We Fix the Net!

Christian Grothoff

Team DÉCENTRALISÉ
Inria Rennes - Bretagne Atlantique

2.10.2014

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

<Journalism> "Knocking down the HACIENDA"

The following slides are from an article[1] I published with

Julian Kirsch (TUM),
Jacob Appelbaum,
Monika Ermert (Heise),
Laura Poitras
and
Henrik Moltke.

[1] "NSA/GCHQ: The HACIENDA-Programm for Internet Colonization", Heise online, 15.8.2014

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

Countries

- Completed full scans of 27 countries including
  - [redacted]
- Completed partial scans of 5 additional countries

Tasking & Access

- To task HACIENDA with a Country or Subnet
  - [redacted]@gchq.gov.uk)
  - CITD alias ([redacted]@gchq.gov.uk)
- Access to the Data
  - At GCHQ, request a GLOBAL SURGE account from [redacted]@gchq.gov.uk)
  - At CSEC, contact
  - At NSA, contact
  - At DSD, contact

NAC NETWORK ANALYSIS CENTRE

[redacted]

Ports

- Pulls back hostname, banners, application names and port status
- Gathers additional information for…
  - 21 (ftp): directory listing
  - 80 (http): content of main page
  - 443 (https): content of main page
  - 111 (rpc): results of rpcinfo

How is it used?

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

Step 3

Hacking in SIGINT

The Hacking Process

1. (**R**)econnaissance
2. (**I**)nfection
3. (**C**)ommand And Control
4. (**E**)xfiltration

Reconnaissance

Publicly Available Information

(Email Address, Location, Network Info, Passwords, etc.)

Research

Hacker

Victim

Enumerate (Network)

Scan (Services)

Operating Systems

Versions

Domain Names

Reconnaissance Infection Command and Control Exfiltration

Reconnaissance

This system is audited for USSID 18 and Human Rights Act compliance
CLASSIFICATION: TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

X-KEYSCORE C2C Session Viewer

Session 1 of 4

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocol
2012-05-16 13:03:20	2CBAB00000M0210	[redacted]		01701	01701	icmp

Session | Header (3) | Meta (7) | GENESIS Contexts (1)

Formatter: WIRESHARK | Send to: Download Session | Mode: Snippet | Options | Search Content: Enter text to search

Quick Clicks

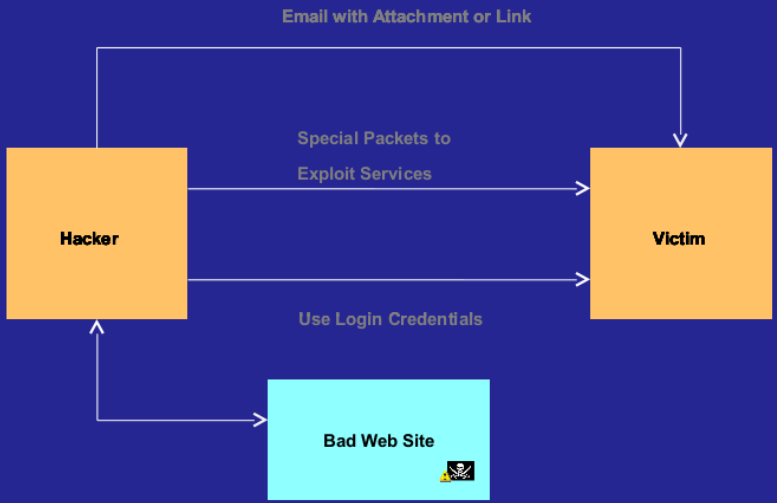
- Session
- One-Click Searches
  - Find fingerprint
    - selector/cadence/task_
    - udp/tunnel/ipv4
    - netmanagement/icmp/s
  - Find traffic on
  - Find application
    - netmanagement/icmp

```
Internet Protocol, Src: 8.8.8.8 (8.8.8.8), Dst: 192.168.0.83 (192.168.0.83)
    Version: 4
    Header Length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 60
    Identification: 0x2d3c (11580)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 51
    Protocol: ICMP (0x01)
    Header checksum: 0x897a [correct]
        [Good: True]
        [Bad : False]
    Source: 8.8.8.8 (8.8.8.8)
    Destination: 192.168.0.83 (192.168.0.83)
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0 ()
    Checksum: 0x52ec [correct]
    Identifier: 0x0001
    Sequence number: 623 (0x026f)
    Data (32 bytes)

0000  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70   abcdefghijklmnop
0010  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi
```

Reconnaissance Infection Command and Control Exfiltration

Infection



Reconnaissance Infection Command and Control Exfiltration

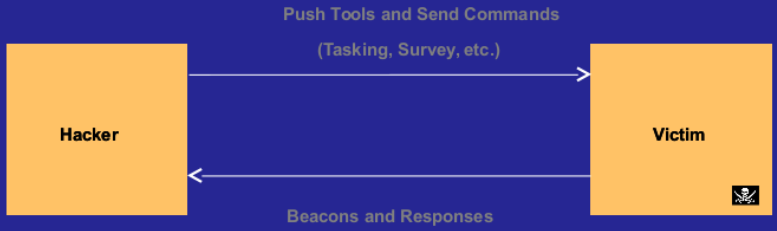
Password Guessing

```
USER Administrator
PASS #mafiavafute197532@%!?*
USER Administrator
PASS sh3l5l1k3p4rty3v3r
USER Administrator
PASS Sh3I5Lik3P4rtY@v3r
USER Administrator
PASS Sh5I8LiK6P8rtY6v5r
USER Administrator
PASS kalimero4cappy
USER Administrator
PASS P@ssword
USER Administrator
PASS P@sswOrd
USER Administrator
PASS P@sswOrd
```

Iraqi Ministry of Finance

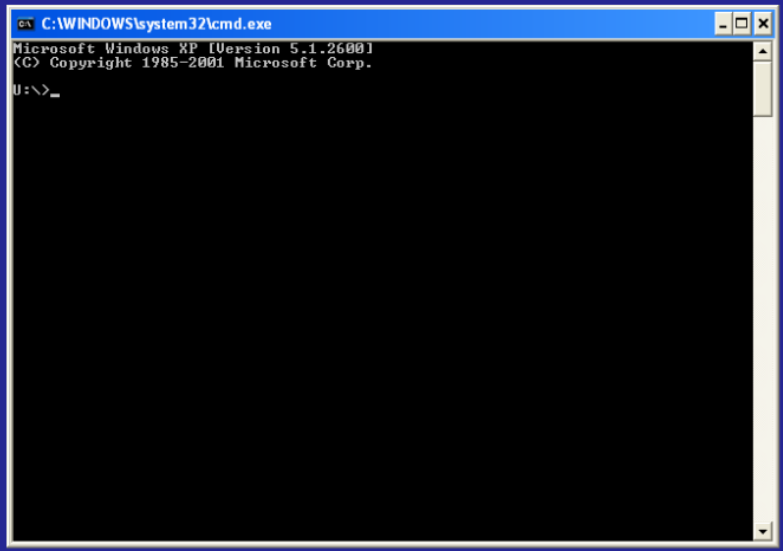
Reconnaissance Infection Command and Control Exfiltration

Command and Control



Reconnaissance Infection **Command and Control** Exfiltration

Windows cmd.exe



Reconnaissance Infection **Command and Control** Exfiltration

Exfiltration

Exfil using known and custom protocols

(Known: HTTP, SMTP, ICMP, FTP, etc)

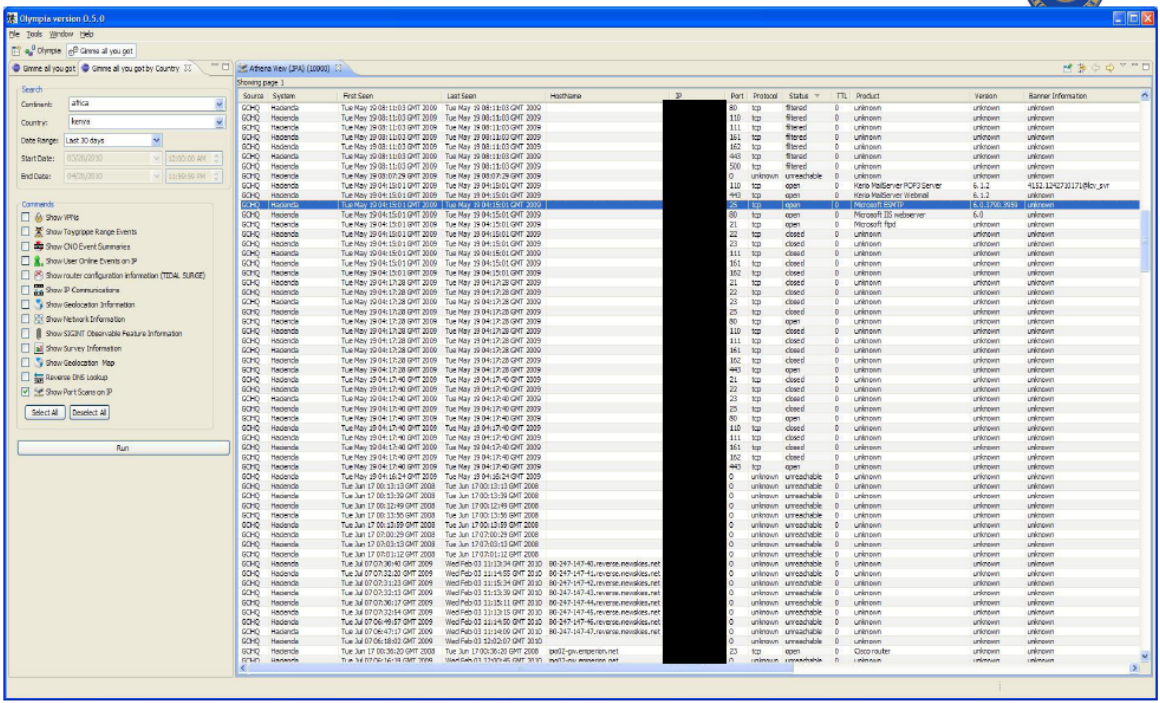
Reconnaissance Infection Command and Control Exfiltration

How is it used?

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

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



BUT, network analysis still manual!

[redacted]

- [redacted] GSM provider
- NSA TAO requested assistance gaining access to the network
- Network analysis using OLYMPIA:
  - DNS query to determine IP address
  - IP address to network range
  - Network range to port scan
  - Are there any vulnerable devices in that range?
- Duration: < 5 minutes

MUGSHOT GOALS

- Automated Target Characterisation and Monitoring
  - Automatically understand everything **important** about **CNE target networks** from passive and active sources.
- Automated Un-Targeted Characterisation
  - Automatically understand everything **important** about **all machines** on the Internet from passive and active sources.

[redacted]

<Research>[2]

Idea: protect administrative TCP services via port knocking

[2] Joint work with Julian Kirsch (Master's thesis, 8'2014)

<Research>[2]

Idea: protect administrative TCP services via port knocking

- Use stealthy knock $\Rightarrow$ SilentKnock

[2] Joint work with Julian Kirsch (Master's thesis, 8'2014)

<Research>[2]

Idea: protect administrative TCP services via port knocking

- Use stealthy knock ⇒ SilentKnock
- Need to protect against MitM attacks ⇒ integrity protection

[2] Joint work with Julian Kirsch (Master's thesis, 8'2014)

<Research>[2]

Idea: protect administrative TCP services via port knocking

- Use stealthy knock ⇒ SilentKnock
- Need to protect against MitM attacks ⇒ integrity protection
- Need to work with NAT ⇒ avoid source IP/port, use TSval for entropy

[2] Joint work with Julian Kirsch (Master's thesis, 8'2014)

<Research>[2]

Idea: protect administrative TCP services via port knocking

- Use stealthy knock ⇒ SilentKnock
- Need to protect against MitM attacks ⇒ integrity protection
- Need to work with NAT ⇒ avoid source IP/port, use TSval for entropy
- Need easy deployment ⇒ in kernel, `setsockopt()` via LD_PRELOAD

[2] Joint work with Julian Kirsch (Master's thesis, 8'2014)

<Research>[2]

Idea: protect administrative TCP services via port knocking

- Use stealthy knock ⇒ SilentKnock
- Need to protect against MitM attacks ⇒ integrity protection
- Need to work with NAT ⇒ avoid source IP/port, use TSval for entropy
- Need easy deployment ⇒ in kernel, `setsockopt()` via LD_PRELOAD
- Implement: `https://gnunet.org/knock`
- Standardize: TCP Stealth (IETF draft, with Julian, Jake, Holger Kenn (MSFT))

[2] Joint work with Julian Kirsch (Master's thesis, 8'2014)

<Research>[2]

Idea: protect administrative TCP services via port knocking

- Use stealthy knock ⇒ SilentKnock
- Need to protect against MitM attacks ⇒ integrity protection
- Need to work with NAT ⇒ avoid source IP/port, use TSval for entropy
- Need easy deployment ⇒ in kernel, `setsockopt()` via LD_PRELOAD
- Implement: `https://gnunet.org/knock`
- Standardize: TCP Stealth (IETF draft, with Julian, Jake, Holger Kenn (MSFT))

Community reaction (so far):

- LKML: don't change the kernel, may introduce new vulnerabilities

[2] Joint work with Julian Kirsch (Master's thesis, 8'2014)

<Research>[2]

Idea: protect administrative TCP services via port knocking

- Use stealthy knock ⇒ SilentKnock
- Need to protect against MitM attacks ⇒ integrity protection
- Need to work with NAT ⇒ avoid source IP/port, use TSval for entropy
- Need easy deployment ⇒ in kernel, `setsockopt()` via LD_PRELOAD
- Implement: `https://gnunet.org/knock`
- Standardize: TCP Stealth (IETF draft, with Julian, Jake, Holger Kenn (MSFT))

Community reaction (so far):

- LKML: don't change the kernel, may introduce new vulnerabilities
- IETF: don't change ISN generation, many problems with it in past

[2] Joint work with Julian Kirsch (Master's thesis, 8'2014)

<Meta> Not Just Mass Surveillance, Not Just Targeted Attacks

- ORBing is just one type of active attack
- We already discussed other attacks, including on institutions

How can we secure networks to avoid totalitarianism?

The Internet is Fundamentally Broken

- Network generally learns too much (network neutrality!)
- Insecure defaults and system complexity
- Key, centralised Internet infrastructure is easily controlled:
  - Number resources (IANA)
  - Domain Name System (Root zone)
  - X.509 CAs (HTTPS certificates)
  - Dominant network service providers (Faceboogle)
- Encryption does not help if PKI is compromised, or plaintext is in the Cloud!

How broken is the Internet? A DNS case study.

What would a simple DNS lookup do? Say for `taler.net`?

- NS of **net** is `a.gtld-servers.net`

How broken is the Internet? A DNS case study.

What would a simple DNS lookup do? Say for `taler.net`?

- NS of **net** is `a.gtld-servers.net`
- NS of **taler.net** is `dns1.name-services.com`

How broken is the Internet? A DNS case study.

What would a simple DNS lookup do? Say for `taler.net`?

- NS of **net** is `a.gtld-servers.net`
- NS of **taler.net** is `dns1.name-services.com`
- NS of `com` is `a.gtld-servers.net`

How broken is the Internet? A DNS case study.

What would a simple DNS lookup do? Say for `taler.net`?

- NS of **net** is `a.gtld-servers.net`
- NS of **taler.net** is `dns1.name-services.com`
- NS of `com` is `a.gtld-servers.net`
- CNAME of **taler.net** is **pixel.net.in.tum.de**

How broken is the Internet? A DNS case study.

What would a simple DNS lookup do? Say for `taler.net`?

- NS of **net** is `a.gtld-servers.net`
- NS of **taler.net** is `dns1.name-services.com`
- NS of `com` is `a.gtld-servers.net`
- CNAME of **taler.net** is **pixel.net.in.tum.de**
- NS of **de** is `n.de.net`

How broken is the Internet? A DNS case study.

What would a simple DNS lookup do? Say for `taler.net`?

- NS of **net** is `a.gtld-servers.net`
- NS of **taler.net** is `dns1.name-services.com`
- NS of `com` is `a.gtld-servers.net`
- CNAME of **taler.net** is **pixel.net.in.tum.de**
- NS of **de** is `n.de.net`
- NS of `de.net` is `ns1.denic.de`

How broken is the Internet? A DNS case study.

What would a simple DNS lookup do? Say for `taler.net`?

- NS of **net** is `a.gtld-servers.net`
- NS of **taler.net** is `dns1.name-services.com`
- NS of `com` is `a.gtld-servers.net`
- CNAME of **taler.net** is **pixel.net.in.tum.de**
- NS of **de** is `n.de.net`
- NS of `de.net` is `ns1.denic.de`
- NS of `denic.de` is `ns1.denic.de`

How broken is the Internet? A DNS case study.

What would a simple DNS lookup do? Say for `taler.net`?

- NS of **net** is `a.gtld-servers.net`
- NS of **taler.net** is `dns1.name-services.com`
- NS of `com` is `a.gtld-servers.net`
- CNAME of **taler.net** is **pixel.net.in.tum.de**
- NS of **de** is `n.de.net`
- NS of `de.net` is `ns1.denic.de`
- NS of `denic.de` is `ns1.denic.de`
- NS of **tum.de** is `dns1.lrz.de`

How broken is the Internet? A DNS case study.

What would a simple DNS lookup do? Say for `taler.net`?

- NS of **net** is `a.gtld-servers.net`
- NS of **taler.net** is `dns1.name-services.com`
- NS of `com` is `a.gtld-servers.net`
- CNAME of **taler.net** is **pixel.net.in.tum.de**
- NS of **de** is `n.de.net`
- NS of `de.net` is `ns1.denic.de`
- NS of `denic.de` is `ns1.denic.de`
- NS of **tum.de** is `dns1.lrz.de`
- NS of `lrz.de` is `dns1.lrz.de`

How broken is the Internet? A DNS case study.

What would a simple DNS lookup do? Say for `taler.net`?

- NS of **net** is `a.gtld-servers.net`
- NS of **taler.net** is `dns1.name-services.com`
- NS of `com` is `a.gtld-servers.net`
- CNAME of **taler.net** is **pixel.net.in.tum.de**
- NS of **de** is `n.de.net`
- NS of `de.net` is `ns1.denic.de`
- NS of `denic.de` is `ns1.denic.de`
- NS of **tum.de** is `dns1.lrz.de`
- NS of `lrz.de` is `dns1.lrz.de`
- NS of **in.tum.de** is `tuminfo1.informatik.tu-muenchen.de`

How broken is the Internet? A DNS case study.

What would a simple DNS lookup do? Say for `taler.net`?

- NS of **net** is `a.gtld-servers.net`
- NS of **taler.net** is `dns1.name-services.com`
- NS of `com` is `a.gtld-servers.net`
- CNAME of **taler.net** is **pixel.net.in.tum.de**
- NS of **de** is `n.de.net`
- NS of `de.net` is `ns1.denic.de`
- NS of `denic.de` is `ns1.denic.de`
- NS of **tum.de** is `dns1.lrz.de`
- NS of `lrz.de` is `dns1.lrz.de`
- NS of **in.tum.de** is `tuminfo1.informatik.tu-muenchen.de`
- NS of `tu-muenchen.de` is `ws-han1.wip-ip.dfn.de`

How broken is the Internet? A DNS case study.

What would a simple DNS lookup do? Say for `taler.net`?

- NS of **net** is `a.gtld-servers.net`
- NS of **taler.net** is `dns1.name-services.com`
- NS of `com` is `a.gtld-servers.net`
- CNAME of **taler.net** is **pixel.net.in.tum.de**
- NS of **de** is `n.de.net`
- NS of `de.net` is `ns1.denic.de`
- NS of `denic.de` is `ns1.denic.de`
- NS of **tum.de** is `dns1.lrz.de`
- NS of `lrz.de` is `dns1.lrz.de`
- NS of **in.tum.de** is `tuminfo1.informatik.tu-muenchen.de`
- NS of `tu-muenchen.de` is `ws-han1.wip-ip.dfn.de`
- NS of `dfn.de` is `ws-han1.wip-ip.dfn.de`

How broken is the Internet? A DNS case study.

What would a simple DNS lookup do? Say for `taler.net`?

- NS of **net** is `a.gtld-servers.net`
- NS of **taler.net** is `dns1.name-services.com`
- NS of `com` is `a.gtld-servers.net`
- CNAME of **taler.net** is **pixel.net.in.tum.de**
- NS of **de** is `n.de.net`
- NS of `de.net` is `ns1.denic.de`
- NS of `denic.de` is `ns1.denic.de`
- NS of **tum.de** is `dns1.lrz.de`
- NS of `lrz.de` is `dns1.lrz.de`
- NS of **in.tum.de** is `tuminfo1.informatik.tu-muenchen.de`
- NS of `tu-muenchen.de` is `ws-han1.wip-ip.dfn.de`
- NS of `dfn.de` is `ws-han1.wip-ip.dfn.de`
- NS of **net.in.tum.de** is `dns1.lrz.de`

How broken is the Internet? A DNS case study.

What would a simple DNS lookup do? Say for `taler.net`?

- NS of **net** is `a.gtld-servers.net`
- NS of **taler.net** is `dns1.name-services.com`
- NS of `com` is `a.gtld-servers.net`
- CNAME of **taler.net** is **pixel.net.in.tum.de**
- NS of **de** is `n.de.net`
- NS of `de.net` is `ns1.denic.de`
- NS of `denic.de` is `ns1.denic.de`
- NS of **tum.de** is `dns1.lrz.de`
- NS of `lrz.de` is `dns1.lrz.de`
- NS of **in.tum.de** is `tuminfo1.informatik.tu-muenchen.de`
- NS of `tu-muenchen.de` is `ws-han1.wip-ip.dfn.de`
- NS of `dfn.de` is `ws-han1.wip-ip.dfn.de`
- NS of **net.in.tum.de** is `dns1.lrz.de`
- A of **pixel.net.in.tum.de** is 131.159.20.32

How broken is the Internet? A DNS case study.

- Glue records and caching logic were not shown

[3] Which has no out-of-bailiwick lookups.

How broken is the Internet? A DNS case study.

- Glue records and caching logic were not shown
- PETS reviewer (rejecting paper on the GNU Name System[3]) asked: "Could you imagine if for every DNS reply we receive today we were shown the trust chain and asked whether we're OK with it?!"

[3] Which has no out-of-bailiwick lookups.

How broken is the Internet? A DNS case study.

- Glue records and caching logic were not shown
- PETS reviewer (rejecting paper on the GNU Name System[3]) asked: "Could you imagine if for every DNS reply we receive today we were shown the trust chain and asked whether we're OK with it?!"
- As deployed, DNSSEC fails on end-to-end authenticity and confidentiality
- DNS remains major source of traffic amplification attacks
- Some US court considered confiscating ccTLDs
- Censorship of non-TLD domain names is already common

[3] Which has no out-of-bailiwick lookups.

How broken is the Internet? A DNS case study.

- Glue records and caching logic were not shown
- PETS reviewer (rejecting paper on the GNU Name System[3]) asked: "Could you imagine if for every DNS reply we receive today we were shown the trust chain and asked whether we're OK with it?!"
- As deployed, DNSSEC fails on end-to-end authenticity and confidentiality
- DNS remains major source of traffic amplification attacks
- Some US court considered confiscating ccTLDs
- Censorship of non-TLD domain names is already common
- How much of this mess does DNSCurve fix again?

[3]Which has no out-of-bailiwick lookups.

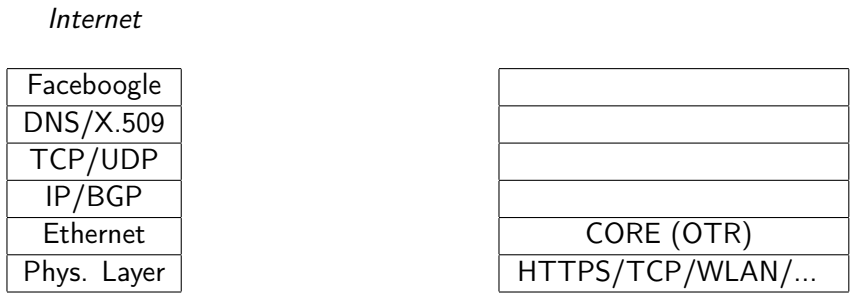
Our Vision (Simplified)

Internet

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

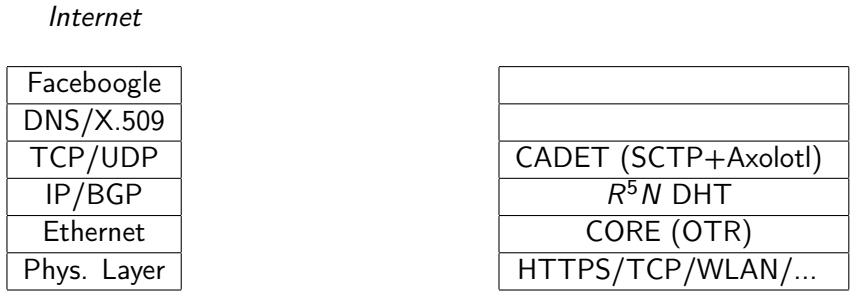
Our Vision (Simplified)

Our Vision (Simplified)

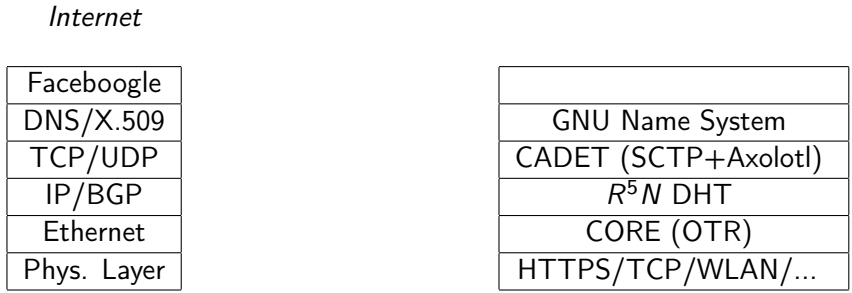


Our Vision (Simplified)

Our Vision (Simplified)



Our Vision (Simplified)



Our Vision (Simplified)

Internet

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

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

Our Vision (Simplified)

Internet

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

GNUnet

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

Fixing the Net

- GNU Name System: decentralised PKI, identity management and name system
- R^5N DHT: decentralised, censorship-resistant key-value store
- CADET: Confidential Ad-hoc Decentralised End-to-End Transport

Fixing the Net

- GNU Name System: decentralised PKI, identity management and name system
- R^5N DHT: decentralised, censorship-resistant key-value store
- CADET: Confidential Ad-hoc Decentralised End-to-End Transport
- Secure decentralised network size estimation
- Advanced cryptography:
  - Secure multiparty scalar product
  - Byzantine fault-tolerant consensus (set union)
  - Fouque's distributed key generation and cooperative encryption
  - Cramer-style electronic voting

Fixing the Net: Applications

- Anonymous file-sharing
- IP-over-GNUnet
- Voice-over-GNUnet
- Decentralised social networking (future)
- Decentralised cooperative news distribution (future)
- Privacy-preserving constraint negotiation (future)

More building blocks

- Semantically extensible Byzantine fault-tolerant multicast
- GNUnet-over-Tor
- BRAHMS (Byzantine fault-tolerant random peer sampling)
- Directory-less onion routing
- Git-over-GNUnet
- ...

More infrastructure

- Secure, libre hardware
- Secure operating systems
- Static analysis
- Regression testing
- ...

Side projects

- Taler: Taxable Anonymous Libre Electronic Reserves
- GNU libextractor – meta data extraction
- GNU libmicrohttpd – HTTP library
- ...

Do you have any questions?

References:

- Julian Kirsch. *Improved Kernel-Based Port-Knocking in Linux*. **Master's Thesis (TUM)**, 2014.
- Julian Kirsch, Christian Grothoff, Monika Ermert, Jacob Appelbaum, Laura Poitras and Henrik Moltke. *NSA/GCHQ: Das HACIENDA-Programm zur Kolonisierung des Internet*. In **Heise Online** 8'2014. Heise Zeitschriften Verlag, 2014.
- 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.

Academics to the rescue?

- Can we enforce ethics to stop research supporting repression?
- Can the research community help journalists with OpSec?
- How do we minimize corruption of research institutions?

Academics to the rescue?

- Can we enforce ethics to stop research supporting repression?
- Can the research community help journalists with OpSec?
- How do we minimize corruption of research institutions?

PETS reviewer (rejecting paper on Knock) writes:
"Overall, this is neat and useful but I am unsure PETS is looking for implementation / kernel development hacks. This may fit better in a blog or in a Linux, coding or sysadmin conference.
Further, there doesn't seem to be a research component to this.
The authors have a research background and know this. It would be more fair to reviewers to not abuse the reviewing system by submitting this paper to venues that are clearly ill suited for these (otherwise nice) results."