

The GNU Name System¹

Christian Grothoff

Technische Universität München

27.12.2013

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

¹Joint 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


gnunet-setup


General Network Transports File Sharing Namestore **GNS**

Editing zone API5QDP7A126P06VV60535PDT50B9L12NK6QP64IE8KNC6E807G0 

Preferred zone name (PSEU):

Master Zone Private Zone Shorten Zone

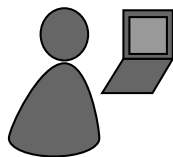


 Save As

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

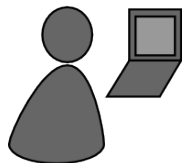


Bob Builder, Ph.D.

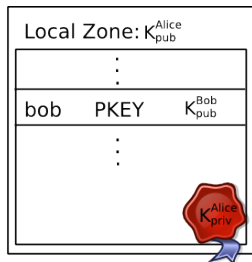
Address: Country, Street Name 23
Phone: 555-12345
Mobile: 666-54321
Mail: bob@H2R84L4JIL3G5C.zkey

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

Delegation

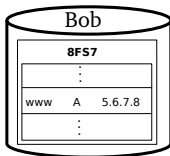
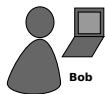


Alice

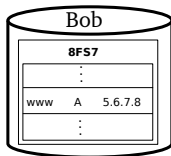
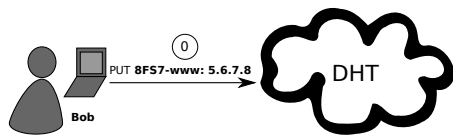


- ▶ Alice learns Bob's public key
- ▶ Alice creates delegation to zone K_{pub}^{Bob} under label **bob**
- ▶ Alice can reach Bob's webserver via **www.bob.gnu**

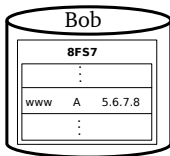
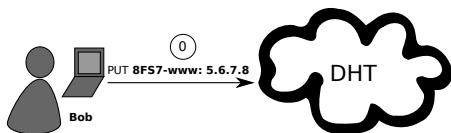
Name Resolution



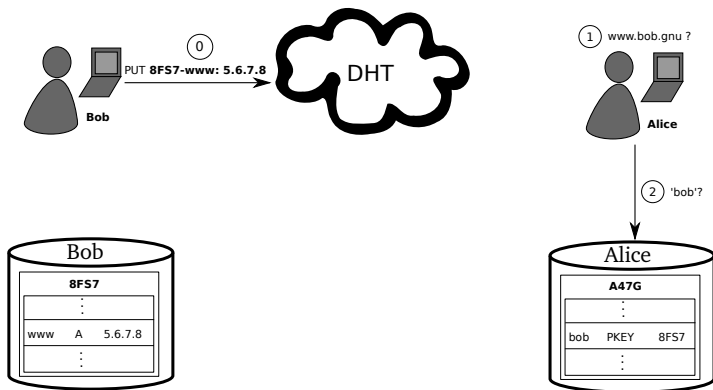
Name Resolution



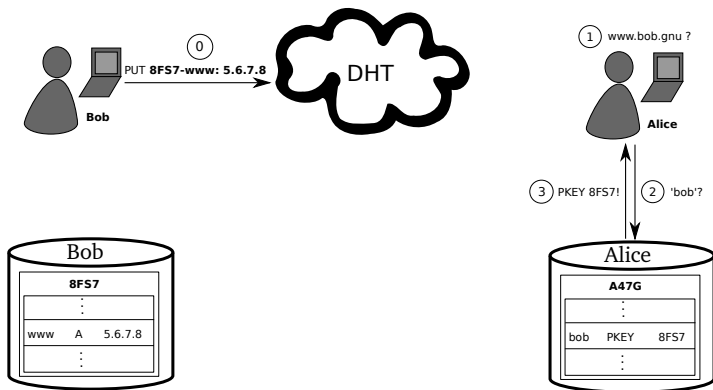
Name Resolution



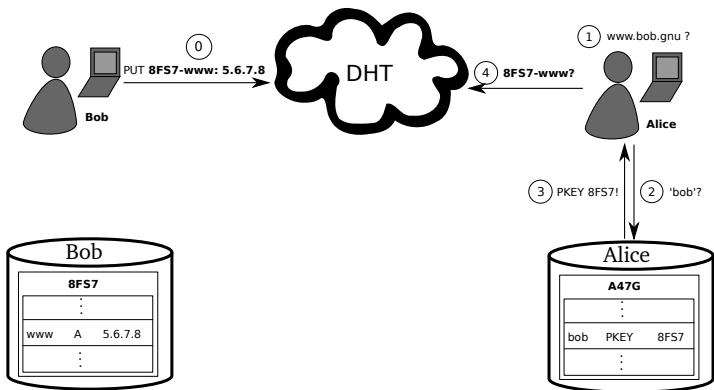
Name Resolution



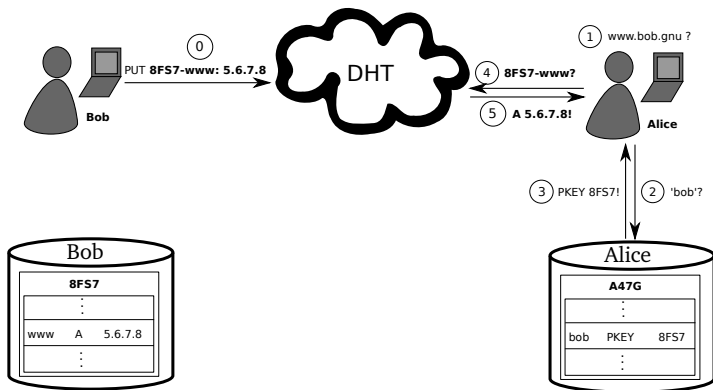
Name Resolution



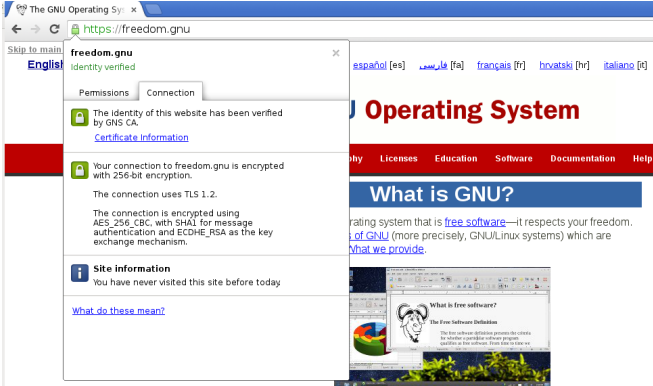
Name Resolution



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 a navigation menu including "Why", "Licenses", "Education", "Software", "Documentation", and "Help". The main heading is "Operating System" and "What is GNU?".

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](#).

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
 - ▶ Web-trouble: Firefox autoblunders “www.gnu” to “www.gnu.com”
 - ▶ 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 \Rightarrow start with social apps!
- ▶ New applications \Leftrightarrow 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:

- ▶ 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.
- ▶ G. Toth. *Design of a Social Messaging System Using Stateful Multicast*. **Master's Thesis (UVA)**, 2013.