Decentralized Public Key Infrastructures

Christian Grothoff

Berner Fachhochschule

11.6.2021
Learning Objectives

The GNU Name System

Private Information Retrieval

Comparisson of Name Systems

Introduction to GNUnet

References
The GNU Name System (GNS) [1]
The GNU Name System\textsuperscript{1}

Properties of GNS

- Decentralized name system with secure memorable names
- Delegation used to achieve transitivity
- Also supports globally unique, secure identifiers
- Achieves query and response privacy
- Provides alternative public key infrastructure
- Interoperable with DNS

\textsuperscript{1} Joint work with Martin Schanzenbach and Matthias Wachs
Zone Management: like in DNS

<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>MX</td>
<td>5, mail.+</td>
<td>end of time</td>
<td></td>
</tr>
<tr>
<td>priv</td>
<td>PKEY</td>
<td>3iQT1G601GUBV055C0J0070EFBBN3DBQ4L95BI8PFLR8UKCVGHG</td>
<td>end of time</td>
<td></td>
</tr>
<tr>
<td>heise</td>
<td>LEHO</td>
<td>heise.de</td>
<td>end of time</td>
<td></td>
</tr>
<tr>
<td>home</td>
<td>AAAA</td>
<td>2a02:2e0:3fe:100::8</td>
<td>end of time</td>
<td></td>
</tr>
<tr>
<td>大学</td>
<td>A</td>
<td>193.99.144.80</td>
<td>end of time</td>
<td></td>
</tr>
<tr>
<td>short</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mail</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>homepage</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcfs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>www</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Welcome to gnunet-setup.
Name resolution in GNS

Bob can locally reach his webserver via www.gnu

Local Zone:

<table>
<thead>
<tr>
<th>www</th>
<th>A</th>
<th>5.6.7.8</th>
</tr>
</thead>
</table>

Bob Bob's webserver

K

Bob pub

K

Bob priv
Bob Builder, Ph.D.
Address: Country, Street Name 23
Phone: 555-12345
Mobile: 666-54321
Mail: bob@H2R84L4JIL3G5C.zkey

Bob gives his public key to his friends, possibly via QR code.
Delegation

- Alice learns Bob’s public key
- Alice creates delegation to zone $K_{\text{pub}}^{Bob}$ under label `bob`
- Alice can reach Bob’s webserver via `www.bob.gnu`
Name Resolution

Bob

Alice

DHT

Bob

Alice

Bob

Alice

8FS7

A47G

www A 5.6.7.8

bob PKEY 8FS7
Name Resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

www      A      5.6.7.8
8FS7
Bob
A47G
...
...
bob     PKEY       8FS7   
Alice

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

0

1

www.bob.gnu ?

8FS7

A47G

bob PKEY 8FS7

8FS7

www A 5.6.7.8

www A 5.6.7.8
Name Resolution

Bob

DHT

Alice

www.bob.gnu ?

1

PUT 8FS7-www: 5.6.7.8

0

... 

www      A      5.6.7.8 

8FS7

Bob

A47G

...

bob     PKEY       8FS7   

Alice

www.bob.gnu ?

1

'bob'?

2
Name Resolution

1. www.bob.gnu ?
2. 'bob'?
3. PKEY 8FS7!

Bob

- 8FS7
  - www: 5.6.7.8

Alice

- A47G
  - bob: PKEY 8FS7
Name Resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

www.bob.gnu?

8FS7-www?

0

0

Bob

DHT

Alice

Bob

8FS7

www

A

5.6.7.8

Alice

A47G

8FS7

bob

PKEY

8FS7!
Name Resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

www.bob.gnu

Bob Alice

DHT

'bob'

PKEY 8FS7!

8FS7-www

A 5.6.7.8!

PUT 8FS7-www: 5.6.7.8

Bob

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

...
GNS as PKI (via DANE/TLSA)

The GNU Project was launched in 1984 to develop the GNU system. The name “GNU” is a recursive acronym for “GNU’s Not Unix!”, “GNU” is pronounced “gno”, as one syllable, like saying “grew” but replacing the r with n.

A Unix-like operating system is a software collection of applications, libraries, and developer tools, plus a program to allocate resources and talk to the hardware, known
Privacy Issue: DHT

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

www.bob.gnu?

'bob'?
PKEY 8FS7!

8FS7-www?

A 5.6.7.8!

PUT 8FS7-www: 5.6.7.8

Bob

8FS7

www A 5.6.7.8

Alice

A47G

bob PKEY 8FS7
Query Privacy: Terminology

\( G \) generator in ECC curve, a point
\( o \) size of ECC group, \( o := |G| \), \( o \) prime
\( x \) private ECC key of zone (\( x \in \mathbb{Z}_o \))
\( P \) public key of zone, a point \( P := xG \)
\( l \) label for record in a zone (\( l \in \mathbb{Z}_o \))
\( R_{P,l} \) 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 $q_{P,l}$

\[ h := H(l, P) \]  \hspace{1cm} (1)

\[ d := h \cdot x \mod o \]  \hspace{1cm} (2)

\[ B_{P,l} := S_d(E_{HKDF(l,P)}(R_{P,l})), dG \]  \hspace{1cm} (3)

\[ q_{P,l} := H(dG) \]  \hspace{1cm} (4)
Query Privacy: Cryptography

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

\[
\begin{align*}
    h & := H(l, P) \quad (1) \\
    d & := h \cdot x \mod o \quad (2) \\
    B_{P,l} & := S_d(E_{HKDF(l,P)}(R_{P,l})), dG \quad (3) \\
    q_{P,l} & := H(dG) \quad (4)
\end{align*}
\]

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

\[
\begin{align*}
    h & := H(l, P) \quad (5) \\
    q_{P,l} & := H(hP) = H(hxG) = H(dG) \Rightarrow \text{obtain } B_{P,l} \quad (6) \\
    R_{P,l} & = D_{HKDF(l,P)}(B_{P,l}) \quad (7)
\end{align*}
\]
Using cryptographic identifiers

- Zone are identified by a public key
- “alice.bob.PUBLIC-KEY” is perfectly legal in GNS!
  \[\Rightarrow\] Globally unique identifiers
GNS Summary

- Interoperable with DNS
- Globally unique identifiers with “.PUBLIC-KEY”
- Delegation allows using zones of other users
- Trust paths explicit, trust agility
- Simplified key exchange compared to Web-of-Trust
- Privacy-enhanced queries, censorship-resistant
- Reliable revocation using flooding with proof-of-work
<table>
<thead>
<tr>
<th>Method</th>
<th>Defense against MiTM</th>
<th>Zone privacy</th>
<th>Privacy vs. network</th>
<th>Privacy vs. operator</th>
<th>Traffic amplification resistance</th>
<th>Censorship resistance</th>
<th>Ease of migration</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>DNSSEC</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>DNSCurve</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>DNS-over-TLS</td>
<td>✓</td>
<td>n/a</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Namecoin</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>RAINS</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>GNS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

*EDNS0
## Key management summary

<table>
<thead>
<tr>
<th>Method</th>
<th>Suitable for personal use</th>
<th>Memorable</th>
<th>Decentralised</th>
<th>Modern cryptography</th>
<th>Understandable</th>
<th>Exposes metadata</th>
<th>Transitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DNSSEC</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DNSCurve</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DNS-over-TLS</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>TLS-X.509</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Web of Trust</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>TOFU</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Namecoin</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>RAINS</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>GNS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Possible Future Work (Project 2, BS thesis)

- Implement Fog-of-Trust (ideally in Rust)
Case study: GNS

DNS is known to suffer from a lack of end-to-end integrity protections. As a result, Chinese "great firewall" DNS manipulation has been shown to impact name resolution even in Europe.

"The GNU Name System (GNS) establishes a new name system using cryptography where zone data, queries and replies are private. The use of a distributed hash table (DHT) implies that resolution costs are comparable to those of DNS. However, states and ISPs cannot monitor or block queries, limiting their ability to protect the public from malicious Web sites. Names are not globally unique, allowing multiple anonymous users to lay claim to the same name. However, the system includes some well-known mappings by default, which users are unlikely to change. Trademarks, copyrights anti-fraud or anti-terrorism judgements can only be enforced against those well-known mappings, which users are able to bypass."

Discuss virtues and vices affected.
**Conclusion**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Philosophy</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>globalist</td>
</tr>
<tr>
<td>DNSSEC</td>
<td>authoritarian</td>
</tr>
<tr>
<td>Namecoin</td>
<td>libertarian (US)</td>
</tr>
<tr>
<td>RAINS</td>
<td>nationalist</td>
</tr>
<tr>
<td>GNS</td>
<td>anarchist</td>
</tr>
</tbody>
</table>

In which world do you want to live?
Exercise

# apt-get install git autoconf automake autopoint gettext
# apt-get install libunistring-dev libgnutls28-dev
# apt-get install openssl gnutls-bin libtool libltdl
# apt-get install libcurl-gnutls-dev libidn11-dev
# apt-get install libsqlite3-dev
$ git clone git://gnunet.org/libmicrohttpd
$ git clone git://gnunet.org/gnunet
$ git clone git://gnunet.org/gnunet-gtk
$ for n in libmicrohttpd gnunet gnunet-gtk do;
    cd $n ; ./bootstrap ; ./configure --prefix=$HOME ...
    make install
    cd ..
done
Exercise

$ gnunet-setup  # enable TCP transport only
$ gnunet-arm -s  # launch peer
$ gnunet-namestore-gtk  # configure your GNS zone
$ gnunet-gns  # command-line resolution
$ gnunet-gns-proxy  # launch SOCKS proxy
$ firefox  # configure browser to use proxy
Matthias Wachs, Martin Schanzenbach, and Christian Grothoff. 
A censorship-resistant, privacy-enhancing and fully decentralized name system. 