DNSSEC Revisited

Hoda Rohani               Anastasios Poulidis
Supervisor: Jeroen Scheerder

System and Network Engineering
July 2014
DNS Main Components

- **Server Side:**
  - Authoritative Servers
  - Resolvers (Recursive Resolvers, cache)

- **Client Side:**
  - Stub resolvers (usually on DNS client machines)

- No authentication at all!
- A client cannot be sure
  - Where an answer really came from
  - If the server replied is telling the truth or not
  - If it received exactly what the server sent
DNS Vulnerabilities

- Fill client or resolving server with forged answer
- Intercept a response packet and modify it
- Set up a fake name server for some zone
- Take control of name servers for some zone (false data)
- Inject bogus data into caches (DNS cache poisoning)
- Response to Non-Existent domains
- Compromise the registry: gain unauthorized access to registrar account and change the victim zone’s delegation to point at bogus name servers
**What Does DNSSEC Protect**

- DNSEC uses public key cryptography and digital signatures to provide:
  - Data origin authentication, Name server authenticity
  - Data integrity
  - Authenticated denial of existence

DNSSEC offers protection against spoofing of DNS data (TSIG)
General DNSSEC Caveats

- Increase Memory and CPU usage and also cost
  - Zone size increases significantly when signed
  - DNSSEC answers are larger
  - Server side & query side impacts
  - Interference by firewalls, proxies

- Increase bandwidth
  - DNSSEc added a lot to DNS packets. Resolvers and name servers need to send and receive these large DNS packets

- Administrative burden: Key Management (generating, publishing and rollover), interaction with parent
Key Rollover

- Not easy and expensive task

- Two methods
  - Pre-publish: ZSK
  - Double signature: KSK
ZSK Rollover: Pre-publish Policy

- Generate new ZSK, add key to zone (remember to increase the serial number)
- Re-sign zone with using old key and KSK

- Time passes … TTL

- Re-sign with the new key but leave the old zsk published in the zone

- After all records signed with the old private key have expired (wait zone propagation time + largest TTL of all records in the zone), remove old key
- Resign one last time
KSK Rollover: Double Signature Policy

- Generate new KSK, add new KSK to the zone and sign the DNSKEY RRset with both keys
- Wait TTL of the zone
- Upload new DS to the parent zone
- When new DS RR appears in the zone, wait TTL of the old DS record
- Remove the old KSK and resign zone
- Remove old DS record from parent
Deployment Status

- Root signed (July 2010), most TLD signed (July 2014 status)
  - TLDS signed: 445 out of 630 (70%) in the root zone in total
  - 435 TLDs have trust anchors published as DS records in the root zone
  - 5 TLDs have trust anchors published in the ISC DLV Repository
Research Questions & Related work

- What is the DNSsec adoption rate among the most popular domains?
- If the DNSsec is deployed in the zone, is it managed and operated properly?
  - What are the causes of bogus DNSsec enabled zone

- Many websites keep statistics of DNSsec deployment
  - But most of them are restricted to the number of checked domains and TLDs
  - They also lack information about maintenance
Methodology

- Gather data: get top one million ranked websites by Alexa
  - Extract their domains
  - Find authoritative servers of domains and ask for data of domain
    - Note their serial number and (in)consistency of their answers
    - Look for RRSIG RRs
    - Check for (no)validated answers
    - Ensure that the zone issues a secure denial of existence for names that do not exist

- Validating Resolvers
  - Our servers and Google public DNS
  - Check to see if those signatures correspond to DNSKEYs served by the zone are valid or not

- Analysis to find out possible errors on the deployment of DNSsec
DNSSEC Validation Status

**Secure:** Unbroken chain from anchor to RRset

**Insecure:** Chain that securely terminates in the parent

**Bogus:** Broken chain
How Many Domains are deploying DNSSEC

- On average 9916 signed domains out of a total of ~930000 (1.066%)
- With an average of 7562 (76%) Validated and 2355 (24%) Not Validated domains.

![DNSsec Adoption Rate](chart.png)
Domain Nameserver (in)consistencies

- On average each domain has 3.5 nameservers
- ~84% of signed domains have multiple nameservers with the same data (8239)
- ~16% of signed domains have multiple nameservers with different data (1568)
  - Inconsistent data
  - Consistent data
235 signed domains have some nameservers with RRSIG data while others don’t have RRSIG.

The returned answer depends on which nameserver is selected by the resolver.
Inconsistency: Different Data in Nameservers

Non-deterministic behavior
Consistency: Different Data in Nameservers

- Differences in A records
Consistent: Different Data in Nameservers

- Differences in RRSIG
- Multiple ZSK keys and signing with different keys
Consistent Data in Nameservers

- ~76% of the asked domains return RRSIGs with AD flag
- ~24% of the asked domains return RRSIGs with no AD flag
Other checks: Common DNSSEC Algorithms

- DSA-SHA1 (0.03%)
- RSA-SHA1 (30%)
- RSA-NSEC3-SHA1 (33%)
- RSA-SHA256 (35%)
- RSA-SHA512 (0.33%)
- ECDSA Curve P-256 with SHA-256 (0.01%)
Other checks: NSEC and NSEC3

- Proof of non-existence
  - Pre-calculated records
  - NSEC vs NSEC3
Other checks: DNSSEC RRSIG Lifetime

- **Signature lifetimes**
  - Default value: Inception time 1 hour before
  - Default value: Expiration 30 days from now
  - Vary between 2 and 3,600 days

- **Be sure about your servers accurate time**
  - Validating resolvers has to check signature validity time
DNSSEC Misconfiguration

- **Missing DS** – no link between parent and child
- **Mismatch DS** – No DNSKEY matching DS in parent zone
  - None of DNSKEY records could be validated by any of DS records, the DNSKEY RRset was not signed by any keys in the chain-of-trust (the DNSSEC chain-of-trust is broken at this point)
- **Missing DNSKEY** – DNSKEY not available to validate RRSIG
- **Missing NSEC** – NSEC RRs not returned by authoritative server
  - No NSEC records in response, no NSEC record could prove that no records of type A
- **Missing RRSIG** – RRSIGs not returned by some servers
- **Bogus RRSIG** - if the zone was signed with different keys than the ones that are published in the zone data
  - DNSSEC signatures did not validate the RRset
- **Expired RRSIG** – Signature in RRSIG are expired
  - DNSSEC signatures did not validate the RRset
Delegation Errors

<table>
<thead>
<tr>
<th>Error</th>
<th>Zone</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing DS</td>
<td>tld.</td>
<td>~57%</td>
</tr>
<tr>
<td>Missing DNSKEY</td>
<td>domain.tld</td>
<td>~14%</td>
</tr>
<tr>
<td>Signature Expired</td>
<td>domain.tld</td>
<td>~13.5%</td>
</tr>
<tr>
<td>Other</td>
<td>tld./domain.tld</td>
<td>~15.4%</td>
</tr>
</tbody>
</table>

[Diagram of Delegation Errors]

DNSKEY/DS/RRSIG

tld.

DNSKEY/DS/RRSIG

domain.tld.

DNSKEY/RRSIG/A
DS Mismatch

```
hoda@amsterdam:~$ dig @8.8.4.4 +dnssec ifma.edu.br
  +                   +                   +                   +                   +
  ;<<>> DIG 9.9.3-P2 <<>> @8.8.4.4 +dnssec ifma.edu.br
  ; (1 server found)
  ; global options: +cmd
  ; Got answer: ;
  ; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 45774
  ; flags: qr xd ra: QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
  ; OPT PSEUDOSECTION:
  ; EDNS: version: 0, flags: do; udp: 512
  ; QUESTION SECTION:
  ;ifma.edu.br.
  ; Query time: 522 msec
  ; SERVER: 8.8.4.4#53(8.8.4.4)
  ; WHEN: Wed Jul 02 01:25:22 CEST 2014
  ; MSG SIZE  rcvd: 40
```
DNSKEY Missing

Turn DNSSEC off but forgot to interact with parent to remove the DS record: found 25 domains
RRSIG Expired Dates

Regular re-signing is part of the administrators’ tasks (not only when changes occur)
Our results showed that few administrators have deployed and maintained DNSSEC properly due to its burden and difficulties. Use scripts and online tools for checking the healthiness of the zone and monitor the zone regularly. Automate regular process as much as possible. Keep all nameservers’ data updated to avoid inconsistencies.
Any Questions?