“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
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
- ...
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

---

2Joint work with Martin Schanzenbach, Matthias Wachs and Patrick Gerber
Zone management

![Zone management interface](image)

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

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

Create a new zone with the given label

Add Zone
Zone label: rms

Select Zone
grothoff
Zone management

Add Zone
Zone label:

Select Zone
 rms

Edit Zone

<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 interface](image)

### Zone Management Interface

**Add Zone**
- Zone label: 

**Select Zone**
- rms

**Edit Zone**

<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>gnu</td>
<td></td>
<td>&lt;new record&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Zone management

![Zone Management Interface](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>www</td>
<td>&lt;new record&gt;</td>
<td>&lt;new name&gt;</td>
</tr>
<tr>
<td></td>
<td>A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CNAME</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MX</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TXT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AAAA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PKEY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LEHO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VPN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PHONE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GNS2DNS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SRV</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TLSA</td>
<td></td>
</tr>
</tbody>
</table>

**Add Zone**
- Zone label: [Input Field]

**Select Zone**
- rms

**Edit Zone**
- Z378HMHARHXWPDBD6D7J0VDYA8ZJ3RPCKFDZPX0XR42SRDFCSB4G

**Expiration**
- Public
Zone management

![Zone management screenshot]

- **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**:
  - Relative
  - Absolute: August 17, 2019
  - Hours: 9
  - Minutes: 56
  - Seconds: 27
Zone management
Zone management

Add Zone
Zone label: [Enter]

Select Zone
rms [Copy] [Delete]

Edit Zone
- Zone label: Z378HMHARHXWPDBD6D70VDYAZJ3RCPKFDZXP0XR42SRDFCSB4G
- Name: www
- Type: A
- Value: 208.118.235.148

- Name: BOX
- Type: 644352022e1edacb350e69317a7f37d769f46f16f437cf8d392319279c93515e1
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 $K_{Bob}^{pub}$ under the label `bob`
Alice can then reach Bob’s Web server under `www.bob.alice`
Name resolution

Bob

DHT

Alice

Bob

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

Alice

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

GNU Name System: 2019 Edition
Name resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

 alice

DHTPUT 8FS7

0

Bob

Alice

...
Name resolution

Bob

DHT

PUT 8FS7-www: 5.6.7.8

Alice

www.bob.alice ?

Bob

8FS7

::

www A 5.6.7.8

::

Alice

A47G

::

bob PKEY 8FS7

::
**Name resolution**

![Diagram showing name resolution process]

1. Bob sends a PUT request to DHT with the name `www.bob.alice`.
2. DHT looks up the name and returns the IP address 5.6.7.8.
3. Alice queries DHT for the name `bob`.
4. DHT responds with the PKEY value `A47G`.

**Interaction with Alice and Bob's databases:**

- **Bob's database:**
  - `8FS7` table:
    - `www` A 5.6.7.8

- **Alice's database:**
  - `A47G` table:
    - `bob` PKEY `8FS7`
Name resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

PKEY 8FS7!

'bob'?

www.bob.alice ?

1

2

3

Bob

8FS7

::

www A 5.6.7.8

::

Alice

A47G

::

bob PKEY 8FS7
Name resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

www.bob.alice ?

www

A

5.6.7.8

8FS7

...  

...  

www

A

5.6.7.8

...  

...  

Bob

DHT

'bob'?

8FS7-www?

PKEY 8FS7!

A47G

...  

...  

www

A

5.6.7.8

...  

...  

Alice

8FS7

PKEY 8FS7!
Name resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

www.bob.alice?

8FS7-www?

A 5.6.7.8!

PKEY 8FS7!

'bob'?

8FS7

www A 5.6.7.8

www A 5.6.7.8

A47G

bob PKEY 8FS7

8FS7
Browser Configuration

![Screenshot of Mozilla Firefox window with Edit menu open]

- **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
Browser Configuration

[Image of Firefox preferences settings with options for ETP Proxy, SOCKS Host, and proxy configuration URL]
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)
Privacy issue: DHT

GNU Name System: 2019 Edition
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 $q_{P,l}$

\[
    h := H(l, P) \quad (1)
\]
\[
    d := h \cdot x \mod n \quad (2)
\]
\[
    B_{P,l} := S_d(E_{HKDF(l,P)}(R_{P,l})), dG \quad (3)
\]
\[
    q_{P,l} := H(dG) \quad (4)
\]
Query privacy: cryptography

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

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

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

\[
\begin{align*}
    h & : = H(l, P) \\
    q_{P,l} & : = H(hP) = H(hxG) = H(dG) \Rightarrow \text{obtain } B_{P,l} \\
    R_{P,l} & = D_{HKDF(l,P)}(B_{P,l})
\end{align*}
\]
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!\(^3\)

\(^3\)This 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