

The GNU name system

Christian Grothoff

Inria Rennes Bretagne Atlantique

11.7.2016

"The Domain Name System is the Achilles heel of the Web." –Tim Berners-Lee

Trouble at the root

- ▶ ICANN asserts ccTLDs are not property to avoid seizure of .ir by US court
- ▶ ICANN approves .xxx despite objections from US conservative groups
- ▶ IETF approves .onion, but rejects .bit
- ▶ EU objects to US/AU/NZ plans for .wine to safeguard EU geographic indications system
- ▶ The Pirate Bay constantly changes its gTLD domain name due to censorship

Controlling gTLDs is about money & power.

Trouble in operations

- ▶ DNS remains a major 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)

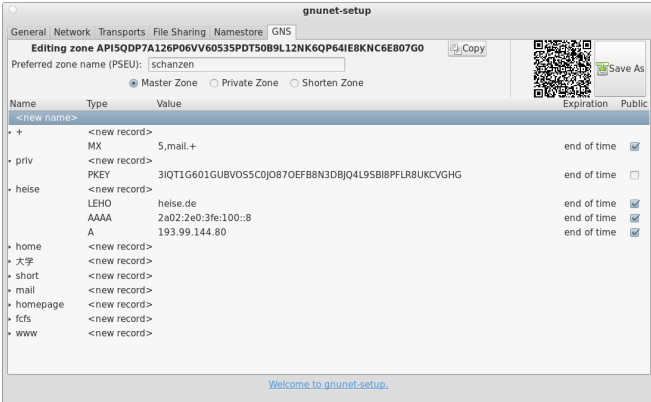
Band aid solutions¹ will **not** fix this.

¹DNS-over-TLS, DNSSEC, DPRIVE, ...

The GNU name system

- ▶ 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

Zone management: like in DNS

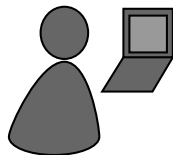


The screenshot shows the 'gnet-setup' application window. At the top, there are tabs for 'General', 'Network', 'Transports', 'File Sharing', 'Namestore', and 'GNS'. The main title is 'Editing zone API5QDP7A126P06VV60535PDT50B9L12NK6QP64IE8KNC6E807G0'. Below this, there is a text field for 'Preferred zone name (PSEU):' containing 'schanzen'. To the right of this field is a 'Copy' button and a QR code. Below the text field are three radio buttons: 'Master Zone' (selected), 'Private Zone', and 'Shorten Zone'. A 'Save As' button is also visible.

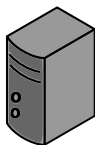
Name	Type	Value	Expiration	Public
<new name>				
+	<new record>			
	MX	5,mail.+	end of time	<input checked="" type="checkbox"/>
priv	<new record>			
	PKEY	3IQT1G601GUBVO55CJO87OEFB8N3DBJQ4L95BI8PFLR8UKCVGHG	end of time	<input type="checkbox"/>
heise	<new record>			
	LEHO	heise.de	end of time	<input checked="" 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>			
fcs	<new record>			
www	<new record>			

At the bottom of the window, there is a blue link: [Welcome to gnet-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



The image shows a business card for Bob Builder, Ph.D. The card is enclosed in a thick black border. In the top left corner is the TUM logo in blue. In the top right corner is a circle with a vertical line through its center. On the left side, there is a large QR code. To the right of the QR code, the name "Bob Builder, Ph.D." is printed in bold black text. Below the name, the contact information is listed in bold black text: "Address: Country, Street Name 23", "Phone: 555-12345", "Mobile: 666-54321", and "Mail: bob@H2R84L4JIL3G5C.zkey".

TUM

Bob Builder, Ph.D.

Address: Country, Street Name 23

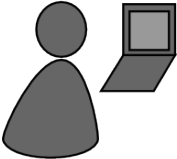
Phone: 555-12345

Mobile: 666-54321

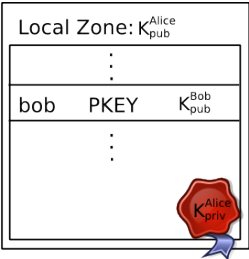
Mail: bob@H2R84L4JIL3G5C.zkey

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

Delegation

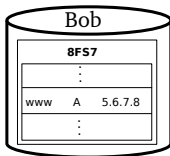
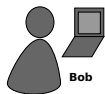


Alice

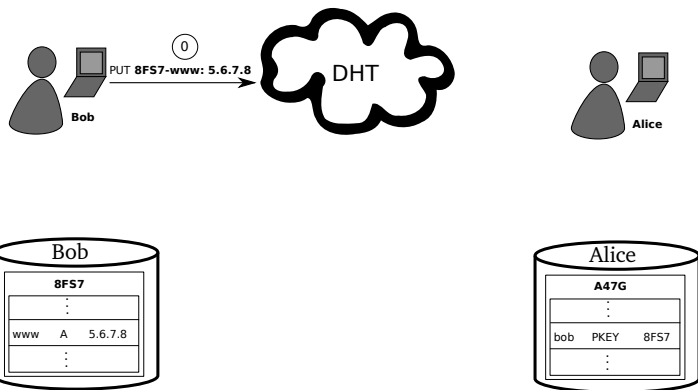


- ▶ Alice learns Bob's public key
- ▶ Alice creates delegation to zone K_{pub}^{Bob} under label **bob**
- ▶ Alice can reach Bob's webserver via **www.bob.gnu**

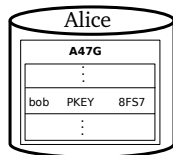
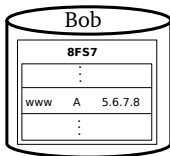
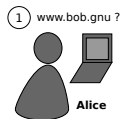
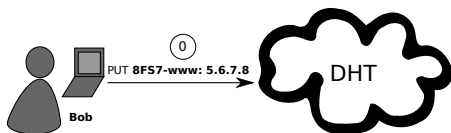
Name resolution



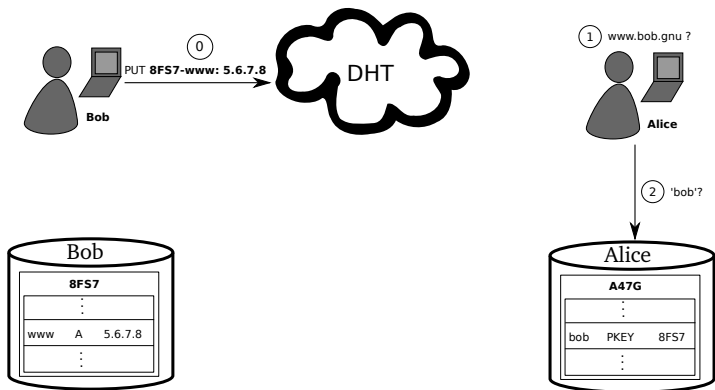
Name resolution



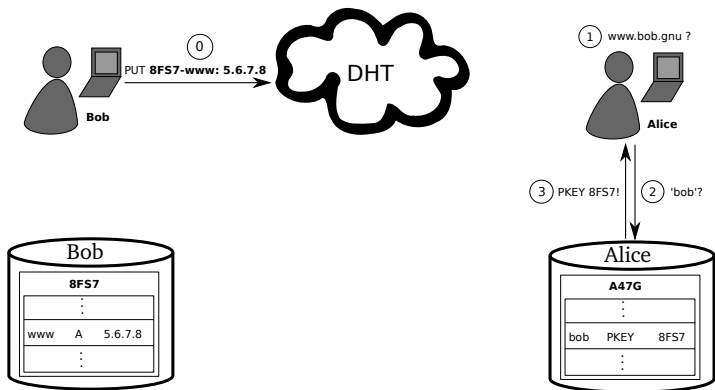
Name resolution



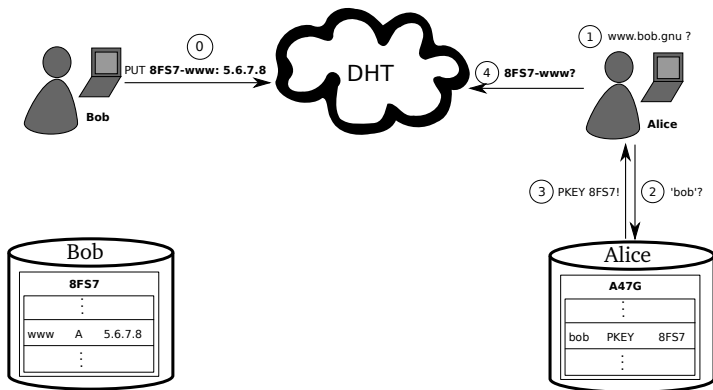
Name resolution



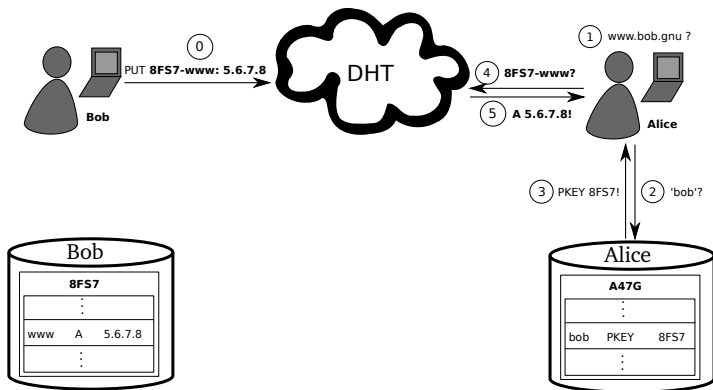
Name resolution



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 is open, showing the following information:

- freedom.gnu** Identity verified
- Permissions: Connection
- The identity of this website has been verified by GNS CA. [Certificate Information](#)
- 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?](#)

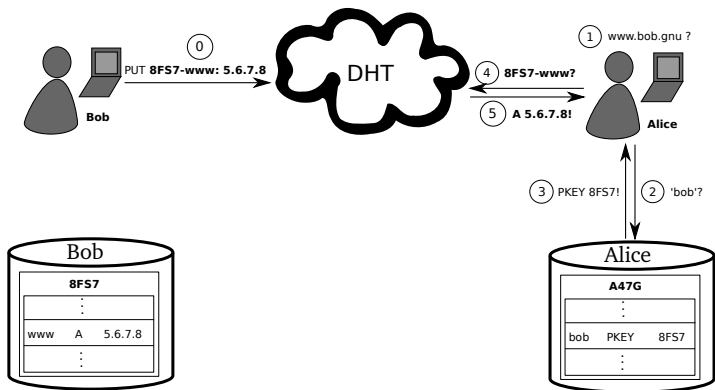
The background shows the Freedom Operating System website with a navigation menu (Why, Licenses, Education, Software, Documentation, Help) and a section titled "What is GNU?".

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](#).

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

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

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

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

The “.zkey” zone

- ▶ “.zkey” is another pTLD, in addition to “.gnu”
 - ▶ In “LABEL.zkey”, the “LABEL” is a public key of a zone
 - ▶ “alice.bob.*KEY*.zkey” is perfectly legal
- ⇒ Globally unique identifiers

Key revocation

- ▶ Revocation message signed with private key (ECDSA)
- ▶ Flooded on all links in P2P overlay, stored forever
- ▶ Efficient set reconciliation used when peers connect
- ▶ Expensive proof-of-work used to limit DoS-potential
- ▶ Proof-of-work can be calculated ahead of time
- ▶ Revocation messages can be stored off-line if desired

Next steps: go global

- ▶ “.gnu” is personal, fine for an address book or OSN
- ▶ But, everyone likes global names! “.fr” is global.

Next steps: go global

- ▶ “.gnu” is personal, fine for an address book or OSN
- ▶ But, everyone likes global names! “.fr” is global.
 - ▶ Scale DHT implementation to deal with millions of records

Next steps: go global

- ▶ “.gnu” is personal, fine for an address book or OSN
- ▶ But, everyone likes global names! “.fr” is global.
 - ▶ Scale DHT implementation to deal with millions of records
 - ▶ Use NSEC/NSEC3 to XFR “.fr” into GNS zone

Next steps: go global

- ▶ “.gnu” is personal, fine for an address book or OSN
- ▶ But, everyone likes global names! “.fr” is global.
 - ▶ Scale DHT implementation to deal with millions of records
 - ▶ Use NSEC/NSEC3 to XFR “.fr” into GNS zone
 - ▶ Hijack “.fr” via NSS like we hijack “.gnu” today

Next steps: go global

- ▶ “.gnu” is personal, fine for an address book or OSN
 - ▶ But, everyone likes global names! “.fr” is global.
 - ▶ Scale DHT implementation to deal with millions of records
 - ▶ Use NSEC/NSEC3 to XFR “.fr” into GNS zone
 - ▶ Hijack “.fr” via NSS like we hijack “.gnu” today
 - ▶ Great: no ICANN/IETF approval for ccTLD needed!
 - ▶ Scale to for all gTLDs supporting DNSSEC
- ⇒ Globally unique identifiers
- ⇒ No out-of-bailiwick lookups
- ⇒ Privacy
- ⇒ Censorship-resistance

Conclusion

- ▶ Plan to obsolete the obsolete DNS protocol
- ▶ No root, no exclusive hierarchy, no control issues
- ▶ Delegation allows using zones of other users
- ▶ Trust paths explicit, trust agility
- ▶ Privacy-enhanced queries, censorship-resistant
- ▶ Reliable revocation

Do you have any questions?

- ▶ Yves Eudes, Christian Grothoff, Jacob Appelbaum, Monika Ermert, Laura Poitras, Matthias Wachs: *MoreCowBell, nouvelles relations sur les pratiques de la NSA*. **Le Monde**, 24.1.2015.
- ▶ Nathan Evans and Christian Grothoff. *R⁵N. Randomized Recursive Routing for Restricted-Route Networks*. **5th International Conference on Network and System Security**, 2011.
- ▶ M. Schanzenbach *Design and Implementation of a Censorship Resistant and Fully Decentralized Name System*. **Master's Thesis (TUM)**, 2012.
- ▶ 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.
- ▶ 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.