راهنمای ضمیمهٔ امنیتی سامانهٔ نام دامنه

DNS Security Extension Tutorial

DNSSEC چیست؟

کارگزار DNS مسئولیت دریافت نام دامنه و بازگرداندن نشانی آی‌پی (IP) کارگزار و اطلاعات دیگری را به عهده دارد، اما هیچ تضمینی برای صحت این اطلاعات به کاربر نمی‌دهد. به همین دلیل همواره خطراتی مانند مسموم شدن اطلاعات حافظهٔ نهانی (Cache Poisoning) در DNS کاربران را تهدید می‌کند. ضمیمهٔ DNSSEC با هدف برطرف کردن این مشکلات و اطمینان بخشیدن به پاسخ دریافتی از کارگزار DNS به‌وجود آمده است. به طور خلاصه، وقتی کاربر نشانی‌ای را در مرورگر خود وارد می‌کند، اطمینان خواهد داشت که نشانی آی‌پی را از گویندهٔ معتبری دریافت کرده است. این کار با بررسی امضاهای دیجیتالی (Digital Signatures) موجود در کارگزار مرجع (Authoritative Server) صورت می‌پذیرد.

قرارداد DNSSEC در سال ۱۹۹۷ معرفی شد و در سال ۱۹۹۹ با انتشار RFC2535 توسط IETF به طور کامل‌تر مطرح شد، اما مشکلات در پیاده‌سازی باعث شده است که هنوز به صورت فراگیر از آن استفاده نشود.

در سال ۲۰۰۱ اولین نسخهٔ نرم‌افزار BIND با قابلیت پشتیبانی از DNSSEC در دسترس عموم قرار گرفت، ولی پس از انجام آزمایشات مختلف، پروژه متوقف شد. اولین و مهم‌ترین مشکل، نحوهٔ ارسال کلیدها از کارگزار مرجع به کارگزار سرپرست و دریافت تعداد زیادی کلید توسط کارگزار سرپرست از کارگزاران زیردست بوده است. مشکل دیگر در نسخهٔ اول DNSSEC، معتبر نبودن پاسخ «عدم وجود نام دامنه» (NXDOMAIN) در کارگزار بود. به همین دلیل نسخهٔ دیگری با معرفی مفاهیمی مانند DS RECORD و NSEC در سال ۲۰۰۲ و ۲۰۰۳ به وجود آمد تا این مشکلات را حل کند.

رکورد DS اثر انگشتی (Fingerprint) از کلید عمومی (Public Key) کارگزار زیردست است که در اختیار کارگزار سرپرست قرار می‌گیرد.

همچنین هر نام دامنه دارای رکورد NSEC شامل نام دامنهٔ بعدی (به ترتیب حروف الفبا) می‌باشد که برای برطرف شدن مشکل اعتبار «پاسخ عدم وجود» به کار می‌رود. پس اگر از کارگزار نام دامنه‌ای درخواست شود که وجود ندارد، نام دامنهٔ بعدی آن (به ترتیب حروف الفبا) به عنوان مدرک صحت پاسخ در اختیار کاربر قرار می‌گیرد.

اولین مرکز ثبتی که این قرارداد DNSSEC را پیاده‌سازی کرد، مرکز ثبت دامنهٔ کشوری se. (سوئد) (در سال ۲۰۰۵) بود. امروزه مراکز ثبت دامنه‌های کشوری br. (برزیل)، bg. (بلغارستان)، cz. (جمهوری چک) و pr. (پورتوریکو) نیز از این نسخه DNSSEC استفاده می‌کنند.

مشکلی این نسخه از DNSSEC این است که فهرست نام‌های دامنه‌های یک کارگزار با استفاده از پیمایش رکوردهای NSEC به راحتی در اختیار عموم قرار می‌گیرد. برای رفع این مشکل، در قرارداد جدید رکوردی به نام NSEC3 معرفی شده است که به جای نام دامنهٔ بعدی، نام کدشدهٔ عددی آن قرار می‌گیرد که قابل استفادهٔ نامناسب نمی‌باشد.

سامانهٔ آزمایشی DNSSEC در ایرنیک

در سامانهٔ آزمایشی DNSSEC در ایرنیک از نسخهٔ دوم قرارداد استفاده می‌شود، که تحت دامنهٔ dnssec.ir پیاده‌سازی شده و در دسترس خواهد بود. ثبت زیردامنه‌ها تحت دامنهٔ dnssec.ir (برای مثال، example.dnssec.ir) برای استفادهٔ آزمایشی برای کاربران ممکن می‌باشد. در مرحلهٔ بعدی این طرح، تمامی نام دامنه‌های ir. به صورت فراگیر از طریق قرارداد DNSSEC در دسترس قرار خواهند گرفت.

کلیدهای DNSSEC

هر کارگزار مرجع DNS که سرویس دهی یک Zone را بر عهده دارد، برای اثبات اعتبار خود در شبکه احتیاج به یک کلید دارد. این کلید با الگوریتمهای مختلف با استفاده از دستوراتی که در زیر توضیح داده می‌شود به وجود می‌آید و کل محتویات Zone را امضا می‌کند (Sign) . برای اینکه کارگزار سرپرست (Parent Server) صحت اعتبار کارگزار فوق را تائید کند باید کلید آن را در اختیار داشته باشد.

تنها دلیل پیدایش DNSSEC ایجاد امنیت در کارگزارهای DNS بوده است و چون یک کلید ثابت می‌تواند امنیت کارگزار را تهدید کند ، لازم است این کلید با روند مشخصی تغییر پیدا کند. ولی با تغییر کلید لازم است کل اطلاعات Zone مجددا با کلید جدید امضا شود و همچنین کارگزار سرپرست باید کلید جدید را جایگزین کلید قبلی بکند که روند وقت‌گیری است ، به همین دلیل برای امضا کردن یک Zone دو کلید مجزا تعریف می‌شود. کلید اول با نام (Zone Signing Key) ZSK برای امضا کردن اطلاعات موجود در Zone مانند رکوردهای A و CNAME و ... به کار می‌رود و کلید دوم به نام (Key Signing Key) KSK برای امضا کردن کلیدهای موجود در فایل Zone یعنی رکوردهای DNSKEY به کار می‌رود.

چون کلید ZSK امضا کردن اطلاعات اصلی Zone را بر عهده دارد برای امنیت بیشتر لازم است هر چند ماه تغییر یابد و چون روند ساختن کلید جدید و امضا کردن Zone بسته به سایز کلید زمان زیادی می‌خواهد به همین دلیل این کلید کوچک در نظر گرفته می‌شود (معمولا ۵۱۲ بیت).

کلید KSK همان طور که گفته شد کلیدی است که برای تایید هویت کارگزار، باید به کارگزار سرپرست داده شود، به همین دلیل تغییر آن بهتر است به صورت سالانه باشد. چون این کلید دیر به دیر تغییر می‌کند بهتر است سایز بزرگتری (معمولا ۲۰۴۸ بیت) داشته باشد. از آنجا که سایز بزرگی برای کلید KSK در نظر گرفتیم، بهتر است به جای خود کلید، امضای آن را در اختیار کارگزار سرپرست قرار دهیم که حجم کمتری دارد. به این امضا DS Record گفته می‌شود.

روند تهیه کلیدهای KSK و ZSK

نکته: دستورات استفاده شده در ادامه این راهنما در نسخه‌های جدید بسته نرم‌افزاری BIND قرار دارند.

برای تهیه کلید ZSK دستور زیر به کار می‌رود:

```
# dnssec-keygen [–a الگوریتم] [–b سایز] [–n نوع] [نام]
```

به عنوان مثال:

```
# dnssec-keygen –a RSASHA1 –b 1024 –n ZONE example.ir
```

توجه شود که برای امضا کردن یک Zone تنها می‌توان از الگوریتم RSASHA1 استفاده کرد که حداقل سایز مورد قبول آن ۵۱۲ بیت می‌باشد.

این دستور ۲ فایل با پسوندهای key. و private. ایجاد می‌کند که key. قسمت عمومی‌کلید است و private. قسمت خصوصی آن می‌باشد و هر دو برای امضا کردن zone مورد نیاز هستند.

برای تهیه کلید KSK دستور زیر به کار می‌رود:

```
# dnssec-keygen [–a الگوریتم] [-b سایز] [-n نوع] [-f KSK] [نام]
```

به عنوان مثال:

```
# dnssec-keygen –a RSASHA1 –b 2048 –n ZONE –f KSK example.ir
```

با دستور زیر کلیدها به فایل zone افزوده می‌شوند:

```
# cat Kexample.ir+*.key >> example.ir.db
```

تنظیمات کارگزاران (Servers Configurations)

در ادامه نحوهٔ تنظیم کارگزاران مرجع (Authoritative) و Resolver برای نرم‌افزارهای BIND (نسخهٔ ۹) و NSD (نسخهٔ ۳) در محیط‌های لینوکس/یونیکس (Linux/UNIX) توضیح داده شده است.

محیط ویندوز تنها از نسخهٔ اول قرارداد DNSSEC پشتیبانی می‌کند، و قادر به کارگزاری برای نسخه‌های دوم و سوم آن نمی‌باشد.

تنظیمات کارگزار مرجع در BIND9

مرحله اول : فعال سازی پشتیبانی از DNSSEC

در فایل named.conf.option و در قسمت options عبارات زیر مورد نیاز است :

```
options {
     dnssec-enable yes;
};
```

مرحله دوم : امضا کردن فایل Zone

با اجرای دستور زیر Zone امضا می‌شود:

```
# dnssec-signzone [–o نام] [-k KSK آدرس کلید] [آدرس فایل zone] [آدرس فایل ZSK]
```

به عنوان مثال:

```
# dnssec-signzone –o example.ir –k KSK Kexample.ir+005+11111.key  example.ir.db Kexample.ir+005+22222.key
```

این دستور ۳ فایل ایجاد می‌کند. مهمترین آنها پسوند signed. دارد که فایل جدید Zone ما می‌باشد.

در named.conf باید عبارت زیر را با شکل جدید آن جایگزین کنیم :

```
zone “example.ir” {
     file “.../example.ir.db”                    قدیم
}


zone “example.ir”{
     file “.../example.ir.db.signed”             جدید
}
```

مرحله سوم: بارگزاری مجدد

برای بارگزاری مجدد BIND دستور زیر را اجرا کنید:

```
# /etc/init.d/bind9 restart
```

اکنون کارگزار DNSSEC آماده است.

مرحله چهارم: واگذاری DS Record به کارگزار سرپرست

برای اینکه کارگزار سرپرست (در این مثال ir.) هویت کارگزار example.ir را تائید کند لازم است DS Record این Zone در اختیار کارگزاران ir. قرار گیرد. پس از تهیهٔ کلیدها در مرحله قبل، فایلی به نام dsset-example.ir ساخته شده است که حاوی DS Record این Zone می‌باشد. این رکورد را باید در اختیار کارگزار سرپرست قرار داد.

تنظیمات کارگزار مرجع NSD3

در قسمت بالا تنظیمات کارگزار BIND را برای سرویس‌دهی DNSSEC شرح دادیم و اکنون به چگونگی تنظیم NSD می‌پردازیم.

در فایل nsd.conf تغییر زیر را انجام می‌دهیم:

```
zone:                                   قدیم
name: example.ir
zonefile: /etc/nsd/example.ir.db


zone:                                   جدید
name: example.ir
zonefile: /etc/nsd/example.ir.db.signed
```

در فایل nsd.zones هم تغییر زیر را اعمال می‌کنیم:

```
zone example.ir  /etc/nsd/example.ir.db             قدیم


zone example.ir  /etc/nsd/example.ir.db.signed      جدید
```

اکنون با اجرای دستور nsdc rebuild فایلها را جایگزین می‌کنیم. سپس با استفاده از دستور nsdc restart کارگزار را دوباره بارگزاری می‌کنیم.

در آخر لازم به ذکر است اگر در پیاده سازی شما مشکلی ایجاد شود می‌توانید از طریق فایل موجود در آدرس /var/log/daemon.log یا /var/log/syslog/ آن را مشاهده و برطرف کنید.

تذکر مهم: فایل Zone باید هر ۳۰ روز یک بار امضا شود ، در غیر این صورت کارگزار از حالت معتبر خارج خواهد شد.

تنظیمات کارگزار Resolver

تنظیمات زیر برای اضافه نمودن قابلیت پشتیبانی از DNSSEC در کارگزارهای resolver کـه از نـرم افـزار Bind اسـتفاده می‌کنند می‌باشد.

در فایل named.conf.option تغییرات زیر مورد نیاز است:

```
options {
     dnssec-enable yes;
     dnssec-validation yes;
}
```

حال کلید عمومی KSK کارگزار example.ir را اینگونه به named.conf اضافه می‌کنیم:

```
trusted-keys {
     "example.ir." 257 3 5
        "AQPJO6LjrCHhzSF9PIVV7YoQ8iE31FXvghx+14E+jsv4uWJR9jLrxMYmsFOGAKWhiis832I
        SbPTYtF8sxbNVEotgf9eePruAFPIg6ZixG4yMO9XGLXmcKTQ/cVudqkU00V7M0cUzsYrhc4g
        PH/NKfQJBC5dbBkbIXJkksPLvFe8lReKYqocYP6Bng1eBTtkA+N+6mSXzCwSApbNysFnm6yf
        ";
};
```

و BIND را دوباره بارگزاری می‌کنیم.

آزمایش صحت تنظیمات کارگزاران

اکنون برای آزمایش تنظیمات فوق از دستور dig استفاده می‌کنیم که پاسخ آن باید به شکل زیر باشد:

```
# dig @localhost +dnssec example.ir.

; <<>> DiG 9.4.2-P2 <<>> @localhost +dnssec example.ir.
```

```
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56868
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1


;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;example.ir. IN A


;; ANSWER SECTION:
example.ir.  96221 IN A 192.168.1.2
example.ir.  96221 IN RRSIG A 5 4 172800 20050528153354 (
     20050428153354 3149 example.ir.
     RTDXj2ZrDAzW4XZgR6nNovArIAt0MbhxNHjDgce84VzN
     y5sSgg8DNizmvw9zRZd73p1lFkmTTb79RQTKcmhHPLeV
     YEXl8kaKl3vkN+ObbeOlbl8ONHKNP8IUeFZJRY/du47z
     /Ao7dJ6IoZLI9Mf0LUGHffRQFc4BCJwcFrgPcUzWR+jO
     5f0nMkh5c1RDZsCndl343NfjReQz8S/fWe3m9aXDjNhs
     seM4BVI2lGssFLoWjcHb3+GsshIu6ErOQtxSw10TRuBM
     83BdwSOfRRdK8XXKRieOMS3+WammFJGpIY4nHapCopXG
     4OkpmqS94ImIdBt8psZaBiTC6Ga5ayOSMA== )


;; Query time: 8 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Apr 29 14:55:57 2005
;; MSG SIZE rcvd: 369
```

بیت **ad** در قسمت flags نشان‌دهندهٔ معتبر بودن پاسخ است.

برطرف کردن مشکلات

در این قسمت مشکلاتی که ممکن است در پیاده سازی با آن روبه‌رو شوید را مورد بررسی قرار می‌دهیم. در صورتی که در روند اجرای کارها هیچ مشکلی وجود نداشته باشد، با اجرای دستور زیر خروجی مطلوب به این صورت خواهد بود:

```
# dig example.ir a
;; [..] status: NOERROR
;; flags: qr rd ra;
```

بهترین پاسخی است که به این عبارت داده می‌شود، qr به معنی پاسخ، rd به معنی نیاز به recursion و ra به معنی وجود امکان recursion است. اما برای تست معتبر بودن پاسخ عبارت زیر مورد نیاز است:

```
# dig example.ir +dnssec a

;; [..] status: NOERROR
;; flags: qr rd ra ad
```

که **ad** به معنی معتبر بودن پاسخ است.

اکنون به بررسی مشکلات احتمالی می‌پردازیم.

عدم نمایش بیت ad

اگر در پاسخ RRsigها نمایش داده شوند ولی بیت ad ایجاد نشود یعنی کارگزار DNSSEC وجود دارد ولی کلیدهای کارگزاران سرپرست (Trust Anchors) به درستی تنظیم نشده است و یا وجود ندارد. پس باید کلیدهای موجود در تنظیمات named.conf مورد بررسی قرار گیرند و اگر کلیدی وجود ندارد ایجاد شود.

```
example.ir. 3600 IN A 192.168.1.2
example.ir. 3600 IN RRSIG A 5 3 3600 20080627122225
20080617122225 46704 example.ir.
```

```
XEkXkv9MCRiGbxO9T0dkNY+3y5EZRB6s6YOk0pFAVUL/y8VDeJphc8yb
K6E/YLvraItdGvIvpy4P1OuIY09BGQ==
```

وضعیت servfail در dig: مشکل در RRSig

اگر مطمئن هستیم که کارگزار ما برای سرویس‌دهی DNSSEC آماده شده است ولی dig حالت servfail دارد، پس ممکن است رکوردهایی وجود داشته باشند که به درستی امضا نشده‌اند. با اضافه کردن عبارت cd+ به دستور می‌توانیم از dig بخواهیم که داده‌ها را هر طور که هستند به ما نمایش بدهد.

```
# dig +dnssec +cd example.ir a
example.ir. 3600 IN A 192.168.1.2
example.ir. 3600 IN RRSIG A 5 3 3600 20080627122225
20080617122225 46704 example.ir. XXXXXXXXXX
```

در عبارت بالا رکورد RRsig نادرست است و با چند X نمایش داده شده است. برای برطرف کردن این مشکل بایـد Zone را مجدداً و با کلید صحیح امضا کنیم.

وضعیت servfail در dig: مشکل در تاریخ امضا

عبارات زیر همان طور که مشاهده می‌شود نشان می‌دهد که تاریخ امضا کردن Zone گذشته است و باید مجددا امضا شود.

```
# dig +dnssec +cd example.ir a
example.ir. 3600 IN A 192.168.1.2
example.ir. 3600 IN RRSIG A 5 3 3600 20080727122225
20080717122225 46704 example.ir.
XEkXkv9MCRiGbxO9T0dkNY+3y5EZRB6s6YOk0pFAVUL/y8VDeJphc8yb
K6E/YLvraItdGvIvpy4P1OuIY09BGQ==
```

وضعیت servfail در dig: مشکل در رکورد DNSKEY

ممکن است مشکل از DNSKEY باشد. برای تشخیص این مشکل، آزمایش زیر را انجام می‌دهیم:

```
# dig +dnssec +cd example.ir
example.ir. 3600 IN A 192.168.1.2
example.ir. 3600 IN RRSIG A 5 3 3600 20080627122225
20080617122225 46704 example.ir.
XEkXkv9MCRiGbxO9T0dkNY+3y5EZRB6s6YOk0pFAVUL/y8VDeJphc8yb
K6E/YLvraItdGvIvpy4P1OuIY09BGQ==
```

همان طور که مشاهده می‌کنیم عبارت بالا امضای یک کلید با شناسه 46704 را نشان می‌دهد. با اجرای دستور زیر شناسه کلید را بررسی می‌کنیم:

```
# dig +cd +multi example.ir dnskey
example.ir. 14400 IN DNSKEY 256 3 5 (
BEAAAAO2oQi7U9m9i495S/XoAk+j8QxxnBHon6fa7nlN
7xoqrSr/xzy3+IerFS1KgJz1gJGbTsGV0WI1/bvAzIEK
Uh+p ) ; key id = 46704
```

مشاهده می‌کنیم که Key ID با شناسه امضای آن یکی است ، پس در این مثال کلید ما درست تنظیم شده است . در صورتی که این اعداد هم‌خوانی نداشته باشند مشکل ما از کلید خواهد بود و باید Zone را با کلید درست امضا کنیم.

وضعیت servfail در dig: مشکل در DS Record

با اجرای دستور زیر صحت DS Record را بررسی می‌کنیم:

```
# dig +norec @localhost example.ir ds
;; >>
HEADER<<opcode:
QUERY, status: NOERROR, id: 29385
```

```
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2
```

مشاهده می‌کنیم که DS Record در کارگزار سرپرست وجود ندارد و دلیل مشکل همین جاست و باید آن را در اختیار کارگزار سرپرست قرار دهیم.

نکات قابل توجه

- اگر کارگزار DNS پشت دیوار آتشین قرار دارد که جلوی عبور بسته‌های (E)DNS بزرگتر از ۵۱۲ بایت را می‌گیرد،باید تنظیمات دیوار آتشین خود را تصحیح کنید و سپس اقدام به ایجاد کلیدهای DNSSEC نمایید.

اطلاعات لازم

کلید عمومی KSK کارگزار dnssec.ir

```
"dnssec.ir." IN DNSKEY 257 3 5
    "AwEAAZz0N4mQylmksechdvqmnZv3U7oqVrgLwV1QdHb8FKrto12FVKxR
     uRnA7JpHylByAtoBCEPq4GbVxjeuTBnVlmkc4eGiLQvQz5RgMTG9UhHe
     nIhDk5UDC+rH6jbc9KU2txOvjKp4CReBPgrrpK3SdncvvjcKVUpNiWsa
     2oluSIvmg3cnlESUf89SwDrjQG+XhB/uCKolFvRcS55wlwvcmE+Bd/8A
     S4l0nb5f8MRxqKRFrwsiaWrwg4yBlDVdsReM0RvS2TIXvXEUgGNZNAon
     Ta7ltpk5p/7TryPXNHeutQljWElqCq3xRFBRPumdh7PeCSm3E1+eA2cq
     bzNorxkfkXM=";
// Key ID= 18043
```