The GNU Name System

secdispatch – IETF 108

https://datatracker.ietf.org/doc/draft-schanzen-gns/

Martin Schanzenbach
Christian Grothoff
Bernd Fix

30/7/2020

GNUnet

The GNU Name System In a Nutshell

Motivation

- DNS remains a source of traffic amplification 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 offensive cyber war (QUANTUMDNS).
- DoT/DoH, DNSSEC, DPRIVE unfortunately do **NOT** fix this.

What is the GNU Name System?[2]

- Fully decentralized name system ⇒ Names are not global.
- Supports globally unique and secure identification.
- Features query and response privacy.
- Provides a public key infrastructure
  - Each zone is associated with a cryptographic key pair.
  - Delegation between zones establishes trust relationship.
- Interoperable with DNS.
- Usable.[1]

[1] User studies conducted in "Decentralized Authentication for Self-Sovereign Identities using Name Systems" (DASEIN) project.

[2] Joint work with Christian Grothoff and Matthias Wachs

Applications

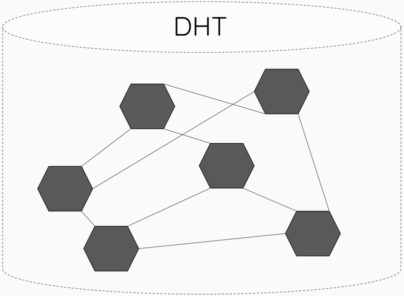
- Identity management: **re:claimID** (`https://reclaim-identity.io`)
- Social Networks: **SecuShare** (`https://secushare.org`)
- Healthcare and IoT: **Accident insurance and private health data**.[3]
- Others: **Chat**, **Host addressing**, . . .

[3] Joint work with University of Applied Sciences Bern, “Decentralized Authentication for Self-Sovereign Identities using Name Systems” (DASEIN)

Technical Overview

Record Storage / Retrieval

- GNS stores records in a **Distributed Hash Table** (DHT).
- DHTs allow us to map keys to values.
- Naive approach: Map domain names to records.
  e.g.: example.com ⇒ A: 1.2.3.4



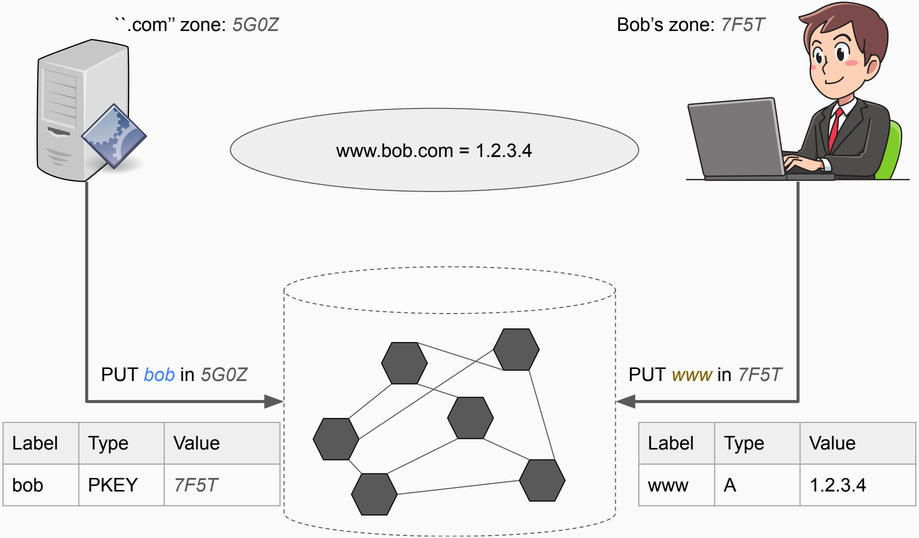
Secure Storage / Retrieval

- **Query privacy**
  - GNS implements a **Private Information Retrieval** (PIR) scheme:
    "a protocol that allows a user to retrieve an item from a server in possession of a database without revealing which item is retrieved."[4]
  - Queries do not reveal domain name.
- **Record confidentiality**: Values in DHT are signed and encrypted by zone owner.
- **Zone privacy**: Zones cannot be enumerated.
- **Censorship and DDoS resistance**: Decentralized, resilient directory.

[4] https://en.wikipedia.org/wiki/Private_information_retrieval

Zone Delegation

- The “NS” equivalent in GNS is called “PKEY”.
- A “PKEY” record contains public zone keys.
- The combination of a “PKEY” record value and a name allows users to query records in a delegated zone.



``.com'' zone: *5G0Z*

Bob's zone: *7F5T*

www.bob.com = 1.2.3.4

PUT *bob* in *5G0Z*

Label	Type	Value
bob	PKEY	*7F5T*

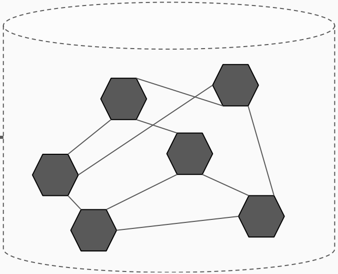
PUT *www* in *7F5T*

Label	Type	Value
www	A	1.2.3.4

www.bob.com?

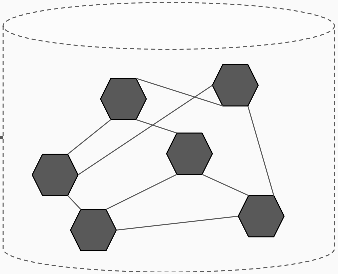
GET *bob* in *5G0Z*

Label	Type	Value
bob	PKEY	*7F5T*



www.bob.com?

GET *www in 7F5T*



Label	Type	Value
www	A	1.2.3.4

Why are we here?

Discussions at IETF/W3C/ICANN

- IETF 93: https://datatracker.ietf.org/doc/slides-93-dnsop-5/
    - Failed attempt to special-use '.gnu' for GNS.
    - Resulting in RFC7686, RFC8244
- STRINT 2014 (W3C/IAB workshop): https://grothoff.org/christian/strint2014.pdf
- IETF 104 IRTF DINRG WG: https://datatracker.ietf.org/doc/slides-104-dinrg-gnu-name-system/
- ICANN66: https://git.gnunet.org/presentations.git/plain/icann66/20191105_icann66_gns.pdf

Current Status

- Who is (and will be) working on it:
  - GNUnet project.
  - Current funding for specfication by NLnet: `https://nlnet.nl/project/GNS/`.
- Implementation
  - Reference implementation in C part of GNUnet: `https://git.gnunet.org/gnunet.git/tree/src/gns`
  - Second implementation in Go: https://github.com/bfix/gnunet-go/tree/master/src/gnunet/service/gns
- Specification
  - Current draft: `draft-schanzen-gns-01`.
  - Status: Documents current implementation. Collecting feedback to improve protocol (and spec).

Next steps

- Address received feedback:
  - Better trust agility to address questions on choice of Hierarchical Deterministic Key Derivation (HKDF). No ”standard” go-to HKDF exists at this time:
    - In draft and implemented: ECDSA (RFC6979) over Curve25519 (RFC8031).
    - Alternatives: Schnorr/Ed25519-based (“Tor-style”).[5]
  - Update to symmetric encryption scheme for IND-CCA.
  - Address other feedback.
- Desired next steps at IETF:
  - Receive feedback from IETF experts on protocol and document.
  - Is this document interesting to any existing IETF/IRTF WG? Should/can a new WG be formed?

[5] BIP32-Ed25519 has issues: `https://forum.web3.foundation/t/key-recovery-attack-on-bip32-ed25519/44`

The GNU Name System

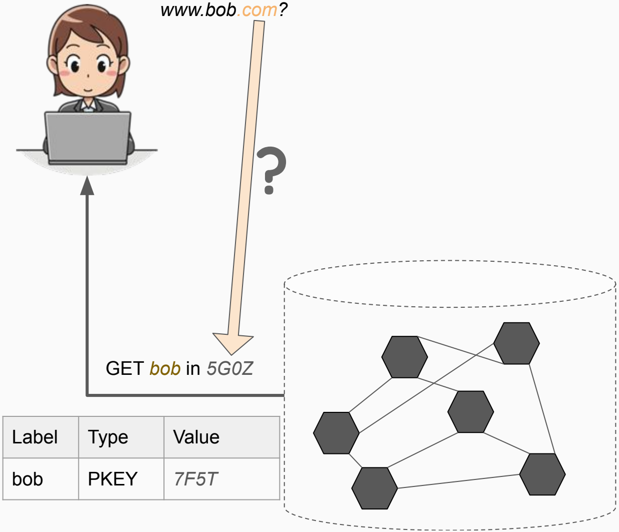
https://gnunet.org

schanzen@gnunet.org
3D11 063C 10F9 8D14 BD24 D147 0B09 98EF 86F5 9B6A

References

1. Matthias Wachs, Martin Schanzenbach and Christian Grothoff. *A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System*. **13th Intern ational Conference on Cryptology and Network Security**, 2014.
2. Martin Schanzenbach, Georg Bramm, Julian Schütte. *reclaimID: Secure, Self-Sovereign Identities Using Name Systems and Attribute-Based Encryption*. **17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom)**, 2018
3. Christian Grothoff, Martin Schanzenbach, Annett Laube, Emmanuel Benoist, Pascal Mainini. *Decentralized Authentication for Self-Sovereign Identities using Name Systems (DASEIN)*. **https://git.gnunet.org/bibliography.git/plain/docs/dasein10.pdf**, 2018.

How do we bootstrap the top-level zones?



www.bob.com?

GET *bob* in *5G0Z*

Label	Type	Value
bob	PKEY	*7F5T*

The GNU Name System Root

“Hyper-hyper local root” concept:

- Resolver ships with initial root zone configuration.
- Root zone configurable *locally* at *each* endpoint.
- User override/extension of root at top-level or subdomain-level for:
    - Circumvent censorship if necessary.
    - Private networks.

Envisioned Governance Model

- Non-profit organization.
- Multi-stakeholder model: Board, supporting organizations, . . .
- Examples for possible stakeholders:
  - Software and OS Distributors
  - Browser vendors
  - Governments
- Funding options:
  - Applications for new top-level domains.
  - Registrations of new top-level domains.
  - . . .