

Peer-to-Peer Systems and Security

The Future Of the Internet

Christian Grothoff

Technische Universität München

June 3, 2014

“You look at this and you say this is insane. It’s insane. And if it is only Hollywood that has to deal with this, OK, that’s fine. Let them be insane. The problem is their insane rules are now being applied to the whole world. This insanity of control is expanding as everything you do touches copyrights” –Lawrence Lessig

GNUnet, a Framework for Secure P2P Networking

GNUnet is more than anonymous file-sharing:

- ▶ Anonymity needs company!
- ▶ Blocking an application that has many uses increases collateral damage
- ▶ Code re-use results in higher-quality code
- ▶ Anonymous file-sharing is hardly the only interesting problem

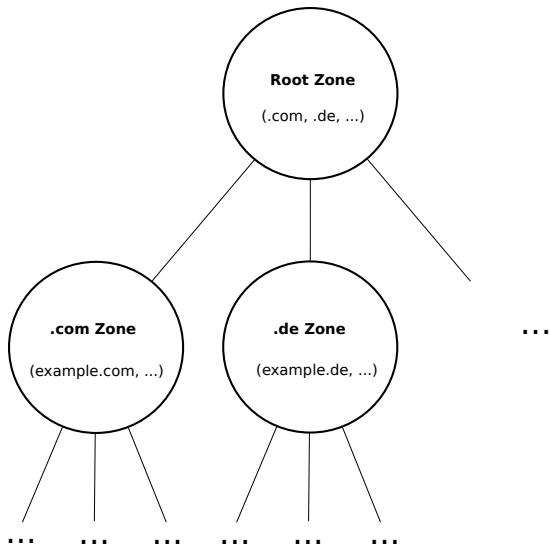
GNUnet, a Framework for Secure P2P Networking

GNUnet is more than anonymous file-sharing:

- ▶ Anonymity needs company!
- ▶ Blocking an application that has many uses increases collateral damage
- ▶ Code re-use results in higher-quality code
- ▶ Anonymous file-sharing is hardly the only interesting problem

Today: visions for GNUnet

Background: Domain Name System



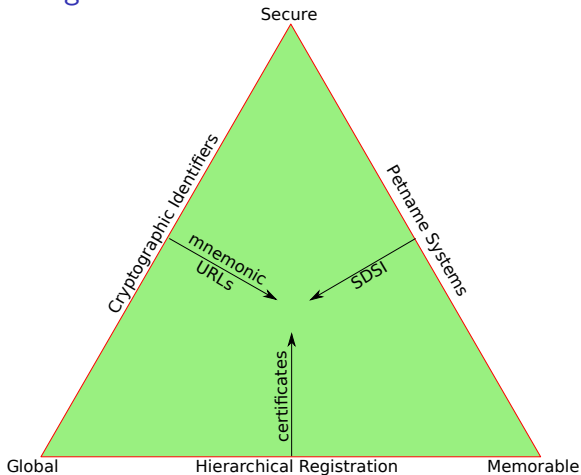
Background: Domain Name System

Who controls the root zone? ICANN? IANA?

"The Internet Corporation for Assigned Names and Numbers (ICANN) currently performs the IANA functions, on behalf of the United States Government, through a contract with NTIA." - <http://www.ntia.doc.gov>

Secure, Memorable, Global: Choose Two

Zooko's Triangle



The GNU Name System¹

Properties of GNS

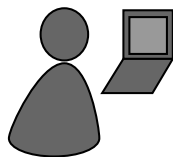
- ▶ Decentralized name system with secure memorable names
- ▶ Delegation used to achieve transitivity
- ▶ Supports globally unique, secure identifiers
- ▶ Achieves query and response privacy
- ▶ Provides alternative public key infrastructure
- ▶ Interoperable with DNS

New applications enabled by GNS

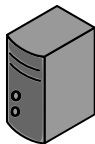
- ▶ Name services hosted in P2P networks
- ▶ Name users in decentralized social networking applications

¹Joint work with Martin Schanzenbach and Matthias Wachs


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 QR code. To the right of the QR code, the name "Bob Builder, Ph.D." is printed in bold black text. Below the name, contact information is listed in bold black text: "Address: Country, Street Name 23", "Phone: 555-12345", "Mobile: 666-54321", and "Mail: bob@H2R84L4JIL3G5C.zkey".

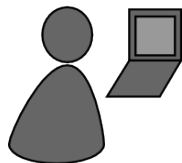
TUM

Bob Builder, Ph.D.

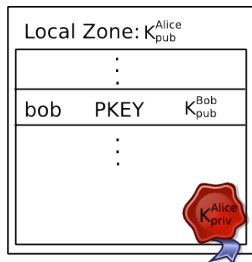
Address: Country, Street Name 23
Phone: 555-12345
Mobile: 666-54321
Mail: bob@H2R84L4JIL3G5C.zkey

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

Delegation

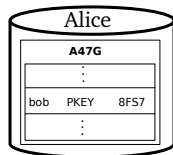
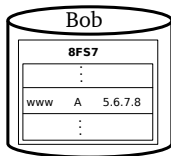


Alice

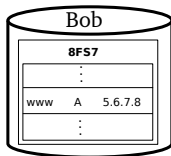
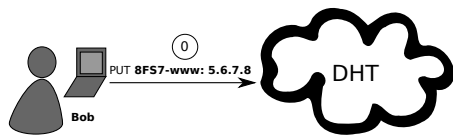


- ▶ Alice learns Bob's public key
- ▶ Alice creates delegation to zone K_{pub}^{Bob} under label **bob**
- ▶ Alice can reach Bob's webserver via **www.bob.gnu**

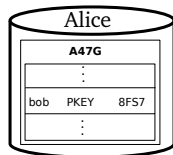
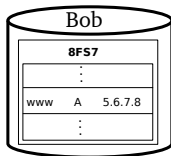
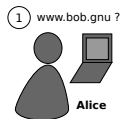
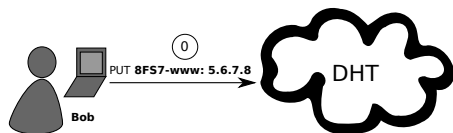
Name Resolution



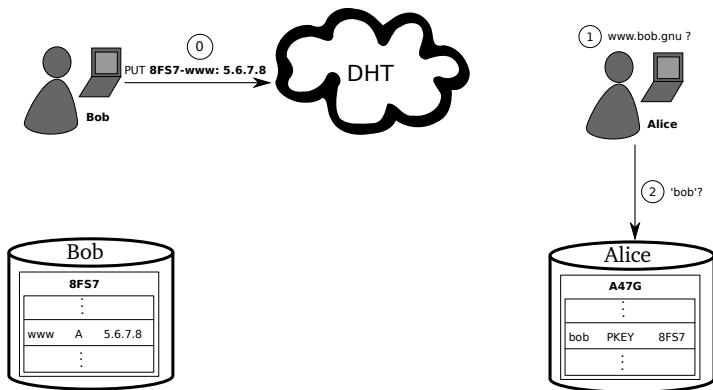
Name Resolution



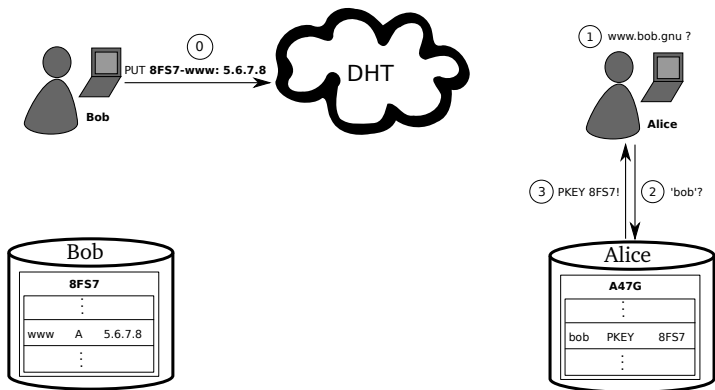
Name Resolution



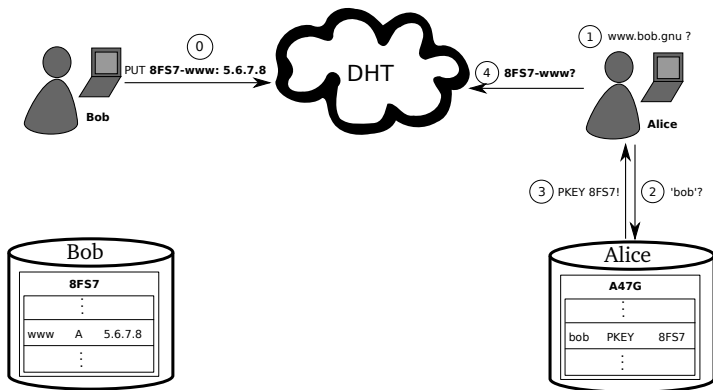
Name Resolution



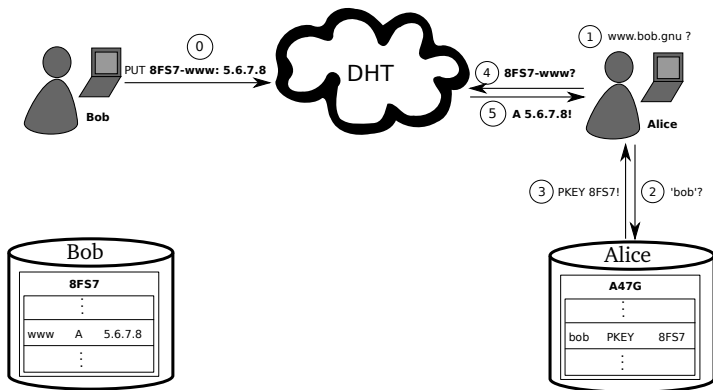
Name Resolution



Name Resolution



Name Resolution



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

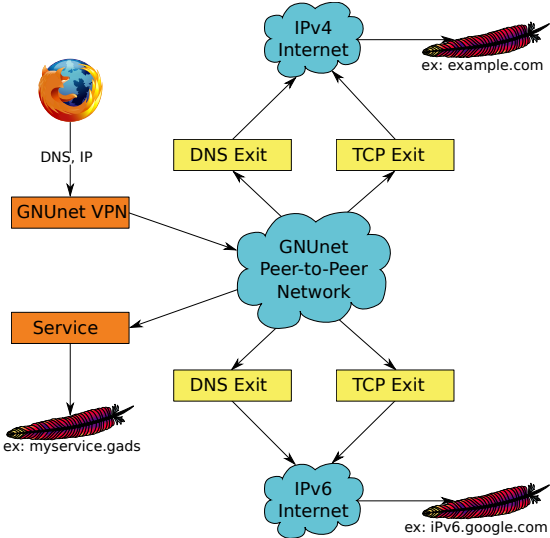
Key Revocation

- ▶ 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

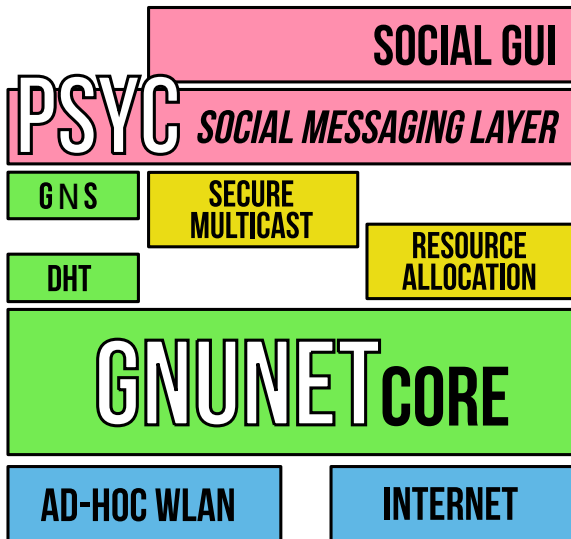
Fun GNS Record Types

- ▶ DNS CERT: store your GPG public key
- ▶ GNS2DNS: delegate to DNS
- ▶ GNUNET VPN: TCP/IP services hosted in GNUnet
- ▶ GNUNET PHONE: have a conversation

IPv6 Transition



Social Networking



Democracy depends on independent reporting

- ▶ Commercialization of US news reporting destroyed US system

Democracy depends on independent reporting

- ▶ Commercialization of US news reporting destroyed US system
- ▶ Political influence in Europe limits utility of public broadcasting

Democracy depends on independent reporting

- ▶ Commercialization of US news reporting destroyed US system
- ▶ Political influence in Europe limits utility of public broadcasting
- ▶ Independent news papers struggle to finance investigative journalism

Democracy depends on independent reporting

- ▶ Commercialization of US news reporting destroyed US system
- ▶ Political influence in Europe limits utility of public broadcasting
- ▶ Independent news papers struggle to finance investigative journalism
- ▶ Information overload (advertising, fast-paced global change)

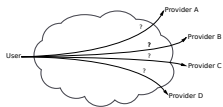
Democracy depends on independent reporting

- ▶ Commercialization of US news reporting destroyed US system
- ▶ Political influence in Europe limits utility of public broadcasting
- ▶ Independent news papers struggle to finance investigative journalism
- ▶ Information overload (advertising, fast-paced global change)
- ▶ Need crowd-sourced, crowd-edited, crowd-filtered, crowd-controlled news agency

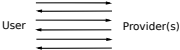
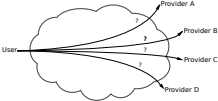
Reuters

- ▶ Copy-on-write editing + references + comments (?)
- ▶ Categorization w. tags + language + timestamp
- ▶ Personalized ranking + SMC-based cooperative ranking
- ▶ Pushing via combined PoW + reputation system
- ▶ Randomization against living in personalized bubble
- ▶ TeX(t)-based

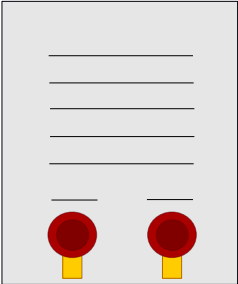
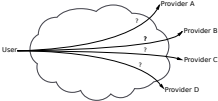
Business Platform



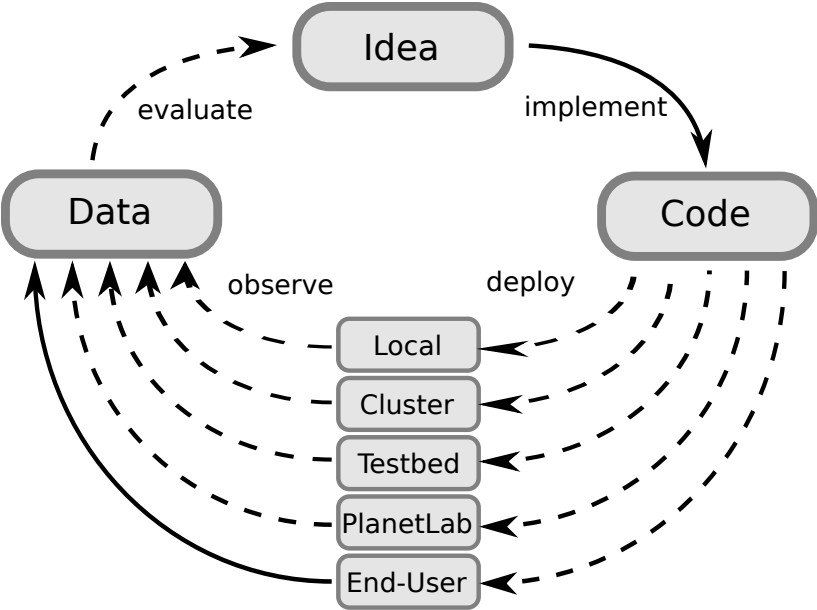
Business Platform



Business Platform



Evaluation: Eclectic



← - supported by our toolchain

Your Projects

- ▶ Taxable anonymous digital cash \Rightarrow Reuters
- ▶ GNUnet support for Git \Rightarrow Reuters
- ▶ Multiplicative secret sharing \Rightarrow Business Platform
- ▶ Brahms \Rightarrow Decentralized Onion Routing
- ▶ Splitstream \Rightarrow Social Networking
- ▶ Socialist Millionaire Problem \Rightarrow GNS Key Exchange

Your Projects

- ▶ Taxable anonymous digital cash \Rightarrow Reuters
- ▶ GNUnet support for Git \Rightarrow Reuters
- ▶ Multiplicative secret sharing \Rightarrow Business Platform
- ▶ Brahms \Rightarrow Decentralized Onion Routing
- ▶ Splitstream \Rightarrow Social Networking
- ▶ Socialist Millionaire Problem \Rightarrow GNS Key Exchange
- ▶ Group OTR \Rightarrow Forum? Mailinglist? Chat?
- ▶ Improved MQTT \Rightarrow E-mail? M2M?

More Projects

- ▶ Cryogenic: Reduce power consumption
- ▶ Knock: Hide open TCP sockets
- ▶ Alternative DHTs (X-vine)
- ▶ More bindings (Java, DBUS, Python)
- ▶ Intrusion-detecting hardware

More Projects

- ▶ Cryogenic: Reduce power consumption
- ▶ Knock: Hide open TCP sockets
- ▶ Alternative DHTs (X-vine)
- ▶ More bindings (Java, DBUS, Python)
- ▶ Intrusion-detecting hardware
- ▶ Smart city transport
- ▶ Secure, libre hardware

The Free Secure Network Systems Group

Research Areas:

- ▶ Network Protocol Analysis, Design & Implementation
- ▶ Measurements & Large-Scale Experiments
- ▶ Privacy, Secure Multiparty Computation
- ▶ Constraint Solving, Optimization

Teaching Areas:

- ▶ P2P Networks
- ▶ Network Security
- ▶ DNS, IPv4, IPv6

Questions?

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