HiNet DNS
DNSSEC

Fan-Chieh Lin
15th,4 ,2021

Agenda

I

Preparation

- Considerations?
- Preference?

II

Process

How to avoid

- service unavailability
- customer complaints

III

Status Quo

- summarized with screenshots

IV

Future

- technical issues
- practical issues

What we prioritize

availability

- HiNet DNS serves **3M+** users
  (and we answer calls)
- HiNet DNS is a national **CII**
  (Critical Information Infra.)

What we planned

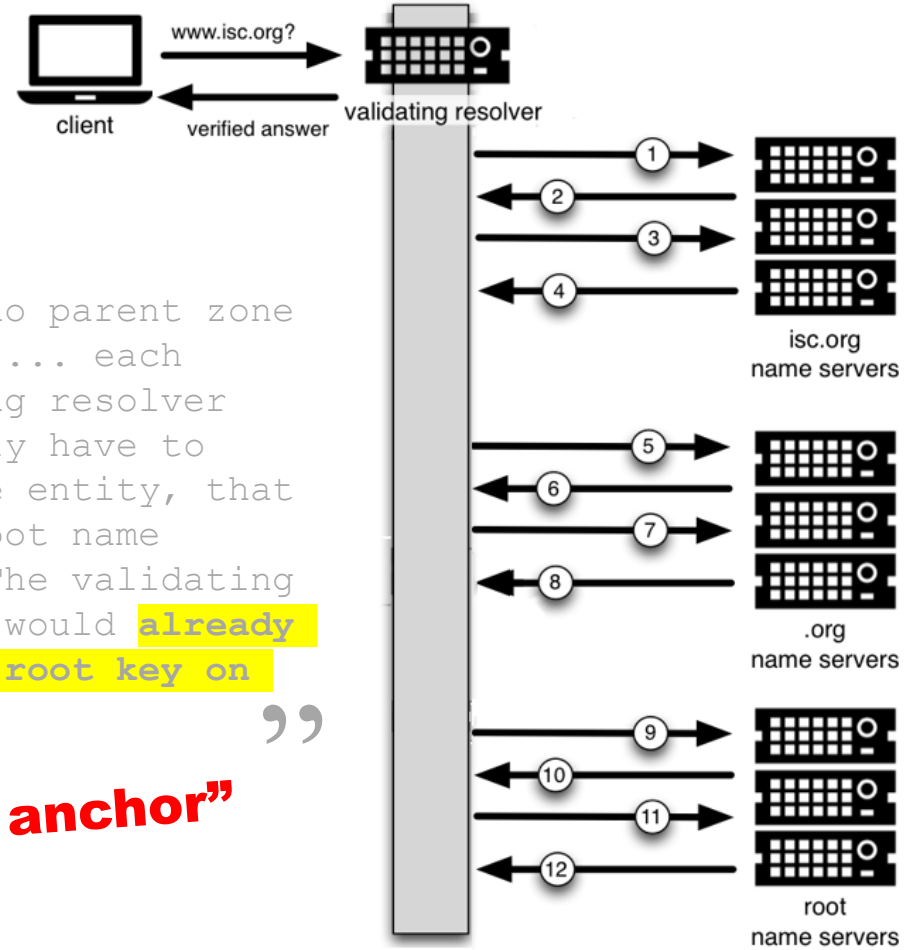
progressive

- to limit the risk of SERVFAIL
- to avoid massive complaint at once

edu.tw

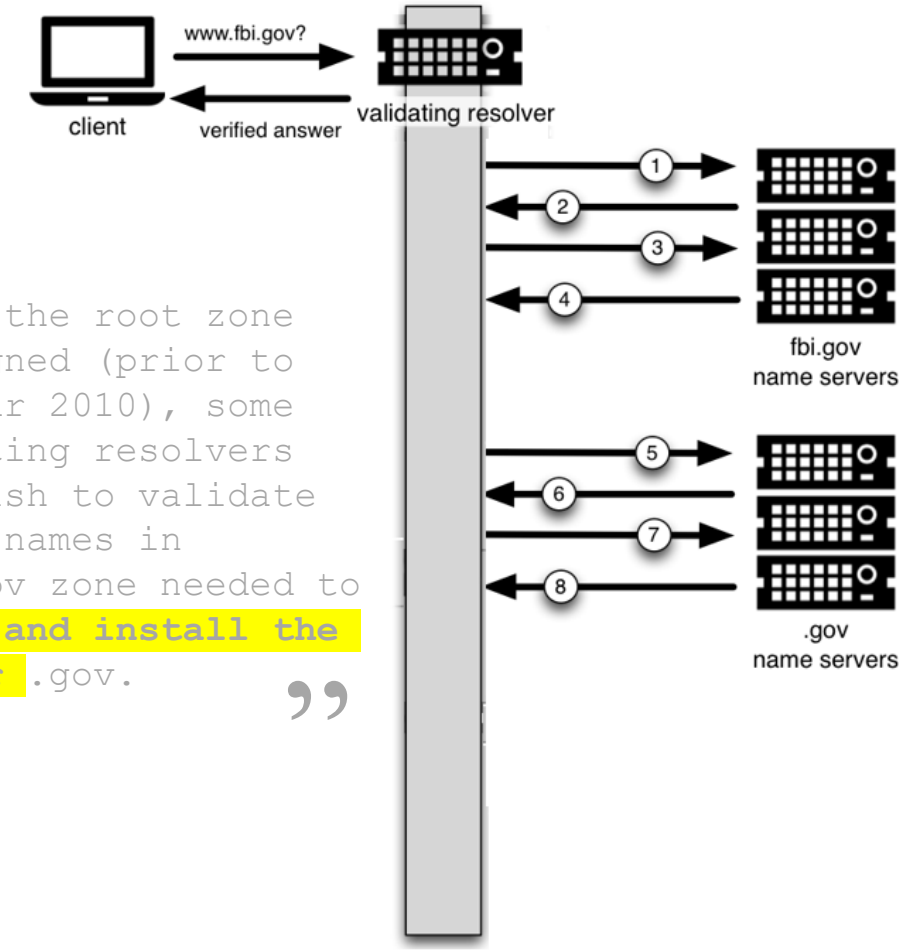
- better technical readiness
  (academic background)
- manageable number of domains
  (vs. com.tw for example)

How CHT Progressively Activate (DNSSEC Validation)



"There's no parent zone for root ... each validating resolver would only have to trust one entity, that is the root name server. The validating resolver would **already have the root key on file**."

"trust anchor"



"before the root zone was signed (prior to the year 2010), some validating resolvers that wish to validate domain names in the .gov zone needed to **obtain and install the key for** .gov."

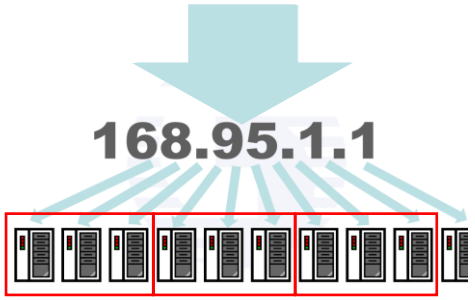
ISC BIND DNSSEC Guide
https://ftp.eenet.ee/pub/isc/dnssec-guide/html/dnssec-guide.html#trust-anchors

How CHT Progressively Activate (DNSSEC Validation)

Pre-assessment → execute → monitor (nervously)

- “manageable” domain count
  - traverse lookup possible
- as few [known DNSSEC-SERVFAIL-to-be] as possible

- rollback plan
- deploy in batches



- periodical lookup *(selected target)*
- alert if SERVFAIL

How CHT Progressively Activate (DNSSEC Validation)

edu.tw

```
C:\Users>dig @168.95.1.1 edu.tw soa

; <<>> DiG 9.12.3-P1 <<>> @168.95.1.1 edu.tw soa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14638
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

AD bit

```
C:\Users>dig @8.8.8.8 edu.tw soa

; <<>> DiG 9.12.3-P1 <<>> @8.8.8.8 edu.tw soa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10554
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

AD bit

com.tw

```
C:\Users>dig @168.95.1.1 com.tw soa

; <<>> DiG 9.12.3-P1 <<>> @168.95.1.1 com.tw soa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60681
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

~~AD bit~~

```
C:\Users>dig @8.8.8.8 com.tw soa

; <<>> DiG 9.12.3-P1 <<>> @8.8.8.8 com.tw soa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48888
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

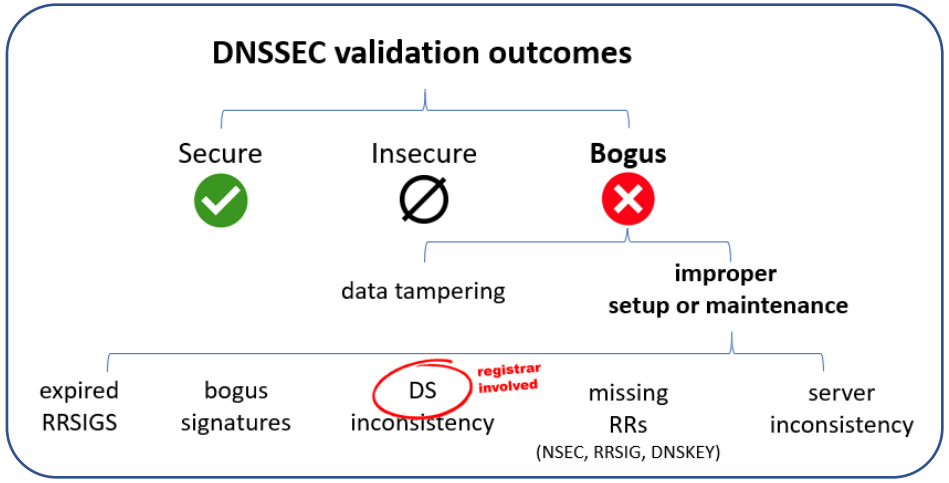
AD bit

Technical Issues

availability threat

- amplification **attack**
  (mitigation other than RRL?)

- more **complexity**



Practical Issues

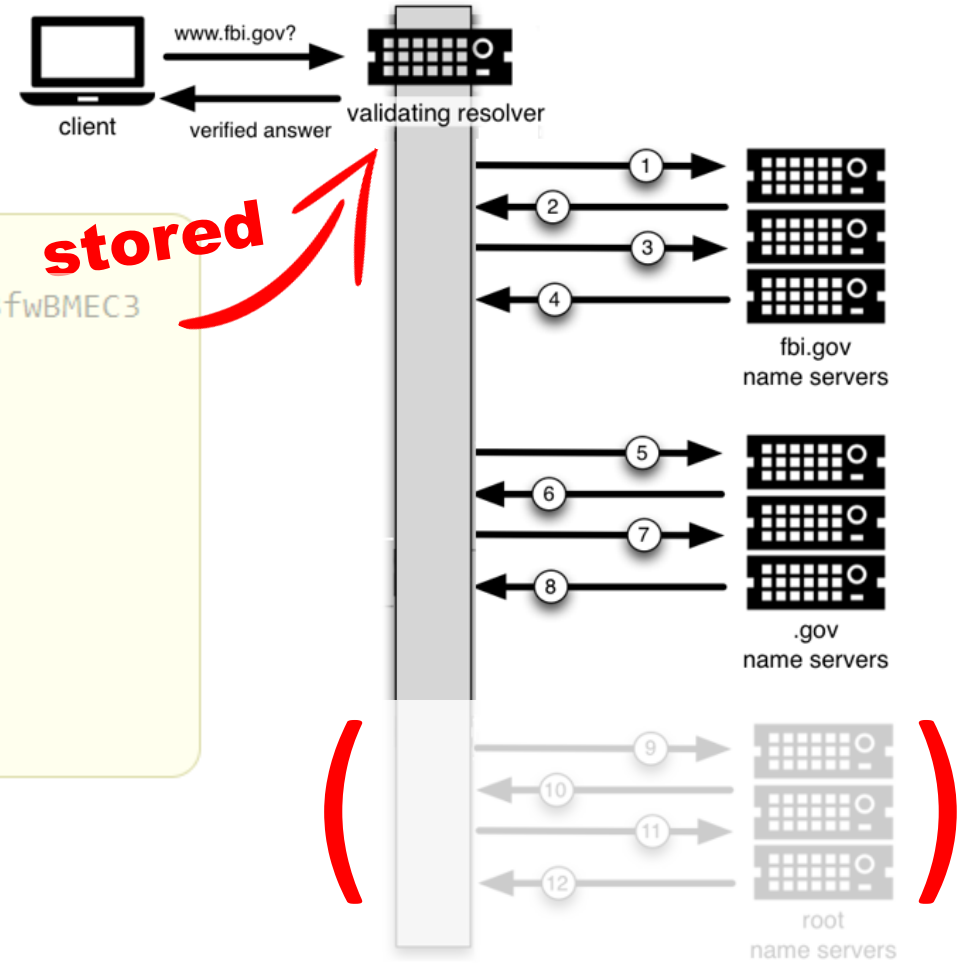
Cost

- more and better servers
  *(therefore more **investments**)*
- maintenance efforts
  - **trouble shooting**
    (expired or missing RRSIG, inconsistent DS …)
  - **explaining**
    (where the problem is & who should be responsible)
  - **monitoring**

credible & readable 3rd party check tool

Plans & Suggestions (about the “progressive activation”)

(trusted) key management



stored

change!

```
trusted-keys {
    gov. 257 3 8 "AQO8daaz7B+yshOfL60rytKd9aOSujgponEw3fwBMEC3
    /+e9XzHw2k+VKnbJTZ+QaVtpfUd1q9HKZIv/ck83Gl5T
    jYKE5jtUZ2kpEDZfVNGv6yx0smtWAXv1nCJS9ohnyOTd
    397eMojGDHqkEC+uojEScZheEkMxzgCZwDAs+/CSU7mS
    uHtCRZn19xlZUd5Gv7yDQ3mbOUwuy30oSk0z1Q5UUPpo
    ihOugIZHFX6Jk7NLiW2wlqfq9qhV4zj7TiBiJY0mCc4z
    HN8/aq2VKDHp2Na7mWzvKyTy+SYQkBQ/08LbPwj9YMc+
    uCzKL6sU/ObHv17EFhD8aPDftTHZvV9L+OZr";
};
```

takes

- monitoring
- notifying? (by TWNIC?)

as for domains other than “edu.tw”…

Thank You

Plans & Suggestions (about security threat)

“amplification attack”

```
;; QUESTION SECTION:
;ghmn.ru.                       IN      ANY

;; ANSWER SECTION:
ghmn.ru.                17794   IN      A       5.135.4.1
ghmn.ru.                17794   IN      A       5.135.4.10
ghmn.ru.                17794   IN      A       5.135.4.11
ghmn.ru.                17794   IN      A       5.135.4.12
ghmn.ru.                17794   IN      A       5.135.4.13
ghmn.ru.                17794   IN      A       5.135.4.14
ghmn.ru.                17794   IN      A       5.135.4.15
ghmn.ru.                17794   IN      A       5.135.4.16
ghmn.ru.                17794   IN      A       5.135.4.17
ghmn.ru.                17794   IN      A       5.135.4.18
ghmn.ru.                17794   IN      A       5.135.4.19
ghmn.ru.                17794   IN      A       5.135.4.2
ghmn.ru.                17794   IN      A       5.135.4.20
ghmn.ru.                17794   IN      A       5.135.4.21
ghmn.ru.                17794   IN      A       5.135.4.22
ghmn.ru.                17794   IN      A       5.135.4.23
ghmn.ru.                17794   IN      A       5.135.4.24
ghmn.ru.                17794   IN      A       5.135.4.25
ghmn.ru.                17794   IN      A       5.135.4.26
ghmn.ru.                17794   IN      A       5.135.4.27
ghmn.ru.                17794   IN      A       5.135.4.28
ghmn.ru.                17794   IN      A       5.135.4.29
ghmn.ru.                17794   IN      A       5.135.4.3
ghmn.ru.                17794   IN      A       5.135.4.30
ghmn.ru.                17794   IN      A       5.135.4.4
ghmn.ru.                17794   IN      A       5.135.4.5
ghmn.ru.                17794   IN      A       5.135.4.6
ghmn.ru.                17794   IN      A       5.135.4.7
ghmn.ru.                17794   IN      A       5.135.4.8
ghmn.ru.                17794   IN      A       5.135.4.9

...
;; MSG SIZE  rcvd: 4016
```

```
C:\Users\FJ Lin>dig @168.95.1.1 fjlin.tw soa

; <<>> DiG 9.12.3-P1 <<>> @168.95.1.1 fjlin.tw soa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4300
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 0c04fb91afed982a859c38325f5f2d730259950aac1ab9c8 (good)
;; QUESTION SECTION:
;fjlin.tw.                      IN      SOA

;; ANSWER SECTION:
fjlin.tw.               3600    IN      SOA     nspl.hinet.net. hostmaster.hinet.net. 2009141640 3600 1800 1209600 3600

;; Query time: 5 msec
;; SERVER: 168.95.1.1#53(168.95.1.1)
;; WHEN: Mon Sep 14 16:44:36 Taipei Standard Time 2020
;; MSG SIZE  rcvd: 126
```

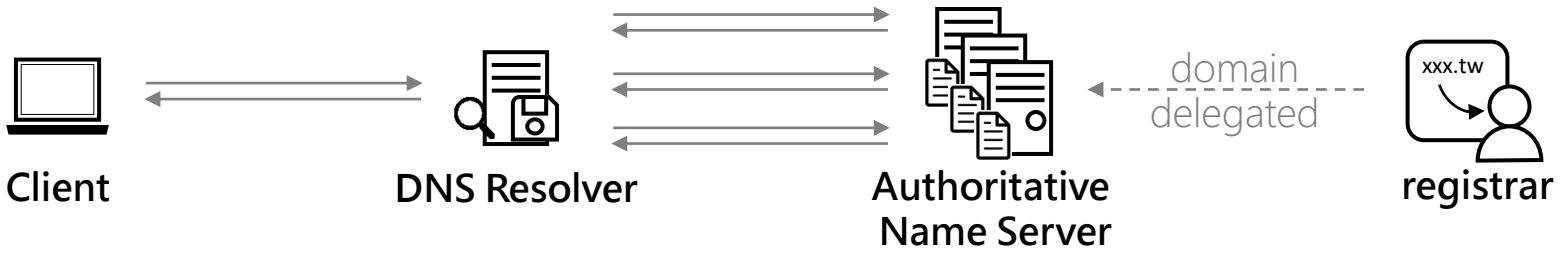
more protections required!!!

126 byte

```
C:\Users\FJ Lin>dig @168.95.1.1 fjlin.tw soa +dnssec

; <<>> DiG 9.12.3-P1 <<>> @168.95.1.1 fjlin.tw soa +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47248
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
; COOKIE: 4f4d69b5aab2d9cd552fa47d5f5f2d773268aeab2e39ea7b (good)
;; QUESTION SECTION:
;fjlin.tw.                      IN      SOA

;; ANSWER SECTION:
fjlin.tw.               3600    IN      SOA     nspl.hinet.net. hostmaster.hinet.net. 2009141640 3600 1800 1209600 3600
fjlin.tw.               3600    IN      RRSIG   SOA 8 2 3600 20201001000000 20200825000000 681 fjlin.tw. ZScpTCvxJiw4MsL
F0I1JfUeEcpUbI2UVo5JQKu8iPaEo5M+Xen5/vfdq 8JTec2Zay5VTpFpMeqByejSlyeEYhTzg/RpuhQgXI6y+zBqZfIhN/d0p XFpRfvu5WekEpwDvWOXuS
Xjse7x56aQaoFDLGTiFle/VH+pzasC7wczq +SX4OXTE7mdTYKWabv378LFHOo7Gg2gdPEDNRgTSNdwNaJty6GeBDIIc QcCjF2ZbbkBGD/0IRb98TBIqTvR
HNjadl/09ejryadfH6TSkZKmTa/Q0 GzQFeVBosWyj9TlykOSvQDzBx845GPSc+pGjw6qJfFJBOLPn1g0xwDkK QFx7/A==

;; Query time: 3 msec
;; SERVER: 168.95.1.1#53(168.95.1.1)
;; WHEN: Mon Sep 14 16:44:39 Taipei Standard Time 2020
;; MSG SIZE  rcvd: 422
```

422 byte (+dnssec, magnified)

Effort has been made



- ✓ explain
  - **Why**
    (benefit)
  - **What**
    (impacts, must-do's)
  - **How**
    (SOP)
- ✓ customer service
  - ticketing system
  - (consultant)

- ✓ keep strengthening
  - hardware capacity and performance
  - software tuning
  - Defense in Depth

(DNSSEC validation)
- ✓ technically ready
- ✓ progressive activation

(DNSSEC signing)
- ✓ technically ready
- ✓ DNS hosting service

- ✓ Accept DS、NS settings