GÉANT
Networks • Services • People

Introduction to DNS and its Security Challenges

Meet the Problems

Tobias Dussa
WP8-T1

Webinar, November 2020

Public

www.geant.org

Game Plan

- Recap on what DNS is and does.
- Security implications of DNS.
- Privacy implication of DNS.
- Questions/discussion/open mike session.

Recap: Previously on “Your Life with DNS (Even If You Did not Know It Was There)”

What is DNS?

- DNS is the “Domain Name System”.
- A means for users of computer systems to map “host names” to IP addresses.
- Decentralized and hierarchical.
- Originally defined in RFC 882 and RFC 883 (November 1983).
- Supersedes the completely-decentralized concept of “host files” which are a nightmare to maintain.

General Concept

- DNS provides technical information about a host name or a domain that a client can request:
    - Mapping of host names to IP addresses,
    - redirections of host names to other host names,
    - mail servers responsible for a given host/domain,
    - DNS servers responsible for a given host/domain,
    - CAs allowed to issue certificates for a given host/domain,
    - and a **lot** of other things.
- Communication via UDP or TCP port 53

Structure of the DNS

- DNS is **hierarchical**:
  - All requests first go to the 13 well-known root servers.
  - Next step is the server responsible for the top-level domain.
  - … then for the second-level domain
  - … then for the next-level domain
  - until the end is reached: the authoritative server.
  - Finally, the actual request goes to that server.
- For performance reasons, replies are cached.
- All the above is usually done by a **resolver**.

DNS Security Implications

First Things First: Fakes

The obvious problem: No authentication.

→ DNS replies can be forged or altered.

Result: You will be redirected to an IP address of the attacker’s choice instead of your legitimate target.

This can also be done via **cache poisoning** of **resolvers** (no interception capabilities required)!

Advanced attack: Injecting malicious data into legitimate **name servers**.

Denial of Service – Attacking You

- Attacker targets **your** ability to **use** DNS by hitting your **resolvers**.
- Denies **you** normal use of the internet.
- Typical example: Overloading by flooding with requests.
- Other possible attack methods include cache poisoning, flooding with (fake) answers, …

Denial of Service – Attacking Your Services

- Attacker targets **your** ability to **provide** DNS services by hitting your **name servers**.
- Denies **everybody** the normal use of your services.
- Attack methods identical to previous attack.
- Crucial difference: DNS servers are meant to be reachable from third parties → this facilitates many attacks.

Denial of Service – Attacking Third Parties

- Attacker targets a **third party's** ability to use the internet by hitting their connectivity.
- Denies **the victim** normal use of their internet uplink.
- Attack method: Send spoofed DNS requests to **your** name servers and/or resolvers with faked sender IP addresses ("DNS reflection").
- If done properly, this amplifies the attack force ("DNS amplification").

Data Leakage – Reconnaissance

- Attackers can request information about an entire DNS zone (“zone transfer”).
- If the name server is configured loosely, then all information will be handed over upon request.
- If the name server does not allow zone transfers, then hosts can be enumerated if they have DNS name records. (Might take a while though, obviously.)

Covert Communication Channels – Data Leakage

- DNS queries can be used to exfiltrate data.
- Not really preventable (unless DNS queries are whitelisted in advance).
- Very hard to detect (if done properly).
- Very low bandwidth.

Covert Communication Channels – Command & Control

- Replies to DNS queries can transport arbitrary data fairly reliably.
- Albeit at a very low bandwidth.
- Can be and is sometimes used by malware to communicate with command-and-control servers (or as a VPN: “DNS tunnelling”).
- (Not to be confused with concepts like fast-flux domain hopping – that is meant to **locate** command-and-control servers in a sneaky but reliable way.)

DNS Privacy Implications

Breadcrumbs – Privacy of Clients or Organisations

- Client network activity usually requires DNS queries.
- A lot can be learned or inferred from these queries.
- Therefore, just using DNS leaks some information about client activity.
- **At least** the first-hop resolver can, in principle, snoop on you.
- More “remote” resolvers can only infer less accurate information, but they still can.

Data Leakage – Privacy Spin

- Severity of this depends on your levels of concern and/or local juristiction, but:
- If computer names are aligned with their main users, for instance like this:

  `dussa-desktop.dfn-cert.de`

  then your name server effectively enumerates your staff.
- (Plus, `trump-notebook.whitehouse.gov` might become a priority target.)

GÉANT
Networks • Services • People

Thank you

Any questions?

www.geant.org

The research leading to these results has received funding from
the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

Bonus Track:
Split DNS

Split DNS – Basics

- Also known as “split-horizon DNS,” “split-view DNS,” “split-brain DNS.”
- “Splits” the DNS “world” into two (or more) parts.
- Answer to DNS queries depend on what “part of the world” the query comes from.
- Often based on the query source IP address.

Split DNS – Use Cases in Practice

- Security should **not** be based solely on Split DNS.
- Often used as a barrier to enhance privacy and make reconnaissance harder.
- Common use cases:
  - Internal versus external view, for instance, of a university: Services that should be used only internally are not announced to the outside.
  - Improved load balancing or connectivity, for instance by returning “physically close” IP addresses for a given host name, based on the source’s geolocation.

Split DNS – Challenges

- If not implemented properly, Split DNS easily collides with DNSSEC, which verifies that a DNS response is unchanged and authentic.
- However, if implemented carefully, most problems can be avoided; see the IETF’s (expired) guideline: `Split-View DNSSEC Operational Practices`
- Another potential headache with regard to security: IPSec. See RFC8598: `Split DNS Configuration for IKEv2`