The GNU Name System

Christian Grothoff Martin Schanzenbach Bernd Fix

The GNU Project & Bern University of Applied Sciences

IETF 116

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

Motivation

- DNS censorship is wide-spread
- DNS is part of the mass surveillance apparatus (MCB)
- DNS is abused for the offensive cyber war (QUANTUMDNS)

Mass surveilance is an attack (RFC 7258) and DNS is known to be part of the problem (RFC 8324).

The GNU Name System

- **Decentralized** name system with secure memorable names
- Delegation used to achieve transitivity
- Also supports globally unique, secure identifiers

`www.example.gns.alt`

```
[gns]
.example.gns.alt = 000G000P02FDZNBAT26ST3NE08T3K3AEKGWGDAPYXPW14WTQWRZHBZH2N4
```

Key Features

GNS is designed so that it could be used to resolve names in the DNS namespace and (given a standards action) resolve or enhance the existing DNS namespace.

- Achieves query and response privacy with cipher agility:
  If zone public key **or** label is secret, **then** the record is secret!
- Globally instant and reliable key revocation
- Supports DANE (PKI!)

Project status

- Draft exists, passed ISE, at IESG conflict review
- Independent implementations in C and Go exist
- UX study shows users cannot tell DNS vs. GNS
- DNS2GNS zone transfer tool *Ascension* runs on ".fr" and other (public) TLDs

```
$ wget https://taler.net/taler-systems.gpg.key
# cat > /etc/apt/sources.list.d/taler.list <<EOF
deb [signed-by=taler-systems.gpg.key] \
https://deb.taler.net/apt/debian stable main
EOF
# apt update
# apt install gnunet gnunet-gtk
```

The pTLD question

- ".alt" draft recommends using ".alt" to avoid conflicts
- GNUnet project runs GANA[1] with ".alt" subdomain registry for alternative domain systems, reserves ".gns.alt" for GNS.
- GNUnet is **Free Software**, users are free to configure *any* TLD.

Recommended for DNS2GNS ascensions of DNS zones!

```
[gns]
.nu = 000G0027X4H7W66FJPS6WFFET3NTWBFERPR1JY07KPR0TWYQXRB4VAH320
.li = 000G002YN1MCFNYT4DFSQVCRNWTZ2X886XASHVJD34Y0AKSN7AG02E8A90
```

[1] https://git.gnunet.org/gana.git

Conclusion

- GNS provides an alternative for the obsolete DNS protocol
- Specification, implementations and migration logic exist
- ".alt" draft would address name space conflict for use-cases where it is a problem
- Draft describing R^5N, the DHT used for storage by GNS: `https://datatracker.ietf.org/doc/draft-schanzen-r5n/`

Do you have any questions?

- Yves Eudes, Christian Grothoff, Jacob Appelbaum, Monika Ermert, Laura Poitras, Matthias Wachs: *MoreCowBell, nouvelles révélations sur les pratiques de la NSA*. **Le Monde**, 24.1.2015.
- Nathan Evans and Christian Grothoff. *R^5N. 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.