

[GNUnet.org](http://GNUnet.org)



Speaker  
IRC:sva  
sva@ccc.de  
twitter@sva



Let's make a GNU one!

pep  
Privacy by Default.

# GNUnet

**1970/80: Internet v1.0.**

Wow, I can access your computer, you can check out mine!  
Awesome!

**2010/20: Internet v1.1.**

Sure I can access other computers and use their services.  
Wait, What? They can also access mine!?

**2025/30: Internet v2.0.**

End-to-end encryption and anonymization of the ways data flows.



# Whats the problem of v1.1.?

Network knows & learns too much  
Insecure defaults & high complexities

Centralized components  
(e.g. IANA, ICANN, DNS, ...)

Administrators can be a target!

Misuse of those flaws happens all over!

# Idea

“GUnet is a **mesh routing layer** for end-to-end encrypted networking and a framework for distributed applications **designed to replace the old insecure Internet protocol stack.**”

GUnet.org

(founded 2002,  
followed in academia)



# Layers

(very hard) simplified version of the Internet:

---

Google, FB & Co

---

DNS/X.509

---

TCP/UDP

---

IP/BGP

---

Ethernet

---

Physical Layer

---



# Layers

## Internet:

---

Google, FB & Co

---

DNS/X.509

---

TCP/UDP

---

IP/BGP

---

Ethernet

---

Physical Layer

---

## GNUnet:

---

...

---

...

---

...

---

...

---

...

---

...

---



# Layers

## Internet:

Google, FB & Co

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Physical Layer

## GNUnet:

...

...

...

...

...

HTTPS/TCP/WLAN/...



# Layers

Start with what we have:

e.g. TCP, UDP, SMTP, HTTP, HTTPS,  
WLAN, Bluetooth, ....

Unreliable, out-of-order packet  
delivery semantics.

Automated Transport Selection  
(ATS) decides.

GNUnet:

---

...

---

...

---

...

---

...

---

...

---

HTTPS/TCP/WLAN/...

---





# Layers

## Internet:

Google, FB & Co

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Physical Layer

## GNUnet:

...

...

...

...

CORE (OTR)

HTTPS/TCP/WLAN/...



# Layers

Off-The-Record encryption  
between peers.

Multiplexes inbound messages by  
type to higher-level subsystems.

Hides connections from/to peers  
that do not speak same higher-  
level protocol.

GNUnet:

...

...

...

...

CORE (OTR)

HTTPS/TCP/WLAN/...



# Layers

## Internet:

Google, FB & Co

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Physical Layer

## GNUnet:

...

...

...

R<sup>5</sup>N DHT

CORE (OTR)

HTTPS/TCP/WLAN/...



# Layers

Decentralized routing algorithm

using distributed hash tables

(randomized version of Kademlia,  
still effective in small networks)

GNUnet:

...

...

...

R<sup>5</sup>N DHT

CORE (OTR)

HTTPS/TCP/WLAN/...



# Layers

## Internet:

Google, FB & Co

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Physical Layer

## GNUnet:

...

...

CADET

R<sup>5</sup>N DHT

CORE (OTR)

HTTPS/TCP/WLAN/...



# Layers

Transport Protocol.  
Has Features of SCTP and Axolotl;  
serves end-to-end-encryption.

Additional services, eg:

Xolotl (sphinx+Axolotl)  
protecting meta data,

Lake (like pond) providing  
mailboxes /asynchronous delivery.

GNUnet:

...

...

CADET

R<sup>5</sup>N DHT

CORE (OTR)

HTTPS/TCP/WLAN/...



# Layers

## Internet:

Google, FB & Co

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Physical Layer

## GNUnet:

...

GNS

CADET

R<sup>5</sup>N DHT

CORE (OTR)

HTTPS/TCP/WLAN/...



# Layers

Secure and decentralized name system, no central root zones or auth.

Provides alternative public key infrastructure.

Interoperable with DNS.

Query and response privacy.

GNUnet:

...

GNS

CADET

R<sup>5</sup>N DHT

CORE (OTR)

HTTPS/TCP/WLAN/...





# Layers

## Internet:

Google, FB & Co

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Physical Layer

## GNUnet:

Applications

GNS

CADET

R<sup>5</sup>N DHT

CORE (OTR)

HTTPS/TCP/WLAN/...



# Layers

File sharing

SecuShare (social networking)

Conversation (VoIP)

p≡p (messaging)

GNU Taler (payments)

MUDs (game)

Your app?

GNUnet:

---

Applications

---

GNS

---

CADET

---

R<sup>5</sup>N DHT

---

CORE (OTR)

---

HTTPS/TCP/WLAN/...

---



# GNUnet wants to...

...protect the privacy of its users and to guard itself against attacks or abuse.

...become a widely used, reliable, open, non-discriminating, egalitarian, unfettered and censorship-resistant system of free information exchange.

...serve as a development platform for the next generation of decentralized Internet protocols."



# Try GNUnet!

`wget https://gnunet.org/gnunet0-11-0pre66`

**(or) clone `gnunet.org/git`**

Follow instructions on the website

Get support via **#GNUnet on freenode**  
and/or via ML e.g. **help-gnunet@gnu.org**

! Report bugs on **gnunet.org/bugs** !

Written in C, but a GNUnet-Java exist, too:  
Start for an API for extensions in Java :)



# Law of Mathematics

## The laws of Australia will trump the laws of mathematics: Turnbull

Despite calling the laws of mathematics 'commendable', the prime minister of Australia told ZDNet the only law that applies in Australia is the law of Australia when it comes to legislating decryption.



By [Chris Duckett](#) and [Asha McLean](#) | July 14, 2017 -- 01:27 GMT (02:27 BST) | Topic: [Security](#)

"The laws of Australia prevail in Australia, I can assure you of that," he said on Friday. "The laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia." **???**

# Law of Gov's wont rescue us...