The GNU Name System

ICANN66

Martin Schanzenbach
11/5/2019
The GNU Name System In a Nutshell
Motivation

- DNS remains a source of traffic amplification DDoS.
- DNS censorship (i.e. by China) causes collateral damage in other countries.
- DNS is part of the mass surveillance apparatus (MCB).
- DNS is abused for offensive cyber war (QUANTUMDNS).
- DoT/DoH, DNSSEC, DPRIVE unfortunately do NOT fix this.
What is the GNU Name System?²

- Fully decentralized name system ⇒ Names are not global.
- Supports globally unique and secure identification.
- Features query and response privacy.
- Provides a public key infrastructure
  - Each zone is associated with a cryptographic key pair.
  - Delegation between zones establishes trust relationship.
- Interoperable with DNS.
- Usable.¹

¹User studies conducted in “Decentralized Authentication for Self-Sovereign Identities using Name Systems” (DASEIN) project.
²Joint work with Christian Grothoff and Matthias Wachs
Applications

- Social Networks: SecuShare (https://secushare.org)
- Healthcare: Accident insurance and private health data.\(^3\)
- Others: Chat, Host addressing, ...

\(^3\) Joint work with FH Bern, “Decentralized Authentication for Self-Sovereign Identities using Name Systems” (DASEIN)
Technical Overview
Record Storage / Retrieval

- GNS stores records in a **Distributed Hash Table** (DHT).
- DHTs allow us to map keys to values.
- Naive approach: Map domain names to records.
  e.g.: example.com $\Rightarrow$ A: 1.2.3.4
Secure Storage / Retrieval

- **Query privacy**
  - GNS implements a **Private Information Retrieval** (PIR) scheme: “a protocol that allows a user to retrieve an item from a server in possession of a database without revealing which item is retrieved.”\(^4\)
  - Queries do not reveal domain name.

- **Record confidentiality**: Values in DHT are signed and encrypted by zone owner.

- **Zone privacy**: Zones cannot be enumerated.

- **Censorship and DDoS resistance**: Decentralized, resilient directory.

\(^4\)https://en.wikipedia.org/wiki/Private_information_retrieval
The “NS” equivalent in GNS is called “PKEY”.

A “PKEY” record contains public zone keys.

The combination of a “PKEY” record value and a name allows users to query records in a delegated zone.
```.com``` zone: `5G0Z`

Bob's zone: `7F5T`

```
www.bob.com = 1.2.3.4
```

<table>
<thead>
<tr>
<th>Label</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bob</code></td>
<td>PKEY</td>
<td><code>7F5T</code></td>
</tr>
</tbody>
</table>

PUT `bob` in `5G0Z`

<table>
<thead>
<tr>
<th>Label</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>www</code></td>
<td>A</td>
<td>1.2.3.4</td>
</tr>
</tbody>
</table>

PUT `www` in `7F5T`
GET *bob* in 5G0Z

<table>
<thead>
<tr>
<th>Label</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bob</td>
<td>PKEY</td>
<td>7F5T</td>
</tr>
</tbody>
</table>

www.bob.com?
<table>
<thead>
<tr>
<th>Label</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>www</td>
<td>A</td>
<td>1.2.3.4</td>
</tr>
</tbody>
</table>
How do we bootstrap the top-level zones?
www.bob.com?

GET bob in 5G0Z

<table>
<thead>
<tr>
<th>Label</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bob</td>
<td>PKAY</td>
<td>7F5T</td>
</tr>
</tbody>
</table>
The GNU Name System Root

“Hyper-hyper local root” concept:

- Resolver ships with initial root zone configuration.
- Root zone configurable *locally* at *each* endpoint.
- User override/extension of root at top-level or subdomain-level for:
  - Circumvent censorship if necessary.
  - Private networks.
Envisioned Governance Model

- Non-profit organization.
- Multi-stakeholder model: Board, supporting organizations, ... 
- Examples for possible stakeholders:
  - Software and OS Distributors
  - Browser vendors
  - Governments
- Funding options:
  - Applications for new top-level domains.
  - Registrations of new top-level domains.
  - ...
Quo Vadis?
Roadmap

• In progress:
  • 2019-2020: Technical specification of GNS protocol, packaging and alternative implementations.\textsuperscript{5}
  • Continuous development and integration into applications.
• 2020−: Establishment of governing body.

\textsuperscript{5}Funded by NLnet under EU Next Generation Internet program (https://nlnet.nl/project/GNS/).
The GNU Name System

https://gnunet.org

schanzen@gnunet.org
3D11 063C 10F9 8D14 BD24 D147 0B09 98EF 86F5 9B6A
