Ascension into the GNU Name System

Automating the migration to the GNU Name System

rexxnor

15. Juni 2019

1 DNS

- Why it sucks
- Attempts to make DNS “secure”

2 GNU Name System (GNS)

- Query privacy

3 Ascension

- Demo
- Outlook

Table of Contents

1 DNS

- Why it sucks
- Attempts to make DNS “secure”

2 GNU Name System (GNS)

- Query privacy

3 Ascension

- Demo
- Outlook

Table of Contents

1 DNS

- Why it sucks
- Attempts to make DNS “secure”

2 GNU Name System (GNS)

- Query privacy

3 Ascension

- Demo
- Outlook

Recap

- Unencrypted
- Censorable
- Privacy nightmare
- Exploitable

Recap

- Unencrypted
- Censorable
- Privacy nightmare
- Exploitable
- Sadly essential

How I thought DNS works [4]

How I thought DNS works [4]

- Hi Root server, I want to know the nameservers for com

How I thought DNS works [4]

- Hi Root server, I want to know the nameservers for com
- Sure, here are the servers for .com

How I thought DNS works [4]

- Hi Root server, I want to know the nameservers for com
- Sure, here are the servers for .com
- Hi .com server, I want to know the nameservers for example.com

How I thought DNS works [4]

- Hi Root server, I want to know the nameservers for com
- Sure, here are the servers for .com
- Hi .com server, I want to know the nameservers for example.com
- Sure, here are the servers for example.com

How I thought DNS works [4]

- Hi Root server, I want to know the nameservers for com
- Sure, here are the servers for .com
- Hi .com server, I want to know the nameservers for example.com
- Sure, here are the servers for example.com
- Hi example.comserver, I want to resolve www.example.com

How I thought DNS works [4]

- Hi Root server, I want to know the nameservers for com
- Sure, here are the servers for .com
- Hi .com server, I want to know the nameservers for example.com
- Sure, here are the servers for example.com
- Hi example.comserver, I want to resolve www.example.com
- Sure –its 93.184.216.34

How it actually works [4]

How it actually works [4]

- Hi root server, I want to resolve www.example.com

How it actually works [4]

- Hi root server, I want to resolve www.example.com
- Not me –try asking the servers for .com

How it actually works [4]

- Hi root server, I want to resolve www.example.com
- Not me –try asking the servers for .com
- Hi .com server, I want to resolve www.example.com

How it actually works [4]

- Hi root server, I want to resolve www.example.com
- Not me –try asking the servers for .com
- Hi .com server, I want to resolve www.example.com
- Not me –try asking the servers for example.com

How it actually works [4]

- Hi root server, I want to resolve www.example.com
- Not me –try asking the servers for .com
- Hi .com server, I want to resolve www.example.com
- Not me –try asking the servers for example.com
- Hi example.comserver, I want to resolve www.example.com

How it actually works [4]

- Hi root server, I want to resolve www.example.com
- Not me –try asking the servers for .com
- Hi .com server, I want to resolve www.example.com
- Not me –try asking the servers for example.com
- Hi example.comserver, I want to resolve www.example.com
- Sure –its 93.184.216.34

How it actually works [4]

- Hi root server, I want to resolve www.example.com
- Not me –try asking the servers for .com
- Hi .com server, I want to resolve www.example.com
- Not me –try asking the servers for example.com
- Hi example.comserver, I want to resolve www.example.com
- Sure –its 93.184.216.34
- QNAME minimization proposed in RFC 7816 [1]

How it actually works [4]

- Hi root server, I want to resolve www.example.com
- Not me –try asking the servers for .com
- Hi .com server, I want to resolve www.example.com
- Not me –try asking the servers for example.com
- Hi example.comserver, I want to resolve www.example.com
- Sure –its 93.184.216.34
- QNAME minimization proposed in RFC 7816 [1]
- In 2016! (29 years after RFCs 1034 [5] and 1035 [6])

Table of Contents

1 DNS

- Why it sucks
- Attempts to make DNS “secure”

2 GNU Name System (GNS)

- Query privacy

3 Ascension

- Demo
- Outlook

DNSSEC

- Signature of records
- Tamper detection
- Trust Anchors
- Authenticity of records
- No encryption

DNS over TLS (DoT)

- Transport encryption to resolver
- Uses established technologies
- Implementations are diverse
- Need a trusted resolver
- Resolver still uses DNS

DNS over HTTPS (DoH)

- Transport encryption to a resolver
- HTTP headers in HTTPS stream
- Filtered out by proxy
- Need to trust resolver
- Resolver still uses DNS

Table of Contents

1. DNS
   - Why it sucks
   - Attempts to make DNS “secure”

2. GNU Name System (GNS)
   - Query privacy

3. Ascension
   - Demo
   - Outlook

Basics [2]

- Decentralized name system using a DHT
- A zone is a keypair
- → Globally unique names using zones public key
- Allows for pet names
- Query and response privacy
- Interoperable with DNS

Developments [2]

- There was “.gnu” as TLD
- GNUnet e.V. did not get “.gnu” TLD
- February 2018 GNUnet v.0.11.0 released
- No more need for “.gnu”
- All current DNS zones can exist in GNS

Differences to DNS

- A "." is a strict zone cut
- Every zone has a globally unique identifier
- i.e.: `X9PR7P1P8JBGJFG9TA57YSDTCXCA6VC33JY84FSG165PP11R3MDG`
- Delegation via PKEY records
  - In zone ccc:
  - `chaostreffbern IN PKEY YD55SVDS0FPSDGG6ZD9QFG8ERPEFA4C3WEY89DMGKXZ4Q08DZ5N0`
  - Resolve `www.YD55SVDS0FPSDGG6ZD9QFG8ERPEFA4C3WEY89DMGKXZ4Q08DZ5N0`
  - Resolve `www.chaostreffbern`
  - or `www.chaostreffbern.ZESSTF52R6CQBGWF8P743GN4JGFRYYCF11NE7Q8MEZ9JN97NS1KG`
  - or `www.chaostreffbern.ccc`
- Fallback resolution via GNS2DNS records
- In zone chaostreffbern
- i.e.: `www IN GNS2DNS chaostreffbern.ch@217.197.129.41`

Table of Contents

1. DNS
   - Why it sucks
   - Attempts to make DNS “secure”

2. GNU Name System (GNS)
   - Query privacy

3. Ascension
   - Demo
   - Outlook

Query privacy: terminology [2]

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 [2] I

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

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

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

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

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

Query privacy: cryptography [2] II

$$h := H(l, P) \tag{5}$$

$$q_{P,l} := H(hP) = H(hxG) = H(dG) \Rightarrow \texttt{obtain } B_{P,l} \tag{6}$$

$$R_{P,l} = D_{HKDF(l,P)}(B_{P,l}) \tag{7}$$

Table of Contents

1 DNS
- Why it sucks
- Attempts to make DNS “secure”

2 GNU Name System (GNS)
- Query privacy

3 Ascension
- Demo
- Outlook

What is Ascension?

- Python tool to migrate DNS zones to GNS
- Uses DNS zone transfer (AXFR)
- Supports incrementeal zone transfer (IXFR)
- Makes ascending into GNS a breeze

How it works

- Transfers a DNS zone from a willing nameserver

How it works

- Transfers a DNS zone from a willing nameserver
- Creates the equivalent structure in GNS

How it works

- Transfers a DNS zone from a willing nameserver
- Creates the equivalent structure in GNS
- Migrates the important records

How it works

- Transfers a DNS zone from a willing nameserver
- Creates the equivalent structure in GNS
- Migrates the important records
- Throws out superfluous records

How it works

- Transfers a DNS zone from a willing nameserver
- Creates the equivalent structure in GNS
- Migrates the important records
- Throws out superfluous records
- Keeps the zone synchronized

Results

DNS Zone	.bfh.ch	.sy	.nu	.se
No. of records	3’200	5’559	1’471’035	8’835’228
No. of GNS zones	183	49	2’174	17’331
Import time	0.25h	0.07h	13h	116h
Bandwidth	0.15 MB	0.24 MB	137 MB	1’273 MB

Tabelle: Experimental results for Ascension

Challenges

- Zone size

Challenges

- Zone size
- Performance

Challenges

- Zone size
- Performance
    - Command execution

Challenges

- Zone size
- Performance
  - Command execution
  - Identity creation

Challenges

- Zone size
- Performance
  - Command execution
  - Identity creation
  - Who the hell would do that? [3]
- Changes to zones

Challenges

- Zone size
- Performance
  - Command execution
  - Identity creation
  - Who the hell would do that? [3]
- Changes to zones
- Not enough TLDs offering zone transfer

Packaging for Debian

- Creating a Debian package python3-ascension

Packaging for Debian

- Creating a Debian package python3-ascension
  - Runs a GNUnet peer
  - Depends on GNUnet (kind of)

Packaging for Debian

- Creating a Debian package python3-ascension
  - Runs a GNUnet peer
  - Depends on GNUnet (kind of)
- Creating the Ascension-bind Debian package

Packaging for Debian

- Creating a Debian package python3-ascension
  - Runs a GNUnet peer
  - Depends on GNUnet (kind of)
- Creating the Ascension-bind Debian package
  - Depends on python3-ascension

Packaging for Debian

- Creating a Debian package python3-ascension
  - Runs a GNUnet peer
  - Depends on GNUnet (kind of)
- Creating the Ascension-bind Debian package
  - Depends on python3-ascension
  - Allows zone transfer on localhost

Packaging for Debian

- Creating a Debian package python3-ascension
  - Runs a GNUnet peer
  - Depends on GNUnet (kind of)
- Creating the Ascension-bind Debian package
  - Depends on python3-ascension
  - Allows zone transfer on localhost
  - Migrates running BIND zones into GNS using Ascension

Packaging for Debian

- Creating a Debian package python3-ascension
    - Runs a GNUnet peer
    - Depends on GNUnet (kind of)
- Creating the Ascension-bind Debian package
    - Depends on python3-ascension
    - Allows zone transfer on localhost
    - Migrates running BIND zones into GNS using Ascension
    - Interactive zone selection

Packaging for Debian

- Creating a Debian package python3-ascension
  - Runs a GNUnet peer
  - Depends on GNUnet (kind of)
- Creating the Ascension-bind Debian package
  - Depends on python3-ascension
  - Allows zone transfer on localhost
  - Migrates running BIND zones into GNS using Ascension
  - Interactive zone selection
  - Running Ascension as a daemon

Table of Contents

1 DNS
- Why it sucks
- Attempts to make DNS “secure”

2 GNU Name System (GNS)
- Query privacy

3 Ascension
- Demo
- Outlook

Demo

Table of Contents

1. DNS
   - Why it sucks
   - Attempts to make DNS “secure”
2. GNU Name System (GNS)
   - Query privacy
3. Ascension
   - Demo
   - Outlook

Outlook

- Add DNSCurve Style records

Outlook

- Add DNSCurve Style records
- `@ IN NS gns–pkey–RFW2RZKJ9Y41F8AJD43VB1NHSTJKKVG32HYPPH5QCVNS7KW75XQ0`

Outlook

- Add DNSCurve Style records
- `@ IN NS gns–pkey–RFW2RZKJ9Y41F8AJD43VB1NHSTJKKVG32HYPPH5QCVNS7KW75XQ0`
- Support for more DNS Servers (PowerDNS, Knot DNS)

Outlook

- Add DNSCurve Style records
- `@ IN NS gns–pkey–RFW2RZKJ9Y41F8AJD43VB1NHSTJKKVG32HYPPH5QCVNS7KW75XQ0`
- Support for more DNS Servers (PowerDNS, Knot DNS)
- Increase performance for zone migration

Outlook

- Add DNSCurve Style records
- `@ IN NS gns-pkey-RFW2RZKJ9Y41F8AJD43VB1NHSTJKKVG32HYPPH5QCVNS7KW75XQ0`
- Support for more DNS Servers (PowerDNS, Knot DNS)
- Increase performance for zone migration
- Anyone wants to create a zone “.ccc”?

- S. Bortzmeyer, “DNS Query Name Minimisation to Improve Privacy,” RFC 7816 (Experimental), RFC Editor, Fremont, CA, USA, pp. 1–11, Mar. 2016. [Online]. Available: https://www.rfc-editor.org/rfc/rfc7816.txt

- C. Grothoff. (2019) Gnu name system: 2019 edition. [Accessed: 2019-06-13]. [Online]. Available: https://grothoff.org/christian/dinrg2019.pdf

- ——. (2019) gnunet-gns can be slow. [Accessed: 2019-06-13]. [Online]. Available: https://bugs.gnunet.org/view.php?id=5743

- G. Huston and J. S. Dama, “Dns privacy,” *The Internet Protocol Journal*, vol. 20, no. 1, 2017.

- P. Mockapetris, “Domain names - concepts and facilities,” RFC 1034 (Internet Standard), RFC Editor, Fremont, CA, USA, pp. 1–55, Nov. 1987, updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936, 8020, 8482. [Online]. Available: https://www.rfc-editor.org/rfc/rfc1034.txt

- ——, “Domain names - implementation and specification,” RFC 1035 (Internet Standard), RFC Editor, Fremont, CA, USA, pp. 1–55, Nov. 1987, updated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604, 7766, 8482. [Online]. Available: https://www.rfc-editor.org/rfc/rfc1035.txt