สร้างความปลอดภัย DNS ของท่านด้วย DNSSEC เพื่อป้องกันการทำงานผิดพลาด

สุชิน เขียวเนตร : เขียน
Mr.Suchin Keawnet
นักวิชาการคอมพิวเตอร์

IC3, MOS 77-881, MOS 77-882, MOS 77-883
suchin@psru.ac.th

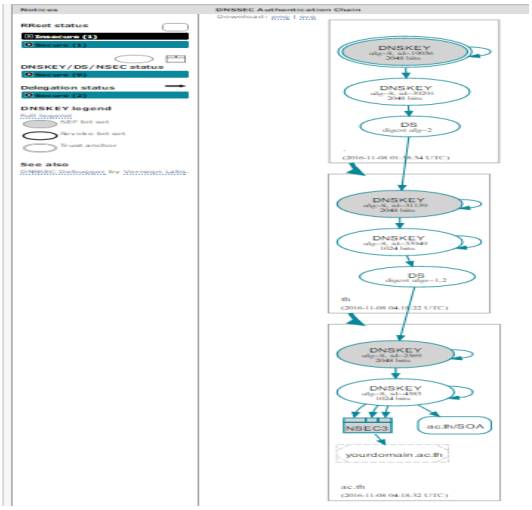
การโจมตี DNS เป็นอีกกระบวนการหนึ่งของผู้ไม่ประสงค์ดีเพื่อทำลายความมั่นคงของระบบเครือข่ายและเพื่อให้เกิดการทำงานผิดพลาด และที่ร้ายแรงหนักที่สุดคือการยึด Domain เพื่อเรียกค่าไถ่ สำหรับบทความนี้จะขอแนะนำการป้องกัน Domain ของเราถูกรบกวน ด้วย DNSSEC : Domain Name System Security Extensions

DNSSEC เป็น Options หนึ่งของ DNS (Domain Name System) เพื่อป้องกันผู้ใช้ (end user) จากการเข้าถึงข้อมูลที่ถูกบิดเบือนจากปลายทางของผู้ไม่ประสงค์ดี DNSSEC จึงมีบทบาทในการเพิ่มความปลอดภัยให้แก่ระบบ DNS ซึ่งทั่วไปแล้วจะมีความเสี่ยงจากการที่อาจจะถูก HACKER หรือผู้ไม่ประสงค์ดีรบกวนกระบวนการทำงาน จุดประสงค์คือ เพื่อลักลอบแทรกแซงกระบวนการทำงานของ Name Resolution ซึ่งเป็นกระบวนการถามตอบระหว่าง Client กับ Name Server เพื่อสืบค้นชื่อโดเมนในระบบ (Domain space) ผ่านทางการทำงานของตัว Resolver ระหว่าง Name server ตัวหนึ่งกับ Name server ตัวอื่นๆ ภายในระบบโดเมน ทำการให้ Resolver ได้รับคำตอบของที่อยู่ปลายทางที่บิดเบือนอันนำไปสู่การแสดงผลที่ช้าลง หรือเข้าเว็บไซต์อื่นที่ ผู้แทรกแซงเตรียมไว้

ที่ในท้ายที่สุดอาจสร้างความเสียหายแก่ผู้ใช้ได้ในหลายรูปแบบ เช่น ส่งผลให้ User หลงเข้าไปยังเครื่องคอมพิวเตอร์ที่ไม่ใช่เครื่องจริง ซึ่งอาจเป็นเครื่องที่ผู้ไม่ประสงค์ดีตั้งใจวางไว้หลอกเก็บข้อมูลที่สำคัญ เช่น ข้อมูลเกี่ยวกับบัญชีธนาคาร, บัตรเครดิต หรือ password เป็นต้น

DNSSEC ทำงานอย่างไร

DNSSEC จัดให้มีกระบวนการตรวจสอบคำตอบที่ Resolver ได้รับมา จาก NS (Name Server) ที่เป็นปลายทางว่าเป็นตัวจริงหรือไม่ โดยกระบวนการที่ Resolver จะรับจากหมายเลข IP จาก NS ปลายทางที่จะเป็นผู้ตอบ และจะดำเนินการโดยใช้ระบบคู่กุญแจแบบ asymmetric key ที่ประกอบไปด้วย private key และ public key โดเมนภายใต้บริการ DNSSEC ใช้วิธีการเข้ารหัสแบบ อสมมาตร หรือการเข้ารหัสแบบ Public-key (Asymmetric Encryption หรือ Public-key Encryption) เป็นอัลกอริทึมแบบ RSASHA1 โดยจะถูกใส่รหัสลับด้วย private key จากทาง Registry ที่ดูแลฐานข้อมูลของโดเมนนั้นๆ เข้ารหัส zone ข้อมูลโดเมนภายใต้ ดอท (.) ที่ Registry นั้นๆดูแลอยู่ และจะแจกจ่าย public key สำหรับการเข้าถึงโดเมนภายในโซนที่ได้รับการเข้ารหัสอีกที Resolver ที่เป็น DNSSEC-awear จะมี public key สำหรับตรวจสอบความถูกต้องของโดเมนปลายทางที่มีการใช้บริการ DNSSEC ด้วยการเข้าคู่กับ private key



ที่มาภาพตัวอย่าง DNSSEC

สร้างความปลอดภัย DNS ของท่านด้วย DNSSEC เพื่อป้องกันการทำงานผิดพลาด

กระบวนก่อนอื่นต้อง config DNS ให้ทำงานได้เสียก่อนตามกระบวนการ การทำ DNS โดยตัวอย่างใช้ bind99 บนระบบปฏิบัติการ Freeebsd10.1 ที่ config DNS ทำงานมาเรียบร้อยแล้วและทำงานได้เป็นปกติ ส่วนนี้คือส่วนเพิ่มเติมจากการทำ DNS เป็น DNSSEC
โดยมีไฟล์ที่เกี่ยวข้องดังนี้

named.conf ไฟล์ เก็บ config ปรับแต่ง bind99
192.168.1.0 ไฟล์เก็บ Zone forward maping
db.yourdomain.ac.th ไฟล์เก็บ Zone reward maping

ให้ทำการปรับแต่งไฟล์เหล่านี้ตามขั้นตอนดังนี้

1. แก้ไข ไฟล์ named.conf เพื่อเพิ่ม Options ให้ DNS สมารถใช้งาน DNSSEC ได้

```
Options {
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside . trust-anchor   yourdomain.ac.th.;
```

2. สร้าง file key

การสร้าง file key เพื่อสร้าง Zone Signing Key(ZSK) สำหรับไว้ใช้ Key ในการลงทะเบียน Zone และ Key Signing Key (KSK) เพื่อใช้ในการสร้าง Key Signing สำหรับลงทะเบียนคีย์(รวม 2 Key)

2.1 **การสร้าง Key Signing สำหรับลงทะเบียนคีย์**

ให้ทำการสร้าง Zone Signing Key (ZSK) สำหรับลงทะเบียน Zone ส่วนมากจะใช้ Zone Forward Mapping (Zone แปลงชื่อ Domain เป็น IP Address) มาทำการสร้าง Key

```
# cd /usr/local/etc/namedb/master
# dnssec-keygen -r/dev/random  -a RSASHA1 -b 1024 -n ZONE   yourdomain.ac.th
หากต้องการทั้งสอง Zone ให้สร้างคีย์สำหรับ Reword Mapping ด้วยคำสั่ง
# dnssec-keygen -r/dev/random  -a RSASHA1 -b 1024 -n ZONE 192.168.1.0
```

ตัวอย่าง ได้ผลเป็น Kyourdomain.ac.th.+005+64092 ชื่อของคีย์ Random เรื่อยๆ ขึ้นอยู่กับรูปแบบของ Algorithm และเวลาของการการสร้างจาก
คำสั่งดังกล่าวจะได้ไฟล์ Kyourdomain.ac.th.+005+64092.key และ Kyourdomain.ac.th.+005+64092.private
สำหรับลงทะเบียนโซน Reverse Mapping (Zone แปลงIP Address เป็นชื่อ Domain)

ตัวอย่าง ได้ผลเป็น K192.168.1.0.+005+59163
ได้ไฟล์ K192.168.1.0.+005+59163.key และ K192.168.1.0.+005+59163.private
แต่จากการทำงานใช้ Zone เดียวก็เพียงพอแล้ว

2.2. การสร้าง Key สำหรับลงทะเบียน Key

Creating the KSK สร้างกุญแจสำหรับอัปเดตโซน

```
# dnssec-keygen –r /dev/random  -f KSK -a RSASHA1 -b 4096  -n  ZONE   yourdomain.ac.th
หากต้องการทั้งสอง Zone ให้สร้างคีย์สำหรับ Reword Mapping ด้วยคำสั่ง
# dnssec-keygen –r /dev/random -f KSK -a RSASHA1 -b 4096 -n ZONE 192.168.1.0
#cd ..
```

ตัวอย่าง ตัวอย่าง ได้ผลเป็น Kyourdomain.ac.th.+005+30799 ได้ไฟล์ Kyourdomain.ac.th.+005+30799.key และ Kyourdomain.ac.th.+005+30799.private

สร้างความปลอดภัย DNS ของท่านด้วย DNSSEC เพื่อป้องกันการทำงานผิดพลาด

สำหรับลงทะเบียนโซน Reverse Mapping (Zone แปลงIP Address เป็นชื่อ Domain)
ตัวอย่าง ได้ผลเป็น K192.168.1.0.+005+42013 ได้ไฟล์ K192.168.1.0.+005+42013.key และ K yourdomain.ac.th.+005+30799.private

3. เพิ่ม Key ลงไปในระบบ Zone file

```
# cd /usr/local/etc/namedb/master
# pico db. yourdomain.ac.th
$include Kyourdomain.ac.th.+005+64092.key; ZSK
$include Kyourdomain.ac.th.+005+30799.key; KSK
```

4. สร้าง Sign Zone

```
# dnssec-signzone –o yourdomain.ac.th. db. yourdomain.ac.th
```

เราจะได้ ไฟล์ db.yourdomain.ac.th.signed และ dsset-yourdomain.ac.th. มา ไฟล์ db.yourdomain.ac.th.signed คือไฟล์ Zoneที่ถูกเข้ารหัสความปลอดภัยแล้ว และไฟล์ dsset-yourdomain.ac.th. คือไฟล์เก็บ key ที่จะเอาไปใส่ใน THNIC ช่อง DNSSEC

5. แก้ไข named.conf

```
# cd /usr/local/etc/namedb
# pico named.conf
```

จาก

```
Zone “ yourdomain.ac.th” {
file “yourdomain.ac.th”;
};
```

เป็น

```
Zone “yourdomain.ac.th” {
file “yourdomain.ac.th.signed”;
};
```

stop และ start Service named อีกครั้ง

```
#/usr/loval/etc/rc.d/named restart
```

6. การทดสอบด้วยคำสั่ง dig

```
#dig @192.168.1.225 yourdomain.ac.th. DNSKEY +dnssec +multiline
```

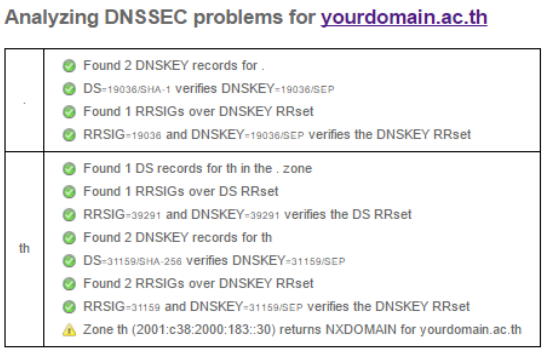
จะได้ผลข้อมูลประมาณดังภาพ

```
root@bsd16:/usr/local/etc/namedb # dig @192.168.1.225 yourdomain.ac.th. DNSKEY +dnssec +multiline
; <<>> DiG 9.9.6 <<>> @192.168.1.225 yourdomain.ac.th. DNSKEY +dnssec +multiline
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47360
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
; yourdomain.ac.th. IN DNSKEY
```

สร้างความปลอดภัย DNS ของท่านด้วย DNSSEC เพื่อป้องกันการทำงานผิดพลาด

```
;; ANSWER SECTION:
 yourdomain.ac.th.          3600 IN DNSKEY 256 3 5 (
                            AwEAAcSLO4znIPXfcwmcrRvZWVJJiX6Ag5GlXJ//fSBG
                            ubdA1EW5Tgz3kshGDWeh7KQAo/54qA3B8L/QXGMAeKzl
                            h1ADo9eFiSfd47XW+lavzxTXXm1FpHHMyhVL1DDLiCxq
                            pwhLq4BiABvuFl8HOR6T70zDsOTprAagzWNYHRtp5drH
                            ) ; ZSK; alg = RSASHA1; key id = 5355
 yourdomain.ac.th.          3600 IN RRSIG DNSKEY 5 3 3600 (
                            20151008094609 20150908094609 5355   yourdomain.ac.th.
                            qo+257GDLjWyuqP+2wGbV806Tww/2Lu3HqnLshnSq/Zi
                            bsWI7lf3FCt4BH5i2acuZFJz+w6llUswcvkdTd1SYfQJ
                            vgMEzVzMoRcTiNCINiNFBptD1W6USZETzgUtGReqtTPf
                            bE4WMoaQq3kI6ZcaHns83MCNE9Y/tLOtTKKfpdo= )
 yourdomain.ac.th.          3600 IN RRSIG DNSKEY 5 3 3600 (
                            20151008094609 20150908094609 7177   yourdomain.ac.th.
                            jLYJctUE/z5MKfOotDPy1IkpVUA5DHNIPyuYtYRGw/Er
                            /7IQrbxU+Eo98fwYkVnL7uocCCLAr5a2xmdifm1AKltN
                            YX+Ebm/MG1om0xpKtyZjxd2l9CQz/W01RLYzNl3WfVtj
                            GdvEHVMKovo1IREDkCq3zLVlkMewt0H8QYqjmaCuWRpb
                            g4CtTswvGBrj/uF5BAiQDE/9f92P6Knuq+aWACrnnK7r
                            mGvkxQe5JFFjT2ivrXspKlYy3SkDnGLIT89JEglXg2OW
                            Ivo+5XQgMWCye/GCzEhpFxU= )
;; Query time: 0 msec
;; SERVER: 192.168.1.225#53(192.168.1.225)
;; WHEN: Tue Sep 08 17:55:17 ICT 2015
;; MSG SIZE  rcvd: 1449
```

ทดสอบจาก url http://dnsviz.net/d/yourdomain.ac.th/dnssec/



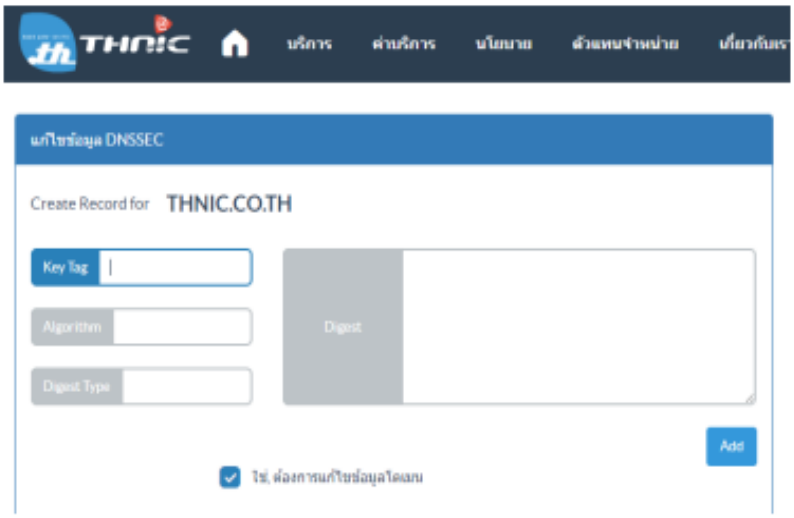
จะเห็นว่ายังไม่ผ่านยังอ่านผิด วิธีนี้แก้ไขได้โดยนำ DS Key (*Delegation Signe*) ไปใส่ที่ THNIC ให้นำ Key ที่ได้จากไฟล์ dsset-yourdomain.ac.th. ไปไปใส่ในระบบรับจด Domain ทั้ง 2 บรรทัด ตัวอย่างเช่น การลงทะเบียนที่ dnssec ที่ thnic.net

7. นำ Key ไปใส่ใน THNIC

ใช้คำสั่ง cat เพื่ออ่านข้อมูลที่อยู่ในไฟล์

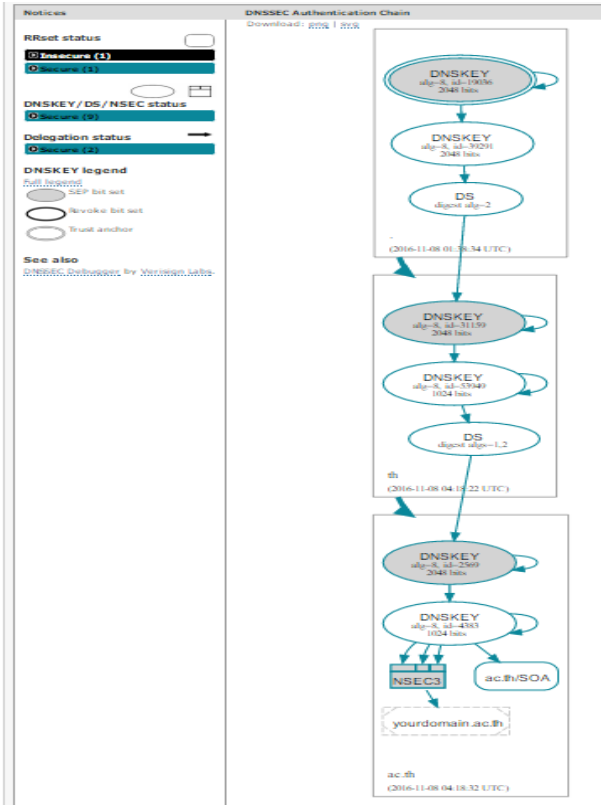
```
#cd /usr/local/etc/namedb
# cat dsset-yourdomain.ac.th.
 yourdomain.ac.th.   IN  DS  7177  5  1   9DA5F0184D641A0F5E7CB94A72A47068171AD016
 yourdomain.ac.th.   IN  DS  7177  5  2   4D23F85E9916D63E2463E9AD39352C26FCF92C2637916AF78BDFB168 ED069CC8
```

สร้างความปลอดภัย DNS ของท่านด้วย DNSSEC เพื่อป้องกันการทำงานผิดพลาด



ทดสอบจาก url http://dnsviz.net/d/yourdomian.ac.th/dnssec/ อีกครั้ง

สร้างความปลอดภัย DNS ของท่านด้วย DNSSEC เพื่อป้องกันการทำงานผิดพลาด

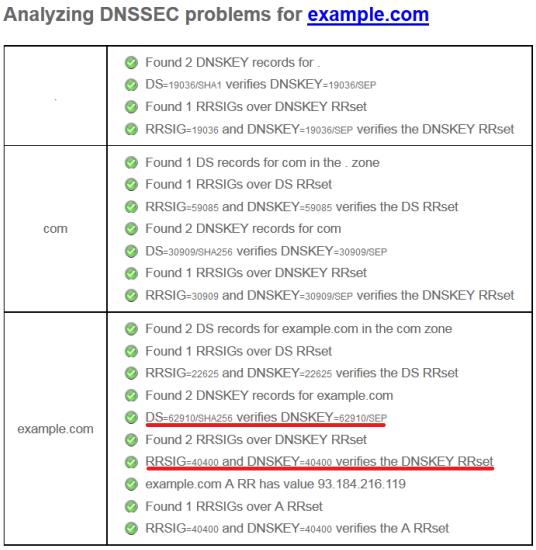


ทดสอบด้วยคำสั่ง dig @8.8.8.8 yourdomain.ac.th. DS อีกครั้ง คราวนี้ ใช้ dns google มาเป็นผู้ถาม

```
root@bsd16:/usr/local/etc/namedb/master # dig @8.8.8.8   yourdomain.ac.th.  DS
; <<>> DiG 9.9.6 <<>> @8.8.8.8   yourdomain.ac.th.  DS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26094
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;  yourdomain.ac.th.                IN      DS
;; ANSWER SECTION:
  yourdomain.ac.th.          IN DS 7177 5 1 9DA5F0184D641A0F5E7CB94A72A47068171AD016
  yourdomain.ac.th.          IN DS 7177 5 2 4D23F85E9916D63E2463E9AD39352C26FCF92C2637916AF78BDFB168
ED069CC8
;; Query time: 1258 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Sep 08 18:06:12 ICT 2015
;; MSG SIZE  rcvd: 123
```

เมื่อได้ผลประมาณนี้เป็นอันว่าเสร็จกระบวนการทำ DNSSEC ทดสอบ http://dnsviz.net/d/yourdomian.ac.th/dnssec/ คลิก debug ดูจะได้ผลพร้อมแสดง key ที่ถูกต้องคล้ายกันดังภาพ

สร้างความปลอดภัย DNS ของท่านด้วย DNSSEC เพื่อป้องกันการทำงานผิดพลาด



ที่มาของรูปภาพ https://www.digitalocean.com/community/tutorials/how-to-setup-dnssec-on-an-authoritative-bind-dns-server--2

คำแนะนำเพิ่มเติม

1. การที่ทำการสร้าง key แล้วเพิ่มเข้าไปในไฟล์ Zone แล้วแต่ไม่ทำงานให้ตรวจสอบดูว่า ไฟล์ key อยู่ใน Folder เดียวกันกับ ไฟล์ zone หรือไม่ ระบบจะไม่ทำงานหาก Permission ไม่ถูก การแก้ปัญหาที่ง่ายที่สุดสร้าง Key ไว้ใน Folder เดียวกัน
2. เนื่องจากว่า Key ของ DNSSEC มีอายุประมาณ 1 ปี ต้องมีการ Renew key ใหม่ ให้ดำเนินการในขั้นตอนข้อที่ 2,3,4,7 อีกครั้งและนำ DS key ไปใส่ในระบบรับจด Domain อีกครั้ง เช่น ตัวอย่างของ THNIC

แหล่งสืบค้นเพิ่มเติม :

1. https://nsrc.org/workshops/2013/nsrc-ait-th-dnssec/raw-attachment/wiki/Agenda/dnssec2013_sigchase_TH.pdf
2. http://www.thnic.co.th/th/dnssec
3. https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
4. https://www.digitalocean.com/community/tutorials/how-to-setup-dnssec-on-an-authoritative-bind-dns-server--2
5. http://dnsviz.net/doc/dnssec/
6.https://www.digitalocean.com/community/tutorials/how-to-setup-dnssec-on-an-authoritative-bind-dns-server—2

บริการบน: linux , FreeBSD , Unix services , Windows Server Services
Article number : 2016011090615