

Résistance des GNUs 2015 Edition

Christian Grothoff

Inria Rennes Bretagne Atlantique

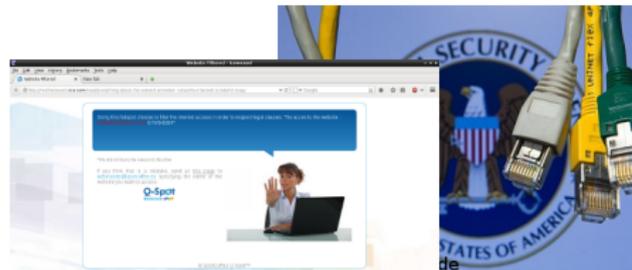
24.3.2015

“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 نشاط مخالف للقيم الاجتماعية أو السياسية أو الثقافية أو الدينية لدرجة الأضرار الفورية المتوقعة.

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



Example 1: Collateral Damage

What is HACIENDA?

- Data reconnaissance tool developed by the CITD team in JTRIG
- Port Scans entire countries
 - Uses nmap as port scanning tool
 - Uses GEOFUSION for IP Geolocation
 - Randomly scans every IP identified for that country



UK TOP SECRET STRAP1
TOP SECRET//COMINT//REL FVEY



Example 1: Collateral Damage

How is it used?

- CNE
 - ORB Detection
 - Vulnerability Assessments
- SD
 - Network Analysis
 - Target Discovery



UK TOP SECRET STRAP1
TOP SECRET//COMINT//REL FVEY

Example 1: Collateral Damage



Communications Security
Establishment

Centre de la sécurité
des télécommunications

TOP SECRET//COMINT



LANDMARK

- ❖ CSEC's Operational Relay Box (ORB) covert infrastructure used to provide an additional level of non-attribution; subsequently used for exploits and exfiltration
- ❖ 2-3 times/year, 1 day focused effort to acquire as many new ORBs as possible in as many non 5-Eyes countries as possible



Canada

Why should you care?

If you are ...

- ▶ ... of any importance in the world, or
- ▶ ... a system or network administrator, or
- ▶ ... a security researcher, or
- ▶ ... in this room, or
- ▶ ... mistaken for any of the above,

Why should you care?

If you are ...

- ▶ ... of any importance in the world, or
- ▶ ... a system or network administrator, or
- ▶ ... a security researcher, or
- ▶ ... in this room, or
- ▶ ... mistaken for any of the above,

then you are probably a target.

So what if they listen to my calls?

- ▶ Kompromat — and you do not get to decide what is bad!
- ▶ Self-censorship
- ▶ Loss of business
- ▶ No privacy \Rightarrow No free press \Rightarrow No liberal democracy

So what if they listen to my calls?

- ▶ Kompromat — and you do not get to decide what is bad!
- ▶ Self-censorship
- ▶ Loss of business
- ▶ No privacy \Rightarrow No free press \Rightarrow No liberal democracy
- ▶ Security services also get you drunk, encourage you to drive, arrest you for drunken driving and then ask you for your customer data.

Example 2: Zersetzung



Discredit a target



- Set up a honey-trap
- Change their photos on social networking sites
- Write a blog purporting to be one of their victims
- Email/text their colleagues, neighbours, friends etc

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

Example 2: Zersetzung



Discredit a company



- Leak confidential information to companies / the press via blogs etc
- Post negative information on appropriate forums
- Stop deals / ruin business relationships

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

Example 2: Zersetzung



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

Targets

- ▶ Labor movement
- ▶ Environmental groups
- ▶ Foreign governments
- ▶ Industrial competitors
- ▶ United Nations
- ▶ European Union

Example 3: Trusting Trust

[edit] (S//NF) Strawhorse: Attacking the MacOS and iOS Software Development Kit

(S) Presenter: ██████████, Sandia National Laboratories

(S//NF) Ken Thompson's gcc attack (described in his 1984 Turing award acceptance speech) motivates the StrawMan work: what can be done of benefit to the US Intelligence Community (IC) if one can make an arbitrary modification to a system compiler or Software Development Kit (SDK)? A (whacked) SDK can provide a subtle injection vector onto standalone developer networks, or it can modify any binary compiled by that SDK. In the past, we have watermarked binaries for attribution, used binaries as an exfiltration mechanism, and inserted Trojans into compiled binaries.

(S//NF) In this talk, we discuss our explorations of the Xcode (4.1) SDK. Xcode is used to compile MacOS X applications and kernel extensions as well as iOS applications. We describe how we use (our whacked) Xcode to do the following things: -Entice all MacOS applications to create a remote backdoor on execution -Modify a dynamic dependency of securityd to load our own library - which rewrites securityd so that no prompt appears when exporting a developer's private key -Embed the developer's private key in all iOS applications -Force all iOS applications to send embedded data to a listening post -Convince all (new) kernel extensions to disable ASLR

(S//NF) We also describe how we modified both the MacOS X updater to install an extra kernel extension (a keylogger) and the Xcode installer to include our SDK whacks.

Example 4: Knowing your Enemies



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

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



Discovery

- Discovered in November 2009
- Existing CNE Access
- WARRIORPRIDE as a sensor
 - REPLICANTFARM for anomaly detection
 - XML info from implant
 - Signature-based detection of anomalous activity and known techniques
 - Noticed: Command-line to create password protected RAR
 - Always the same password
- Retrieved files associated with activity
 - Identified unknown malware through reverse engineering
 - Collecting email from specific, targeted accounts
 - "Felt like" a FI-collecting tool
 - Pointed to first discovered LP
 - Provided initial comms analysis to allow signature deployment in passive collection

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

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

Canada

Décentralisé

inria
Informatiques mathématiques

Example 4: Knowing your Enemies



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

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



Victimology: Iran

- Iranian MFA
- Iran University of Science and Technology
- Atomic Energy Organization of Iran
- Data Communications of Iran
- Iranian Research Organization for Science Technology, Imam Hussein University
- Malek-E-Ashtar University

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

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

Canada

Décentralisé

inria
Informatiques mathématiques

Example 4: Knowing your Enemies



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

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



Victimology: Global

- Five Eyes
 - Possible targeting of a French-language Canadian media organization
- Europe
 - Greece
 - Possibly associated with European Financial Association
 - France
 - Norway
 - Spain
- Africa
 - Ivory Coast
 - Algeria

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

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

Canada

Décentralisé

Infria
Informatiques mathématiques

Example 4: Knowing your Enemies



Communications Security
Establishment Canada

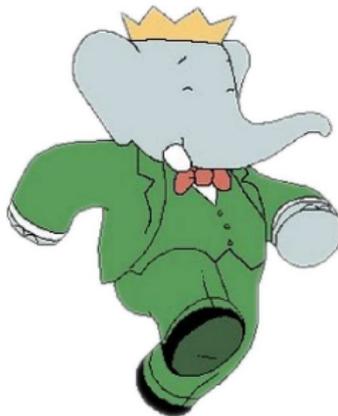
Centre de la sécurité
des télécommunications Canada

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



Attribution: Binary Artifacts

- ntrass.exe
 - DLL Loader uploaded to a victim as part of tasking seen in collection
 - Internal Name: Babar
 - Developer username: titi
- Babar is a popular French children's television show
- Titi is a French diminutive for Thierry, or a colloquial term for a small person



Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

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

Canada

Décentralisé

inria
Informatiques mathématiques

Example 4: Knowing your Enemies



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

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



Attribution: Language

- ko used instead of kB – a quirk of the French technical community
- English used throughout C2 interface, BUT phrasing and word choice are not typical of a native English speaker
 - An attempt at obfuscation?
- Locale option of artifact within spear-phishing attack set to "fr_FR"

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

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

Canada

Décentralisé

inria
Informatiques mathématiques

Example 4: Knowing your Enemies



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

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



Attribution: Intelligence Priorities

- Iranian science and technology
 - Notably, the Atomic Energy Organization of Iran
 - Nuclear research
- European supranational organizations
 - European Financial Association
- Former French colonies
 - Algeria, Ivory Coast
- French-speaking organizations/areas
 - French-language media organization
- Doesn't fit cybercrime profile

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

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

Canada

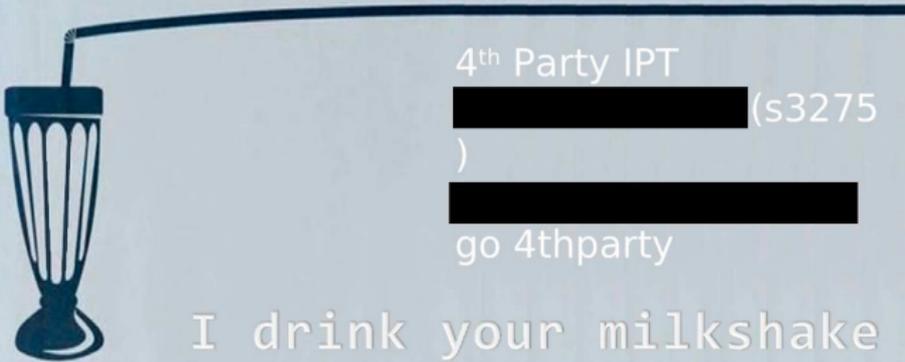
Décentralisé

Infomatiques mathématiques
Inria

Example 5: Pwning your Enemies

TOP SECRET//COMINT//REL TO USA, FVEY

(U) Fourth Party Opportunities



4th Party IPT
[REDACTED] (s3275
)
[REDACTED]
go 4thparty

I drink your milkshake

TOP SECRET//COMINT//REL TO USA, FVEY

Example 5: Pwning your Enemies

(TS//SI//REL) Is there "fifth party" collection? | Round Table

(TS//SI//REL) Yes. There was a project that I was working last year with regard to the South Korean CNE program. While we aren't super interested in SK (things changed a bit when they started targeting us a bit more), we were interested in North Korea and SK puts a lot of resources against them. At that point, our access to NK was next to nothing but we were able to make some inroads to the SK CNE program. We found a few instances where there were NK officials with SK implants on their boxes, so we got on the exfil points, and sucked back the data. That's fourth party. (TS//SI//REL) However, some of the individuals that SK was targeting were also part of the NK CNE program. So I guess that would be the fifth party collect you were talking about. But once that started happening, we ramped up efforts to target NK ourselves (as you don't want to rely on an untrusted actor to do your work for you). But some of the work that was done there was able to help us gain access. (TS//SI//REL) I know of another instance (I will be more vague because I believe there are more compartments involved and parts are probably NF) where there was an actor we were going against. We realized there was another actor that was also going against them and having great success because of a 0 day they wrote. We got the 0 day out of passive and were able to re-purpose it. Big win. (TS//SI//REL) But they were all still referred to as fourth party.

answered 2 days ago

UNCLASSIFIED//FOUO

 (CIV-NSA)

[Add A Comment](#) | [Show 1 Comment \(1 new\)](#)

Example 6: Thank Security Standards

Acknowledgements

The National Institute of Standards and Technology (NIST) gratefully acknowledges and appreciates contributions by Mike Boyle and Mary Baish from NSA for assistance in the development of this Recommendation. NIST also thanks the many contributions by the public and private sectors.

(From NIST standard SP 800-90A on DUAL-EC-DRBG.)

Example 6: Thank Security Standards

TOP SECRET//COMINT//REL TO USA, FVEY

SSL Exploitation

- Not impossible!
- RSA key exchange “easy” to do because of fixed key.
- EDH key exchange not exploitable by the “easy” way. ☹

TOP SECRET//COMINT//REL TO USA, FVEY

Example 6: Thank Security Standards

CONFIDENTIAL//COMINT

Problems in processing

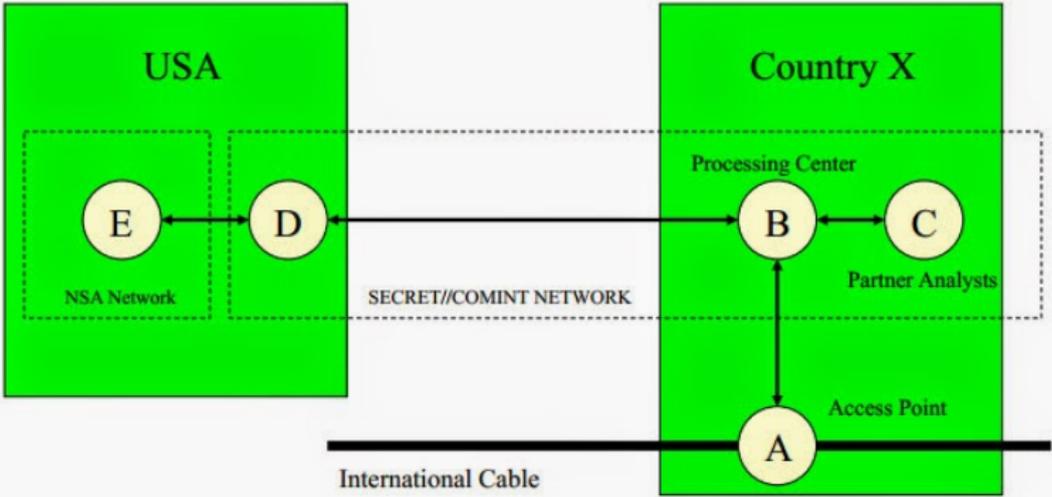
- Literally millions of sessions per day
- Need to have good filtering and selection
- Need both sides of conversation
- USSID 18 issues

CONFIDENTIAL//COMINT

Example 7: Owning the Network



RAMPART-A Typical Operation



TOP SECRET//COMINT//NOFORN

Example 7: Owning the Network



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)

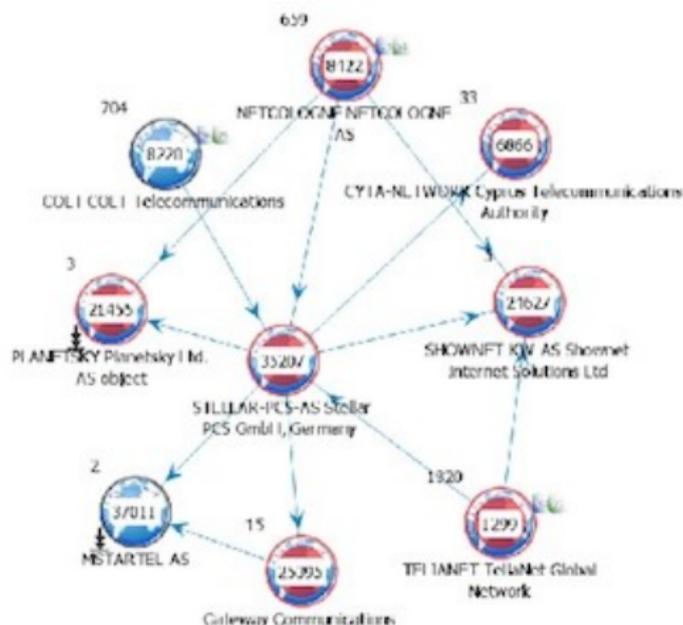
(* limited only by available data)

TS//SI//REL TO USA, FVEY



Example 7: Owning the Network

TOP SECRET STRAP1



Generated via TeasureMap

The Internet is Broken

Administrators have power.

Power attracts Mexican drug cartels.

Adversary model: Mexican drug cartel

- ▶ They took your family, and will brutally kill them if you do not give them what they want.
- ▶ Under these circumstances, you must still not be able to assist, and the public system design must make that clear.
- ▶ Thus, the cartel has nothing to gain from abducting your family and will not bother with it.

System administrators are targets of such an adversary.

Political solutions?

Politicians are ...

- ▶ ... having Kompromat collected against them.
- ▶ ... generally not understanding the technology.
- ▶ ... limited in their influence to one country.
- ▶ ... unlikely to invest time in issues 2% of the population cares about.

Political solutions?

Politicians are ...

- ▶ ... having Kompromat collected against them.
- ▶ ... generally not understanding the technology.
- ▶ ... limited in their influence to one country.
- ▶ ... unlikely to invest time in issues 2% of the population cares about.

Politics could make it worse, but will not fix it!

Conclusion

- ▶ Cyberwar: Battle of the spy-agencies' bots
- ▶ Offensive and defensive goals of agencies conflict
- ▶ Our security services will **not** protect us

“World War III is a guerrilla information war with no division between military and civilian participation.” –Marshall McLuhan

The Internet is Broken

- ▶ Network generally learns too much
- ▶ Insecure defaults and high system complexity (HTTP 2.0)
- ▶ Centralized Internet infrastructure requires administration:
 - ▶ Number resources (IANA)
 - ▶ Domain Name System (Root zone)
 - ▶ X.509 CAs (HTTPS certificates)
- ▶ Administrators have power, and power attracts Mexican drug cartel

The Internet is Broken

- ▶ Network generally learns too much
- ▶ Insecure defaults and high system complexity (HTTP 2.0)
- ▶ Centralized Internet infrastructure requires administration:
 - ▶ Number resources (IANA)
 - ▶ Domain Name System (Root zone)
 - ▶ X.509 CAs (HTTPS certificates)
- ▶ Administrators have power, and power attracts Mexican drug cartel
- ▶ Self-organizing systems aka P2P systems offer a way forward!

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 (being) built using GUNet

- ▶ Anonymous and non-anonymous file-sharing
- ▶ IPv6–IPv4 protocol translator and tunnel
- ▶ GNU Name System: censorship-resistant replacement for DNS
- ▶ Conversation: secure, decentralised VoIP
- ▶ SecuShare, a social networking application
- ▶ Taler: Taxable Anonymous Libre Electronic Reserves
- ▶ ...

GNUnet 0.10.x Release Status¹

- ▶ GNUnet 0.10.x is an alpha release
- ▶ GNUnet 0.10.x works on GNU/Linux, OS X, W32, likely Solaris
- ▶ GNUnet 0.10.x has known bugs (see <https://gnunet.org/bugs/>)
- ▶ GNUnet 0.10.x lacks documentation
- ▶ GNUnet 0.10.x is non-trivial to install
- ▶ GNUnet 0.10.x has a somewhat steep learning curve

We hope to release 0.10.x+1 with fewer bugs, better documentation,

...

¹x = 2 expected any day now.

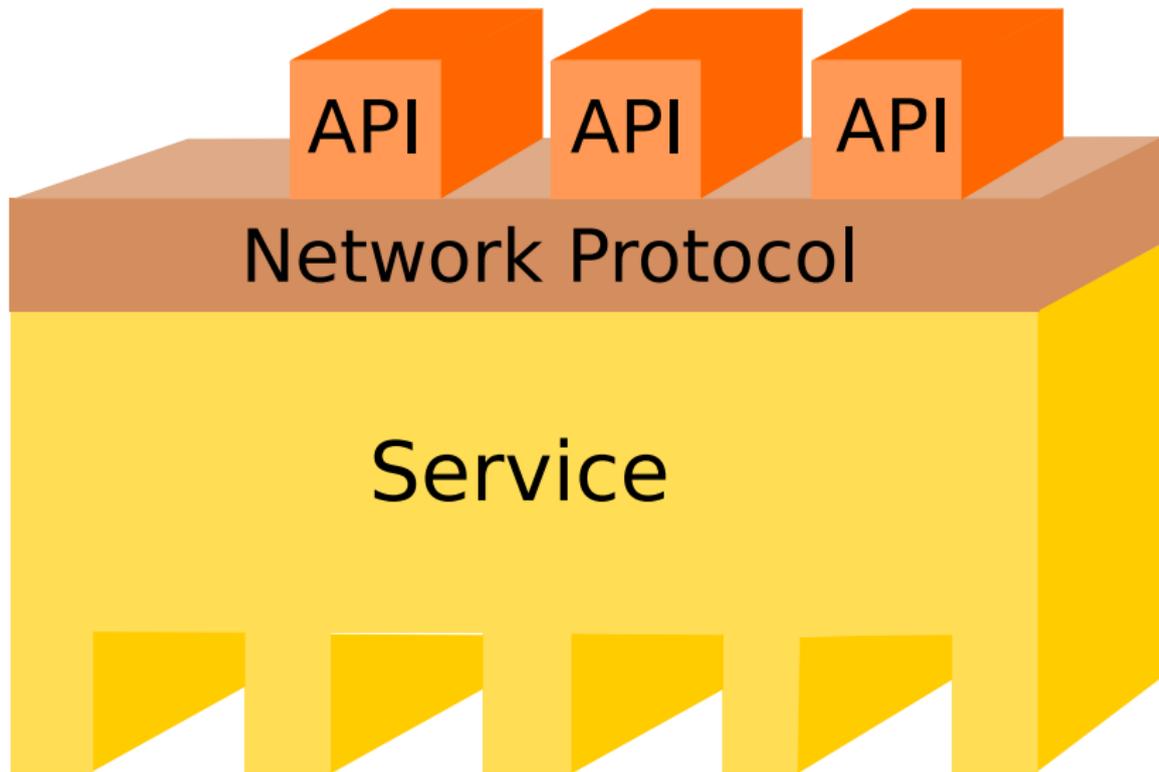
GNUnet Architecture: Goals

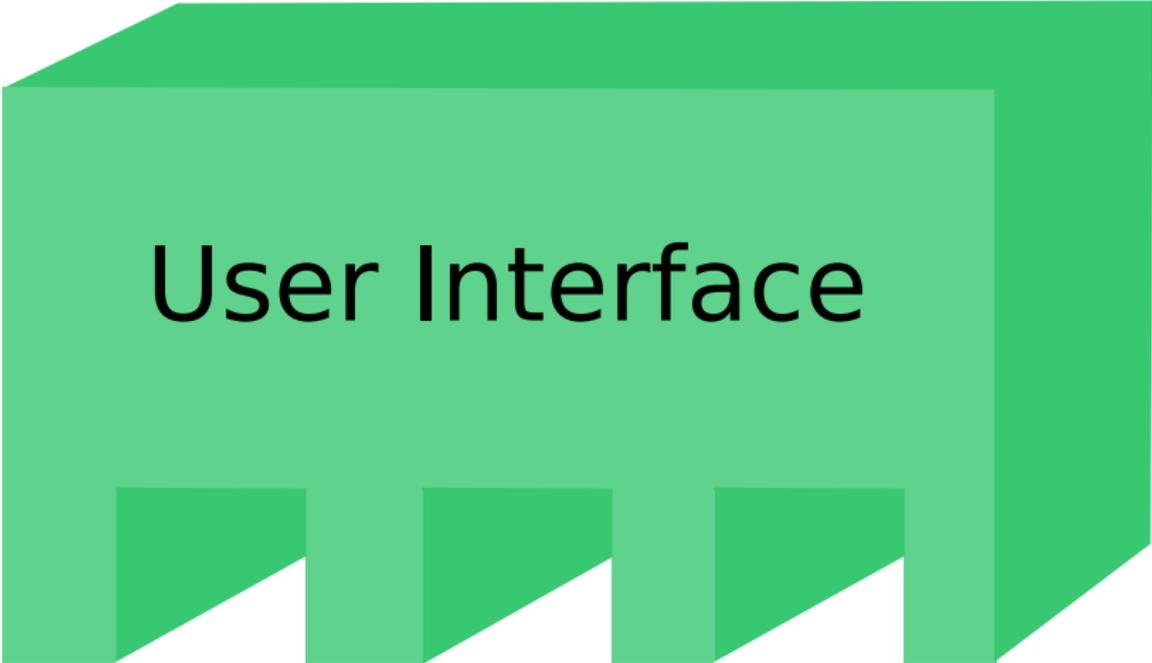
- ▶ Security
- ▶ Extensibility
- ▶ Portability
- ▶ Performance
- ▶ Usability

Architecture against Insanity

Problem	Solution
Deadlocks, races	Use event loop, forbid threads
Memory corruption	Multi-process, static analysis
Uninitialized data	Wrappers around std. C functions
Memory leaks	Multi-process, dynamic analysis
Arithmetic issues	ARM, static analysis

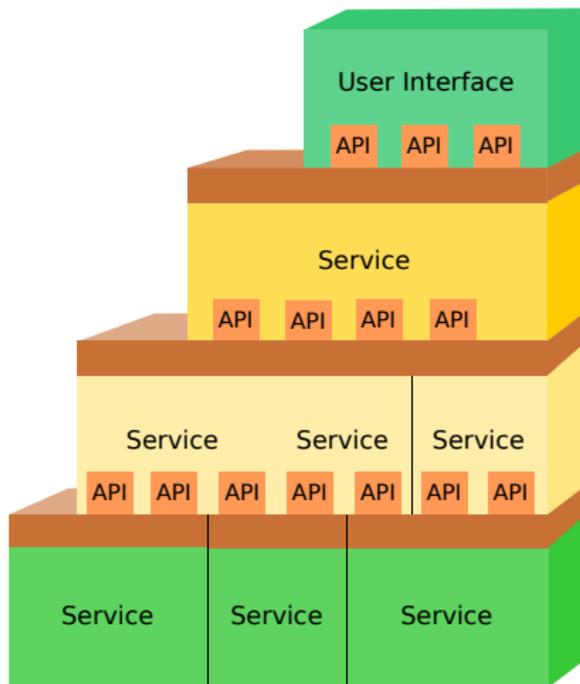
Multi-Process: A Service





User Interface

Multi-Process: A GUnet Peer



A GUNet Service is a Process

- ▶ If all subsystems are used, GUNet would currently use ≈ 40 processes (services and daemons)
 - ▶ user interfaces increase this number further
 - ▶ systemd-like `gnunet-service-arm` starts them
 - ▶ services are manipulated using the respective command-line tool
- ⇒ `gnunet-arm -s` starts GUNet

A peak at the technology

- ▶ GNU Name System: censorship-resistant replacement for DNS
- ▶ GNU Taler: Taxable Anonymous Libre Electronic Reserves

The GNU Name System (GNS)

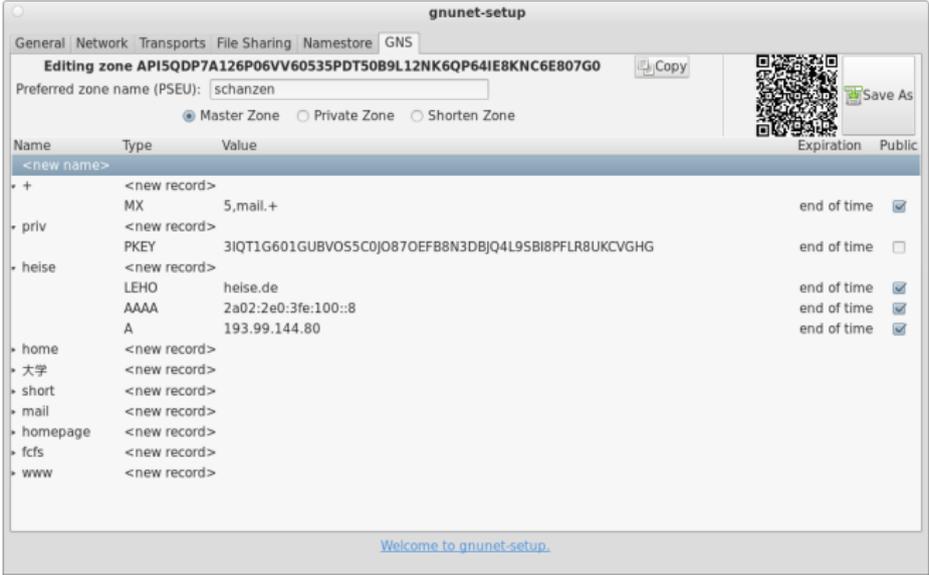
Properties of GNS

- ▶ Decentralized name system with secure memorable names
- ▶ Delegation used to achieve transitivity
- ▶ Also supports globally unique, secure identifiers
- ▶ Achieves query and response privacy
- ▶ Provides alternative public key infrastructure
- ▶ Interoperable with DNS

Uses for GNS in GNUnet

- ▶ Identify IP services hosted in the P2P network
- ▶ Identities in social networking applications

Zone management: like in DNS

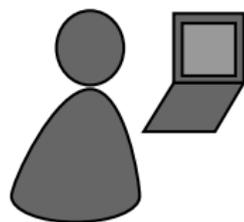


The screenshot shows the 'gnunet-setup' application window. The 'Namestore' tab is active, showing the 'GNS' section. The title bar reads 'Editing zone API5QDP7A126P06VV60535PDT50B9L12NK6QP64IE8KNC6E807G0'. The 'Preferred zone name (PSEU):' field contains 'schanzen'. There are three radio buttons: 'Master Zone' (selected), 'Private Zone', and 'Shorten Zone'. A QR code and a 'Save As' button are visible on the right. Below is a table of records:

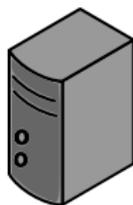
Name	Type	Value	Expiration	Public
<new name>				
+ >	<new record>			
	MX	5,mail.+	end of time	<input checked="" type="checkbox"/>
priv >	<new record>			
	PKEY	3IQ1G601GUBVO55C0J0870EFB8N3DBJQ4L9SBI8PFLR8UKCVGHG	end of time	<input type="checkbox"/>
heise >	<new record>			
	LEHO	heise.de	end of time	<input 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

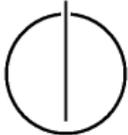
Local Zone: K_{pub}^{Bob}		
www	A	5.6.7.8
		

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

Secure introduction



TUM



Bob Builder, Ph.D.

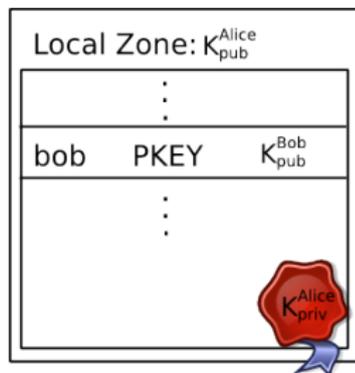
Address: Country, Street Name 23
Phone: 555-12345
Mobile: 666-54321
Mail: bob@H2R84L4JIL3G5C.zkey

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

Delegation

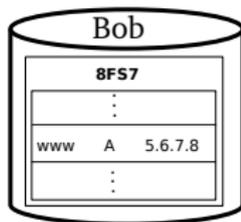
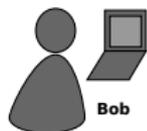


Alice

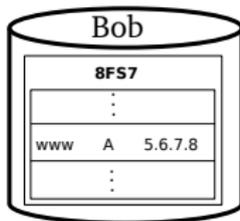


- ▶ Alice learns Bob's public key
- ▶ Alice creates delegation to zone K_{pub}^{Bob} under label **bob**
- ▶ Alice can reach Bob's webserver via **www.bob.gnu**

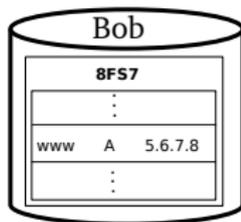
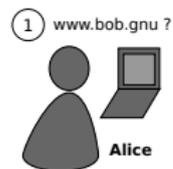
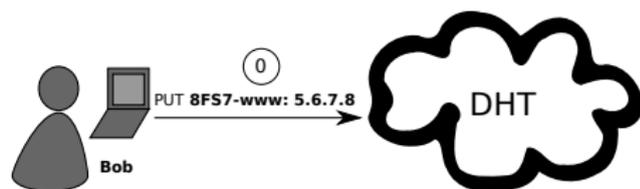
Name resolution



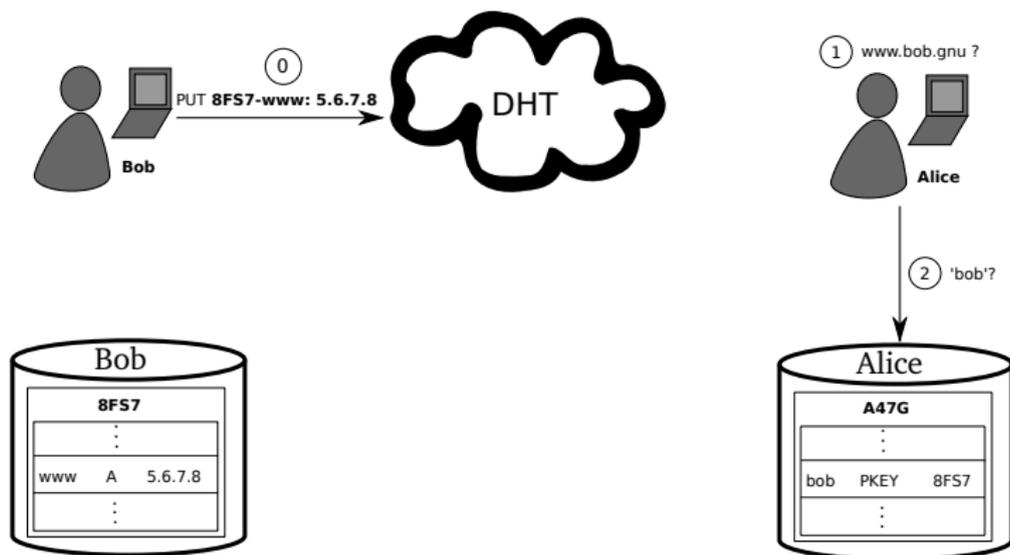
Name resolution



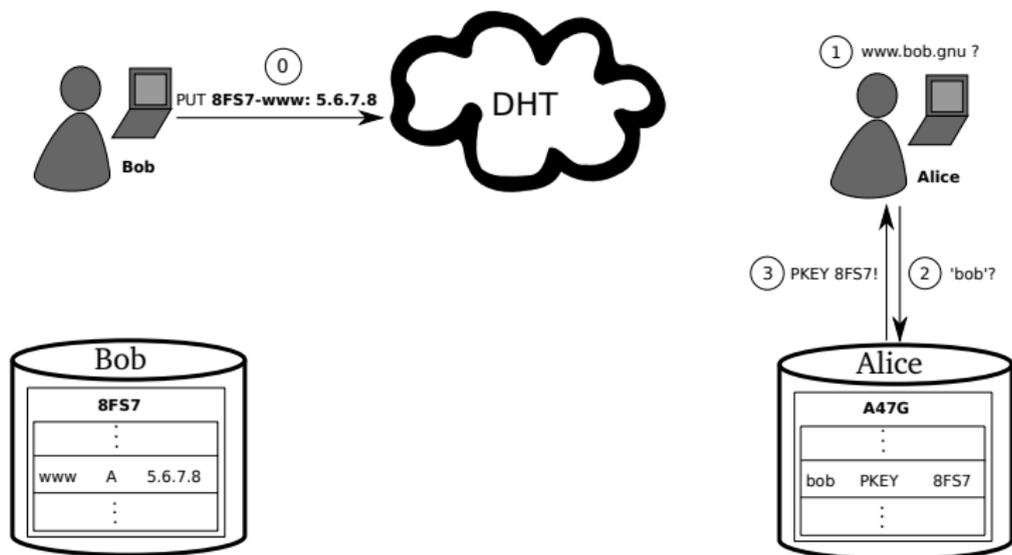
Name resolution



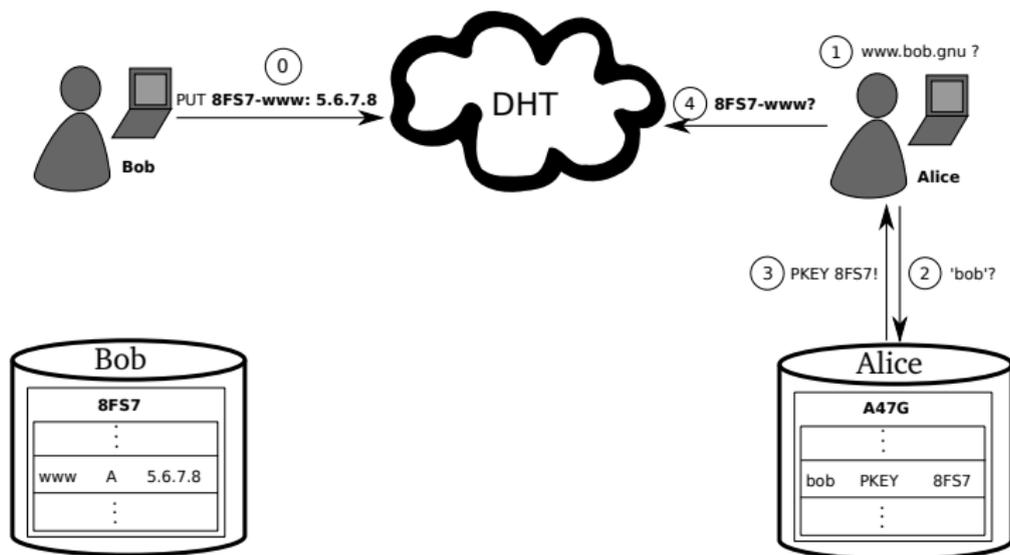
Name resolution



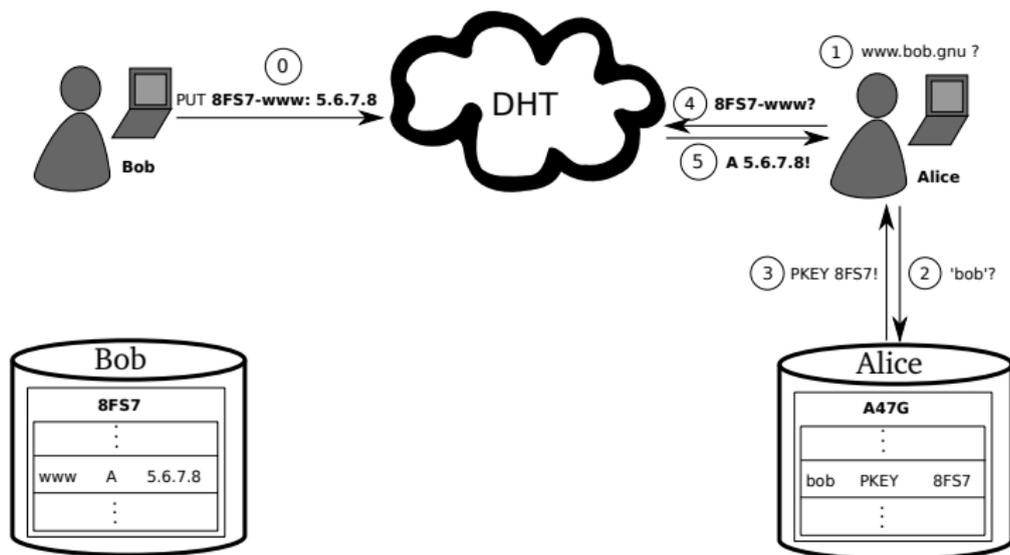
Name resolution



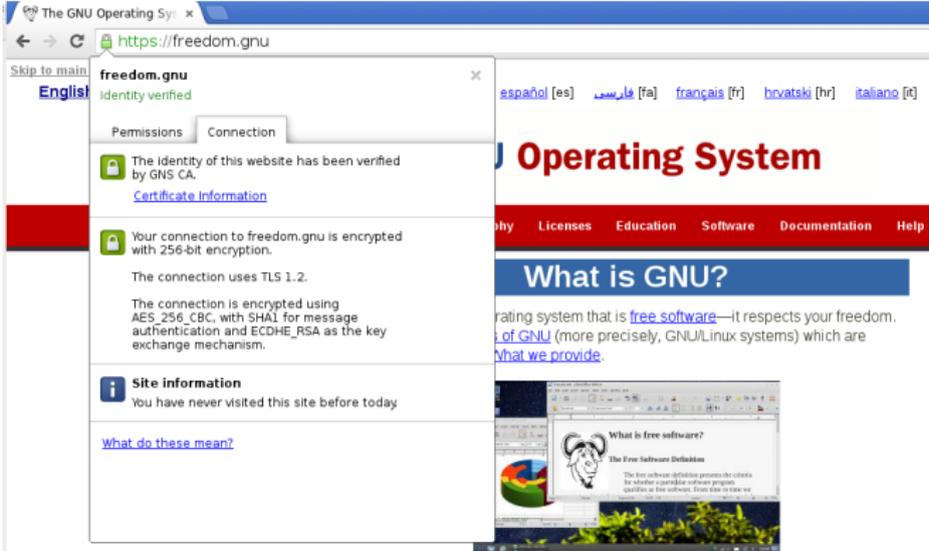
Name resolution



Name resolution



GNS as PKI (via DANE/TLSA)



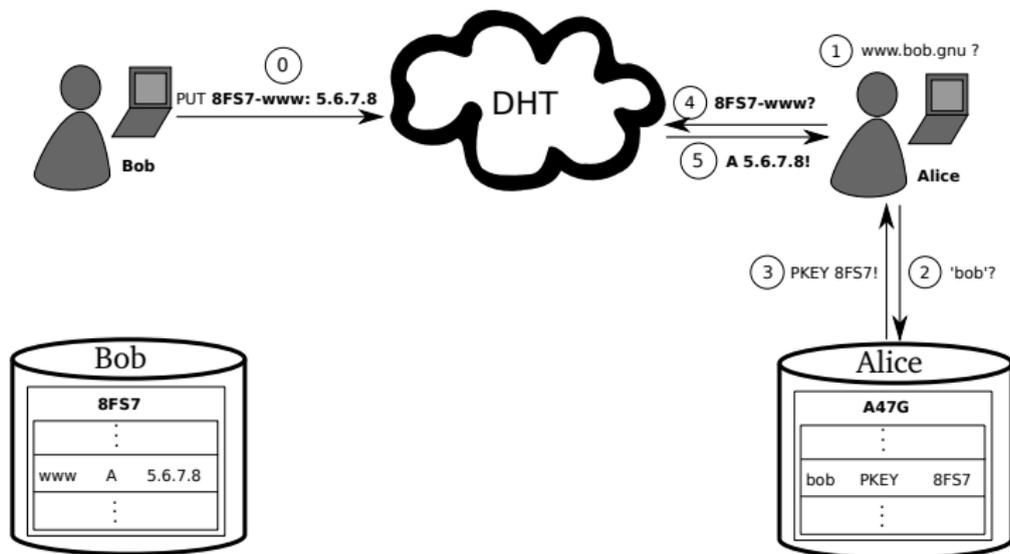
The screenshot shows a web browser window with the address bar displaying `https://freedom.gnu`. A security warning dialog box is overlaid on the page. The dialog box has a title bar that says "freedom.gnu" and "identity verified". It has two tabs: "Permissions" and "Connection". The "Connection" tab is active, showing a green lock icon and the text: "The identity of this website has been verified by GNS CA." Below this, there is a link for "Certificate Information". Another green lock icon is shown with the text: "Your connection to freedom.gnu is encrypted with 256-bit encryption." Below this, it says "The connection uses TLS 1.2." and "The connection is encrypted using AES-256 CBC, with SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism." There is also a "Site information" section with an information icon, stating "You have never visited this site before today" and a link "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 there is a section titled "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 $q_{P,I}$

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

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

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

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

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

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)

Summary

- ▶ Interoperable with DNS
- ▶ Delegation allows using zones of other users
- ▶ Trust paths explicit, trust agility
- ▶ Simplified key exchange compared to Web-of-Trust
- ▶ Privacy-enhanced queries, censorship-resistant
- ▶ Reliable revocation



Modern economies need a currency.

Motivation



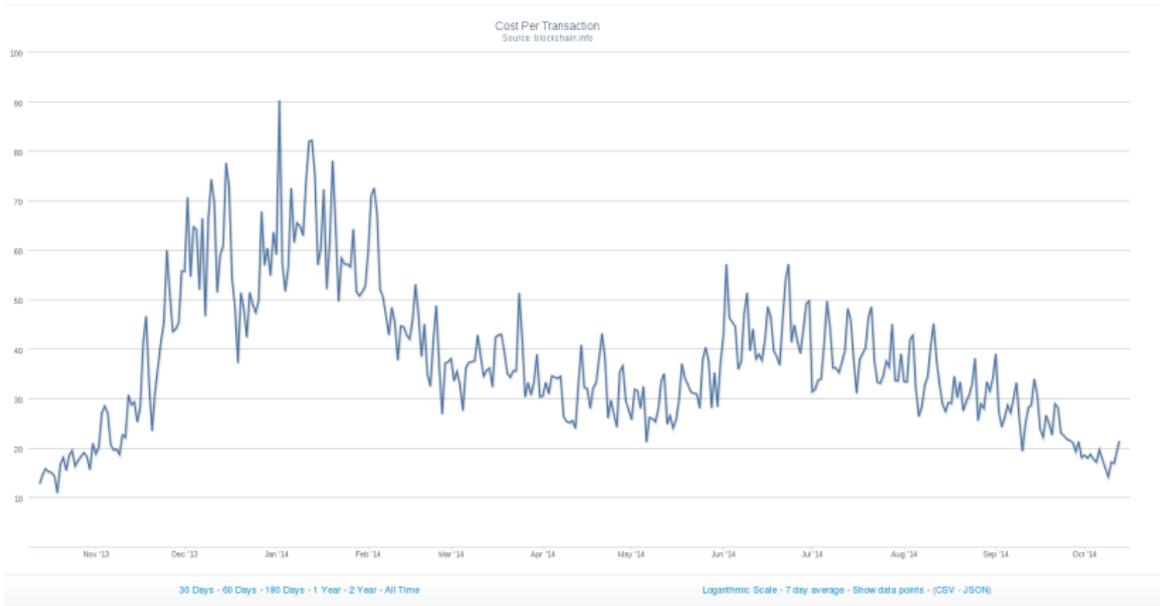
Modern economies need a currency online.

SWIFT?



SWIFT/Mastercard/Visa are too transparent.







- ▶ All BitCoin transactions are public
- ▶ BitCoin does not come with privacy guarantees
 - ⇒ BitCoin was enhanced with “laundering” services
 - ⇒ ZeroCoin and successors offer full anonymity



- ▶ All BitCoin transactions are public
- ▶ BitCoin does not come with privacy guarantees
 - ⇒ BitCoin was enhanced with “laundering” services
 - ⇒ ZeroCoin and successors offer full anonymity

Is society ready for an anarchistic economy?

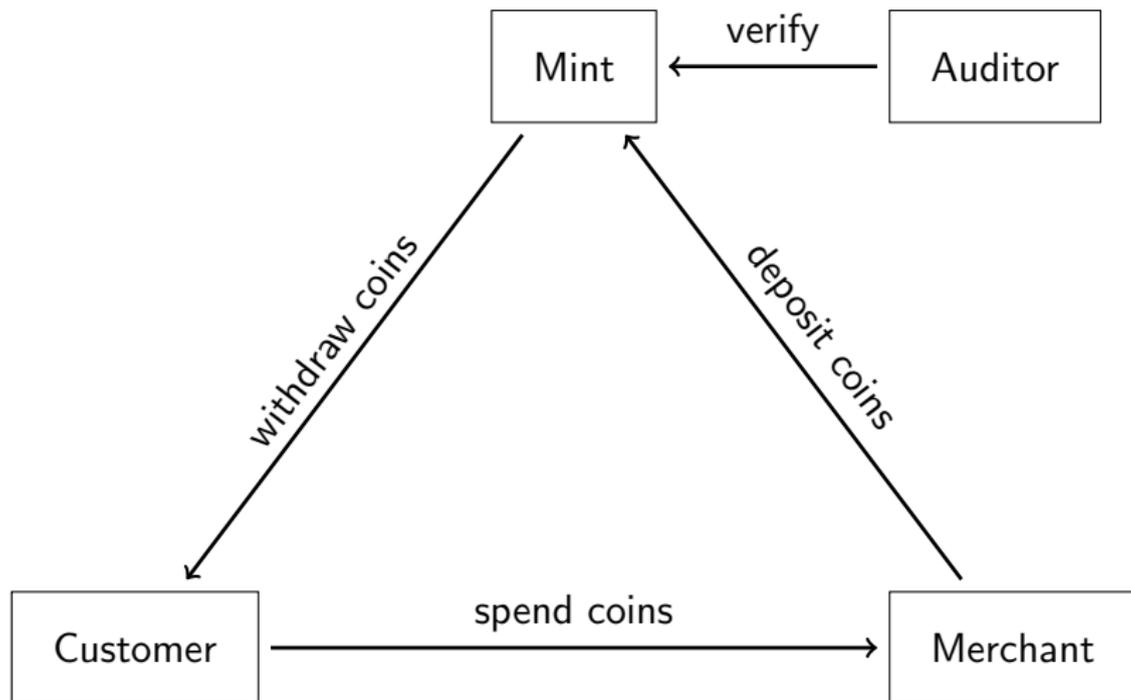
Let's make cash **digital** and **socially responsible**.

Let's make cash **digital** and **socially responsible**.

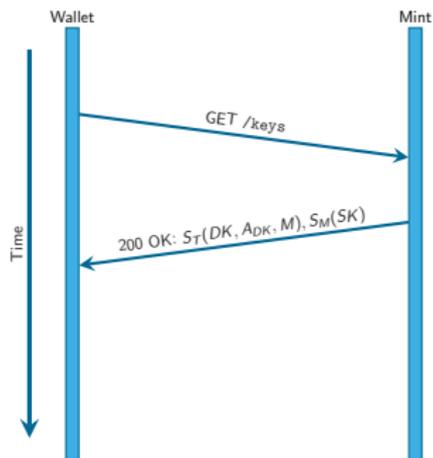


Taxable, Anonymous, Libre, Practical, Resource Friendly

Architecture of GNU Taler

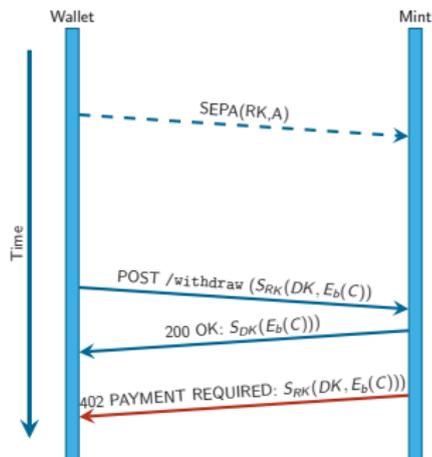


Taler /keys



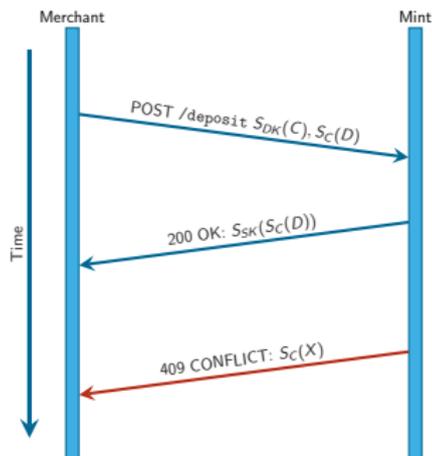
- T Financial regulator key
- DK RSA public key ("denomination key")
- A_{DK} Value of coins signed by DK
- M Offline master key of mint
- SK Online signing key of mint

Taler /withdraw/sign



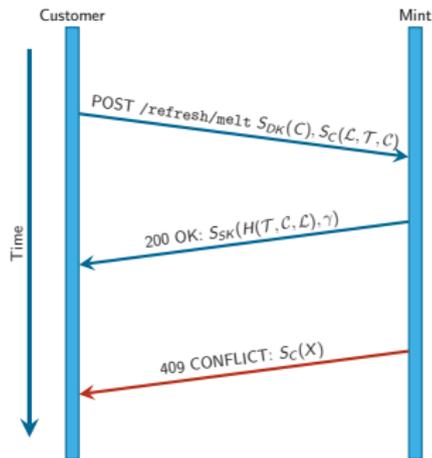
- RK Reserve key
- A Some amount, $A \geq A_{DK}$
- b Blinding factor
- $E_b()$ RSA blinding
- C Coin key
- $S_{DK}()$ (Blind) signature

Taler /deposit



- DK Denomination key
- $S_{DK}()$ RSA signature using DK
- C Coin key
- $S_C()$ EdDSA signature using C
- D Deposit details
- SK Signing key
- $S_{SK}()$ EdDSA signature using SK
- X Conflicting deposit details

Taler /refresh/melt



κ System-wide security parameter

$K := ECDHE(T, C)$

$E_K()$ Symmetric encryption using key K

$DK^{(i)}$ List of denomination keys

$C^{(i)}$ List of coin keys

$b^{(i)}$ List of blinding factors

$E_{b^{(i)}}()$ Blinding with respective $b^{(i)}$

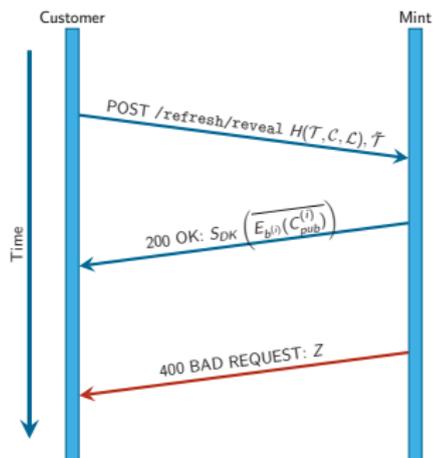
\mathcal{T} $[T_{pub}]_{\kappa}$

\mathcal{L} $[E_K(b^{(i)}, C_{priv}^{(i)})]_{\kappa}$

\mathcal{C} $[E_{b^{(i)}}(C_{pub}^{(i)}, DK^{(i)})]_{\kappa}$

γ Random value in $[0, \kappa)$

Taler /refresh/reveal

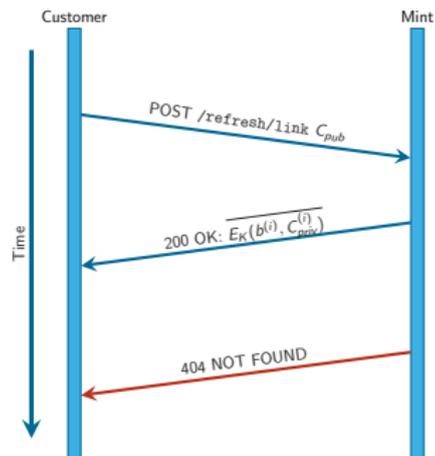


\tilde{T} $[T_{priv}]_{\kappa \setminus \gamma}$

$\overline{E_{b(i)}(C^{(i)})}$ Blinded coins from C at γ

Z Cut-and-choose mismatch information

Taler /refresh/link



$\overline{E_K(b^{(i)}, C_{priv}^{(i)})}$ Linkage data \mathcal{L} at γ

Summary

- ▶ GUNet: A future Internet for liberal societies
- ▶ GNU Taler: A payment system focused on ethics

How can you help?

- ▶ Anonymity: protect yourself (use Tor, Pond, etc.)
- ▶ Baseline: encrypt your harddrive, encrypt your e-mail
- ▶ Coding: bugfixes, GUI design (it's just XML!), new ideas
- ▶ Documentation: improvements, translations

How can you help?

- ▶ Anonymity: protect yourself (use Tor, Pond, etc.)
- ▶ Baseline: encrypt your harddrive, encrypt your e-mail
- ▶ Coding: bugfixes, GUI design (it's just XML!), new ideas
- ▶ Documentation: improvements, translations
- ▶ Égalité: run a peer, not a server
- ▶ Fraternité: share resources and knowledge
- ▶ Liberté: write free software

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.

Conclusion

- ▶ This is **not** about the NSA
- ▶ Chinese, French, German, Russian agencies do the same

Conclusion

- ▶ This is **not** about the NSA
- ▶ Chinese, French, German, Russian agencies do the same
- ▶ It is about governments against their citizens
- ▶ It is about rich against poor

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.
- ▶ M. Schanzenbach *Design and Implementation of a Censorship Resistant and Fully Decentralized Name System*. **Master's Thesis (TUM)**, 2012.
- ▶ Christian Grothoff, Bart Polot and Carlo von Loesch. *The Internet is broken: Idealistic Ideas for Building a GNU Network*. **W3C/IAB Workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)**, 2014.
- ▶ 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.

“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)