Security Impact of DNS Delegation Structure and Configuration Problems

Jochen Kögel, Sebastian Kiesel
Institute of Communication Networks and Computer Engineering
University of Stuttgart
{koegel,kiesel}@ikr.uni-stuttgart.de

This work was funded by T-Com Corporate Security

October 11, 2006
Agenda

Motivation
DNS principles
Problems - delegation structure and configuration
Possible solutions
Conclusion and Outlook
Motivation

DNS

- Mainly used for
  - Domain name ↔ IP address lookup (A records)
  - E-mail: application layer routing (MX records)
    - Load balancing
    - Backup servers

- Proven scalability and flexibility
- Became one of the building blocks of the Internet

Next to IP transport, it is something that "just works"
Motivation

Problems with DNS
• No integrity protection in DNS replies (spoofing, cache poisoning, etc)

Current security approach
1. Take DNS as untrusted lookup mechanism
2. For sensitive applications:
   Use http over TLS for authenticating peers

→ This solution works. At least for web applications.
NGNs: new applications for DNS

Characteristics of NGNs (e.g., IMS): high security requirements
- "Closed" platforms
  - Policy enforcement by session based filtering at platform edge (Session Border Controllers)
- No full IP connectivity to the Internet or other NGNs
- Application layer routing
NGNs: new applications for DNS

**Motivation**

**ENUM**

Retrieve service URIs of base on phone number

```plaintext
3.2.1.9.4.e164.arpa.

14400 IN NAPTR 1 10 "u" "E2U+sip" "!^.*!sip:+123@c.de!"

14400 IN NAPTR 1 20 "u" "E2U+msg" "!^.*!mailto:bob@c.de!"
```
NGNs: new applications for DNS

Federation policies

Provide policies for incoming connections (draft-lendl-domain-policy-ddds)

c.de.

IN NAPTR 10 10 "U" "D2P+SIP:fed "!^.*$!http://sip.voipfed.de/!"
Motivation

NGNs: new applications for DNS

SRV Records

Generalized MX records for application layer routing

```plaintext
_sip._udp.b.de.  7200 IN SRV 0 0 5060 ingress-sbc.b.de.
_sip._udp.c.de.  7200 IN SRV 0 0 5060 sbcl.c.de.
```
NGNs: new applications for DNS

Essential routing information stored in DNS

- "http-over-TLS workaround" not sufficient anymore
- Security and reliability of the DNS itself becomes essential
DNS Principles

DNS

application

www.uni-stuttgart.de?

A 129.69.8.151

Internet

DNS

A 129.69.8.151

www.uni-stuttgart.de?
DNS Principles

Replication – increased performance and availability
Delegation – each NS knows only parts of the data
Delegation – each NS knows only parts of the data
Institute of Communication Networks and Computer Engineering

University of Stuttgart

Query algorithm in Resolver – simpler clients & caching possible

Internet

WWW

application
stub resolver

resolving
name server

www.uni-stuttgart.de ?

ask for A record of www.uni-stuttgart.de
de IN NS a.nic.de (+ IP Address)

ask for A record of www.uni-stuttgart.de
... IN NS dns1.belwue.de (+ IP Address)

ask for A record of www.uni-stuttgart.de
	www.uni-stuttgart.de IN A 129.69.8.151

A 129.69.8.151

recursive queries

iterative queries
DNS Delegation and Server Structure

DNS Name Space

(root) → de → org → de

www

uni-kl

uni-stuttgart

ftp

web

gnu

www

www

www
ttf

www
DNS Delegation and Server Structure

DNS Name Space

Internet with Delegated Name Servers
DNS Delegation
Institute of Communication Networks and Computer Engineering

University of Stuttgart

• All potentially involved NS have to be trusted
Impact of delegation: complex administration

Administrators of different domains are involved

- Administrator of parent zone: needs to know for each delegated zone
  - Names of delegated NS
  - IP addresses of delegated NS (glue records) – if in the same subdomain

- Administrator of delegated zone: master server needs to know
  - Addresses of slave servers that are allowed to copy data

- Administrator of replicating (slave) servers need to know
  - For which zones they act as delegated NS
  - Master server for retrieving zone data
Impact of delegation: problems

- **Outdated NS/IP address:** Servers that are not responsible for the zone are queried: "Lame delegations"\(^1\)
  - NS might refuse to answer
  - NS might give wrong answer (NXDOMAIN, Fake A)
  - NS might serve as resolver and perform iterative queries for the name

- **Glue records not present**
  - Additional queries for NS’s IP necessary
    - Additional latency
    - More (potentially compromised) servers contribute to answer

---

Delegation - examples

www.ebay.com

- Delegation structure without problems (almost)

Black: Delegation with glue record
Red: Delegation without glue record
Blue: Answer
Delegation structure - examples

www.siemens.com

- Missing glue for 3 of 4 NS
Delegation structure - examples

www.ikr.uni-stuttgart.de

- Paths with different number of NS - inconsistent zone data
- Root servers inconsistent – j.root-servers.net does not know e164.arpa
- Lots of glue records missing → much more NS potentially involved
Example: ENUM lookup

- Ask for NAPTR record of 5.2.6.4.2.0.3.1.8.6.9.4.e164.arpa
  - `...IN NS ns.sunet.se... (no glue)`

Additional lookup for A of ns.sunet.se

- Ask for A record of ns.sunet.se
  - `...IN NS c.ns.se + A (glue)...`
- Ask for A record of ns.sunet.se
  - `...IN NS server.nordu.net... (no glue)`

Additional lookup for A of server.nordu.net

- Ask for A record of server.nordu.net
  - `...IN NS a.gtld-servers.net + A (glue)...`
- Ask for A record of server.nordu.net
  - `...IN NS server.nordu.net + A (glue)...`
- Ask for A record of server.nordu.net
  - `...IN A 193.10.252.19...`
- Ask for A record of ns.sunet.se
  - `...IN A 192.36.125.2...`
DNS Problems

- DNS administration is evidently error-prone
  - Even Root NS do not host the same data
  - Wrong information in parent zone causes "Lame Delegations"
- Missing glue records
  - Additional lookups to other NS required
  - Number of potentially involved servers unknown in advance
  - Every server that possibly can contribute to the result must be trusted

- A high, unknown number of (potentially compromised) servers potentially contribute to answers
- Integrity of DNS?
DNSSEC

- DNS Security Extensions RFC4033-4035 (March 2005)
- Protection of DNS Records by digital signatures
- Pre-configured public keys in Resolvers for establishing trust chain
- PKI-like administration required
  - Distribution of new (Root-) Keys
    - How to replace pre-configured keys in resolvers?
  - For each new zone: new keys have to signed by parent zone

⇒ Might lead to the same administrative problems
⇒ Signatures expire, are invalid... ⇒ affects service availability
Possible solutions

Local copy

Be Independent of the distributed DNS infrastructure
- Keep a local, verified copy of essential DNS data
- Transfer of complete zone files required

New DNS architecture

Build a centralized, replicated DNS architecture
- Idea: keep all DNS data in "Root-Servers", no delegations
- For migration: delegation still possible

- Paradigm shift
- Only a few servers have to be trusted
- Provisioning? → For further study

Conclusion and Outlook

Conclusion

- New applications (e.g. VoIP Platforms): more than name-to-IP lookup
  - Secure and reliable DNS required (http-over-TLS does not help)
- Current DNS: complex, error-prone administration
  - Integrity not guaranteed
- DNSSEC might lead to the same administrative problems

Outlook: Which is the best solution?

- DNSSEC
- Local copy
- Paradigm shift: centralized DNS
  - No general answer possible
  - Further evaluation necessary