

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



Source: esmont



Source: gaWand.org



Where We Are



الموقع محظور

أسف! إن الموقع الذي أردت تصفحه قد أُحجب وذلك بسبب إحتوائه على نشاط مخالف للقيم الاجتماعية أو السياسية أو الثقافية أو الدينية لخدمة الإمارات العربية المتحدة.

في حالة أردت فتح موقع قد أُحجب الرجاء قم بتصفة إستشارة الملاحظات المقدمة على موقعنا.

We apologize the site you are attempting to visit has been blocked due to its content being inconsistent with the religious, cultural, political and moral values of the United Arab Emirates.

If you think this site should not be blocked, please visit the [Feedback Form](#) available on our website.

SITE BLOCKED

Source: wikileaks.org



Not Just Monitoring

- ▶ 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 System¹

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

¹Joint work with Martin Schanzenbach and Matthias Wachs

Zone Management: like in DNS


gnunet-setup


General Network Transports File Sharing Namestore **GNS**

Editing zone API5QDP7A126P06VV60535PDT50B9L12NK6QP64IE8KNC6E807G0 

Preferred zone name (PSEU):

Master Zone Private Zone Shorten Zone

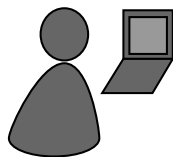


 Save As

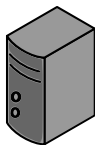
Name	Type	Value	Expiration	Public
<new name>				
+ >	<new record>			
	MX	5,mail.+	end of time	<input checked="" type="checkbox"/>
priv >	<new record>			
	PKEY	3IQ1TG601GUBVO55C0J087OEFB8N3DBJQ4L9SBI8PFLR8UKCVGHG	end of time	<input type="checkbox"/>
heise >	<new record>			
	LEHO	heise.de	end of time	<input checked="" type="checkbox"/>
	AAAA	2a02:2e0:3fe:100::8	end of time	<input checked="" type="checkbox"/>
	A	193.99.144.80	end of time	<input checked="" type="checkbox"/>
home >	<new record>			
大学 >	<new record>			
short >	<new record>			
mail >	<new record>			
homepage >	<new record>			
fcfs >	<new record>			
www >	<new record>			

[Welcome to gnunet-setup.](#)


Name resolution in GNS



Bob




Bob's webserver

Local Zone: K_{pub}^{Bob}		
www	A	5.6.7.8
		


- ▶ Bob can locally reach his webserver via **www.gnu**

Secure introduction



TUM

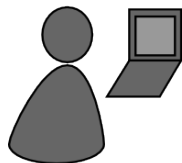


 **Bob Builder, Ph.D.**

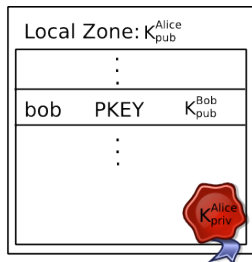
Address: Country, Street Name 23
Phone: 555-12345
Mobile: 666-54321
Mail: bob@H2R84L4JIL3G5C.zkey

- ▶ Bob gives his public key to his **friends**, possibly via QR code

Delegation

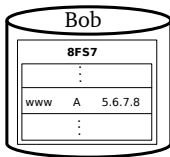
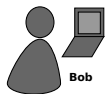


Alice

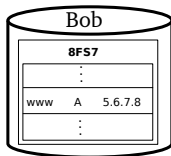
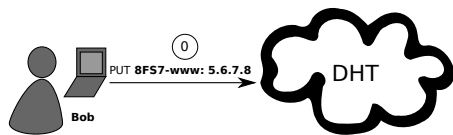


- ▶ Alice learns Bob's public key
- ▶ Alice creates delegation to zone K_{pub}^{Bob} under label **bob**
- ▶ Alice can reach Bob's webserver via **www.bob.gnu**

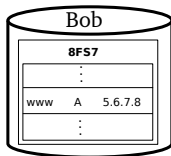
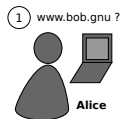
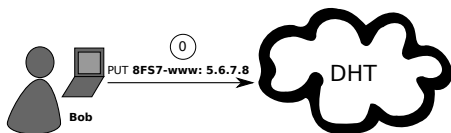
Name Resolution



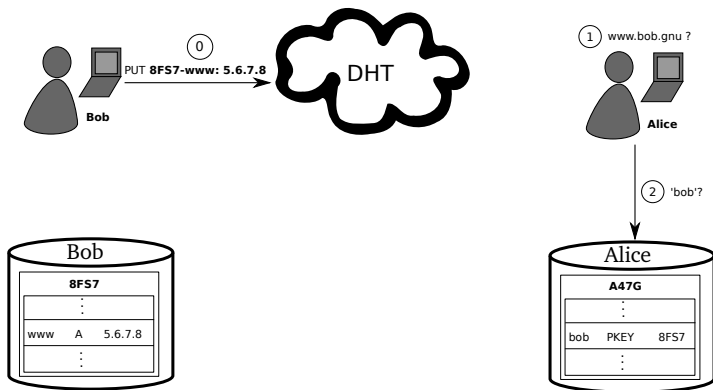
Name Resolution



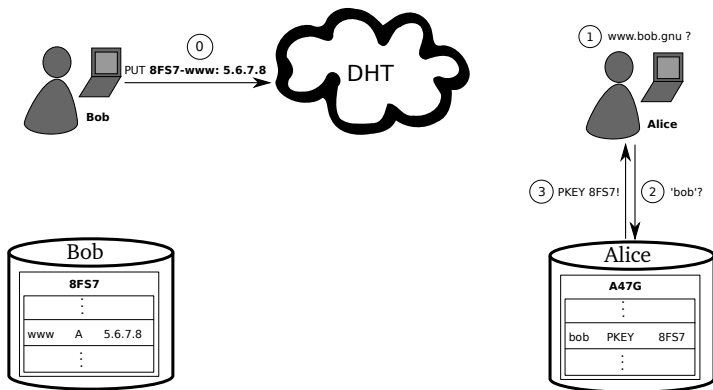
Name Resolution



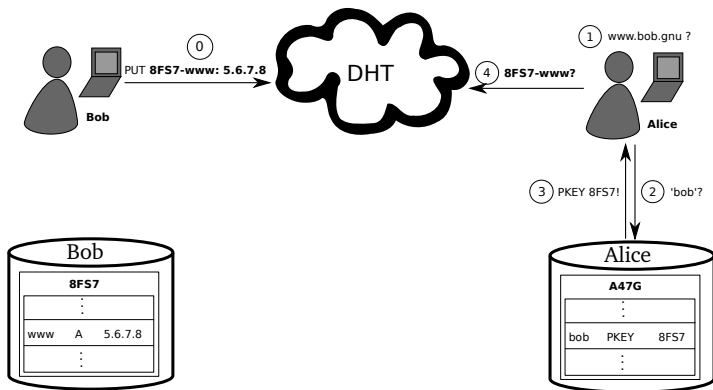
Name Resolution



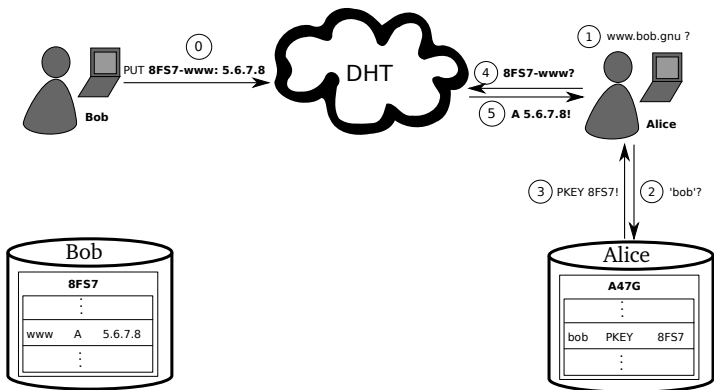
Name Resolution



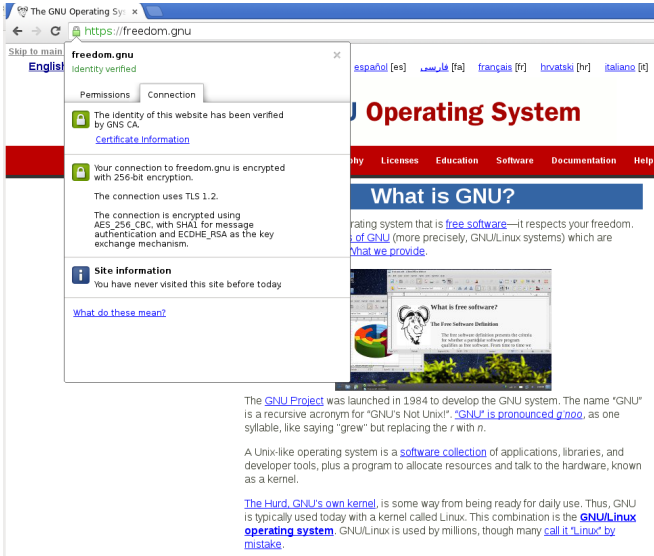
Name Resolution



Name Resolution



GNS as PKI (via DANE/TLSA)



The screenshot shows a web browser window with the address bar displaying `https://freedom.gnu`. A security warning dialog box is open, titled "freedom.gnu" with the subtext "identity verified". The dialog has two tabs: "Permissions" and "Connection".

Permissions

- The identity of this website has been verified by GNS CA. [Certificate Information](#)

Connection

- Your connection to freedom.gnu is encrypted with 256-bit encryption. The connection uses TLS 1.2. The connection is encrypted using AES_256_CBC, with SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism.

Site information

- You have never visited this site before today. [What do these mean?](#)

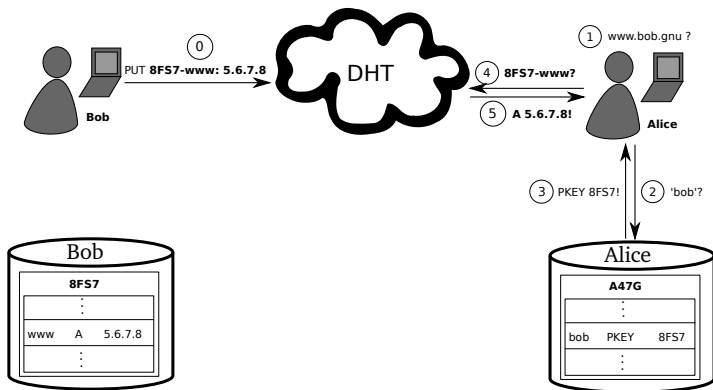
The background of the browser shows the GNU Operating System website, with the title "Operating System" in large red letters. Below the title is a navigation menu with links for "Why", "Licenses", "Education", "Software", "Documentation", and "Help". A blue banner below the menu says "What is GNU?". Below the banner, there is text: "operating system that is [free software](#)—it respects your freedom. of GNU (more precisely, GNU/Linux systems) which are [What we provide](#)." Below this text is a small image of a computer screen displaying a slide titled "What is free software?" with a cartoon character and a Linux logo.

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 *g'noo*, 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



Query Privacy: 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 $q_{P,l}$

Query Privacy: Cryptography

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

$$h := H(I, P) \quad (1)$$

$$d := h \cdot x \pmod n \quad (2)$$

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

$$q_{P,I} := H(dG) \quad (4)$$

Query Privacy: Cryptography

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

$$h := H(I, P) \quad (1)$$

$$d := h \cdot x \pmod n \quad (2)$$

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

$$q_{P,I} := H(dG) \quad (4)$$

Searching for records under label I in zone P

$$h := H(I, P) \quad (5)$$

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

$$R_{P,I} = D_{HKDF(I,P)}(B_{P,I}) \quad (7)$$

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 autocracy.

Do you have any questions?

References:

- ▶ Nathan Evans and Christian Grothoff. *R5N. Randomized Recursive Routing for Restricted-Route Networks*. **5th International Conference on Network and System Security**, 2011.
- ▶ Matthias Wachs, Martin Schanzenbach and Christian Grothoff. *On the Feasibility of a Censorship Resistant Decentralized Name System*. **6th International Symposium on Foundations & Practice of Security**, 2013.
- ▶ M. Schanzenbach *Design and Implementation of a Censorship Resistant and Fully Decentralized Name System*. **Master's Thesis (TUM)**, 2012.