“Developers of new name resolution systems that must work in existing contexts actually have no choice: they must use a Special-Use Domain Name to segregate a portion of the namespace for use with their system.” –RFC 8244
Context

GNU Name System: 2019 Edition
Applications in GNUnet (under development)

- Anonymous and non-anonymous publishing
- IPv6–IPv4 protocol translation and tunnelling
- **GNU Name System**: censorship-resistant replacement for DNS
- Conversation: secure, decentralized voice communication
- SecuShare: social networking
- GNU Taler: privacy-friendly payments
- ...

GNU Name System: 2019 Edition 2/39
DNS troubles

- DNS remains a source of traffic amplification for 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 the offensive cyber war (QUANTUMDNS)

Band aid solutions\(^1\) will **not** fix this.

\(^1\)DNS-over-TLS, DoH, DNSSEC, DPRIVE, ...
The GNU name system

- Decentralized name system ⇒ Names are not global
- Supports globally unique (& secure) identification
- Achieves query and response privacy
- Provides public key infrastructure
- Interoperable with DNS

\[^2\]Joint work with Martin Schanzenbach, Matthias Wachs and Patrick Gerber
Zone management
Zone management

Add Zone
Zone label: rms

Select Zone
grothoff

Edit Zone 6F510ZG3BMARZ2J4DK0MT70FW5ADXW7PHEGM5ZN1JR43HQF3F1XG

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Value</th>
<th>Expiration</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;new name&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>www</td>
<td></td>
<td>&lt;new record&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Zone management

Add Zone
- Zone label: 

Select Zone
- rms

Edit Zone
- Z378HMHARHXWPDBD6D7J0VDYA8ZJ3RPCKFDZPX0XR42SRDFCSB4G

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Value</th>
<th>Expiration</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;new name&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Zone management
Zone management
Zone management

![Zone management interface](image)

**Name**
- www

**Destination IPv4 Address**
- 208.118.235.148

**Options**
- Record is public (visible to other users)
- Record is a shadow record (valid after other records expire)

**Expiration Time**
- Absolute

**Calendar**

<table>
<thead>
<tr>
<th>August</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun</td>
<td>Mon</td>
</tr>
<tr>
<td>31</td>
<td>28</td>
</tr>
<tr>
<td>32</td>
<td>4</td>
</tr>
<tr>
<td>33</td>
<td>11</td>
</tr>
<tr>
<td>34</td>
<td>18</td>
</tr>
<tr>
<td>35</td>
<td>25</td>
</tr>
<tr>
<td>36</td>
<td>1</td>
</tr>
</tbody>
</table>

![Calendar]

**Hours:** 9  -  +
**Minutes:** 56  -  +
**Seconds:** 27  -  +
Zone management

The image shows a graphical interface for managing zones in the GNU Name System. The interface includes options for adding and selecting zones, along with a detailed view of zone configuration details.
Zonenmanagement

GNU Name System: 2019 Edition

Tanggal: 12/39
Zone management

Add Zone
Zone label:

Select Zone
rms

Edit Zone
Name Type Value
<new name>

www <new record>
A 208.118.235.148
BOX 6443522022e1e12dacb350e69317a7f37d769f46f16f437cf8d392319279c93515ef
Name resolution in GNS

Bob can now reach his Web server under www.bob
Secure Introduction

Bob Builder, Ph.D.

Address: Country, Street Name 23
Phone:    555-12345    
Mobile:   666-54321
Mail:       bob@H2R84L4JIL3G5C

- Bob provides his public key to his friends, i.e. via QR code
Alice learns Bob’s “public” key
Alice creates a delegation to zone $K_{pub}^{Bob}$ under the label $bob$
Alice can then reach Bob’s Web server under www.bob.alice
Name resolution

Bob

DHT

Alice

<table>
<thead>
<tr>
<th>8FS7</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>www  A  5.6.7.8</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A47G</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>bob  PKEY  8FS7</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Name resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

Bob

<table>
<thead>
<tr>
<th>8FS7</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>www  A  5.6.7.8</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Alice

<table>
<thead>
<tr>
<th>A47G</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>bob  PKEY  8FS7</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

GNU Name System: 2019 Edition
Name resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

1 www.bob.alice ?

Alice

GNU Name System: 2019 Edition
Name resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

www.bob.alice?

1

8FS7

www A 5.6.7.8

Bob

A47G

Alice

bob PKEY 8FS7

GNU Name System: 2019 Edition
Name resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

www.bob.alice ?

PKEY 8FS7!

'bob'?
Name resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

www.bob.alice ?

PKEY 8FS7!

'bob'?

PKEY 8FS7?

bob  PKEY 8FS7

www      A      5.6.7.8

8FS7

GNU Name System: 2019 Edition
Name resolution

1. Alice requests the name resolution for `www.bob.alice`.
2. Alice queries the DHT for `bob`.
3. Alice receives the key `8FS7`.
4. Alice sends a PUT request to `8FS7-www` to store `www` and `5.6.7.8`.
5. Bob retrieves `5.6.7.8` from `8FS7-www`.

Bob's DHT entry:

<table>
<thead>
<tr>
<th>8FS7</th>
<th>:</th>
</tr>
</thead>
<tbody>
<tr>
<td>www</td>
<td>A 5.6.7.8</td>
</tr>
<tr>
<td>:</td>
<td>:</td>
</tr>
</tbody>
</table>

Alice's DHT entry:

<table>
<thead>
<tr>
<th>A47G</th>
<th>:</th>
</tr>
</thead>
<tbody>
<tr>
<td>:</td>
<td>:</td>
</tr>
</tbody>
</table>

PUT request:

```
PUT 8FS7-www: 5.6.7.8
```
Browser Configuration

![Firefox Edit Menu]

- **Undo**: Ctrl + Z
- **Redo**: Ctrl + Shift + Z
- **Cut**: Ctrl + X
- **Copy**: Ctrl + C
- **Paste**: Ctrl + V
- **Delete**: Del
- **Select All**: Ctrl + A
- **Find**: Ctrl + F
- **Preferences**
Browser Configuration
Browser Configuration
What is GNU?

GNU is an operating system that is free software—that is, it respects users’ freedom. The GNU operating system consists of GNU packages (programs specifically released by the GNU Project) as well as free software released by third parties. The development of GNU made it possible to use a computer without software that would trample your freedom.

We recommend installable versions of GNU (more precisely, GNU/Linux

Planet GNU

LibreJS 7.15 released. GNU LibreJS aims to address the JavaScript problem described in Richard Stallman’s article The JavaScript Trap*. LibreJS is a free add-on for GNU IceCat and other M...
Privacy issue: DHT
Query privacy: terminology

- $G$: generator in ECC curve, a point
- $n$: size of ECC group, $n := |G|$, $n$ prime
- $x$: private ECC key of zone ($x \in \mathbb{Z}_n$)
- $P$: public key of zone, a point $P := xG$
- $l$: label for record in a zone ($l \in \mathbb{Z}_n$)
- $R_{P,l}$: set of records for label $l$ in zone $P$
- $q_{P,l}$: query hash (hash code for DHT lookup)
- $B_{P,l}$: block with encrypted information for label $l$ in zone $P$ published in the DHT under $q_{P,l}$
Publishing records $R_{P,l}$ as $B_{P,l}$ under key $q_{P,l}$

\[
\begin{align*}
    h & : = H(l, P) \\
    d & : = h \cdot x \mod n \\
    B_{P,l} & : = S_d(E_{HKDF(l, P)}(R_{P,l})), dG \\
    q_{P,l} & : = H(dG)
\end{align*}
\]
Query privacy: cryptography

Publishing records $R_{P,l}$ as $B_{P,l}$ under key $q_{P,l}$

\[ h : = H(l, P) \]  
\[ d : = h \cdot x \mod n \]  
\[ B_{P,l} : = S_d(E_{HKDF(l,P)}(R_{P,l})), dG \]  
\[ q_{P,l} : = H(dG) \]

Searching for records under label $l$ in zone $P$

\[ h : = H(l, P) \]  
\[ q_{P,l} : = H(hP) = H(hxG) = H(dG) \Rightarrow \text{obtain } B_{P,l} \]  
\[ R_{P,l} = D_{HKDF(l,P)}(B_{P,l}) \]
Globally unique identifiers

- Public keys are globally unique
- Users can use any public key (in a base32 encoding) as a TLD
- "alice.bob.KEY" is a valid, globally unique identifier
Key revocation

- Revocation message signed with private key (ECDSA)
- Flooded on all links in P2P overlay, stored forever
- Efficient set reconciliation used when peers connect
- Expensive proof-of-work used to limit DoS-potential
- Proof-of-work can be calculated ahead of time
- Revocation messages can be stored off-line if desired
Latest political developments

Originally, GNS used pTLD “.gnu” as protocol switch. draft-grothoff-iesg-special-use-p2p-names tried to make this official following RFC 6761.

- IETF’s dnsop refused to follow RFC 6761 for us, only Apple and Facebook have political power to get “free” TLDs (“.local”, “.onion”)

- But, RFC 8244 (quote from slide 1) is wrong:

  **Our latest release allows users to override *any* domain name**

- Can override “ietf.org”, or “.fr”, or “.bob” by simply specifying a GNS public key for that domain in configuration:
  - Usability greatly improved (thank you, IETF)
  - Transparency reduced for users: usability study showed users cannot tell DNS vs. GNS

- gnunet-dns2gns is DNS proxy speaking DNS resolving some names via GNS
Latest technical developments

- Demonstrated scaling of DHT implementation to deal with millions of records
- Implemented `gnunet-zoneimport` to import DNS records by single query (given list of names)
- Implemented Ascension to import DNS records via AXFR
- Imported “.fr” into GNS zone based on public name list and brute force zone transfer
- Imported “.se” and “bfh.ch” using AXFR
Conclusion and outlook

- The DNS monopoly is over.
- GNS is simpler than DNS: no glue, no NSEC3, no RRSIG
- GNS provides private name resolution and censorship resistance
- GNS does not require ICANN or a root zone or IANA special-use TLDs
- Operators should no longer be advised about “.gnu”, but about name resolution protocol diversity without any signalling
- GNUnet will include domain → public key map in default configuration
  ⇒ Donate just 130,000 EUR to GNUnet e.V. today to get yours!³

³This is a special discount for dnsop members.
Questions?

More Information on the Web:

▶ https://gnunet.org/gns
▶ Slides will be published at https://grothoff.org/christian/.

“When governments fear the people, there is liberty. When the people fear the government, there is tyranny. The strongest reason for the people to retain the right to keep and bear arms is, as a last resort, to protect themselves against tyranny in government.”

—Thomas Jefferson