów nazw domeny .pl skrótów z kluczy kryptograficznych.

Bezpieczeństwo DNS

Bezpieczeństwo systemu DNS od lat jest tematem rozważań. Eksperci są zgodni co do potrzeby zastosowania nowych mechanizmów. Do tej pory brakowało spójnego rozwiązania, które byłoby możliwe do wdrożenia globalnie, przy zachowaniu istniejącej infrastruktury. Oczekuje się, że lekarstwem na podatności systemu nazw będzie DNSSEC, rozszerzenie protokołu DNS, które z pomocą kryptografii asymetrycznej eliminuje specyficzne dla ruchu DNS zagrożenia związane z fałszowaniem transmisji. Pojęcia takie jak zatruwanie DNS *(ang. cache poisoning)* czy atak Kamińskiego mogą już niedługo odejść w niepamięć.

Wdrożenie DNSSEC oznacza dla przeciętnego użytkownika Internetu, że po wpisaniu poprawnego adresu strony WWW w swojej przeglądarce, nie zostanie on przekierowany na fałszywy serwer, a przynajmniej nie za sprawą DNS. Tym samym wzrośnie bezpieczeństwo korzystania ze stron banków, stron rządowych, czy też sklepów internetowych i kont pocztowych. Dla abonentów i rejestratorów domen oraz dostawców Internetu nowe rozszerzenie to przede wszystkim możliwość podniesienia standardów bezpieczeństwa.

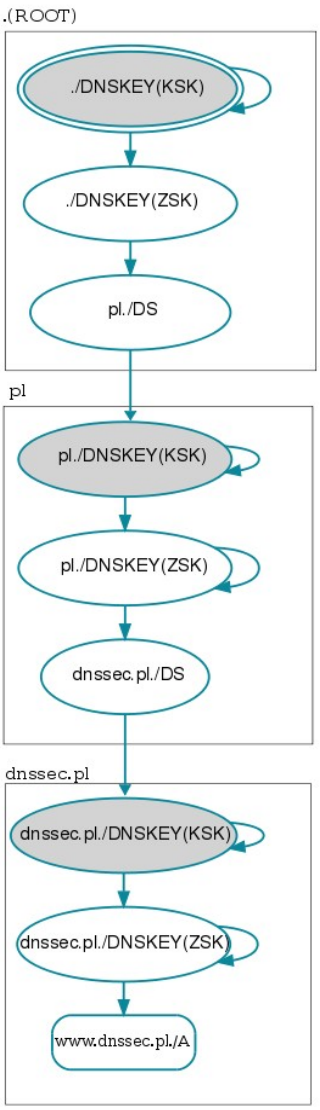
Jak to działa?

W strefie zabezpieczonej DNSSEC każda autorytatywna informacja posiada podpis cyfrowy (rekord RRSIG), a do jego weryfikacji udostępniany jest zestaw kluczy publicznych (rekord DNSKEY). Wyróżnia się dwa typy kluczy: ZSK *(ang. zone signing key)* podpisujący wszystkie autorytatywne rekordy w strefie oraz KSK (key signing key), który podpisuje tylko zestaw kluczy. Taki podział został dokonany ze względów praktycznych, klucz KSK jest z reguły dłuższy i rzadziej wymieniany. Zarówno KSK jak i ZSK dzielą się na część publiczną udostępnianą w strefie oraz prywatną wykorzystywaną do generowania podpisów.

Aby możliwe było weryfikowanie odpowiedzi, musi istnieć tzw. łańcuch zaufania, który rozpoczyna się od punktu zaufania *(ang. trust anchor)*, czyli po prostu klucza, któremu ufamy. Zawsze jest to KSK (w idealnej sytuacji dla strefy ROOT), który podpisuje ZSK, a ten wszystkie autorytatywne informacje w strefie, w tym także wprowadzone przez DNSSEC nowe rekordy typu DS *(ang. delegation signer)*. Zawierają one kryptograficzne skróty klucza KSK delegowanych stref.

Przeanalizujmy jak wygląda łańcuch zaufania dla przykładowej nazwy podpisanej DNSSEC, np. www.dnssec.pl. Ufamy KSK strefy ROOT, a więc także podpisanemu przez niego ZSK, ten z kolei podpisuje rekord DS dla nazwy pl, który wskazuje na klucz KSK w strefie pl. Pozwala to uznać ten KSK za zaufany i tak powstaje pierwsze ogniwo w naszym łańcuchu. Kolejne są wynikiem iteracji po drzewie DNS aż do osiągnięcia serwera autorytatywnego dla dnssec.pl, który posiada podpisany właściwym kluczem ZSK rekord dla nazwy www.dnssec.pl (np. A lub AAAA).

Za sprawdzenie łańcucha zaufania oraz poprawności podpisów odpowiada resolver rekursywny. O ile nie żądamy inaczej (poprzez ustawienie w zapytaniu bitu CD *(ang. checking disabled)*), wykrycie niepoprawności skutkuje zwróceniem błędu SERVFAIL. Jeśli dane są poprawnie zweryfikowane w odpowiedzi jest ustawiany bit AD *(ang. authenticated data)*.



Ilustracja 1: Łańcuch zaufania dla nazwy www.dnssec.pl

Jak zabezpieczyć swoją strefę?

W procesie zabezpieczenia strefy rozszerzeniem DNSSEC można wyróżnić 3 kroki:

1) wygenerowanie kluczy
2) podpisanie pliku strefy
3) umieszczenie rekordu DS w strefie nadrzędnej.

Przyjrzyjmy się jak to wygląda w praktyce. W poniższym przykładzie zostały wykorzystane narzędzia dostarczane przez oprogramowanie BIND w wersji 9.7.

Załóżmy, że strefą , którą chcemy podpisać będzie dnssec.pl. Zaczynamy od generowania kluczy za pomocą programu dnssec-keygen. Wykorzystujemy KSK i ZSK o długościach odpowiednio 1024 i 2048 bitów, algorytm RSA/SHA-256 oraz rozszerzenie NSEC3:

```
/etc/bind/keys# dnssec-keygen -3 -a RSASHA256 -b 1024 dnssec.pl
Generating key pair.........................++++++ ..++++++
Kdnssec.pl.+008+18930

/etc/bind/keys# dnssec-keygen -3 -f KSK -a RSASHA256 -b 2048 dnssec.pl
Generating key
pair.....................................................................
+++ ...................................................+++
Kdnssec.pl.+008+63691
```

Dla każdego klucza powstają dwa pliki, które zawierają jego część publiczną (.key) oraz prywatną (.private). Ta pierwsza jest reprezentowana w postaci rekordów DNSKEY, które należy umieścić w pliku strefy a następnie podpisać go za pomocą programu dnssec-signzone:

```
/etc/bind/master# dnssec-signzone -S -K /etc/bind/keys/ -3 123456 -o dnssec.pl. dnssec.pl
Fetching ZSK 18930/RSASHA256 from key repository.
Fetching KSK 63691/RSASHA256 from key repository.
Verifying the zone using the following algorithms: RSASHA256.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked
dnssec.pl.signed
```

Wynikiem powyższej operacji jest plik dnssec.pl.signed zawierający podpisaną strefę. W konfiguracji BIND należy podmienić ścieżkę, tak aby strefa została zaczytana z nowo powstałego pliku. Kolejnym krokiem jest przeładowanie usługi nazw:

```
# rndc reconfig
```

W logach można zaobserwować wpis informujący o załadowaniu podpisanej strefy:

```
Mar  8 13:45:51 tmaster named[18904]: zone dnssec.pl/IN: loaded serial 2 (DNSSEC signed)
```

Brawo, podpisaliśmy dnssec.pl! Jednak aby możliwe było zbudowanie łańcucha zaufania konieczne jest umieszczenie rekordu DS w strefie nadrzędnej (w tym przypadku .pl). Zauważmy, że program dnssec-signzone wygenerował plik, który zawiera DS dla naszej strefy. Za pomocą bezpiecznego kanału należy przekazać te dane do podmiotu odpowiedzialnego za rejestrację domeny.

```
/etc/bind/keys/# cat dsset-dnssec.pl.
dnssec.pl.              IN DS 63691 8 1 3E97B74D29D7D90BAC76D7BAF999AF3DBFCCE679
dnssec.pl.              IN DS 63691 8 2
4779B9F9E722B0F6F1B764484BE3D1F55B3D34632858FD2DBAA8DE93 1EA5D9DA
```

Strefa podpisana. Co dalej?

Klucze należy cyklicznie wymieniać. W przypadku KSK ten proces wymaga ingerencji w strefę nadrzędną (wymiana DS). Pamiętajmy, że dane pochodzące z serwerów autorytatywnych znajdują się przez określony czas w pamięci resolverów rekursywnych. W związku z tym proces wymiany kluczy musi być dobrze zaplanowany. Powinniśmy postępować według zaleceń z dokumentu RFC 4641, który opisuje dwie metody: prepublikacji *(ang. pre-publish key rollover)* oraz podwójnego podpisywania *(ang. double signature zone signing key rollover)*.

Proces zarządzania kluczami można zautomatyzować. Wraz z rozwojem DNSSEC powstaje coraz więcej narzędzi wspierających procesy administracyjne, wśród najpopularniejszych należy wymienić openDNSSEC. Oprogramowanie to potrafi we właściwym czasie dokonać niezbędnej operacji związanej z wymianą klucza lub generowaniem podpisu, jednak aktualizacja DS w strefie nadrzędnej zazwyczaj będzie wymagać naszej ingerencji.

Ponieważ podpisy mają ustalony okres ważności (domyślnie 30 dni) konieczne jest ich odnawianie. Oprogramowanie BIND posiada zaimplementowaną funkcjonalność, dzięki której nowe podpisy są generowane automatycznie zanim wygasną stare.

Jak włączyć obsługę DNSSEC na resolverze rekursywnym?

Dostawców Internetu z pewnością bardziej zainteresuje możliwość włączenia obsługi DNSSEC na resolverach rekursywnych. W BIND w tym celu wystarczy ustawić dwie opcje:

```
dnssec-enable yes;
dnssec-validation yes;
```

oraz skonfigurować punkt zaufania.

W repozytoriach dystrybucji linuksowych coraz częściej oprogramowanie usługi nazw posiada już skonfigurowany punkt zaufania i jest nim KSK strefy ROOT. Należy pamiętać, że ten klucz będzie się zmieniać i trzeba pobierać jego nowe wersje. Istnieją jednak mechanizmy ułatwiające ten proces. Oprogramowanie BIND od wersji 9.7 implementuje mechanizm śledzenia zmian kluczy opisany w dokumencie RFC 5011. Aby korzystać z automatycznego zarządzania kluczami wystarczy dodać aktualny KSK do sekcji "managed-keys", a jego nowe wersje będą automatycznie pobierane:

```
managed-keys {
        "." initial-key 257 3 8 "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/
VHL496M/QZxkjf5/Efucp2gaD X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS Qageu
+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq QxA+Uk1ihz0=";
};
```

Skąd wiadomo, że DNSSEC działa?

O tym, że odpowiedź DNS została poprawnie zweryfikowana informuje resolver rekursywny poprzez ustawienie bitu AD w odpowiedzi. Użytkownik może oczekiwać, że skoro otrzymał odpowiedź, a strefa jest zabezpieczona DNSSEC, to weryfikacja się powiodła, w przeciwnym razie zostałby zwrócony błąd SERVFAIL. Warty polecenia jest DNSSEC validator - dodatek do przeglądarki Firefox, opracowany przez rejestr czeski. To narzędzie dla każdej wyświetlanej strony podaje informację o zabezpieczeniach DNSSEC. Na rysunku przykład dla www.nic.cz.

Ilustracja 2: Wtyczka DNSSEC validator

O czym trzeba pamiętać?

Skuteczność DNSSEC jest taka, jak siła zabezpieczeń kryptograficznych. Tylko przy zachowaniu odpowiednich standardów będzie ona wysoka.

Materiał kryptograficzny powinien być przechowywany w należyty sposób. O ile to możliwe, części prywatne kluczy powinny znajdować się poza maszyną, która świadczy usługę DNS. Wówczas nawet skompromitowany serwer nie będzie w stanie serwować fałszywych rekordów, ponieważ nie zostaną one podpisane. Dla zwiększenia bezpieczeństwa warto rozważyć przechowywanie klucza prywatnego np. na zaszyfrowanym nośniku w sejfie, a w przypadku stref o krytycznym znaczeniu (duże rejestry, instytucje rządowe, banki) zastosowanie urządzeń HSM *(ang. hardware security module)*. Ich konstrukcja gwarantuje, że materiał kryptograficzny nie wycieknie na zewnątrz. Często umożliwiają także tworzenie bezpiecznych scenariuszy autoryzacji, które determinują obecność kilku osób do wykonania krytycznej operacji *(ang. two-man rule)*. Takie urządzenia są wykorzystywane w krajowym rejestrze domeny .pl prowadzonym przez NASK.

Warto pamiętać także o tym, aby zapewnić dostatecznie dobre źródło losowych danych maszynie wykonującej operacje na materiale kryptograficznym. Za cenę kilkuset dolarów można nabyć specjalny moduł sprzętowy, który zapewni losowość na dobrym poziomie.

Na koniec ważna uwaga dla ISP. Za weryfikację DNSSEC odpowiada resolver rekursywny, o powodzeniu tego procesu końcowy odbiorca jest informowany jedynie poprzez ustawienie bitu AD w odpowiedzi. Bezpieczeństwo transmisji na linii resolver rekursywny - stacja robocza jest więc krytyczne dla całego procesu. Aby DNSSEC był skuteczny należy zapewnić należytą bliskość odbiorcy i maszyny odpowiedzialnej za rozwiązywanie nazw. Powinny one znajdować się w tej samej, zaufanej sieci.

Czy DNSSEC ma jakieś wady?

Konsekwencją wdrożenia DNSSEC jest zwiększona ilość danych w systemie DNS. Wiąże się to z koniecznością zaangażowania większych zasobów dyskowych i pamięciowych na serwerach autorytatywnych. W przypadku resolverów rekursywnych obserwuje się wzrost zapotrzebowania na moc obliczeniową niezbędną do weryfikacji podpisów. Wdrożeniu DNSSEC towarzyszy zwiększenie rozmiaru transmisji. Szczególną uwagę należy zwrócić na wzrost rozmiaru pakietu UDP, w skrajnych przypadkach może być to przyczyną zakłócenia komunikacji DNS. Pamiętajmy, że protokół DNS jest obecny w Internecie niemal od jego początków i wciąż mogą istnieć konfiguracje firewalli blokujące pakiety UDP większe niż 512 bajtów. Są to jednak sytuacje skrajne. DNSSEC bywa również wykorzystywany do ataków bazujących na różnicy wielkości zapytania i odpowiedzi *(ang. amplification attack)*, jednak podatność ta stanowi naturalną cechę systemu DNS i występuje obecnie także w strefach nie podpisanych DNSSEC.

Stan wdrożenia DNSSEC w Polsce i na świecie

Strefa ROOT została podpisana 15 lipca 2010 r., co dało zielone światło dla globalnego wdrożenia. Według stanu na marzec 2012 zabezpieczonych DNSSEC jest 84 spośród 312 stref najwyższego poziomu. Należy dodać, że są to w większości najbardziej znaczące rejestry, takie jak .com, .gov, a także największe europejskie ccTLD (m.in. .de, .uk, .pl, .fr).

19 grudnia 2011 r. NASK podpisał strefę .pl, a także 152 strefy funkcjonalne i regionalne, np. com.pl, waw.pl. Rekord DS dla nazwy .pl został umieszczony w strefie ROOT 9 lutego 2012 r. Od 4 czerwca 2012 r. rozpoczął przyjmowanie rekordów DS nazw zarejestrowanych w domenie .pl, co oznacza, że każdy abonent domeny z końcówką ".pl" ma możliwość zabezpieczenia jej poprzez DNSSEC.

Niniejszy artykuł został opublikowany w czasopiśmie "IT w administracji" nr 5/2012