

The GNU Name System

Christian Grothoff

Inria Rennes Bretagne Atlantique

2.7.2015

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

Where We Are



Where We Are



الموقع محظور

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

في حالة أردت فتح الموقع قد أُحجب الرجاء قم بتصفحة 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



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.

MORECOWBELL: Meta Data of the Internet



NSA/CSS Threat Operations Center

Cyber Profiling and Operations Support (V43)

(U) MORECOWBELL

(S//REL) A Covert
HTTP/ DNS
Monitoring System for
Operations Support



TOP SECRET//COMINT//REL FVEY

MORECOWBELL: Meta Data of the Internet



(U) What is MORECOWBELL?

- (S//REL) MORECOWBELL (MCB) is a V43 developed system used to support V3 and JFCC-Network Warfare Operations
- (S//REL) Built on the PACKAGEDGOODS infrastructure and cover mechanisms.
- (S//REL) Deployed on a covered infrastructure on the public Internet
- (S//REL) Performs DNS lookups and HTTP requests against targets on regular intervals
- (S//REL) Used to track changes to DNS resolution as well as up/down status of websites

TOP SECRET//COMINT//REL FVEY



(U) How Does it Work?

- (U) Consists of:
 - (U//FOUO) Central tasking system housed in V43 office Spaces
 - (S//REL) Several covertly rented web servers (referred to as bots) in: Malaysia, Germany, and Denmark
- (S//REL) The MCB bots utilize open DNS resolvers to perform thousands of DNS lookups every hour.
- (S//REL) MCB bots have the ability to perform HTTP GET requests (mimicking a user's web browser)
- (S//REL) The data is pulled back to the NSA every 15-30 minutes
- (S//REL) Data Currently available on NSANet via web services

TOP SECRET//COMINT//REL FVEY



(U) Benefits

- (S//REL) MCB enables the NTOC to monitor thousands of Internet websites in near real-time
 - (S//REL) Foreign government websites
 - (S//REL) Terrorist/Extremist web forums
 - (S//REL) Malware Domains (callback or beacon addresses)
 - (S//REL) U.S. Government websites via Request for Technical Assistance from Homeland Security
- (S//REL) Currently used to support Battle Damage Indication after CNA and for Situation Awareness
- (S//REL) OPSEC: unattributable to the USG

TOP SECRET//COMINT//REL FVEY

$$1+1=2$$

- ▶ NSA “kills based on meta data” –Michael Hayden (former NSA director)
- ▶ DNS makes it trivial to gather meta data about most Internet activities

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

Where We Are



الموقع محظور

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

في حالة أردت فتح الموقع قد أُحجب الرجاء قم بتصفحة 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



JTRIG: Übertralls of the Internet



EFFECTS: Definition



- “Using online techniques to make something happen in the real or cyber world”
- Two broad categories:
 - Information Ops (influence or disruption)
 - Technical disruption
- Known in GCHQ as Online Covert Action
- The 4 D’s: Deny / Disrupt / Degrade / Deceive

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Encryption to the Rescue?

- ▶ Centralized Internet infrastructure is easily controlled¹:
 - ▶ 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!
- ▶ Encryption alone does not protect meta data

¹Deny (censor), Disrupt (DDoS), Deceive (redirect)

The GNU Name System (GNS)²

Properties of GNS


- ▶ Decentralized name system with secure memorable names
- ▶ Provides alternative public key infrastructure
- ▶ Interoperable with DNS
- ▶ Achieves query and response privacy

²Joint 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

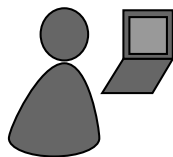


 Save As

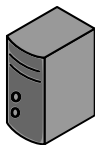
Name	Type	Value	Expiration	Public
<new name>				
+ >	<new record>			
	MX	5,mail.+	end of time	<input checked="" type="checkbox"/>
priv >	<new record>			
	PKEY	3IQ1TG601GUBVO55C0J0870EFB8N3DBJQ4L9SBI8PFLR8UKCVGHG	end of time	<input type="checkbox"/>
heise >	<new record>			
	LEHO	heise.de	end of time	<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>			
fdfs >	<new record>			
www >	<new record>			

[Welcome to gnunet-setup.](#)

Name resolution in GNS



Bob




Bob's webserver

Local Zone: K_{pub}^{Bob}		
www	A	5.6.7.8

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

Secure introduction



TUM

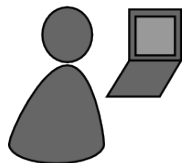


Bob Builder, Ph.D.

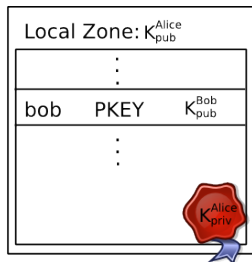
Address: Country, Street Name 23
Phone: 555-12345
Mobile: 666-54321
Mail: bob@H2R84L4JIL3G5C.zkey

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

Delegation

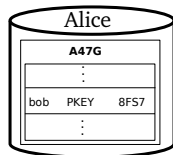
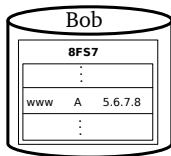


Alice

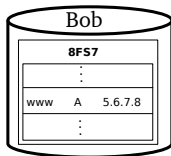
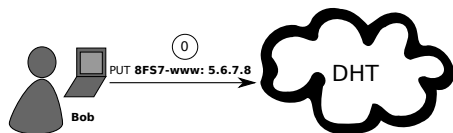


- ▶ Alice learns Bob's public key
- ▶ Alice creates delegation to zone K_{pub}^{Bob} under label **bob**
- ▶ Alice can reach Bob's webserver via **www.bob.gnu**

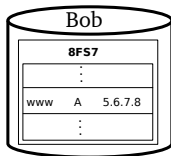
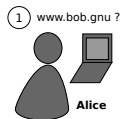
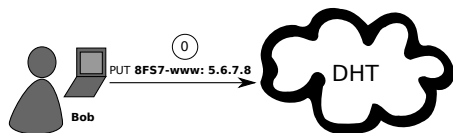
Name Resolution



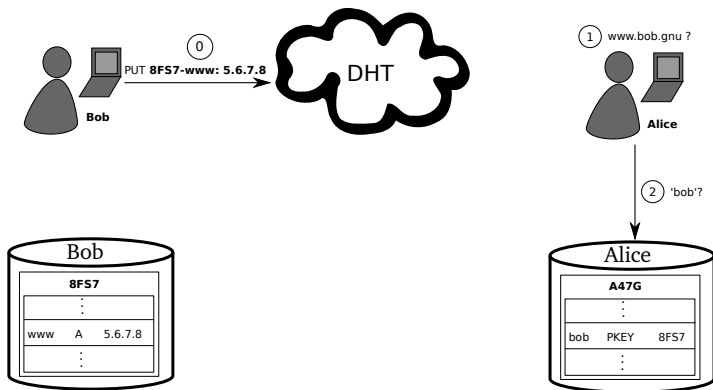
Name Resolution



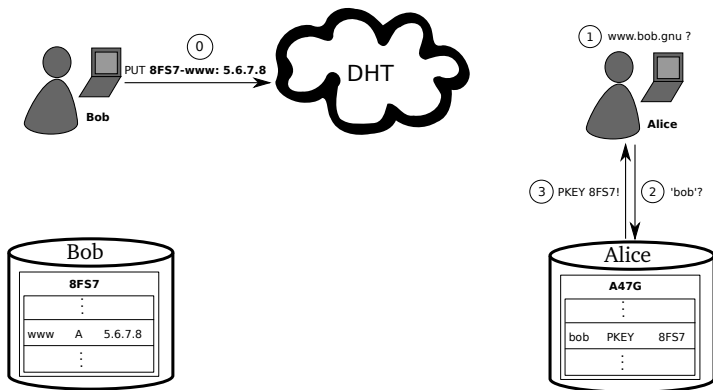
Name Resolution



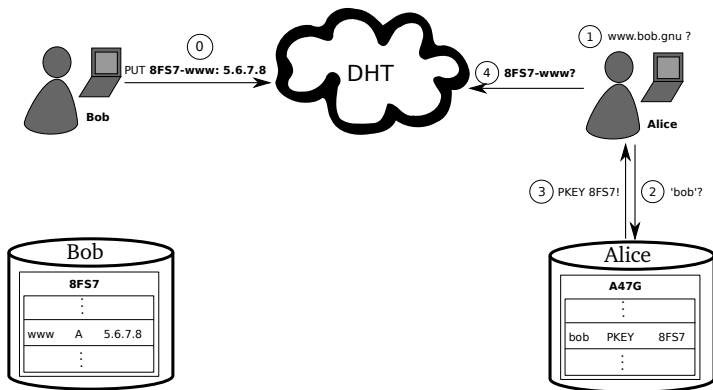
Name Resolution



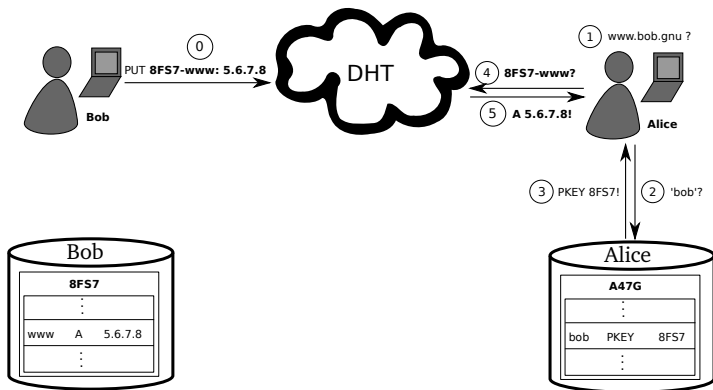
Name Resolution



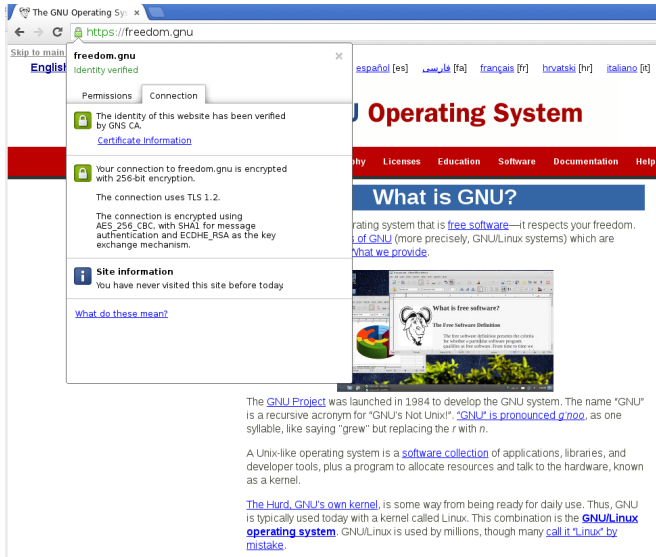
Name Resolution



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 overlaid on the page. The dialog box has a title bar that says "freedom.gnu" and "identity verified". It contains the following information:

- Permissions** tab is selected.
- A green lock icon indicates that the identity of the website has been verified by GNS CA. A link for "Certificate Information" is provided.
- A green lock icon indicates that the connection to freedom.gnu is encrypted with 256-bit encryption. It specifies that the connection uses TLS 1.2 and is encrypted using AES-256 CBC, with SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism.
- Site information** section states: "You have never visited this site before today." A link "What do these mean?" is provided.

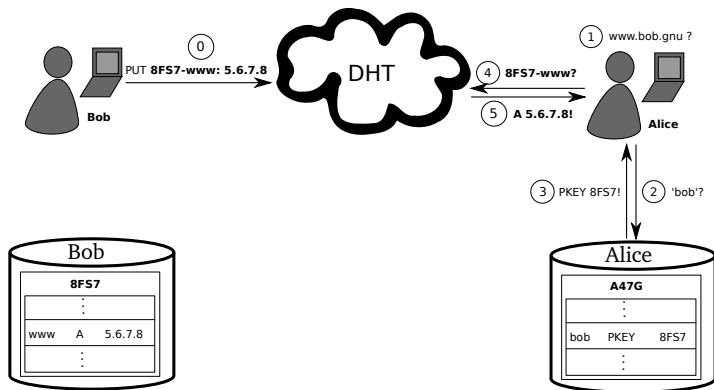
The background of the browser shows the GNU Operating System website. The main heading is "GNU Operating System" in red. Below it is a navigation menu with links for "Why", "Licenses", "Education", "Software", "Documentation", and "Help". A blue banner below the menu says "What is GNU?". The text below the banner reads: "The GNU operating system that is [free software](#)—it respects your freedom. It is a part of GNU (more precisely, GNU/Linux systems) which are [What we provide](#)."

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

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

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

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

The “.zkey” zone

- ▶ “.zkey” is another pTLD, in addition to “.gnu”
 - ▶ In “LABEL.zkey”, the “LABEL” is a public key of a zone
 - ▶ “alice.bob.*KEY*.zkey” is perfectly legal
- ⇒ Globally unique identifiers

Key revocation

- ▶ Revocation message signed with private key (ECDSA)
- ▶ Flooded on all links in P2P overlay, stored forever
- ▶ Efficient set reconciliation used when peers connect
- ▶ Expensive proof-of-work used to limit DoS-potential
- ▶ Proof-of-work can be calculated ahead of time
- ▶ Revocation messages can be stored off-line if desired

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

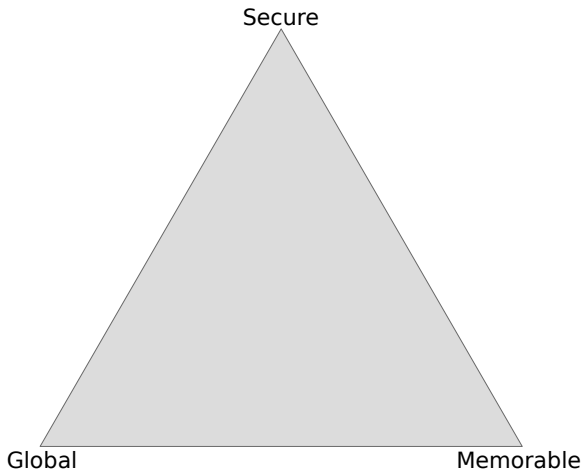
Shadow Records

- ▶ 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

Fun GNS record types

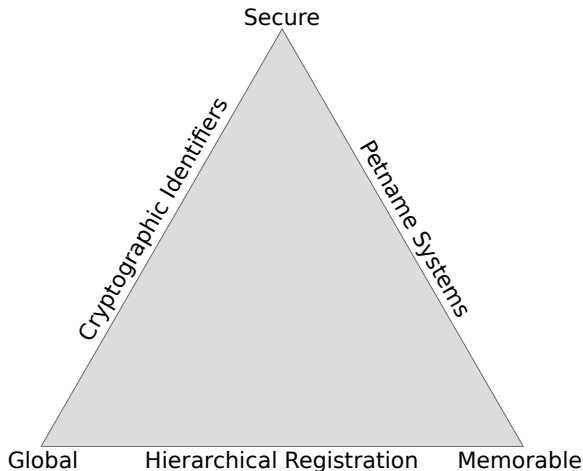
- ▶ BOX: store TLSA records *with* A/AAAA record
- ▶ VPN: TCP/IP services hosted in GUNet
- ▶ PHONE: have a conversation
- ▶ CERT: store your GPG public key (WiP)
- ▶ TOR: store your hidden service descriptor (WiP)

Zooko's Triangle



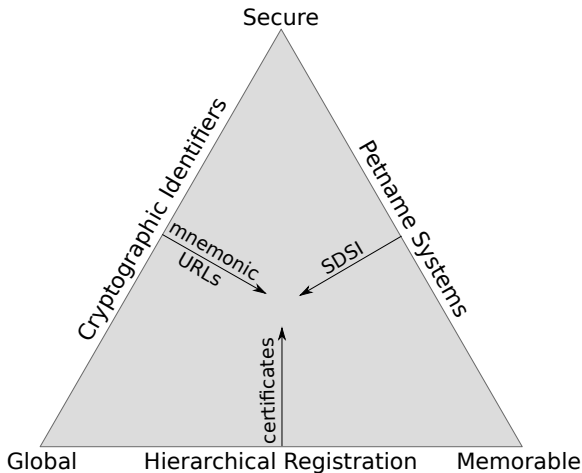
A name system can only fulfill **two!**

Zooko's Triangle



DNS, “.onion” IDs and /etc/hosts/ are representative designs.

Zooko's Triangle



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.

“Totalitarianism is man’s escape from the fearful realities of life into the virtual womb of the leader. (...) The mystic center is in control of everything; man need no longer assume responsibility for his own life. The order and logic of the prenatal world reign. There is peace and silence, the peace of utter submission.”

–Joost A. Merloo, *Rape of the Mind* (1956)

The NSA's TREASUREMAP

TS//SI//REL TO USA, FVEY



(U) What is TREASUREMAP?

(U//FOUO) Capability for building a near real-time, interactive map of the global internet.

Map the entire Internet – Any device*, anywhere, all the time

(U//FOUO) We enable a wide range of missions:

- Cyber Situational Awareness – *your own network plus adversaries'*
- Common Operation Pictures (COP)
- Computer Attack/Exploit Planning / Preparation of the Environment
- Network Reconnaissance
- Measures of Effectiveness (MOE)

(* limited only by available data)

TS//SI//REL TO USA, FVEY

Little Horror Show of Internet Security

- ▶ MAC address spoofing, MAC address tracking, packet sniffing
- ▶ IP address spoofing, IPv6 tracking, packet sniffing, geo-blocking
- ▶ BGP traffic redirection (sniffing, malicious endpoint), route instability, topology discovery
- ▶ TCP SYN flooding, RST injection, TCP sequence prediction, port scanning, TCP unfriendliness (DoS), connection sniffing
- ▶ DNS cache poisoning, distributed reflection DoS, domain lock-up, phantom domain/random subdomain/NXDOMAIN DoS, DNS tunneling & DNS fragmentation, NSEC(3) zone walking attacks
- ▶ TLS renegotiation, version rollback, BEAST, LOGJAM, POODLE, CRIME, BEACH, RC4, Truncation & FREAK attacks

Our Vision (Simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

Our Vision (Simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

HTTPS/TCP/WLAN/...

Our Vision (Simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

CORE (OTR)
HTTPS/TCP/WLAN/...

Our Vision (Simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

R^5N DHT
CORE (OTR)
HTTPS/TCP/WLAN/...

Our Vision (Simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

CADET (Axolotl+SCTP)
R^5N DHT
CORE (OTR)
HTTPS/TCP/WLAN/...

Our Vision (Simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

GNU Name System
CADET (Axolotl+SCTP)
R^5N DHT
CORE (OTR)
HTTPS/TCP/WLAN/...

Our Vision (Simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

Applications
GNU Name System
CADET (Axolotl+SCTP)
R^5N DHT
CORE (OTR)
HTTPS/TCP/WLAN/...

Our Vision (Simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

GNUnet

Applications
GNU Name System
CADET (Axolotl+SCTP)
R^5N DHT
CORE (OTR)
HTTPS/TCP/WLAN/...

Applications?

- ▶ Anonymous file-sharing (`gnunet-fs-gtk`)
- ▶ Conversation (`gnunet-conversation-gtk`)
- ▶ Asynchronous messaging
(<https://pond.imperialviolet.org/>)
- ▶ Synchronous messaging (<http://www.matrix.org/>)
- ▶ Social networking (<http://www.secushare.org/>)
- ▶ Payment (<http://www.taler.net/>)
- ▶ ...

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.



source : www.05active-internet.com/

Namecoin

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