#### 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<sup>1</sup> I published with

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

<sup>&</sup>lt;sup>1</sup>"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

 Completed partial scans of 5 additional countries



# **Tasking & Access**

To task HACIENDA with a Country or Subnet

@gchq.gov.uk)

@gchq.gov.uk)

· Access to the Data

CITD alias

 At GCHQ, request a GLOBAL SURGE account from @gchq.gov.uk)

- At CSEC, contact
- At NSA, contact
- At DSD, contact



## 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





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

### Step 3

### Hacking in SIGINT



### **The Hacking Process**

- (R)econnaissance
- 2. (I)nfection

1.

- 3. (c)ommand And Control
- 4. (E)xfiltration



#### Reconnaissance

#### Publicly Available Information

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



Reconnaissance Infection Command and Control Exfiltration



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

#### Reconnaissance

This system is audited for USSID 18 and Human Rights Act compliance

X-KEYSCORE C2C Session Viewer										
4 4 Session 1 of 4	> N   O									
Datetime Case Notation		From IP	To IP	From F	ort To Port	Protocol L				
2012-05-16 13:03:20 2CBA	00000M0210			01701	01701	icmp 1				
2012-05-16 13:03:20 2CBAH Session Header (3) Meta (7) WRESHAPK Quick Clicks (4) Session MRESHAPK Concentrations Concentr	GENESIS Context Version: 4 Version: 4 Neader Len Different: CO000 0  Toteal Jeeg Identifice Flags: 040  0 Fragment 0 Trimeto li Protocoll: Neader che (Goodi [Rad :	col, Src: 8.8.8.9 (8.8.8), Det col, Src: 8.8.8.9 (8.8.8), Det gth: 20 bytes ated Services Field: 0x00 (BSCF 0 = Differentiated Services Cc 0 = ECN-Cepable Transport (SC 0 = ECN-C: 0 this 60 tons: 0x2ds (11580) De Reserved bit: Not set Don't fragment: Not set More fragment: Not set ffeet: 0 ve: 51 ICNNF (0x01) Sclaums: 0x897a [correct] True]	: 192.168.0.83 (192.168.0.8 0x00: Default; ECB: 0x00) depoint: Default (0x00)	Enter text to search	01701	icmp 1				
¢ · · · · · · · · · · · · · · · · · · ·	Source: 8. Destinatio Internet Contr Type: 0 [S Code: 0 [] Checksum: Identifier Sequence n Data [32 b 0000 61 62 63	8.8.8 (9.8.8.9) n: 192.160.0.83 (192.160.0.83) b Mesnage Protocol bho (ping) reply) Dx52ac [correct] : 0x0001 umber: 633 (0x026f)								

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	Iragi Ministry of Finance
USER	Administrator	
PASS	kalimero4cappy	
USER	Administrator	
PASS	P@ssword	
USER	Administrator	
PASS	P@sswOrd	
USER	Administrator	
PASS	P@ssw0rd	

Reconnaissance Infection Command and Control Exfiltration



#### **Command and Control**





Reconnaissance Infection Command and Control Exfiltration



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

#### Windows cmd.exe

C:\WINDOWS\system32\cmd.exe	- 🗆 🗙
Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp.	-
U:\>_	
	-

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





Communications Security Establishment Centre de la sécurité des télécommunications

### 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



#### TOP SECRET//COMINT



Communications Security Establishment Centre de la sécurité des télécommunications



Ohmote of Ginna all you got											
ne al you got 🤤 Ginne al you got by Country 🔅 💦 🗖 🗆	Athene View (JPA) (100	00) [3]									<b>남</b> 第 (2 4)
xh	Showing page 1										
	Source System	First Seen	Lagt Seen	Hasthiane	p	Port P	rotocol Status -	T	1. Product	Version	Banner Information
inent: africa 🖉	GCHQ Hadenda		Tue May 19 08:11:03 GMT 2009			10 10		0	unknown	unknown	unknown
ntrus kenya	GCHQ Haciencla	Tue May 19 08: 11:03 GMT 2009				10 to		0	unknown	unknown	unknown
an man	GCHQ Hadenda	Tue Nay 19 08: 11:03 GMT 2009				111 10		0	unknown	unknown	unknown
Ranges Last 30 days	GCHQ Hadenda	Tue May 19 08: 11:03 GMT 2009				161 10		0	unknown	unimerinu	unknown
	GCHQ Hadenda GCHO Hadenda	Tue Nay 19 08: 11:03 GMT 2009 Tue Nay 29 08: 11:03 GMT 2009	Tue May 19 08:11:03 GWT 2009			162 tq 143 tq		0	unknown	unknown	unknown
Date: 03/28/2330 💉 32:00:00 AM 🗘	GCHO Hacenda	Tue Ney 19 08:11:03 GMT 2009				20 to		0	unknown	unknown	unkrown
ata: 04/25/2030 V 11:50:50 PM 2	60H0 Hadenda	Tue Nev 19 08:07:29 GMT 2009					known urreachable		Linkingen	unimour	unknown
and a destant of another of	GCHQ Hadenda	Tue Nay 19 04: 15:01 GMT 2009				10 10		0	Kerio MalServer POP3 Server	6.1.2	4152.1242730171(Blov_svr
	GCHO Hadenda	Tue May 19 04: 15:01 GMT 2009	Tue May 29 04:15:01 GMT 2029			13 10		0	Kerio MalServer Webnal	6.1.2	unknown
nends	6CHQ Hadenda	Tue May 29.04: 15:01 GMT 2009	Tue May 29 04:15:01 GMT 2009			5 10		0	Microsoft ESNTP	6.0.3700.395	9 unknown
Show VPNs	GCHQ Hacienda	Tue May 19 04: 15:01 GMT 2009			8	10 to		0	Microsoft IIS webserver	6.0	unknown
Show Toyprippe Range Events	GCHQ Hadenda	Tue Nay 19 04: 15:01 GMT 2009				1 to 12 to 13 to		0	Microsoft flpd	unknown	unknown
	GCHQ Hadenda	Tue May 19 04: 19:01 GMT 2009				12 10		0	unknown	unictevin	unknown
Show CNO Event Summaries	GCHQ Hadenda GCHQ Hadenda	Tue May 19 04: 15:01 GMT 2009				13 10		0	unknown	unknown	unknown
Show User Online Events on IP	GCHQ Hadenda GCHQ Hadenda	Tue May 29 04: 15:01 GMT 2009 Tue May 29 04: 15:01 GMT 2009				111 1cj 161 tcj		0	unenseen	unknown	unknown
	GCHQ Hedende	Tue Ney 19 04: 15:01 (911 2009				101 103 162 103			unknown	unknown	unkrown
Show router configuration information (TEDAL SURGE)	GCHQ Hadenda		Tue May 19 04:17:28 GMT 2009			1 10		0	unknown	unicopera	unknown
Show IP Communications	GCHO Hadenda		Tue Nay 19 04:17:28 GNT 2009			2 10		0	Linknown	unknown	unknown
Show Geolocation Information	GCHQ Hadenda		Tue Nay 29 04:17:28 GNT 2029			13 10		0	unknown	unknown	unknown
	GCHQ Hadenda	Tue Ney 19 04: 17:20 GMT 2009				5 10	p closed	0	unknown	unizgern	unknown
Show Network Information	SCHQ Hadenda		Tue May 19 04:17:28 GMT 2009			10 tc;		0	unknown	unknown	unknown
Show SIGINT Observable Feature Information	GCHQ Hadenda	Tue May 19 04: 17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009			10 10		0	unknown	unimerinu	unknown
al Show Survey Information	GCHQ Hadenda	Tue May 19 04: 17:28 GMT 2009				111 30		0	unknown	unknown	unknown
	GCHQ Hadenda	Tue May 19 04: 17:28 GMT 2009				161 10		0	unknown	unknown	unknown
Shaw Geolocation Map	GCHQ Hadenda GCHQ Hadenda	Tue May 39 04: 17:28 GMT 2009 Tue May 39 04: 17:28 GMT 2009				162 to 163 to		0	unknown	unknown	unknown
Reverse DNS Lookup	GCHQ Hadenda	Tue Nay 19 04: 17:40 GMT 2009				H3 tq 21 tq 12 tq 13 tq			unknown	unknown	unknown
e Show Part Scens on ₽	GCHO Hadenda	Tue Nay 29 04: 17:40 GMT 2009				2 10		0	Linknown	unknown	unknown
C Show Part Sciens on P	GCHO Hadenda	Tue Nay 29 04:17:40 GMT 2009				13 10		0	Linknown	unknown	unknown
ect Al Deselect Al	GCHQ Hedende	Tue Ney 19 04: 17:40 GMT 2009				5 10	n cioned	0	unknown	unizgen	unknown
sect all Luesteect all	GCHQ Hadenda	Tue Nay 19 04: 17:40 GMT 2009			2	10 to		0	unknown	unknown	unknown
	GCHQ Hadenda	Tue May 19 04: 17:40 GMT 2009				10 10		0	unknown	unknown	unknown
	GCHQ Hadenda		Tue May 29 04:17:40 GMT 2029			111 30		0	unknown	unknown	unknown
Run	GCHQ Haciencia	Tue May 29 04:17:40 GMT 2009				161 tq		0	unknown	unknown	unknown
	GCHQ Hadenda	Tue May 19 04: 17:40 GMT 2009				162 to		0	unknown	unknown	unknown
	GCHQ Hadenda GCHQ Hadenda		Tue May 19 04:17:40 GMT 2009 Tue May 19 04:16:24 GMT 2009			H3 10	p open iknown unreachable		unknown	unknown	unknown
	GCHQ Hadenda		Tue Jun 17:00:13:13 GMT 2009				known urreachable		unknown	unknown	unknown
	GCHO Haciencia		Tue Jun 1700:13:39 GMT 2008				known urreachable		unknown	unknown	unknown
	GCHQ Hedende	Tue 3m 17 00: 17:49 GMT 2008					known urreachable		urknown	unknown	unknown
	GCHQ Hadenda		Tue 3m 1700: 13:56 GMT 2008				known urreachable		urknown	unknown	unknown
	GCHQ Hadenda	Tue Jun 17 00: 13:59 GMT 2008	Tue Jun 17 00: 13:59 GMT 2008				known unreachable		unknown	unionovinu	unknown
	GCHQ Hadenda		Tue Jun 1707:00:29 GMT 2008		0		iknown umeachable		unknown	unknown	unknown
	GCHQ Hacienda		Tue Jun 1707:03:13 GMT 2008		0		known urreachable		unknown	unknown	unknown
	GCHQ Hadenda		Tue 3m 1707:01:12 GMT 2008		9		known urreachable		unknown	unknown	unknown
	GCHQ Hadenda	Tue Jul 07 07:30:43 GMT 2009		80-247-147-40, reverse, newskies, net	9		known urreachabk		unknown	unknown	unknown
	GCHQ Hadenda GCHD Hadenda	Tue 3d 07 07:32:20 GMT 2009 Tue 3d 07 07:31:23 GMT 2009		80-247-147-41, reverse, newskies, net 80-247-147-42, reverse, newskies, net			known unreachable	0	unknown	unknown	unknown
	GCHQ Hapenda GCHO Hapenda	Tue Jul 07 07:32:13 GMT 2009		80-247-147-42, reverse, nevisions, ret 80-247-147-43, reverse, revolves, ret	1		known unreachable	0	unknown	unknown	unknown
	GCHQ Hadenda	Tue 3al 0707:32:13 GMT 2009		50-247-147-43.reverse.mevaloes.ret 50-247-147-44.reverse.mevaloes.ret			internation internation		unknown	unknown	unkrown
	GCHO Hadenda	Tue 3d 07 07:32:54 GMT 2009		80-247-147-45, reverse, newskies, net	2		known unreachable	P	unknown	unimourn	unknown
	GCHQ Hadenda	Tue 34 07 06/49/57 GMT 2009		80-247-147-45, reverse, nevisites, net			known urreadiable	0	unknown	unknown	unknown
	GCHQ Hadenda	Tue 3al 07 06:47:17 GMT 2009		80-247-147-47, reverse, nevalues, net	0		known umeachable		unknown	unknown	unknown
	GCHQ Hacienda	Tue Jul 07/06:18:02 GMT 2009	Wed Feb 03 12:02:07 GMT 2010		0	) un	known urreachable	0	unknown	unknown	unknown
	GCHQ Hadenda		Tue 3un 17/00:36:20 GMT 2006			13 fc		0	Cisco router	unkzigern	unknown
	GTHD Hadapela	The 3x4 07 CE 16:19 CMT 2009					destant umanitable		unimean	interest	Internet

🔹 BUT, network analysis still manual! Canadä

#### TOP SECRET//COMINT



Communications Security Centre de la sécurité des télécommunications



- 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</p>



### **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.





<sup>&</sup>lt;sup>2</sup>Joint work with Julian Kirsch (Master's thesis, 8'2014)



• Use stealthy knock  $\Rightarrow$  SilentKnock

<sup>&</sup>lt;sup>2</sup>Joint work with Julian Kirsch (Master's thesis, 8'2014)



- $\blacktriangleright \text{ Use stealthy knock} \Rightarrow \mathsf{SilentKnock}$
- $\blacktriangleright$  Need to protect against MitM attacks  $\Rightarrow$  integrity protection

<sup>&</sup>lt;sup>2</sup> Joint work with Julian Kirsch (Master's thesis, 8'2014)



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

<sup>&</sup>lt;sup>2</sup> Joint work with Julian Kirsch (Master's thesis, 8'2014)

 $< \text{Research} >^2$ 

- Use stealthy knock  $\Rightarrow$  SilentKnock
- $\blacktriangleright$  Need to protect against MitM attacks  $\Rightarrow$  integrity protection
- $\blacktriangleright$  Need to work with NAT  $\Rightarrow$  avoid source IP/port, use TSval for entropy
- $\blacktriangleright$  Need easy deployment  $\Rightarrow$  in kernel, setsockopt() via LD\_PRELOAD

<sup>&</sup>lt;sup>2</sup>Joint work with Julian Kirsch (Master's thesis, 8'2014)

 $< \text{Research} >^2$ 

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

<sup>&</sup>lt;sup>2</sup>Joint work with Julian Kirsch (Master's thesis, 8'2014)

 $< \text{Research} >^2$ 

- Use stealthy knock  $\Rightarrow$  SilentKnock
- $\blacktriangleright$  Need to protect against MitM attacks  $\Rightarrow$  integrity protection
- $\blacktriangleright$  Need to work with NAT  $\Rightarrow$  avoid source IP/port, use TSval for entropy
- $\blacktriangleright$  Need easy deployment  $\Rightarrow$  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

<sup>&</sup>lt;sup>2</sup> Joint work with Julian Kirsch (Master's thesis, 8'2014)

 $< \text{Research} >^2$ 

- Use stealthy knock  $\Rightarrow$  SilentKnock
- $\blacktriangleright$  Need to protect against MitM attacks  $\Rightarrow$  integrity protection
- $\blacktriangleright$  Need to work with NAT  $\Rightarrow$  avoid source IP/port, use TSval for entropy
- $\blacktriangleright$  Need easy deployment  $\Rightarrow$  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

<sup>&</sup>lt;sup>2</sup>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!



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

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

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

- 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

- 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 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 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 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 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 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 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 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 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 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

- 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

Glue records and caching logic were not shown

<sup>&</sup>lt;sup>3</sup>Which has no out-of-bailiwick lookups.

- Glue records and caching logic were not shown
- PETS reviewer (rejecting paper on the GNU Name System<sup>3</sup>) 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?!"

<sup>&</sup>lt;sup>3</sup>Which has no out-of-bailiwick lookups.

- Glue records and caching logic were not shown
- PETS reviewer (rejecting paper on the GNU Name System<sup>3</sup>) 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

<sup>&</sup>lt;sup>3</sup>Which has no out-of-bailiwick lookups.

- Glue records and caching logic were not shown
- PETS reviewer (rejecting paper on the GNU Name System<sup>3</sup>) 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?

<sup>&</sup>lt;sup>3</sup>Which has no out-of-bailiwick lookups.

Internet

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

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



Internet
Faceboogle
DNS/X.509
TCP/UDP
IP/BGP
R<sup>5</sup>N DHT
Ethernet
CORE (OTR)
Phys. Layer
HTTPS/TCP/WLAN/...

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

CADET (SCTP+Axolotl)	
<i>R</i> ⁵ <i>N</i> DHT	
CORE (OTR)	
HTTPS/TCP/WLAN/	

Internet

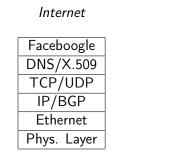
Faceboogle	
DNS/X.509	
TCP/UDP	
IP/BGP	
Ethernet	
Phys. Layer	

GNU Name System
CADET (SCTP+Axolotl)
<i>R</i> ⁵ <i>N</i> DHT
CORE (OTR)
HTTPS/TCP/WLAN/

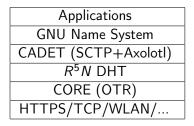
Internet

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

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



#### GNUnet



### 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
- ► ...

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."