DNSSEC Deployment in .TW

- Chen, Cheng-Yi
  Department Technology
  Taiwan Network Information Center
Outlines

- Top-Level Domains (TLDs) signed with DNSSEC
- Zones signed with DNSSEC in .TW
- DNSSEC test report and deployment in .TW
  - DNSSEC test report
  - Deployment setting of DNSSEC
- DNSSEC deployment report for .TW, TANET(.edu.tw) and GSN(.gov.tw)
Top-Level Domains (TLDs) signed with DNSSEC

- 816 TLDs in the root zone in total
- 643 TLDs are signed
- 636 TLDs have trust anchors published as DS records in the root zone

Ref:
1. TLD DNSSEC Report (2015-02-11)
2. DNSSEC Deployment Report (2015-02-10)
Outlines

- Top-Level Domains (TLDs) signed with DNSSEC
- **Zones signed with DNSSEC in .TW**
- DNSSEC test report and deployment in .TW
  - DNSSEC test report
  - Deployment setting of DNSSEC
- DNSSEC deployment report for .TW, TANET(.edu.tw) and GSN(.gov.tw)
Zones signed with DNSSEC in .TW

<table>
<thead>
<tr>
<th>Domain</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>tw</td>
<td>19</td>
</tr>
<tr>
<td>com.tw</td>
<td>15</td>
</tr>
<tr>
<td>net.tw</td>
<td>4</td>
</tr>
<tr>
<td>org.tw</td>
<td>4</td>
</tr>
<tr>
<td>idv.tw</td>
<td>12</td>
</tr>
<tr>
<td>edu.tw</td>
<td>23</td>
</tr>
<tr>
<td>gov.tw</td>
<td>43</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>120</strong></td>
</tr>
</tbody>
</table>
Outlines

- Top-Level Domains (TLDs) signed with DNSSEC
- Zones signed with DNSSEC in .TW
- **DNSSEC test report and deployment in .TW**
  - DNSSEC test report
  - Deployment setting of DNSSEC
- DNSSEC deployment report for .TW, TANET(.edu.tw) and GSN(.gov.tw)
DNSSEC test report of authoritative server

- Test environment
  - 200K domain names
  - 40K, 80K, 120K, 160K, 200K signed domain names
  - 610K domain name queries include 10K wrong domain name queries
**DNSSEC test report of authoritative server**

- **Result**

<table>
<thead>
<tr>
<th></th>
<th>cpu</th>
<th>ram</th>
<th>network</th>
<th>Load</th>
<th>Rrt(AVG)</th>
<th>qps</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>26%</td>
<td>No significant change</td>
<td>276k/s</td>
<td>1.5</td>
<td>0.0008</td>
<td>19251</td>
</tr>
<tr>
<td>20%</td>
<td>53%</td>
<td>No significant change</td>
<td>457k/s</td>
<td>1</td>
<td>0.0009</td>
<td>18811</td>
</tr>
<tr>
<td>40%</td>
<td>63%</td>
<td>No significant change</td>
<td>634k/s</td>
<td>1.1</td>
<td>0.0009</td>
<td>17838</td>
</tr>
<tr>
<td>60%</td>
<td>63%</td>
<td>No significant change</td>
<td>783k/s</td>
<td>1.1</td>
<td>0.001</td>
<td>15615</td>
</tr>
<tr>
<td>80%</td>
<td>57%</td>
<td>No significant change</td>
<td>1000k/s</td>
<td>1.6</td>
<td>0.001</td>
<td>16830</td>
</tr>
<tr>
<td>100%</td>
<td>64%</td>
<td>No significant change</td>
<td>1900k/s</td>
<td>1.6</td>
<td>0.001</td>
<td>16446</td>
</tr>
</tbody>
</table>
DNSSEC test report of authoritative server

- Conclusion
  - No significant change of CPU loading
  - No significant change of memory usage
  - 2 ~ 5x network bandwidth usage
DNSSEC test report of cache server

- Test environment
  - 200K domain names
  - 0%, 100% signed domain names
  - 600K normal domain name queries
  - Test run with/without cache
  - Log CPU, memory usage and system load
DNSSEC test report of cache server

1. no-dnssec
   no cache

2. no-dnssec
   have cache

3. dnssec
   no cache

4. dnssec
   have cache
## DNSSEC test report of cache server

<table>
<thead>
<tr>
<th></th>
<th>qps</th>
<th>ram</th>
<th>Network In/out</th>
<th>CPU</th>
<th>Load</th>
<th>Rrt(平均)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1st NO DNSSEC</strong></td>
<td>4596</td>
<td>No significant change</td>
<td>1060k/s 1060k/s</td>
<td>12%</td>
<td>No significant change</td>
<td>0.004320</td>
</tr>
<tr>
<td><strong>2nd NO DNSSEC</strong></td>
<td>2389</td>
<td>No significant change</td>
<td>900k/s 1330k/s</td>
<td>5%</td>
<td>No significant change</td>
<td>0.000654</td>
</tr>
<tr>
<td><strong>1st DNSSEC</strong></td>
<td>4434</td>
<td>No significant change</td>
<td>3700k/s 4600k/s</td>
<td>35%</td>
<td>No significant change</td>
<td>0.004495</td>
</tr>
<tr>
<td><strong>2nd DNSSEC</strong></td>
<td>1478</td>
<td>No significant change</td>
<td>600k/s 7000k/s</td>
<td>8%</td>
<td>No significant change</td>
<td>0.001200</td>
</tr>
</tbody>
</table>
DNSSEC test report of cache server

- DNSSEC DNS cache server with cached data
  - Increase CPU loading slightly
  - No significant change of memory usage
  - 5.5x network bandwidth usage
  - Could response about 60% queries in a second
Outlines

- Top-Level Domains (TLDs) signed with DNSSEC
- Zones signed with DNSSEC in .TW
- DNSSEC test report and deployment in .TW
  - DNSSEC test report
  - Deployment setting of DNSSEC
- DNSSEC deployment report for .TW, TANET(.edu.tw) and GSN(.gov.tw)
DNSSEC setting of Bind

- In named.conf
  dnssec-enable yes;

- In zone
  update-policy local;
  key-directory "/Path/to/keys";
  auto-dnssec maintain;
  inline-signing yes;
Update DS record

- Registrar
  - Start/Disable/Update DS every 10 mins
  - Start/Disable/Update DS to registry via DNSSEC API

- Registry
  - Update DS record per zone dynamically
Key rollover schedule

- Key generator: dnssec-keygen

- Zone Sign Key rollover every 1 month
  Parameter: -I +33d -D +35d

- Key Sign Key rollover every 1 year
  Parameter: -I +367d -D +368d
Outlines

- Top-Level Domains (TLDs) signed with DNSSEC
- Zones signed with DNSSEC in .TW
- DNSSEC test report and deployment in .TW
  - DNSSEC test report
  - Deployment setting of DNSSEC
- DNSSEC deployment report for .TW, TANET(.edu.tw) and GSN(.gov.tw)
DNSSEC deployment report for .TW

- 2010  Connect to DNSSEC Security Chain
- 2011/11 Enable DNSSEC for .TW and .台灣
- 2012/06 Enable DNSSEC for 2nd tier domain names
- 2012/10 EPP/API DNSSEC DS record upload function, Allow user to activate DNSSEC for their domain names
- 2013  DNSSEC Promotion Committee
- 2014/08 DNSSEC deployment report meeting
Zones signed with DNSSEC in .TW

<table>
<thead>
<tr>
<th>Domain</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>tw</td>
<td>19</td>
</tr>
<tr>
<td>com.tw</td>
<td>15</td>
</tr>
<tr>
<td>net.tw</td>
<td>4</td>
</tr>
<tr>
<td>org.tw</td>
<td>4</td>
</tr>
<tr>
<td>idv.tw</td>
<td>12</td>
</tr>
<tr>
<td>edu.tw</td>
<td>23</td>
</tr>
<tr>
<td>gov.tw</td>
<td>43</td>
</tr>
<tr>
<td>Total</td>
<td>120</td>
</tr>
</tbody>
</table>
Total DNSSEC Queries in .TW

During Jun-14 ~ Jul-14 lost some DNS query log from outside.
DNSSEC queries / total DNS queries is about 2% ~ 3%.
Increased DNSSEC queries from IPv6.
DNSSEC deployment report for TANET (edu.tw)

- DNS system for TANET
DNSSEC deployment report for TANET (edu.tw)

- Enable DNSSEC for DNS system
  - Region Network Center : 9/13 (69.2%)
  - County Network Center : 3/22 (13.6%)
  - Colleges/Universities : 10/161 (6.2%)

- DNSSEC query status of DNS system
  - Authoritative DNS Server : 79.7% queries
  - Resolver DNS Server : 54.4% queries
**DNSSEC deployment report for GSN (gov.tw)**

- **DNS system for GSN**
  - Phase I & II had been done.

### Phase I
- nat.gov.tw (GSN)

### Phase II
- Reorg DNS
- Web servers -1

### Phase III
- Not reorg DNS
- Web servers -2

- .com.tw
- .gov.tw (GSN)
- .tw
- .edu.tw
- nctu.edu.tw
DNSSEC deployment report for GSN (gov.tw)

DNSSEC Deployment Status for GSN

- Finished, 4, 22%
- Ongoing, 12, 67%
- Technical problem, 2, 11%
GSN DNSSEC Monitor

Setup

Notification

Upload DS record

Check DNS setting

Add to monitor list

Generate Report

Send Error Notification

Monitoring
## GSN DNSSEC Monitor Report

### DNSSEC query report in last 24 hours

| Domain      | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|-------------|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| mofa.gov.tw | x | x |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| ftc.gov.tw  | x | x | x |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| mof.gov.tw  |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| cbc.gov.tw  | x | x |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| fnpc.gov.tw | x | x |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| mohw.gov.tw |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| dgos.gov.tw |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| fnp.gov.tw  |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| mnd.gov.tw  | x | x | x | x | x | x | x | x | x | x |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| npe.gov.tw  | x | x | x | x | x | x | x | x | x | x |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| gov.tw      |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| pno.gov.tw  |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| ocac.gov.tw |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| moj.gov.tw  |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| hakka.gov.tw|   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| dgbas.gov.tw|   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| sec.gov.tw  |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| moc.gov.tw  | x | x | x | x | x | x | x | x | x | x |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |

### Normal

- mofa.gov.tw
- ftc.gov.tw
- cbc.gov.tw
- fnpc.gov.tw
- mohw.gov.tw
- dgos.gov.tw
- fnp.gov.tw
- mnd.gov.tw
- npe.gov.tw
- gov.tw
- pno.gov.tw
- ocac.gov.tw
- moj.gov.tw
- hakka.gov.tw
- dgbas.gov.tw
- sec.gov.tw
- moc.gov.tw

### Failed

- mofa.gov.tw
- ftc.gov.tw
- mof.gov.tw
- cbc.gov.tw
- fnpc.gov.tw
Thank You