A Public Key Infrastructure for Social Movements in the Age of Universal Surveillance

Christian Grothoff

Technische Universität München

24.01.2014

“Never doubt your ability to change the world.” –Glenn Greenwald
Where We Are
Where We Are
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
- Achieves query and response privacy
- Provides alternative public key infrastructure
- Interoperable with DNS

\[^1\] 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>&lt;new record&gt;</td>
<td>5.mail.+</td>
<td>end of time</td>
<td></td>
</tr>
<tr>
<td>prv</td>
<td>&lt;new record&gt;</td>
<td>3IQT1G601GUBVOS5C0J0870EF8B8N3DBJQ4L95BI8PFLR8UKCVGHG</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>AAAAA</td>
<td>2a02:2e0:3fe:100::8</td>
<td>end of time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>193.99.144.80</td>
<td>end of time</td>
<td></td>
</tr>
<tr>
<td>home</td>
<td>&lt;new record&gt;</td>
<td>大学</td>
<td></td>
<td></td>
</tr>
<tr>
<td>short</td>
<td>&lt;new record&gt;</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mail</td>
<td>&lt;new record&gt;</td>
<td>homepage</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>fcf</td>
<td>www</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Welcome to gnunet-setup.
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

DHT

Alice

Bob

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

Alice

<table>
<thead>
<tr>
<th>bob</th>
<th>PKEY</th>
<th>8FS7</th>
</tr>
</thead>
</table>

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

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

www.bob.gnu ?

Bob

Alice

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

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

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Bob

www       A       5.6.7.8

Alice

PUT 8FS7-www: 5.6.7.8

DHT

Alice

bob     PKEY       8FS7   

www.bob.gnu ?

Alice

\[\text{PUT 8FS7-www: 5.6.7.8} \]

\[\text{DHT} \]

\[\text{Alice} \]

\[\text{bob PKEY 8FS7} \]

\[\text{www.bob.gnu ?} \]
Name Resolution

1. Alice requests the URL www.bob.gnu.
2. The DHT server looks up the 'bob' key.
3. Bob responds with the PKEY 8FS7.
4. Alice performs a PUT request for 8FS7-www: 5.6.7.8.
Name Resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

www.bob.gnu?

8FS7-www?

PKEY 8FS7!

'bob'?
Name Resolution

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>bob  PKEY 8FS7</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

DHT

1. www.bob.gnu?
2. 'bob'? 8FS7-ww?
3. PKEY 8FS7!
4. 8FS7-ww?
5. A 5.6.7.8!

PUT 8FS7-www: 5.6.7.8
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 "gnew", 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.
Privacy Issue: DHT

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

www bob.gnu?

1

8FS7-www?

4

A 5.6.7.8!

5

PKEY 8FS7!

3

'bob'?

2

www

A 5.6.7.8

Bob

Alice

8FS7

A47G

bob PKEY 8FS7

8FS7

www A 5.6.7.8

...
Query Privacy: Terminology

\( G \) generator in ECC curve, a point

\( n \) size of ECC group, \( n := |G|, \ n \text{ prime} \)

\( x \) 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 $q_{P,l}$

\[ h := H(l, P) \]  \hspace{1cm} (1)
\[ d := h \cdot x \mod n \]  \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) \\ 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*}
Conclusion

- Decentralization is necessary
- Decentralization creates challenges for research:
  - Privacy-enhancing network protocol design
  - Secure software implementations
  - Software engineering and system architecture
  - Programming languages and tool support
Conclusion

- Decentralization is necessary
- Decentralization creates challenges for research:
  - Privacy-enhancing network protocol design
  - Secure software implementations
  - Software engineering and system architecture
  - Programming languages and tool support

We must decentralize or accept authocracy.
Do you have any questions?

References: