

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

Christian Grothoff

• • • • Berner Fachhochschule
Technik und Informatik



11.02.2020

Context



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.**

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.**

GNUet Design Goals

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

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 solutions¹ will **not** fix this.

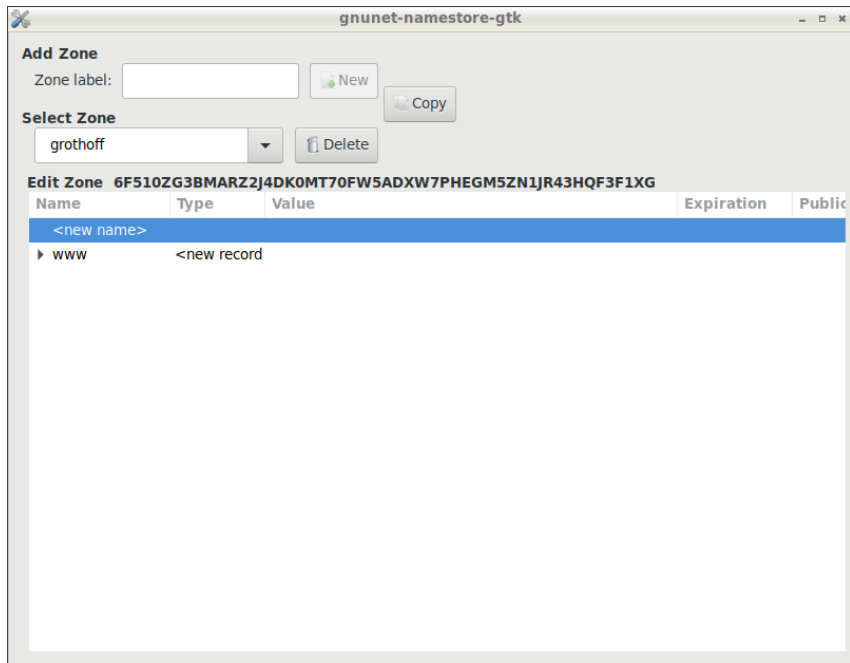
¹DNS-over-TLS, DoH, DNSSEC, DPRIVE, ...

The GNU name system²

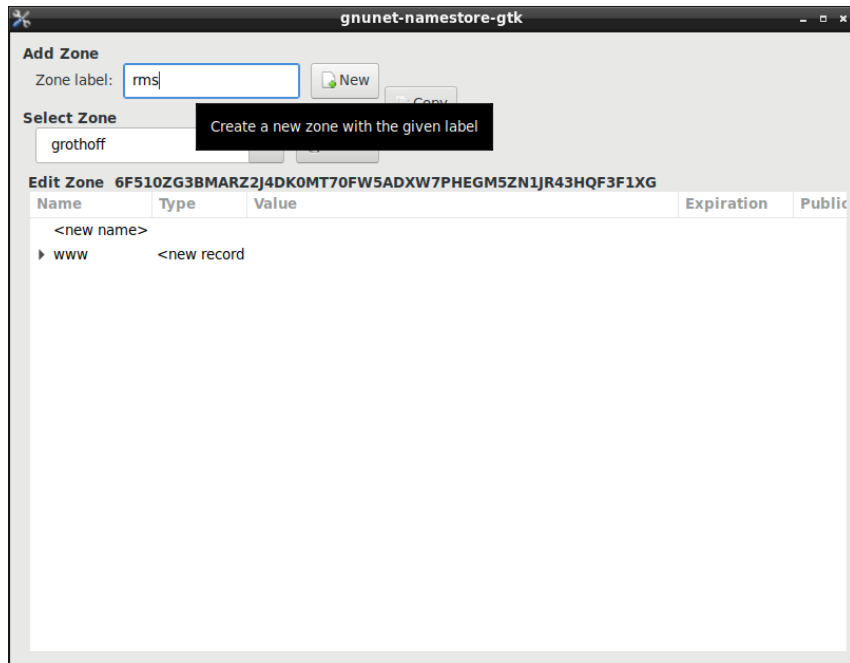
- ▶ Decentralized name system \Rightarrow Names are not global
- ▶ Supports globally unique (& secure) identification
- ▶ Achieves query and response privacy
- ▶ Provides public key infrastructure
- ▶ Interoperable with DNS

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

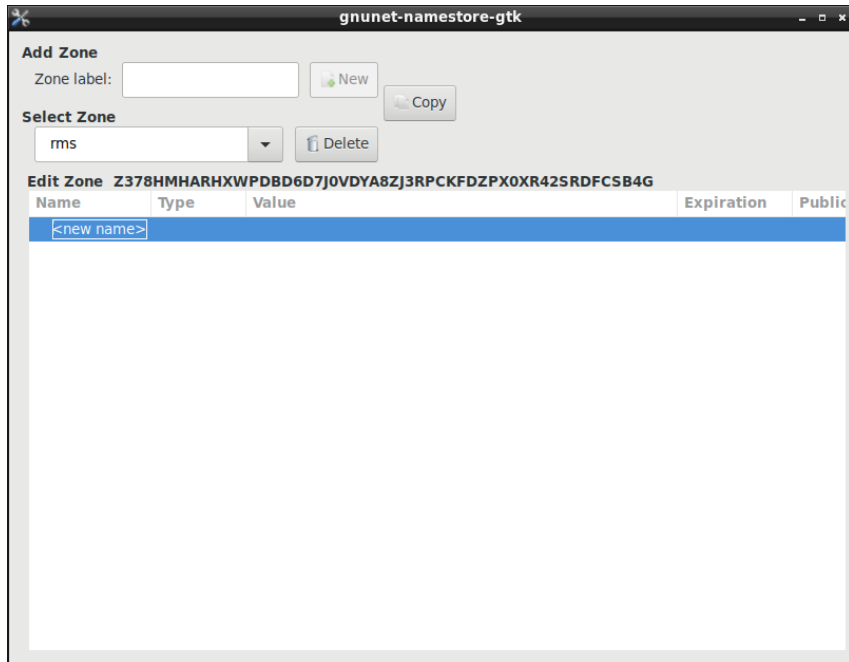
Zone management



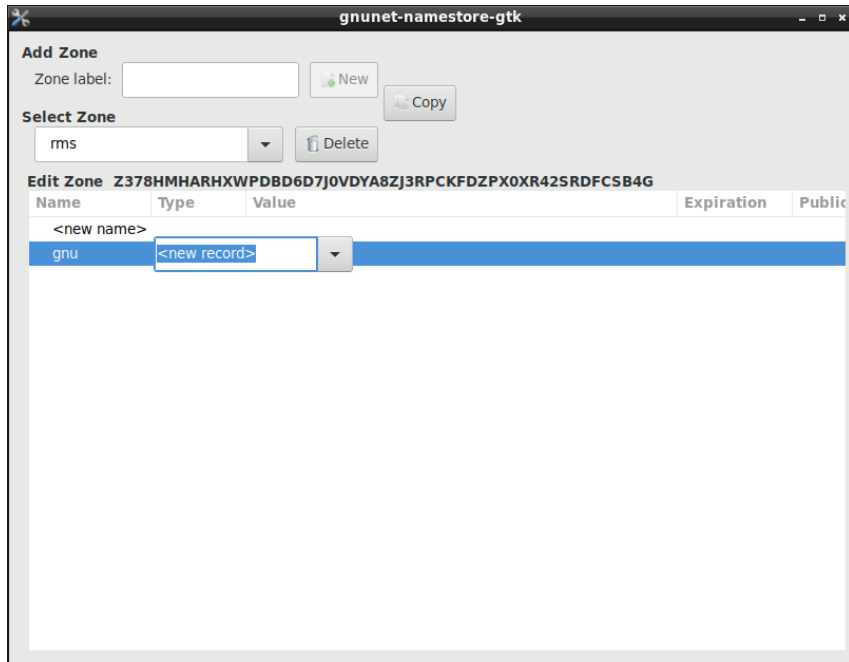
Zone management



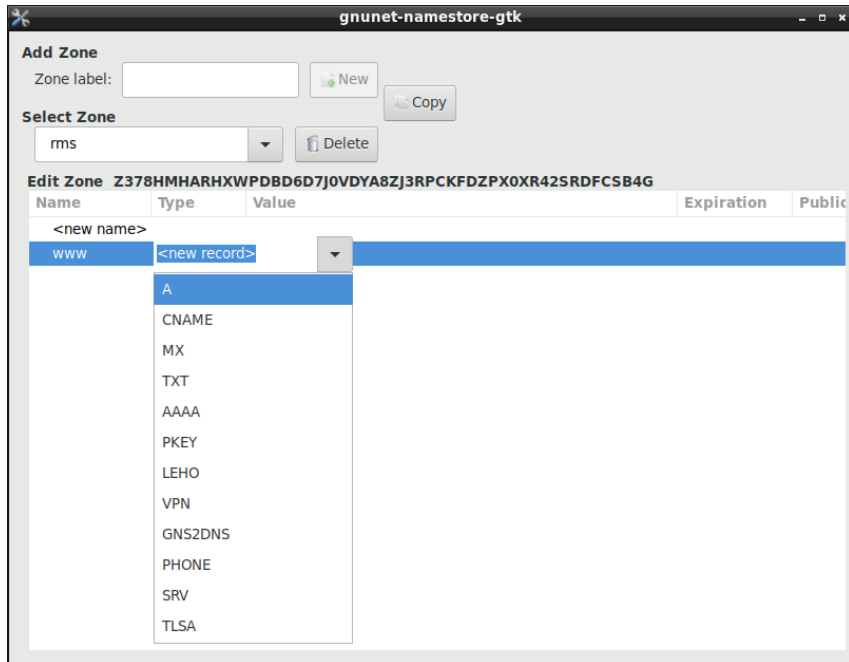
Zone management



Zone management



Zone management



Zone management

gnunet-namestore-gtk

Name

www in rms

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

< August > < 2019 >

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	28	29	30	31	1	2	3
32	4	5	6	7	8	9	10
33	11	12	13	14	15	16	17
34	18	19	20	21	22	23	24
35	25	26	27	28	29	30	31
36	1	2	3	4	5	6	7

Hours: 9 - + Minutes: 56 - + Seconds: 27 - +

Cancel Save

Zone management

The screenshot shows the 'gnunet-namestore-gtk' application window. It has three main sections: 'Add Zone', 'Select Zone', and 'Edit Zone'.
1. 'Add Zone': Includes a 'Zone label:' text input field, a 'New' button, and a 'Copy' button.
2. 'Select Zone': Includes a dropdown menu showing 'rms' and a 'Delete' button.
3. 'Edit Zone': The title is 'Edit Zone Z378HMHARHXWPDBD6D7J0VDYA8ZJ3RPCKFDZPX0XR42SRDFCSB4G'. It contains a table with columns: Name, Type, Value, Expiration, and Public. The table has one row for 'www' with Type 'A', Value '8', and Expiration 'Sat Aug 17 10:56:27 2019'. A dropdown menu is open over the 'Type' column, listing various DNS record types: A, CNAME, MX, TXT, AAAA, PKEY, LEHO, VPN, GNS2DNS, PHONE, SRV, and TLSA (which is highlighted).

Name	Type	Value	Expiration	Public
<new name>				
www	A	8	Sat Aug 17 10:56:27 2019	<input checked="" type="checkbox"/>

Zone management

gnunet-namestore-gtk

Name
Port: - + Protocol: tcp Label in

TLSA Record Information
Usage: CA Constr. Service Cert. Constr. Trust Anchor Assertion Domain Issued Cert.
Selector: Full certificate Subject public key
Matching-Type: Full contents SHA-256 SHA-512

Certificate:

Import from:

Options
 Record is public (visible to other users)
 Record is a shadow record (valid after other records expire)

Expiration Time
 Relative Absolute Never

< August > < 2019 >

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	28	29	30	31	1	2	3
32	4	5	6	7	8	9	10
33	11	12	13	14	15	16	17
34	18	19	20	21	22	23	24
35	25	26	27	28	29	30	31
36	1	2	3	4	5	6	7

Hours: - + Minutes: - + Seconds: - +

Zone management

gnunet-namestore-gtk

Name
Port: 443 - + Protocol: tcp Label: www in rms

TLSA Record Information
Usage: CA Constr. Service Cert. Constr. Trust Anchor Assertion Domain Issued Cert.
Selector: Full certificate Subject public key
Matching-Type: Full contents SHA-256 SHA-512
Certificate:
2e1e12dacb350e69317a7f37d769f46f16f437cf8d392319279c93515e5600baed3d3acd5dc83b673e8c60cf7
fba0dce00a4d162a3b966a3ebf72487c376fca0

Certificate:

Import from: www.gnu.org

Options
 Record is public (visible to other users)
 Record is a shadow record (valid after other records expire)

Expiration Time
 Relative Absolute Never

< August > < 2019 >

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	28	29	30	31	1	2	3
32	4	5	6	7	8	9	10
33	11	12	13	14	15	16	17
34	18	19	20	21	22	23	24
35	25	26	27	28	29	30	31
36	1	2	3	4	5	6	7

Hours: 16 - + Minutes: 7 - + Seconds: 30 - +

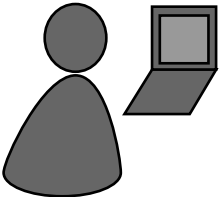
Zone management

The screenshot shows a window titled "gnunet-namestore-gtk". It has three main sections:

- Add Zone:** A text input field for "Zone label:" with a "New" button to its right and a "Copy" button below it.
- Select Zone:** A dropdown menu showing "rms" and a "Delete" button to its right.
- Edit Zone:** A title bar for the current zone: "Z378HMHARHXWPDBD6D7JOVDYA8ZJ3RPCKFDZPX0XR42SRDFCSB4G". Below this is a table with columns "Name", "Type", and "Value".

Name	Type	Value
<new name>		
www	<new record	
	A	208.118.235.148
	BOX	6 443 52 2 0 2 2e1e12dacb350e69317a7f37d769f46f16f437cf8d392319279c93515e5

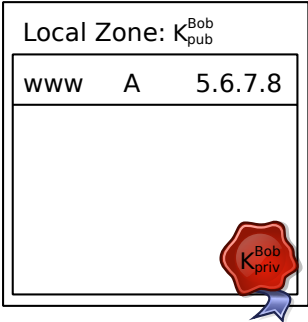
Name resolution in GNS



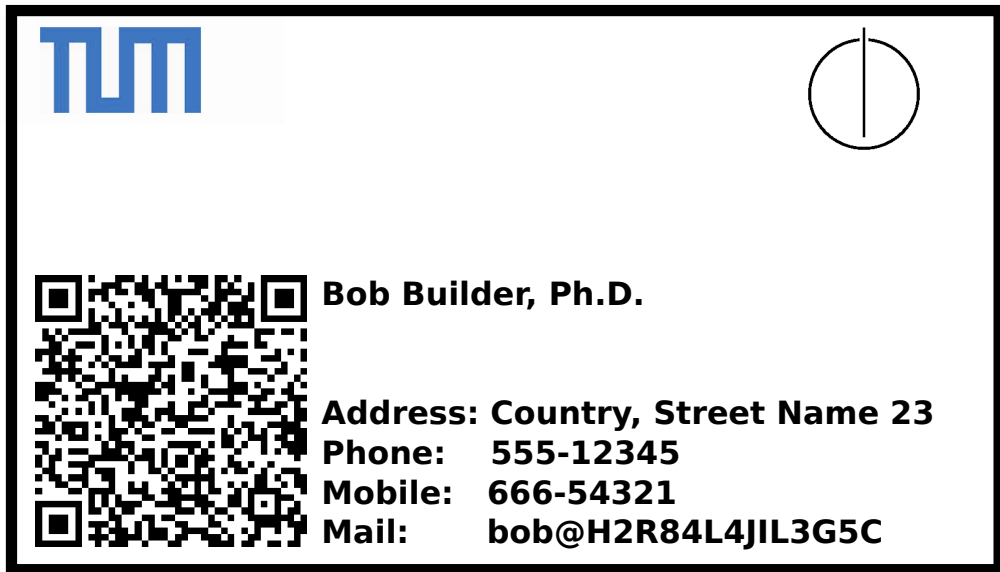
Bob



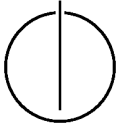
Bob's webserver



- ▶ Bob can now reach his Web server under **www.bob**



TUM



Bob Builder, Ph.D.

Address: Country, Street Name 23

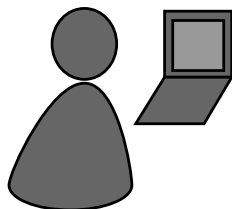
Phone: 555-12345

Mobile: 666-54321

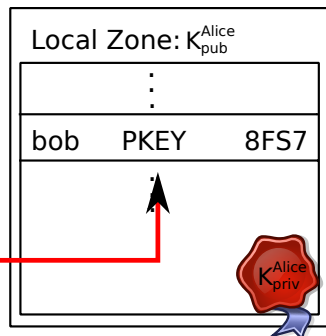
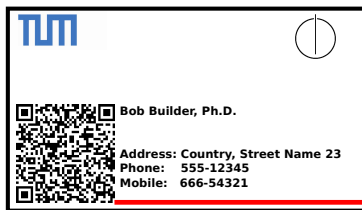
Mail: bob@H2R84L4JIL3G5C

- ▶ Bob provides his public key to his friends, i.e. via QR code

Delegation

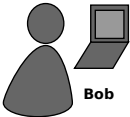


Alice



- ▶ 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**

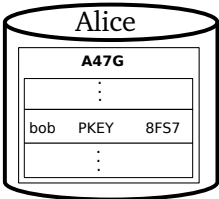
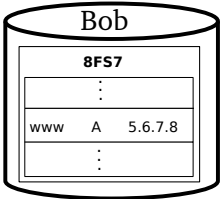
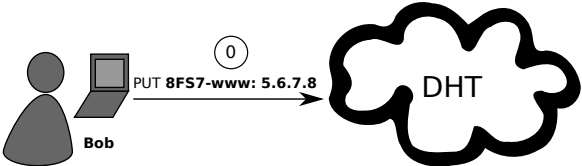
Name resolution



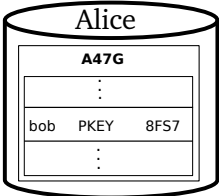
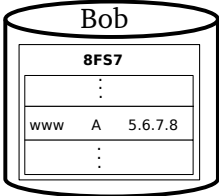
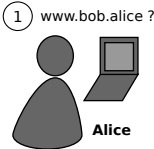
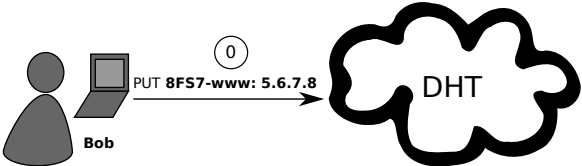
Bob			
8FS7			
⋮			
www	A	5.6.7.8	
⋮			

Alice		
A47G		
⋮		
bob	PKEY	8FS7
⋮		

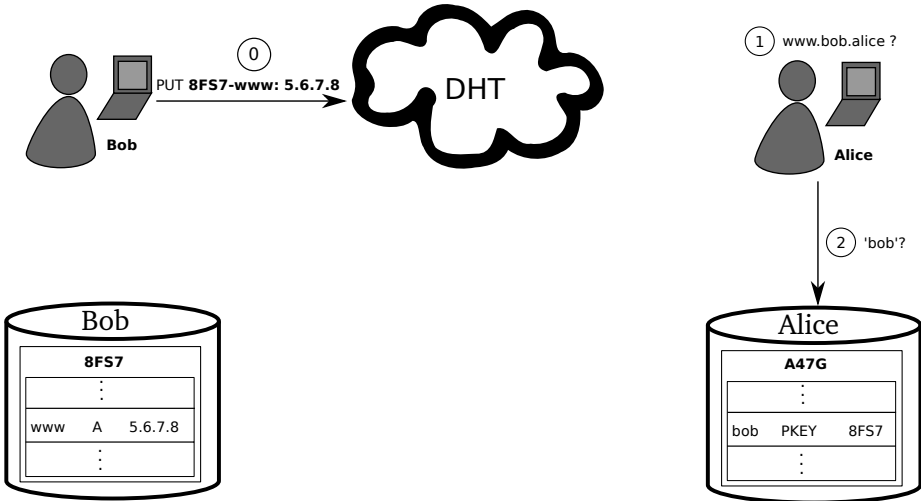
Name resolution



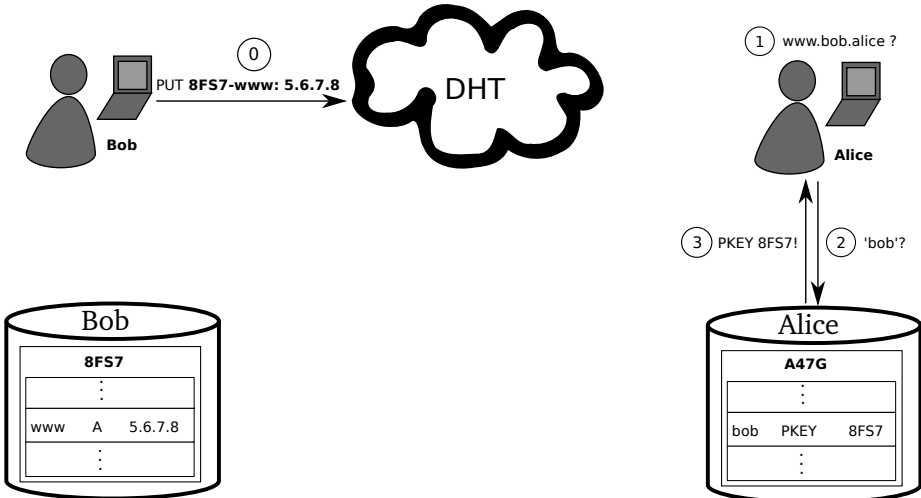
Name resolution



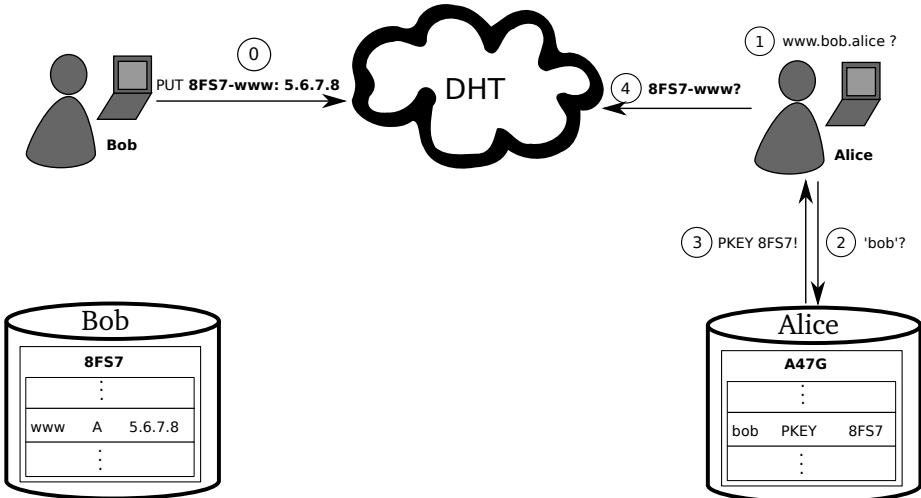
Name resolution



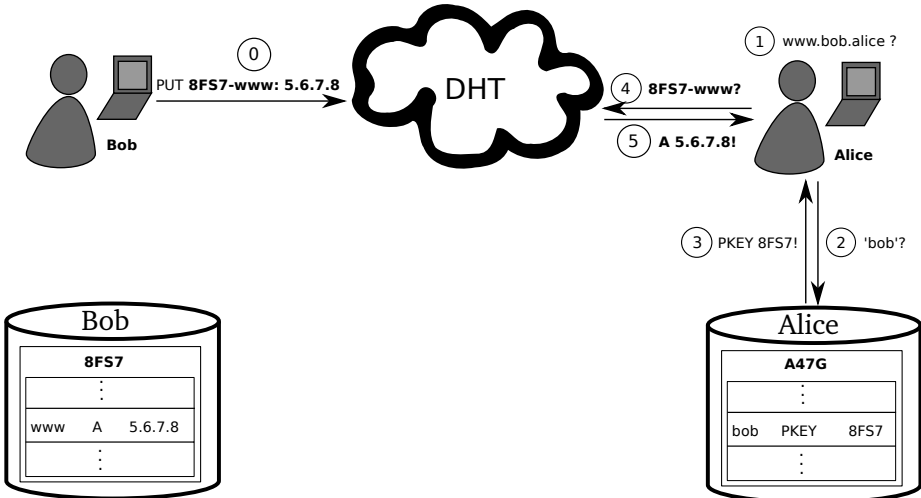
Name resolution



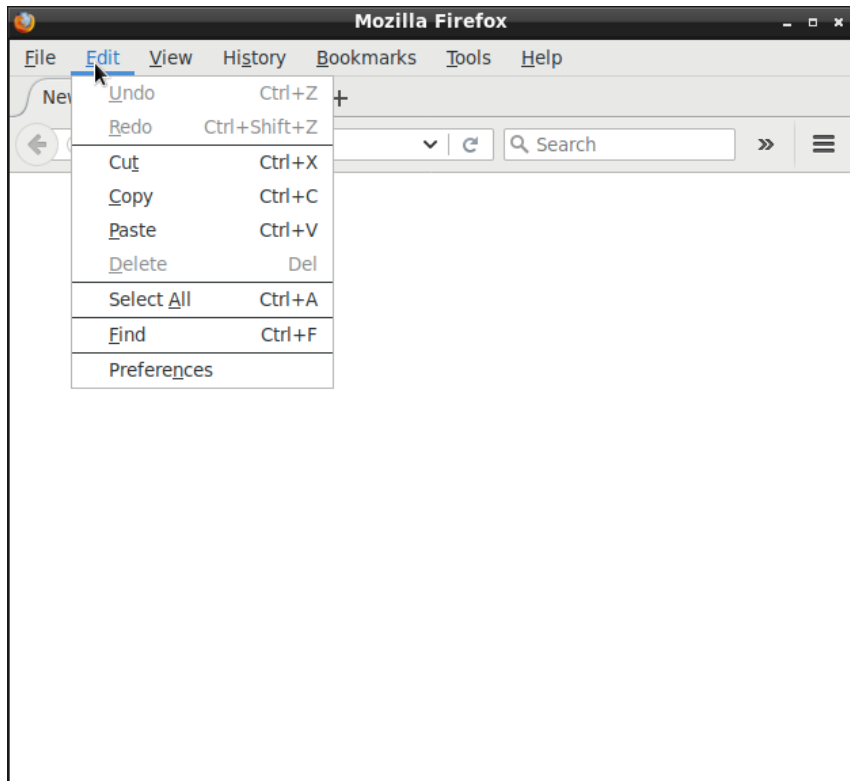
Name resolution



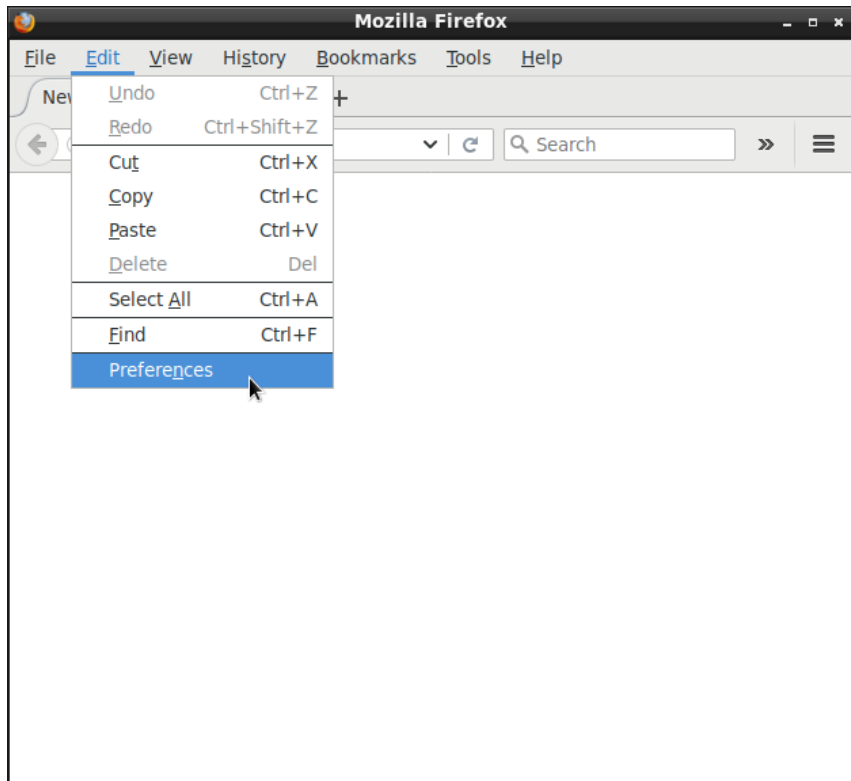
Name resolution



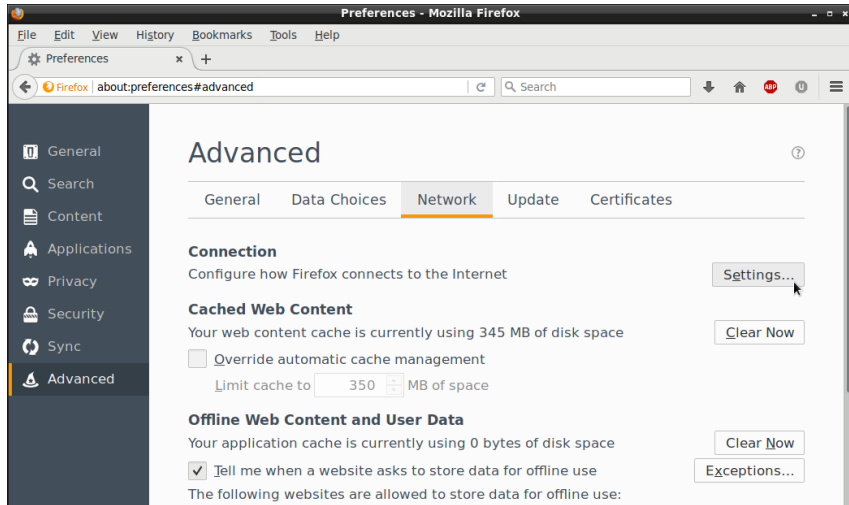
Browser Configuration



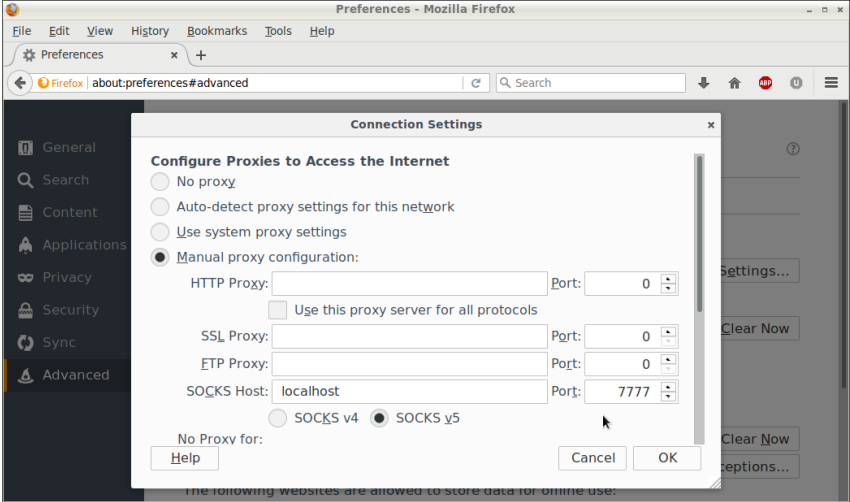
Browser Configuration



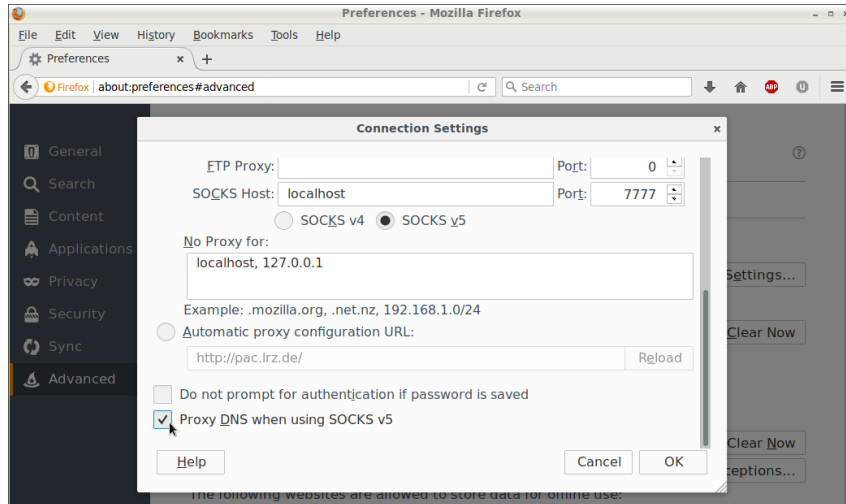
Browser Configuration



Browser Configuration



Browser Configuration



Browser Usage

The screenshot shows a Mozilla Firefox browser window titled "The GNU Operating System and the Free Software Movement - Mozilla Firefox". The address bar shows "https://www.rms". The page content includes a navigation menu with links for "EDUCATION", "SOFTWARE", "DOCUMENTATION", and "HELP GNU". A prominent red button says "JOIN THE FSF". Below it, a section titled "Free Software Supporter" has a form for an "email address" and a "Sign up" button. The main content area features a heading "What is GNU?" followed by a paragraph explaining GNU as free software. A sidebar on the right contains a "Planet GNU" section with a link to "LibreJS 7.15 released".

The GNU Operating System and the Free Software Movement - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Preferences x The GNU Operating S... x +

https://www.rms

Why GNU/Linux? Search

العربية [ar] [es] فارسی [fa] français [fr] italiano [it] 日本語 [ja] 한국어 [ko] lietuvių [lt] uij Shqip [sq] українська [uk] 简体中文 [zh-cn] 繁體中文 [zh-tw]

JOIN THE FSF

Free Software Supporter

email address Sign up

EDUCATION SOFTWARE DOCUMENTATION HELP GNU

What is GNU?

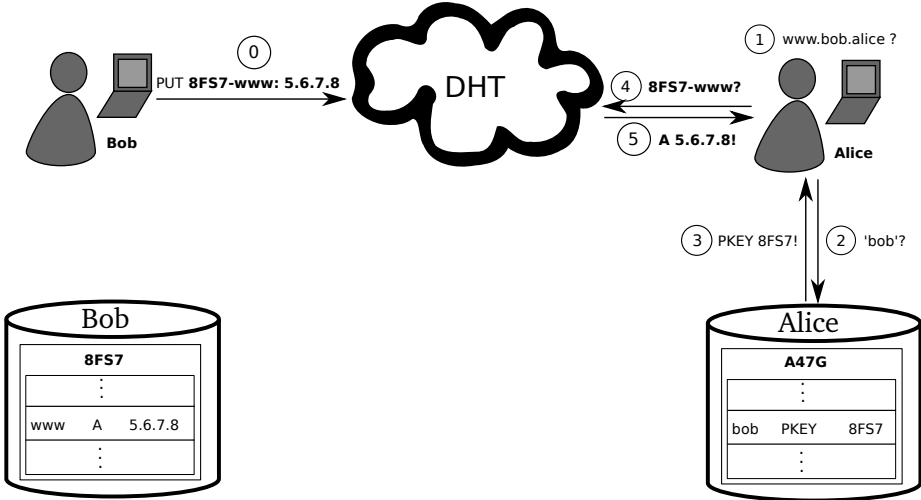
GNU is an operating system that is [free software](#)—that is, it respects users' freedom. The GNU operating system consists of GNU packages (programs specifically released by the GNU Project) as well as free software released by third parties. The development of GNU made it possible to use a computer 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



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 $q_{P,l}$

$$h := H(l, P) \tag{1}$$

$$d := h \cdot x \pmod n \tag{2}$$

$$B_{P,l} := S_d(E_{HKDF(l,P)}(R_{P,l})), dG \tag{3}$$

$$q_{P,l} := H(dG) \tag{4}$$

Private Information Retrieval

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

$$h := H(l, P) \tag{1}$$

$$d := h \cdot x \pmod n \tag{2}$$

$$B_{P,l} := S_d(E_{HKDF(l,P)}(R_{P,l})), dG \tag{3}$$

$$q_{P,l} := H(dG) \tag{4}$$

Searching for records under label l in zone P

$$h := H(l, P) \tag{5}$$

$$q_{P,l} := H(hP) = H(hxG) = H(dG) \Rightarrow \text{obtain } B_{P,l} \tag{6}$$

$$R_{P,l} = D_{HKDF(l,P)}(B_{P,l}) \tag{7}$$

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



XING

News

diaspora*



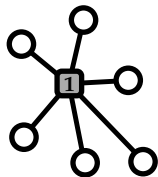
Bitmessage

Friendship

tinder.

gnusocial

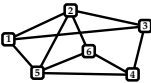
Architectures for Social Networks



Centralized



Federated



Decentralized



diaspora*



[matrix]



Bitmessage



gnusocial



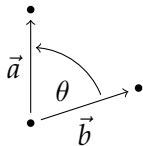
Secure Multiparty Computation

- ▶ 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 \equiv Scalar product

Motivation

► Scalarproduct \Rightarrow Cosinus-Similarity:



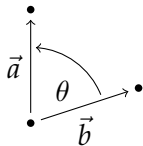
$$\vec{a} \cdot \vec{b} = \|\vec{a}\| \cdot \|\vec{b}\| \cos \theta \quad (8)$$

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

Collaborative Filtering \equiv Scalar product

Motivation

- ▶ Scalarproduct \Rightarrow Cosinus-Similarity:



$$\vec{a} \cdot \vec{b} = \|\vec{a}\| \cdot \|\vec{b}\| \cos \theta \quad (8)$$

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

Properties

- ▶ Private inputs remain protected (given limited number of interactions)
- ▶ Efficient in bandwidth and computation

The Protocol³

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:

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

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.

³Joint work with Tanja Lange

Preliminary experimental results

Länge	ECC-2 ²⁰	ECC-2 ²⁸
25	2 s	29 s
50	2 s	29 s
100	2 s	29 s
200	3 s	30 s

The pre-computation for ECC-2²⁸ is $\times 16$ more expensive than for ECC-2²⁰, 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:

- ▶ Matthias Wachs, Martin Schanzenbach and Christian Grothoff. *A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System*. **13th International Conference on Cryptology and Network Security**, 2014.
- ▶ Geert Lovink and Miriam Rasch. *Unlike Us Reader: Social Media Monopolies and their Alternatives*. Institute of Network Cultures, 2013.
- ▶ John Naughton. *Death by drone strike, dished out by algorithm*, **The Guardian**, 21.2.2016.
- ▶ Lee Fang. *The CIA is investing in firms that mine your Tweets and Instagram photos*. **The Intercept**, 14.4.2016.

More Information on the Web:

- ▶ <https://gnunet.org/>
- ▶ <https://taler.net/>
- ▶ <https://grothoff.org/christian/>