Use-Cases for Private Information Retrieval and Secure Multiparty Computation in Modern Network Architecture

Christian Grothoff

11.02.2020
Internet Design Goals (David Clark, 1988)

1. Internet communication must continue despite loss of networks or gateways.
2. The Internet must support multiple types of communications service.
3. The Internet architecture must accommodate a variety of networks.
4. The Internet architecture must permit distributed management of its resources.
5. The Internet architecture must be cost effective.
6. The Internet architecture must permit host attachment with a low level of effort.
7. The resources used in the internet architecture must be accountable.
Design Choices for a Civil Network!

Internet Design Goals (David Clark, 1988)

1. Internet communication must continue despite loss of networks or gateways.
2. The Internet must support multiple types of communications service.
3. The Internet architecture must accommodate a variety of networks.
4. The Internet architecture must permit distributed management of its resources.
5. The Internet architecture must be cost effective.
6. The Internet architecture must permit host attachment with a low level of effort.
7. The resources used in the internet architecture must be accountable.

GNUnet Design Goals

1. GNUnet must be implemented as Free Software.
2. GNUnet must minimize the amount of personally identifiable information exposed.
3. The GNUnet must be fully distributed and resilient to external attacks and rogue participants.
4. GNUnet must be self-organizing and not depend on administrators or centralized infrastructure.
5. GNUnet must inform the user which other participants have to be trusted when establishing private communications.
6. GNUnet must be open and permit new peers to join.
7. GNUnet must support a diverse range of applications and devices.
8. GNUnet must use compartmentalization to protect sensitive information.
9. The GNUnet architecture must be resource efficient.
10. GNUnet must provide incentives for peers to contribute more resources than they consume.
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
- ...

Use-Cases for PIR and SMC
Part I: Private Information Retrieval
Back to the Internet: 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

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

Add Zone
Zone label: <new name>

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: rms

Select Zone
grothoff

Create a new zone with the given label

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

Use-Cases for PIR and SMC
Zone management

Add Zone
Zone label:

Select Zone
rms

Edit Zone
Name  Type  Value  Expiration  Public
<new name>
gnu  <new record>
Zone management
Zone management

[Image of zone management software interface]

- **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
  - Never
  - Selected date: August 17, 2019
  - Hours: 9
  - Minutes: 56
  - Seconds: 27

[Button options: Cancel, Save]
Zone management

Use-Cases for PIR and SMC
Zone management
Zone management

Use-Cases for PIR and SMC


Expiration Time:
- August
- Calendar with dates:
  - Sun: 31, 28, 29, 30
  - Mon: 4, 5, 6
  - Tue: 11, 12, 13
  - Wed: 18, 19, 20
  - Thu: 25, 26, 27
  - Fri: 1
  - Sat: 2
- Hours: 16, Minutes: 7, Seconds: 30
- Save button

Expiration Date: 2019-08-17
Zone management

Use-Cases for PIR and SMC
Name resolution in GNS

Bob can now reach his Web server under www.bob
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
Delegation

- 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>Bob</th>
<th>Alice</th>
</tr>
</thead>
<tbody>
<tr>
<td>8FS7</td>
<td>A47G</td>
</tr>
<tr>
<td>www</td>
<td>A</td>
</tr>
<tr>
<td>5.6.7.8</td>
<td>PKEY</td>
</tr>
</tbody>
</table>

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

Use-Cases for PIR and SMC
Name resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

Use-Cases for PIR and SMC
Name resolution

Bob

PUT 8FS7-www: 5.6.7.8

DHT

Alice

www.bob.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>

Use-Cases for PIR and SMC
Name resolution

Bob

DHT

Alice

PUT 8FS7-www: 5.6.7.8

0

1 www.bob.alice?

2 'bob'?

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>
</tbody>
</table>

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

1. Bob queries DHT for "www.bob.alice".
2. DHT responds with "bob".
3. Bob encrypts "www: 5.6.7.8" and stores it in the DHT.
4. Alice queries DHT for "bob".
5. DHT responds with "www: 5.6.7.8".
6. Alice decrypts the response and retrieves the IP address.
Name resolution

Use-Cases for PIR and SMC
Name resolution

0. Bob PUT 8FS7-www: 5.6.7.8

1. www.bob.alice?

2. 'bob'?

3. PKEY 8FS7!

4. 8FS7-www?

5. A 5.6.7.8!

Use-Cases for PIR and SMC
Browser Configuration
Browser Configuration
Browser Configuration

Advanced

Connection
Configure how Firefox connects to the Internet

Cached Web Content
Your web content cache is currently using 345 MB of disk space
- Override automatic cache management
- Limit cache to 350 MB of space

Offline Web Content and User Data
Your application cache is currently using 0 bytes of disk space
- Tell me when a website asks to store data for offline use
The following websites are allowed to store data for offline use:
Browser Configuration
Browser Configuration

Use-Cases for PIR and SMC
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

Bob sends a PUT request to the DHT with the key 'bob' and value 8FS7-www: 5.6.7.8.

Alice receives the DHT request and responds with the key 8FS7-www and value A 5.6.7.8.

Bob's local storage shows the entry www www 8FS7 5.6.7.8.

Alice's local storage shows the entry 'bob' PKEY 8FS7.
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 \( q_{P,l} \)
Private Information Retrieval

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

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

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)

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

\[ h := H(l, P) \]  \hspace{1cm} (5)
\[ q_{P,l} := H(hP) = H(hxG) = H(dG) \Rightarrow \text{obtain } B_{P,l} \]  \hspace{1cm} (6)
\[ R_{P,l} = D_{HKDF(l,P)}(B_{P,l}) \]  \hspace{1cm} (7)
Part II: Secure Multiparty Computation
Core features of social networking applications

▶ Users create profiles and messages ("user-generated content")
▶ Users connect to each other and/or subscribe to channels
▶ Communication happens over those connections

Why?
Core features of social networking applications

- Users create profiles and messages ("user-generated content")
- Users connect to each other and/or subscribe to channels
- Communication happens over those connections

Why?

Management of information overload via collaborative filtering
Application Domains

**Business**
- LinkedIn
- XING

**News**
- Diaspora*
- Bitmessage

**Friendship**
- Tinder
- GNU Social
Architectures for Social Networks

Centralized

Federated

Decentralized

Use-Cases for PIR and SMC
Secure Multiparty Computation

- Alice and Bob have private inputs $a_i$ and $b_i$.
- Alice and Bob run a protocol to collaboratively compute $f(a_i, b_i)$.
- Only one of them learns the result.
- Adversary model: honest but curious.
Collaborative Filtering ≡ Scalar product

Motivation

- **Scalarproduct ⇒ Cosinus-Similarity:**

\[
\vec{a} \cdot \vec{b} = ||\vec{a}|| \cdot ||\vec{b}|| \cos \theta \tag{8}
\]

\[\iff \cos \theta = \frac{\vec{a} \cdot \vec{b}}{||\vec{a}|| \cdot ||\vec{b}||} \tag{9}\]
Collaborative Filtering $\equiv$ Scalar product

### Motivation

- **Scalar product $\Rightarrow$ Cosinus-Similarity:**

  $\vec{a} \cdot \vec{b} = ||\vec{a}|| \cdot ||\vec{b}|| \cos \theta$  \hspace{1cm} (8)

  $\Leftrightarrow \cos \theta = \frac{\vec{a} \cdot \vec{b}}{||\vec{a}|| \cdot ||\vec{b}||}$  \hspace{1cm} (9)

### Properties

- Private inputs remain protected (given limited number of interactions)
- Efficient in bandwidth and computation
The Protocol\textsuperscript{3}

Alice’s public key is $A = g^a$, her private key is $a$. Alice sends to Bob $(g_i, h_i) = (g^{r_i}, g^{r_i a + a_i})$ with random values $r_i$ for $i \in M$. Bob replies with:

$$\left(\prod_{i \in M} g_i^{b_i}, \prod_{i \in M} h_i^{b_i}\right) = \left(\prod_{i \in M} g_i^{b_i}, (\prod_{i \in M} g_i^{b_i})^a g^{\sum_{i \in M} a_i b_i}\right)$$

Alice can then compute:

$$\left(\prod_{i \in M} g_i^{b_i}\right)^{-a} \cdot \left(\prod_{i \in M} g_i^{b_i}\right)^{a} \cdot g^{\sum_{i \in M} a_i b_i} = g^{\sum_{i \in M} a_i b_i}.$$

If $\sum_{i \in M} a_i b_i$ is sufficiently small, Alice can efficiently compute the scalar product by solving the DLP.

\textsuperscript{3}Joint work with Tanja Lange
The pre-computation for ECC-2^{28} is $\times 16$ more expensive than for ECC-2^{20}, as the table grows with $\sqrt{n}$.
Conclusion

- GNU name system is a PKI using private information retrieval
- SMC can be used to efficiently perform collaborative filtering
- Cryptography can help us build better privacy-preserving decentralized networks!

This was only a short introduction. GNUnet includes other cool cryptographic protocols.
Questions?

Literature:


More Information on the Web:

- https://gnunet.org/
- https://taler.net/
- https://grothoff.org/christian/