The GNU Name System

Christian Grothoff

Technische Universität München

27.12.2013

“Never doubt your ability to change the world.” –Glenn Greenwald

Joint work with Martin Schanzenbach and Matthias Wachs
Trust in Authority: DARPA’s Legacy

- Centralized Internet infrastructure is easily controlled:
  - Number resources (IANA)
  - Domain Name System (Root zone)
  - DNSSEC root certificate
  - X.509 CAs (HTTPS certificates)
  - Major browser vendors (CA root stores!)
- Encryption does not help if PKI is compromised!
The GNU Name System

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

Uses for GNS

- Identify services hosted in P2P networks
- Identity management for social networking applications
Zone Management: like in DNS

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Value</th>
<th>Expired</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>&lt;new record&gt;</td>
<td>MX 5.mail.+</td>
<td>end of time</td>
<td></td>
</tr>
<tr>
<td>priv</td>
<td>&lt;new record&gt;</td>
<td>PKEY 3QT1G601GUBV055C0J087OE8B8N3D8BJQ4L95B18FPL8UKCVGHG</td>
<td>end of time</td>
<td></td>
</tr>
<tr>
<td>heise</td>
<td>&lt;new record&gt;</td>
<td>LEHO heise.de</td>
<td>end of time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AAAA</td>
<td>2a02:2e0:3fe:100::8</td>
<td>end of time</td>
<td></td>
</tr>
<tr>
<td>home</td>
<td>&lt;new record&gt;</td>
<td>A 193.99.144.80</td>
<td>end of time</td>
<td></td>
</tr>
</tbody>
</table>
Bob can locally reach his webserver via **www.gnu**
Secure introduction

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 $K_{Bob}^{pub}$ under label `bob`
- Alice can reach Bob’s webserver via `www.bob.gnu`
Name Resolution

Bob

Alice

DHT

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      A      5.6.7.8

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

1 www.bob.gnu ?

Bob

Alice

8FS7

www A 5.6.7.8

A47G

bob PKEY 8FS7
Name Resolution

Bob

0

PUT 8FS7-www: 5.6.7.8

DHT

1 www.bob.gnu ?

A47G

8FS7

Bob

www A 5.6.7.8

Alice

2 'bob'?

bob PKEY 8FS7

Alice

PUT 8FS7-www: 5.6.7.8

www A 5.6.7.8
Name Resolution

Bob sends PUT 8FS7-www: 5.6.7.8 to DHT.

Alice looks up 'bob' in DHT.

Bob stores www as A 5.6.7.8 in his database.

Alice stores bob as PKEY 8FS7 in her database.
Name Resolution

1. www.bob.gnu?
2. 'bob'?
3. PKEY 8FS7!
4. 8FS7-www?

Bob:
- PUT 8FS7-www: 5.6.7.8

Alice:
- A47G
- bob PKEY 8FS7
- 8FS7-www: 5.6.7.8
Name Resolution

0. PUT 8FS7-www: 5.6.7.8

1. www.bob.gnu?

2. 'bob'?

3. PKEY 8FS7!

4. 8FS7-www?

5. A 5.6.7.8!

Bob

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

Alice

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

DHT
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 gnu, 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 as a kernel.

The Hurd, GNU’s own kernel, is some way from being ready for daily use. Thus, GNU is typically used today with a kernel called Linux. This combination is the GNU/Linux operating system. GNU/Linux is used by millions, though many call it “Linux” by mistake.
Other GNS Features

- Query privacy using cryptography
- Cryptographic identifiers (“.zkey”)
- dns2gns proxy, DNS compatible record types
- Key revocation by P2P flooding
- Name shortening using “NICK” records
- Shadow records for fast transitions

Talk tonight at 9:45pm
GNS Issues

- Legacy applications expect absolute names
GNS Issues

- Legacy applications expect absolute names
- Web-trouble: absolute links, virtual hosts, X509 CN
GNS Issues

- Legacy applications expect absolute names
- Web-trouble: absolute links, virtual hosts, X509 CN
- Depends on censorship-resistant DHT ⇒ latency
  ⇒ Talk tonight at 9:45pm
Conclusion and Future Work

- Decentralization is necessary, hierarchical systems are broken
- DNS and Web are tightly coupled $\Rightarrow$ start with social apps!
Conclusion and Future Work

› Decentralization is necessary, hierarchical systems are broken
› DNS and Web are tightly coupled ⇒ start with social apps!
› New applications ⇔ new (GNS) record types
› Namecoin should support delegation to GNS
Conclusion and Future Work

- Decentralization is necessary, hierarchical systems are broken
- DNS and Web are tightly coupled $\Rightarrow$ start with social apps!
- New applications $\Leftrightarrow$ new (GNS) record types
- Namecoin should support delegation to GNS
- Should we allow delegation to DNS from a security point-of-view?
Do you have any questions?

References:


