

Let's make a GNU one!

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





GNUnet

1970/80: Internet v1.0.

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

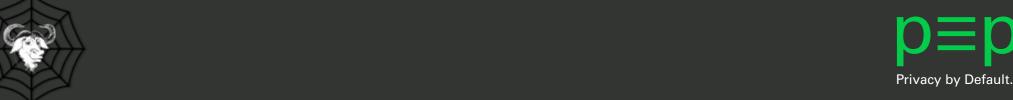
Awesome!

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

"GNUnet 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.**"

GNUnet.org

(founded 2002, followed in academia)





(very hard) simplified version of the Internet:

Google, FB & Co

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Physical Layer





<u>Internet:</u>

Google, FB & Co

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Physical Layer

<u>GNUnet:</u>

...

• • • •

...

...

...





<u>Internet:</u>

Google, FB & Co

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Physical Layer

<u>GNUnet:</u>

...

...

...

...

...





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.

<u>GNUnet:</u>

•••

...

...

...

...





<u>Internet:</u>

Google, FB & Co

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Physical Layer

<u>GNUnet:</u>

...

...

...

...

CORE (OTR)





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.

<u>GNUnet:</u>

• • • •

. . . .

. . . .

. . .

CORE (OTR)





<u>Internet:</u>

Google, FB & Co

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Physical Layer

<u>GNUnet:</u>

...

. . .

. . .

R⁵N DHT

CORE (OTR)





Decentralized routing algorithm using distributed hash tables (randomized version of Kademlia,

still effective in small networks)

GNUnet:

. . .

. . .

. . . .

R⁵N DHT

CORE (OTR)





<u>Internet:</u>

Google, FB & Co

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Physical Layer

<u>GNUnet:</u>

...

. . .

CADET

R⁵N DHT

CORE (OTR)





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.

<u>GNUnet:</u>

• • •

. . . .

CADET

R⁵N DHT

CORE (OTR)





<u>Internet:</u>

Google, FB & Co

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Physical Layer

<u>GNUnet:</u>

...

GNS

CADET

R⁵N DHT

CORE (OTR)





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

R⁵N DHT

CORE (OTR)





<u>Internet:</u>

Google, FB & Co

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Physical Layer

<u>GNUnet:</u>

Applications

GNS

CADET

R⁵N DHT

CORE (OTR)





File sharing

SecuShare (social networking)

Conversation (VoIP)

p≡p (messaging)

GNU Taler (payments)

MUDs (game)

Your app?

GNUnet:

Applications

GNS

CADET

R⁵N DHT

CORE (OTR)





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!

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...