Meta**Tor**

building a **meta web** to prevent censorship and data retention

written by **R**ahra & **C**reo

https://www.reverse.tk/whocanutrust

Why do we need to be protected**?**

Censorship

Data Retention

Electronic Eavesdropping

Why do we need to be protected?

Censorship
2006

Myanmar
technology by Fortinet
opposition party blocking
full data retention

China
The Golden Shield Project
started in 11/2003

Why do we need to be protected?

Censorship
2006

imprisonment for the freedom of opinion
(2006)

China: 62
Iran: 132
Syrien: 4

Why do we need to be protected?

Data Retention
2006/07/08

European Union
EU Directive 2006/24/EG

hold-back time between 6 and 24 months

launch in germany 01.01.2008

What can Tor do for us**?**

Tor - “The Onion Router”

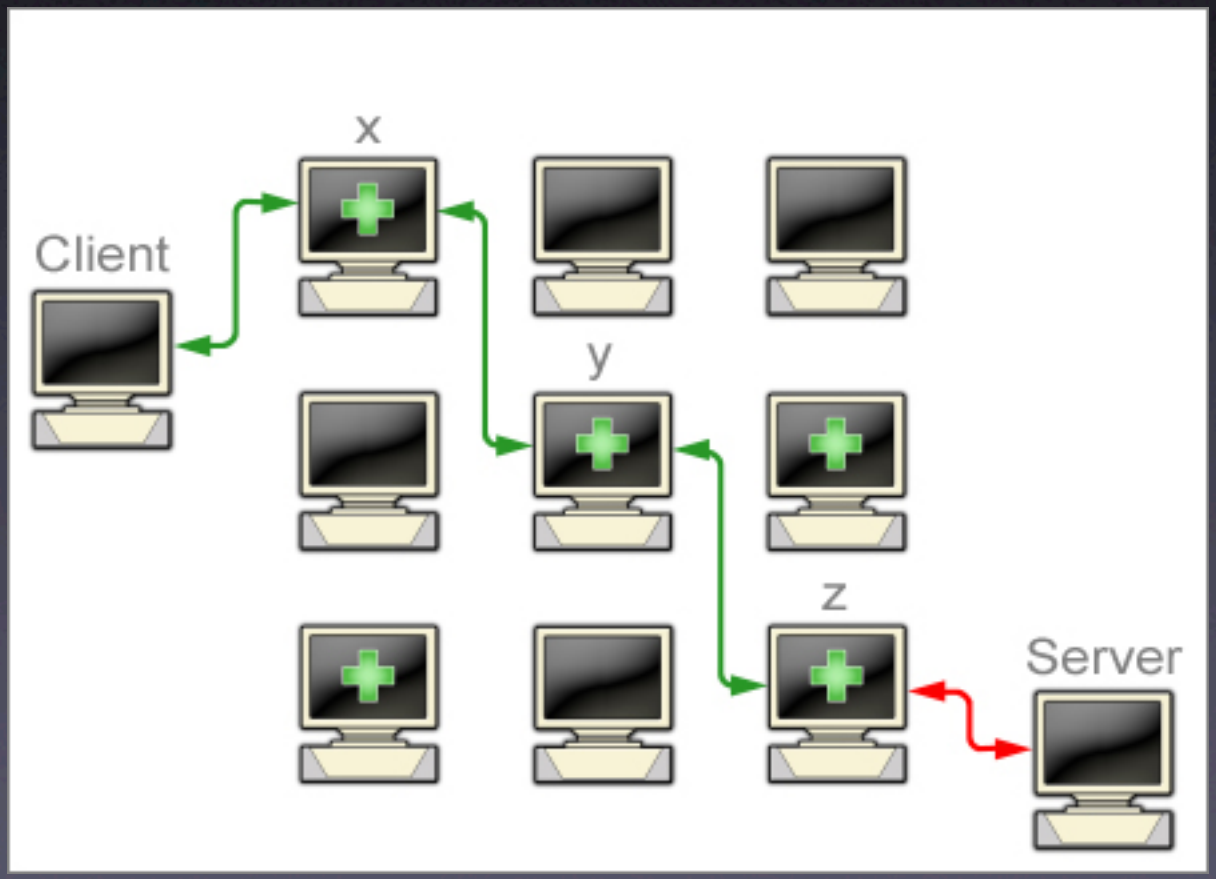
Data is **encrypted** and relayed over other Tor nodes

The Server never knows **who** requested the content

Tor undercuts firewalls and data analysis technologies

What can Tor do for us?

Tor - “The Onion Router”



Where is the **catch**?

Exit Nodes

fully responsible for all data being sent and requested

vital for throughput and anonymity

very rare, compared with the number of users participating due to legal reasons

unencrypted information leaves the network

Where is the **catch**?

Exit Nodes

news 08.09.2006 12:27

Anonymisierungsserver bei Razzia beschlagnahmt

Networld / 08.09.2006 / 15:36 Trackback Versenden Druck

Staatsanwaltschaft beschlagnahmt Anonymisierungsserver

Durch deutsche Tor-Server sollen Kinderpornos geschleust worden sein

the solution: Meta**Tor**

HIDDEN SERVICES

designed to keep information inside the tor cascade

.onion keys are used instead of ip adresses

neither client **nor** server know each other
due the whole communication process,
so the publisher and the consumer reap
the benefits of **full anonymity**

another catch: usability and feasibility

.onion keys:

are hard to remember
(ever tried to remember nnqtnsoohprzqcke.onion?)

are not suitable for virtual host technologies
as used by apache (no multihosting is possible)

may change - change your ISP and your .onion
key will change

Meta**Tor** and TNS (**Tor** Name Service)

72.5.124.61

www.sun.com

nnqtnsoohprzqcke.onion

sun.meta

Meta**Tor** and TNS (**Tor** Name Service)

Phase I

Implement new TLDs

.meta
.privacy
...

PRO

low-cost (~ 5 USD p.a.)
needed to maintain TNS
rest goes into **Tor** Funds

CONTRA

risk of lost anonymity
through payments

Increase application usability

MetaTor and TNS (Tor Name Service)

Phase 2

Increase application usability

FireTor

ThunderTor

Increase application usability

built-in Tor client and TNS resolver

same usage as the original applications

built-in bypass security to keep data inside Tor

Thank **You**

Send us your thoughts and ideas to

creo@reverse.tk **rahra**@reverse.tk

or join us at

https://www.reverse.tk/whocanutrust