The GNU Name System

A Public Key Infrastructure for Social Movements in the Age of Universal Surveillance

Christian Grothoff

Inria

Oct 4th 2016

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

A Matter of Life and Death

The Intercept reports in February 2014:

- ▶ NSA identifies targets based on meta data (social graph, location profiles, cell-phone tracking)
- ▶ Joint Special Operations Command (JSOC) uses geolocation of SIM card for assassinations using drone strikes
- ▶ No due process, no immanent threat, no consent of foreign government, no declaration of war

"F3: Find, Fix, Finish" is state terrorism facilitated by networks.

Not Just Monitoring

- FOXACID, QUANTUM* and MUSCULAR use man-in-the-middle attacks.
- NSA uses NSLs to force companies to disclose private keys.

Not Just Monitoring

- ▶ FOXACID, QUANTUM* and MUSCULAR use man-in-the-middle attacks.
- ▶ NSA uses NSLs to force companies to disclose private keys.
- ▶ Targets include:
  - ▶ Journalists
  - ▶ Environmental groups
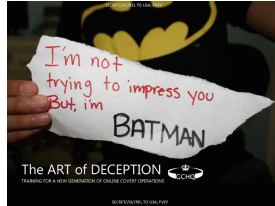 - ▶ UN Climate Change Conference in Copenhagen

Where We Are

Where We Are

Where We Are

Source: csmon

Source: gawand.org

Source: boingboing.com

Do you ❤ your brand?

Encryption to the Rescue?

- 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[1]

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

---

[1]Joint work with Martin Schanzenbach and Matthias Wachs

Zone Management: like in DNS

Name resolution in GNS

Local Zone: K_{pub}^{Bob}

www	A	5.6.7.8

K_{priv}^{Bob}

Bob   Bob's webserver

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

Secure introduction

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

Local Zone: K_{pub}^{Alice}

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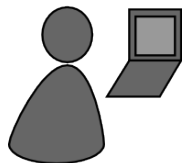
K_{priv}^{Alice}
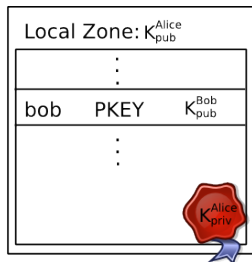
- Alice learns Bob's public key
- Alice creates delegation to zone K_{pub}^{Bob} under label **bob**
- Alice can reach Bob's webserver via **www.bob.gnu**

Name Resolution

Name Resolution
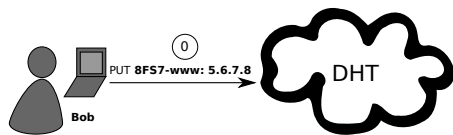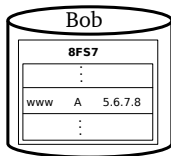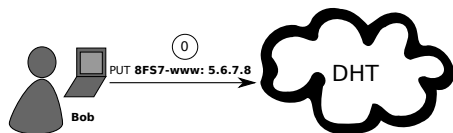
Name Resolution
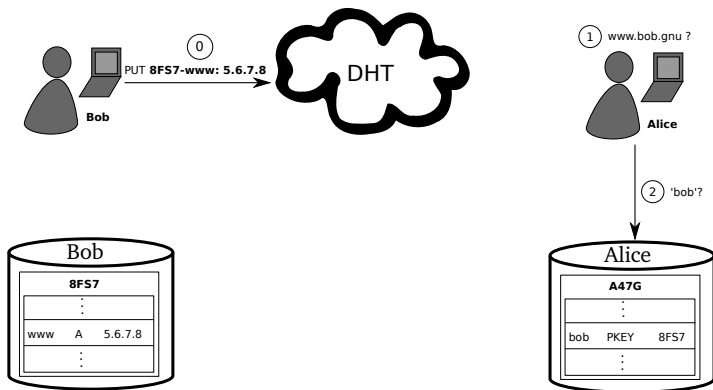
Name Resolution
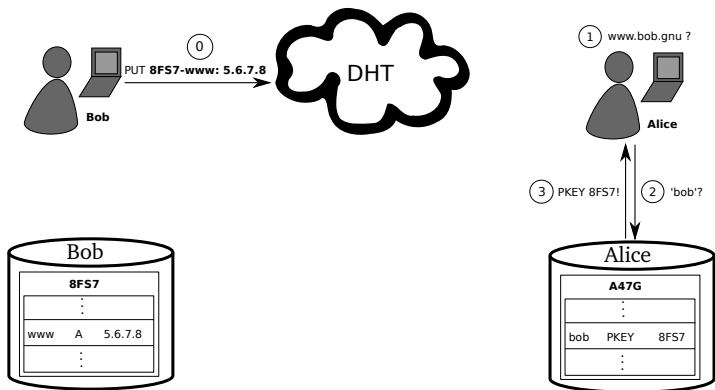
Name Resolution
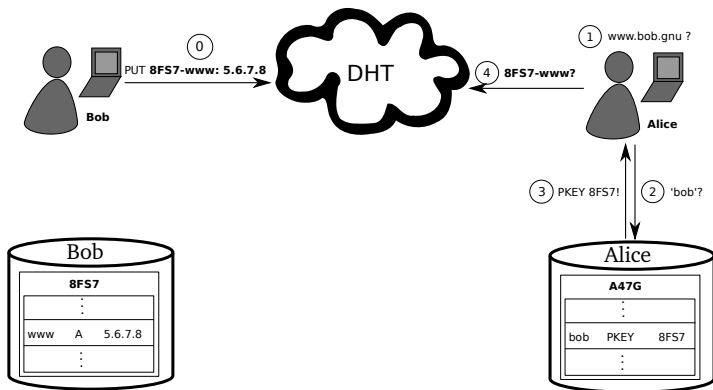
Name Resolution

Name Resolution

GNS as PKI (via DANE/TLSA)

Privacy Issue: DHT

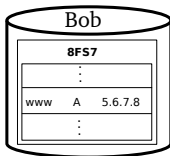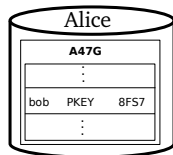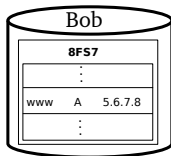# Query Privacy: Terminology

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 $q_{P,I}$

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

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

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

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

Query Privacy: Cryptography

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

$$h := H(l, P) \tag{1}$$
$$d := h \cdot x \mod n \tag{2}$$
$$B_{P,l} := S_d(E_{HKDF(l,P)}(R_{P,l})), dG \tag{3}$$
$$q_{P,l} := H(dG) \tag{4}$$

Searching for records under label l in zone P

$$h := H(l, P) \tag{5}$$
$$q_{P,l} := H(hP) = H(hxG) = H(dG) \Rightarrow \texttt{obtain } B_{P,l} \tag{6}$$
$$R_{P,l} = D_{HKDF(l,P)}(B_{P,l}) \tag{7}$$

A Laundry List of Features

Revocation

Revocation Basics

- ▶ Revocation certificate (RC): message signed with private key
- ▶ Peer receives new valid RC, floods to all neighbours
- ▶ All peers store all valid RCs forever
- ⇒ Expensive operation ⇒ proof-of-work

Revocation

Revocation Basics

- ▶ Revocation certificate (RC): message signed with private key
- ▶ Peer receives new valid RC, floods to all neighbours
- ▶ All peers store all valid RCs forever
- ⇒ Expensive operation ⇒ proof-of-work

Revocation Magic

- ▶ Peers maybe offline during initial flood
- ▶ Network might be temporarily partitioned
- ⇒ Need to reconsile revocation sets on connect

Whenever two peers establish a P2P connection, they must compute the set union of their RC sets!

The ".zkey" pTLD

- "LABELS.*PKEY*.zkey" format
- PKEY is the public key of the zone
- Works a bit like ".onion"
- ⇒ Globally unique identifiers!

Bob Builder, Ph.D.

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

NICKnames

- "alice.bob.carol.dave.gnu" is a bit long for Edward (".gnu")
- Also, we need to trust Bob, Carol and Dave (for each lookup)
- Finally, Alice would have liked to be called Krista (just Bob calls her Alice)

NICKnames

- "alice.bob.carol.dave.gnu" is a bit long for Edward (".gnu")
- Also, we need to trust Bob, Carol and Dave (for each lookup)
- Finally, Alice would have liked to be called Krista (just Bob calls her Alice)
- "NICK" records allow Krista to specify her preferred NICKname
- GNS adds a "NICK" record to each record set automatically
- Eve learns the "NICK", and GNS creates "krista.short.gnu"

NICKnames

- "alice.bob.carol.dave.gnu" is a bit long for Edward (".gnu")
- Also, we need to trust Bob, Carol and Dave (for each lookup)
- Finally, Alice would have liked to be called Krista (just Bob calls her Alice)
- "NICK" records allow Krista to specify her preferred NICKname
- GNS adds a "NICK" record to each record set automatically
- Eve learns the "NICK", and GNS creates "krista.short.gnu"
- Memorable, short trust path in the future! TOFU!
- Krista better pick a reasonably unique NICK.

Shadow Records

- Records change
- Expiration time controls validity, like in DNS
- DHT propagation has higher delays, compared to DNS

Shadow Records

- Records change
- Expiration time controls validity, like in DNS
- DHT propagation has higher delays, compared to DNS
- SHADOW is a flag in a record
- Shadow records are only valid if no other, non-expired record of the same type exists

Practical Concerns

- Name registration
- Support for browsing
- New record types
- Integration with applications
- State of the implementation

Registering a name in GNS

- Bob gives his PKEY to his **friends** via QR code

- or registers it at the **GNUnet fcfs** authority *pin.gnu* as "bob"

- → Bob's friends can resolve his records via *.*petname*.gnu

- → or *.bob.pin.gnu

From DNS to GNS

Names are not globally unique, but ...

... we need support for Virtual Hosting!

... we need support for SSL!

From DNS to GNS

Names are not globally unique, but ...
... we need support for Virtual Hosting!
... we need support for SSL!

Solution: Client Side SOCKS Proxy

Legacy Hostname (LEHO) Records

LEHO records give a hint about the DNS name the server expects.
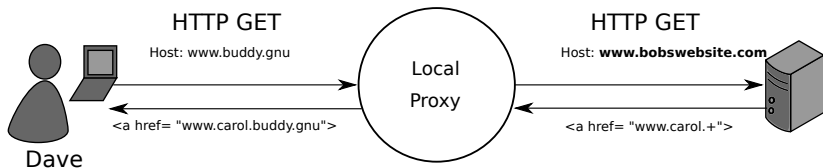
Legacy Hostname (LEHO) Records

LEHO records give a hint about the DNS name the server expects.
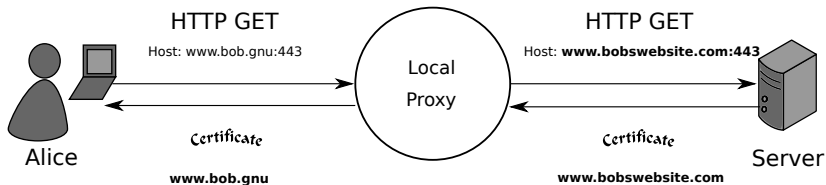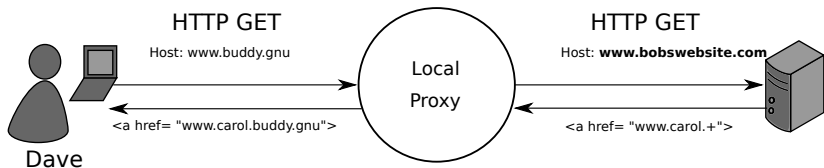
Relative Names

- GNS records can contain ".+"
- CNAME: "server1.+"
- MX: "mail.+"
- ".+" stands for "relative to current zone"

Supporting this for links in browsers would be nice.

New Record Types

- PKEY: delegate to another GNS zone
- NICK: preferred names for shortening
- LEHO: legacy hostname

New Record Types

- PKEY: delegate to another GNS zone
- NICK: preferred names for shortening
- LEHO: legacy hostname
- GNS2DNS: delegate to DNS
- VPN: peers hosting TCP/IP services
- PHONE: call users using `gnunet-conversation`

DNS Delegation

- Delegate to DNS using GNS2DNS records
- GNS2DNS record specifies:
    - Name of DNS resolver (i.e. "ns1.example.com" or "piratedns.+")
    - DNS domain to continue resolution in (i.e. "example.com" or "piratebay.org")
- GNS will first resolve DNS resolver name to A/AAAA record
- GNS will then resolve "*left.of.gns2dns.*example.com" using DNS

VPN Delegation

- Delegates to GNUnet VPN
- VPN record specifies:
    - Identity of hosting peer (no anonymity!)
    - Service identifier (hash code)
- GNS can map VPN record to A/AAAA record of `gnunet-vpn` tunnel

PHONE service

- PHONE record specifies:
  - Identity of hosting peer (no anonymity yet!)
  - Line number (to support multiple phones per peer)
- `gnunet-conversation` uses *reverse lookup* for caller ID

Application Integration

- SOCKS proxy (`gnunet-gns-proxy`)
- NSS plugin
- DNS packet interception (`gnunet-dns-service`)
- GNS (C) API
- GNS (IPC) protocol
- GNS command-line tool

Current State

- GNS part of GNUnet since 0.9.3
- Crypto changed to Curve25519 in 0.10.0
- Internationalized Domain Names are supported

Current State

- GNS part of GNUnet since 0.9.3
- Crypto changed to Curve25519 in 0.10.0
- Internationalized Domain Names are supported
- Installation is "non-trivial" (for your parents)
- SOCKS proxy is known to be problematic

Next Steps

- Improve DHT scalability and performance
- Import DNS TLDs (".fr" is open data)
- Interoperate with GnuPG / Web-of-Trust
- Integrate with social networking applications
- Install widely by providing easy-to-use packages

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 and planetary collapse.

Do you have any questions?

References:

- ▶ Nathan Evans and Christian Grothoff. *R^5N: 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.

- ▶ Christian Grothoff, Bart Polot and Carlo von Loesch. *The Internet is broken: Idealistic Ideas for Building a GNU Network*. **W3C/IAB Workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)**, 2014.

- ▶ Jeffrey Burdges, Florian Dold, Christian Grothoff and Marcello Stanisci. *Enabling Secure Web Payments with GNU Taler*. **SPACE 2016**.

- ▶ Christian Grothoff and Jens Porup. *The NSAs SKYNET program may be killing thousands of innocent people*. **ARS Technica**, 3/2016.
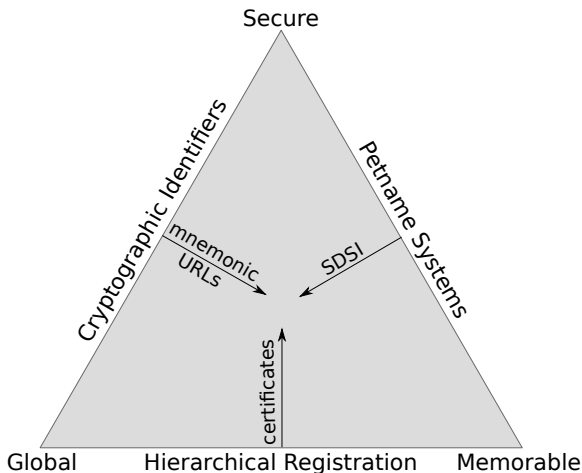
Zooko's Triangle
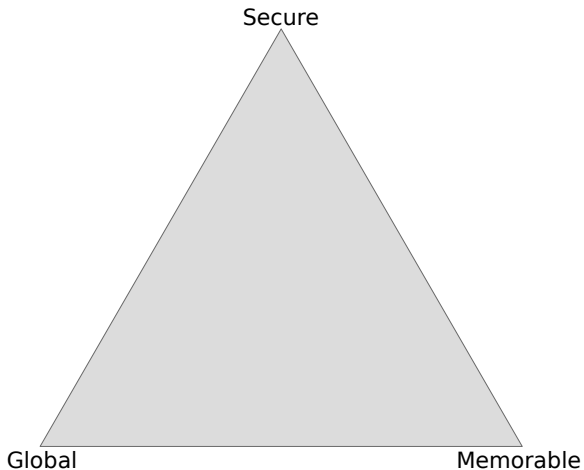
A name system can only fulfill **two**!

Zooko's Triangle
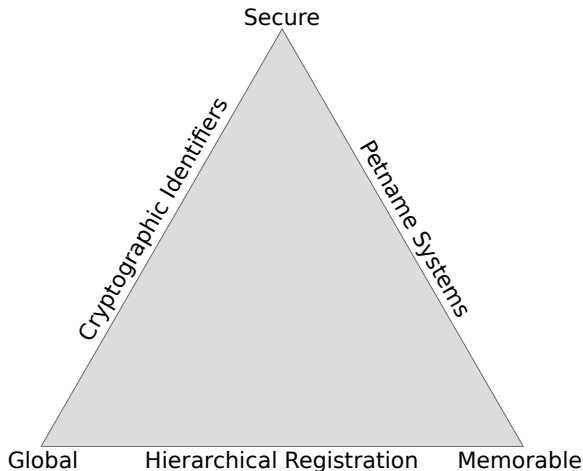
DNS, ".onion" IDs and /etc/hosts/ are representative designs.

Zooko's Triangle

DNSSEC security is broken by design (adversary model!)

Namecoin

Namecoin

- Memorable:

Namecoin

- Memorable: Check
- Global:

Namecoin

- Memorable: Check
- Global: Check
- Secure:

Namecoin

- Memorable: Check
- Global: Check
- Secure: different adversary model!

Namecoin

- Memorable: Check
- Global: Check
- Secure: different adversary model!
⇒ Availability of names (registration rate) is restricted

Namecoin

- ▶ Memorable: Check
- ▶ Global: Check
- ▶ Secure: different adversary model!
- ⇒ Availability of names (registration rate) is restricted
- ⇒ Adversary must not have 51% compute power