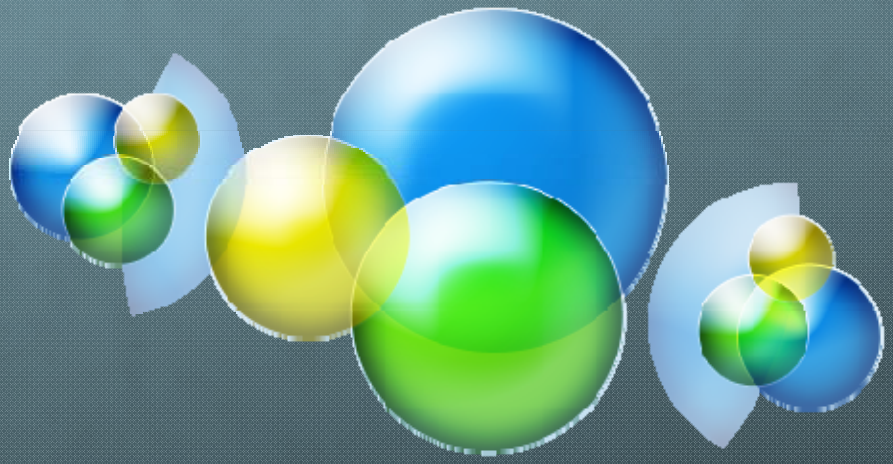

DNSSEC 建置經驗分享

Agenda

- About DNSSEC
- DNSSEC Authoritative Server 建置

About DNSSEC

- 傳統的DNS沒有安全機制，容易遭受攻擊
  - Spoofing
  - Man-in-the-Middle Attack
  - Cache Poisoning Attack
- 在解析網域名稱的過程中加上驗證的機制
- 當遇到DNS 請求時，會先回上層取得DNSKEY來做認證比對，確保解析網域名稱的過程是安全的，才能進行或回應下一步驟的DNS 請求

About DNSSEC

- Based on PKI (Public Key Infrastructure)
  - Public Key / Private Key
  - Hashing
  - Signature (數位簽章)
- 三大保證
  - 來源驗證性 (Origin Authentication)
  - 資料完整性 (Data Integrity)
  - 受驗證的不存在性 (Authenticated Denial of Existence)
- Resource Record : DS & RRSIG

DNSSEC Authoritative Server 建置經驗分享

- Platform : ubuntu 12.04 LTS
- Bind 9.8.1-P1
- Installation:
  - root@Ubuntu# aptitude install bind9 dnsutil
  - 安裝後會設定爲開機後自動啓動
- 系統預設安裝在 /etc/bind 下
- 修改組態檔 / 產生Key / 簽署Zone File / 維護

/etc/bind/named.conf

include “/etc/bind/named.conf.option”;

include “/etc/bind/named.conf.local”;

include “/etc/bind/named.conf.default-zone”;

named.conf.option

```
options {
        directory "/var/cache/bind";
        dnssec-enable yes;
        dnssec-lookaside auto;
        dnssec-validation auto;
        allow-query-cache { any; };
        allow-query { any; };
        recursion yes;
        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
        listen-on { any; };
}
```

named.conf.local

```
zone "tcrc.edu.tw." {
        type master;
        auto-dnssec maintain;
        update-policy local;
        file "/etc/bind/zone.tcrc.edu.tw.signed";
        key-directory "/etc/bind/dnskey";
        allow-transfer{
                163.28.82.5;
                163.28.80.3;
        };
        allow-query{
                any;
        };
};
```

產生Key

```
dnssec-keygen \
-a NSEC3RSASHA1 \
-b 2048 \
-f KSK \
-r /dev/urandom \
-K /etc/bind/dnskey \
tcrc.edu.tw
```

- -a 選擇金鑰演算法
- -b 設定金鑰長度
- -f 金鑰flag設定
- -r 亂數來源
- -K 金鑰儲存目錄

簽署網域

```
dnssec-signzone \
-3 57 \
-H 100 \
-K /etc/bind/dnskey \
-o tcrc.edu.tw \
-S \
-u \
-z \
/etc/bind/zone.tcrc
```

- -3 NSEC3使用的salt值
- -H NSEC3使用的iteration值
- -K 存放金鑰的資料夾
- -o 網域名稱
- -S Smart signing
- -u 更新NSEC/NSEC3
- -z 用KSK來簽署網域

驗證

- dig @ns1.tcrc.edu.tw +dnssec +multiline –t dnskey tcrc.edu.tw

```
;; ANSWER SECTION:
tcrc.edu.tw.            999999 IN DNSKEY 257 3 7 (
                                AwEAAa64DgNfJanLUbYTyqlxEK4lB5urFUdm/ZYqHbIb
                                DY0aVFiXH3Z2W0x56WMAdUHTkkr+x8JdFGrSnGKbW/Hw
                                nQ/F2rzoDqgU5eqR1KtqePQlNsXhwqxyR3kb06ob55pn
                                46HkinSx3K2aeKjym88aMJcaW7uTJW+4AEqpfFrKy+gx
                                6RJpjU3Ax3vBLKv3+Ngw3EC4fUdcU2HGJaluq09sj7fx
                                xx1h10oENfwdzHxF852Bl/yvW3GrXNRuPPsoiBgPx1Ar
                                M+jyI/VOFdOYJnd/h04QBaPFNSDKYvHpUMvLf2WE5Bkn
                                mNHbx1HOK5nFyX31rs5B4CwCWE2K3LZtxBrX+Dc=
                                ) ; key id = 45528
tcrc.edu.tw.            999999 IN RRSIG DNSKEY 7 3 999999 20121020012749 (
                                20120920012749 45528 tcrc.edu.tw.
                                drWP0d5mzKFgb524uMlSRk75CKhrefvG9J9f51KFcx/3
                                J9u0R+Dk9UdIoJePTTBkZN6+JzjPwxtRe4YLN8RXjvA1
                                XTvqL8webPgUdOwNYbc/yQZTL5X+NO1oaQ8bhN5HDiE/
                                ajdI5N5G2W/TUHuWvtvAaNFV+KhvaRH5Voic9ZTVLj1Q
                                UVty9Oh0n0tcJmXLEI3gFl6tjF096IAIt9ikcfNQdsGD
                                haCUSKh2iV/x9Kqi5slDI61vnqK8/YtIEyRylun7+A3/
                                Zw306reMmlWKsoLaEiwJ6Zz6sNfSFKeKZxQvoca88eEG
                                UgG1C0y0WW7cceeLW/xITkXQvjvW3/V30w== )
```

建立信任鏈

- 進入存放金鑰的目錄
- 輸入
  - **dnssec-dsfromkey Ktcrc.edu.tw.+aaa+bbbb**

```
root@ns1:/etc/bind/dnskey# dnssec-dsfromkey Ktcrc.edu.tw.+007+45528
tcrc.edu.tw. IN DS 45528 7 1 [redacted]
tcrc.edu.tw. IN DS 45528 7 2 [redacted]4
```

- 將**DS record**送交給**DNS**上層管理單位登錄

網域維護

- RR修改
  - 修改原始zone file (rndc freeze)
  - 凍結zone
  - 簽署zone file
  - 解凍zone使其生效 (rndc thaw)
- 退回DNS
  - 要求上層拿掉DS record

謝謝聆聽