

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

Christian Grothoff

Technische Universität München

24.01.2014

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

Where We Are



Source: esmont



Source: gaWand.org



Where We Are



الموقع محظور

أسف! إن الموقع الذي أردت تصفحه قد أُحجب وذلك بسبب إحتوائه على نشاط مخالف للقيم الاجتماعية أو السياسية أو الثقافية أو الدينية لخدمة الإمارات العربية المتحدة.

في حالة أردت فتح موقع قد أُحجب الرجاء قم بتصفة إستشارة الملاحظات الموضوعة على موقعنا.

We apologize the site you are attempting to visit has been blocked due to its content being inconsistent with the religious, cultural, political and moral values of the United Arab Emirates.

If you think this site should not be blocked, please visit the [Feedback Form](#) available on our website.

SITE BLOCKED

Source: wikileaks.org



History: ECHELON

- ▶ SIGINT collection network of AU, CA, NZ, UK and US
- ▶ Baltimore Sun reported in 1995 that Airbus lost a \$6 billion contract in 1994 after NSA reported that Airbus had been bribing officials to secure the contract.
- ▶ Used to facilitate Kenetech Windpower's espionage against Enercon in 1994-1996.



Former US listening station at Teufelsberg, Berlin.

The Enemy Within

“In February, the UK based research publication Statewatch reported that the **EU had secretly agreed** to set up an international telephone tapping network via a secret network of committees established under the “third pillar” of the Maastricht Treaty covering cooperation on law and order. (...) EU countries (...) should agree on **international interception standards (...) to co-operate closely with the FBI** (...). Network and service providers in the EU will be obliged to install **tappable** systems and to place under **surveillance** any person or group when served an interception order. These plans have never been referred to any European government for scrutiny (...) despite the **clear civil liberties issues** raised by such an **unaccountable** system. (...) The German government estimates that the mobile phone part of the package alone will cost 4 billion D-marks.”

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)
- ▶ Content of calls and identity of individuals is often not even considered
- ▶ Joint Special Operations Command (JSOC) uses geolocation of SIM card for assassinations using drone strikes
- ▶ Individual in possession of SIM card is sometimes not even identified prior to strike

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

Not Just Monitoring

- ▶ NSA TAO infiltrated 85,000 computer systems world-wide (Der Spiegel, 12'2013).
- ▶ FOXACID, QUANTUM* and MUSCULAR use man-in-the-middle attacks.
- ▶ NSA compromises cryptographic standards and uses NSLs to force companies to disclose private keys.

Not Just Monitoring

- ▶ NSA TAO infiltrated 85,000 computer systems world-wide (Der Spiegel, 12'2013).
- ▶ FOXACID, QUANTUM* and MUSCULAR use man-in-the-middle attacks.
- ▶ NSA compromises cryptographic standards and uses NSLs to force companies to disclose private keys.
- ▶ The targets are social movements:
 - ▶ Anonymous
 - ▶ Wikileaks
 - ▶ Environmental groups (for example, the UN Climate Change Conference in Copenhagen)

Where We Are



Source: esmont



Source: gaWand.org



Where We Are



الموقع محظور

أسف! إن الموقع الذي أردت تصفحه قد أُحجب وذلك بسبب إحتوائه على نشاط مخالف للقيم الاجتماعية أو السياسية أو الثقافية أو الدينية لخدمة الإمارات العربية المتحدة.

في حالة أردت فتح موقع قد أُحجب الرجاء قم بتصفة إستشارة الملاحظات الموضحة على موقعنا.

We apologize the site you are attempting to visit has been blocked due to its content being inconsistent with the religious, cultural, political and moral values of the United Arab Emirates.

If you think this site should not be blocked, please visit the [Feedback Form](#) available on our website.

SITE BLOCKED

Source: wikileaks.org



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 System¹

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

¹Joint work with Martin Schanzenbach and Matthias Wachs

Zone Management: like in DNS


gnunet-setup


General Network Transports File Sharing Namestore **GNS**

Editing zone API5QDP7A126P06VV60535PDT50B9L12NK6QP64IE8KNC6E807G0 

Preferred zone name (PSEU):

Master Zone Private Zone Shorten Zone



 Save As

Name	Type	Value	Expiration	Public
<new name>				
+ >	<new record>			
	MX	5,mail.+	end of time	<input checked="" type="checkbox"/>
priv >	<new record>			
	PKEY	3IQ1TG601GUBVO55C0J087OEFB8N3DBJQ4L9SBI8PFLR8UKCVGHG	end of time	<input type="checkbox"/>
heise >	<new record>			
	LEHO	heise.de	end of time	<input checked="" type="checkbox"/>
	AAAA	2a02:2e0:3fe:100::8	end of time	<input checked="" type="checkbox"/>
	A	193.99.144.80	end of time	<input checked="" type="checkbox"/>
home >	<new record>			
大学 >	<new record>			
short >	<new record>			
mail >	<new record>			
homepage >	<new record>			
fcfs >	<new record>			
www >	<new record>			

[Welcome to gnunet-setup.](#)

Secure introduction



TUM

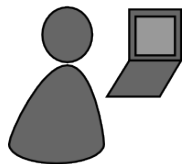


 **Bob Builder, Ph.D.**

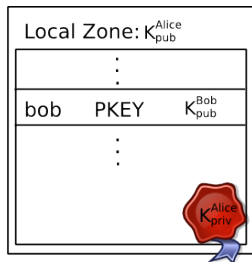
Address: Country, Street Name 23
Phone: 555-12345
Mobile: 666-54321
Mail: bob@H2R84L4JIL3G5C.zkey

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

Delegation

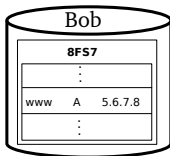


Alice

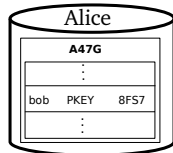
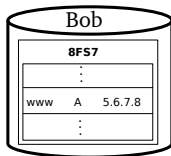
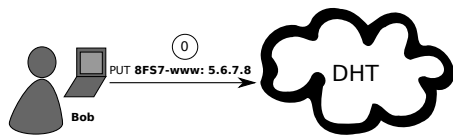


- ▶ Alice learns Bob's public key
- ▶ Alice creates delegation to zone K_{pub}^{Bob} under label **bob**
- ▶ Alice can reach Bob's webserver via **www.bob.gnu**

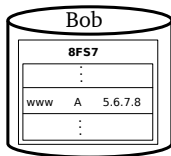
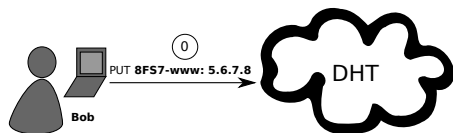
Name Resolution



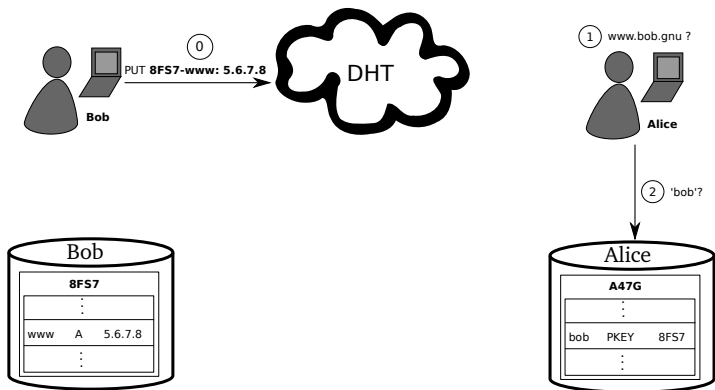
Name Resolution



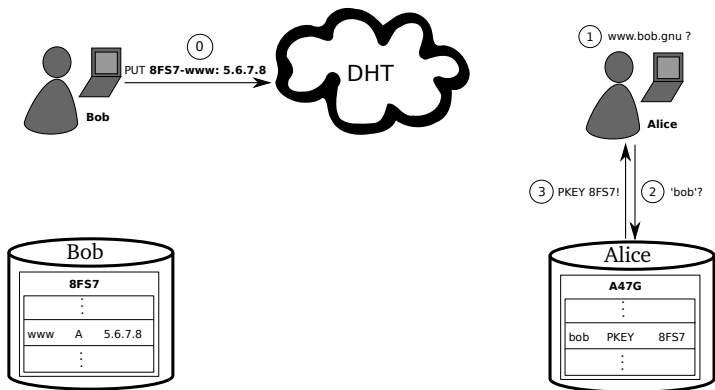
Name Resolution



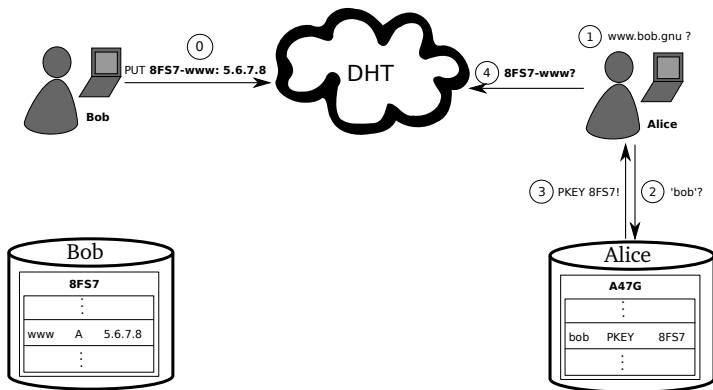
Name Resolution



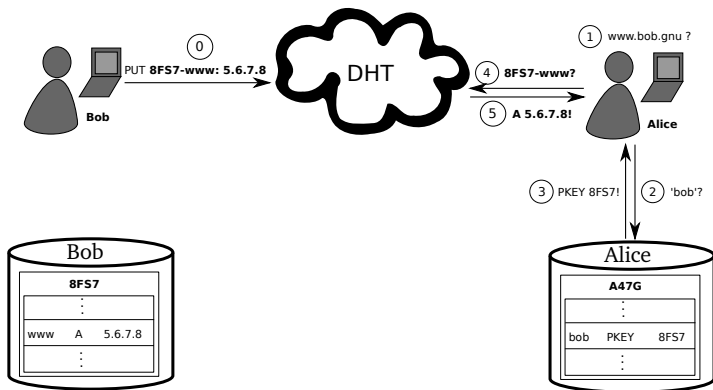
Name Resolution




Name Resolution



Name Resolution



GNS as PKI (via DANE/TLSA)



The screenshot shows a web browser window with the address bar displaying `https://freedom.gnu`. A security warning dialog box is open, titled "freedom.gnu" with the subtext "identity verified". The dialog has two tabs: "Permissions" and "Connection".

Permissions

- The identity of this website has been verified by GNS CA. [Certificate Information](#)

Connection

- Your connection to freedom.gnu is encrypted with 256-bit encryption. The connection uses TLS 1.2. The connection is encrypted using AES_256_CBC, with SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism.

Site information

- You have never visited this site before today. [What do these mean?](#)

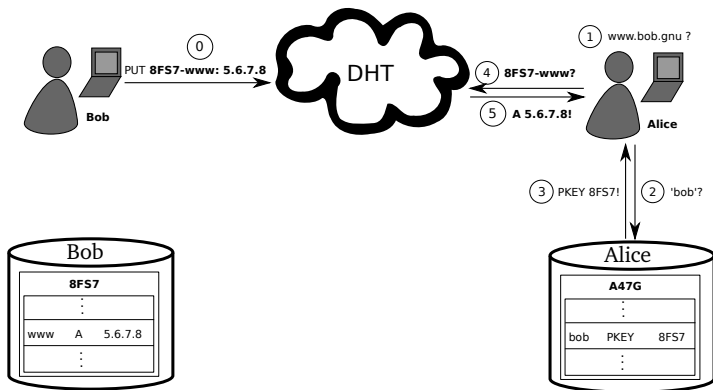
The background of the browser shows the GNU Operating System website, with a navigation menu including "Why", "Licenses", "Education", "Software", "Documentation", and "Help". The main heading is "Operating System" and "What is GNU?".

The [GNU Project](#) was launched in 1984 to develop the GNU system. The name "GNU" is a recursive acronym for "GNU's Not Unix!". "GNU" is pronounced *g'noo*, as one syllable, like saying "grew" but replacing the *r* with *n*.

A Unix-like operating system is a [software collection](#) of applications, libraries, and developer tools, plus a program to allocate resources and talk to the hardware, known as a kernel.

[The Hurd, GNU's own kernel](#), is some way from being ready for daily use. Thus, GNU is typically used today with a kernel called Linux. This combination is the [GNU/Linux operating system](#). GNU/Linux is used by millions, though many [call it "linux" by mistake](#).

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 $q_{P,I}$

$$h := H(I, P) \quad (1)$$

$$d := h \cdot x \pmod n \quad (2)$$

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

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

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

$$h := H(I, P) \quad (5)$$

$$q_{P,I} := H(hP) = H(hxG) = H(dG) \Rightarrow \text{obtain } B_{P,I} \quad (6)$$

$$R_{P,I} = D_{HKDF(I,P)}(B_{P,I}) \quad (7)$$

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 reconcile 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!



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 ...

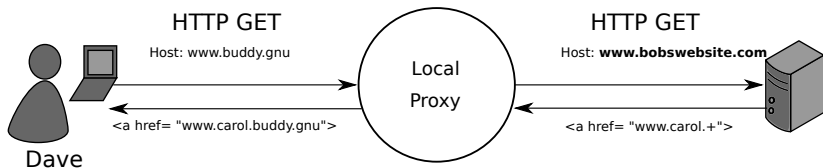
... we need support for Virtual Hosting!

... we need support for SSL!

Solution: Client Side SOCKS Proxy

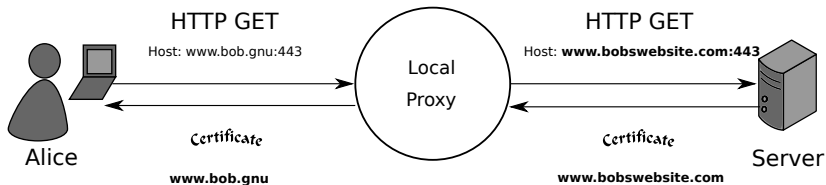
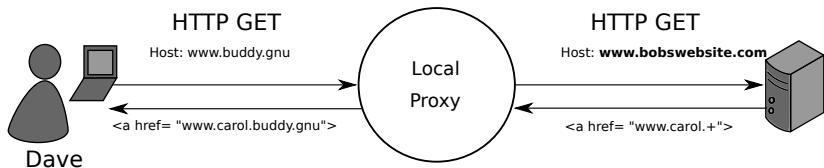
Legacy Hostname (LEHO) Records

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.



Long-Term Vision

- ▶ Integration with browser and HTTP server
- ▶ HTTP server receives “GNS-Zone: PKEY” instead of “Hostname”
- ▶ HTTP client uses “TLSA” record of GNS, instead of “LEHO”

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, too.

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 GUNet 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 GUNet since 0.9.3
- ▶ Crypto changed to Curve25519 in 0.10.0
- ▶ Internationalized Domain Names are supported

Current State

- ▶ GNS part of GUNet 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
- ▶ No GUI for TLSA/CERT records yet

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



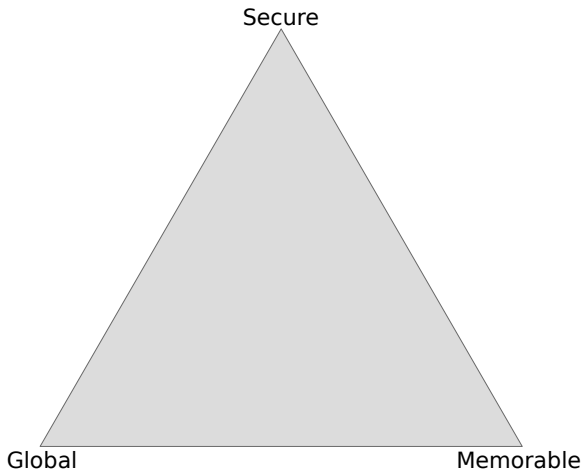
We must decentralize or accept autocracy and planetary collapse.

Do you have any questions?

References:

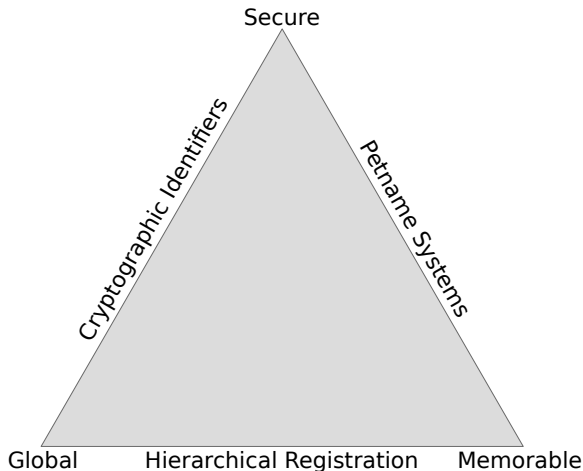
- ▶ Nathan Evans and Christian Grothoff. *R5N. Randomized Recursive Routing for Restricted-Route Networks*. **5th International Conference on Network and System Security**, 2011.
- ▶ Matthias Wachs, Martin Schanzenbach and Christian Grothoff. *On the Feasibility of a Censorship Resistant Decentralized 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.

Zooko's Triangle



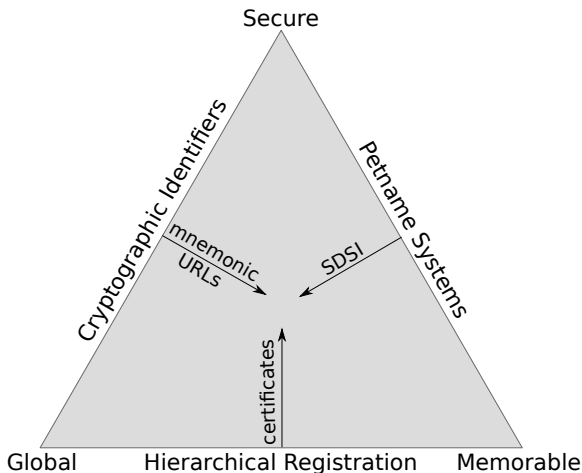
A name system can only fulfill **two!**

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