DÉCENTRALISÉ NOW!

NSA broke the Internet — Now we have to build a GNU one!

Christian Grothoff

Inria Rennes - Bretagne Atlantique

27.11.2014

Dé central isé

> “Never doubt your ability to change the world.” –Glenn Greenwald

Doctor's Warning

This presentation is a wild mixture of

- Journalistic work
- Political analysis
- Technological solutions

If you experience trauma, this may be unrelated to the style of the presentation.

Disclaimer: This is NOT about the Five Eyes

> “In February, the UK based research publication Statewatch reported that the **EU had secretely agreed** to set up an international telephone tapping network via a secret network of committees established under the “third pillar” of the Mastricht Treaty covering co-operation on law and order. (...) EU countries (...) should agree on **international interception standards (...) to co-operate closely with the FBI** (...). Network and service providers in the EU will be obliged to install **tappable** systems and to place under **surveillance** any person or group when served an interception order. These plans have never been referred to any European government for scrutiny (...) despite the **clear civil liberties issues** raised by such an **unaccountable** system. (...) The German government estimates that the mobile phone part of the package alone will cost 4 billion D-marks.”

Scientific and Technological Options Assessment (STOA), “An Appraisal of Technologies of Political Control”, European Parliament, PE 166499, 6 January 1998.

Debate in the US

US discussion focuses on spying on US citizens and legality under US law.

Frank Church (D-Idaho):

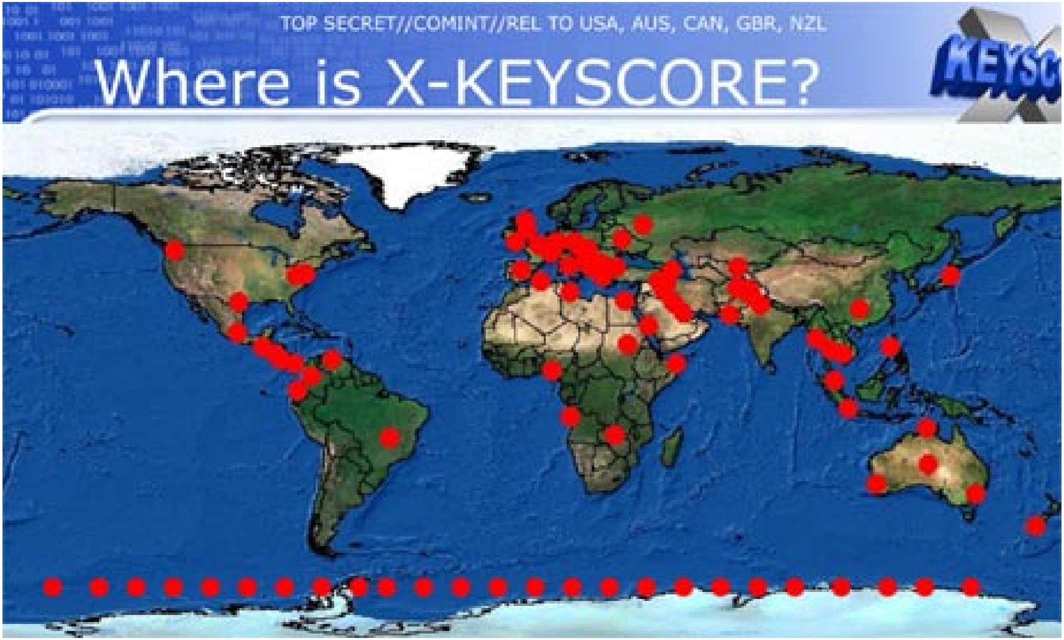
> “The NSA’s capability at any time could be turned around on the American people, and **no American would have any privacy left**, such is the capability to monitor everything: telephone conversations, telegrams, it doesn’t matter.”

Cyberwar

Presidential Policy Directive 20, issued October 2012 and released by Edward Snowden, outlines U.S. cyberwar policy:

> “Offensive Cyber Effect Operations (OCEO) can offer unique and unconventional capabilities to **advance U.S. national objectives** around the world with little or no warning to the adversary or target and with potential effects ranging from **subtle** to severely damaging. (...)
> The United States Government shall identify potential targets of national importance where OCEO can offer a favorable **balance of effectiveness and risk** as compared with other instruments of national power, establish and maintain OCEO capabilities integrated as appropriate with other U.S. offensive capabilities, and execute those capabilities in a manner consistent with the provisions of this directive.”

X-KEYSCORE

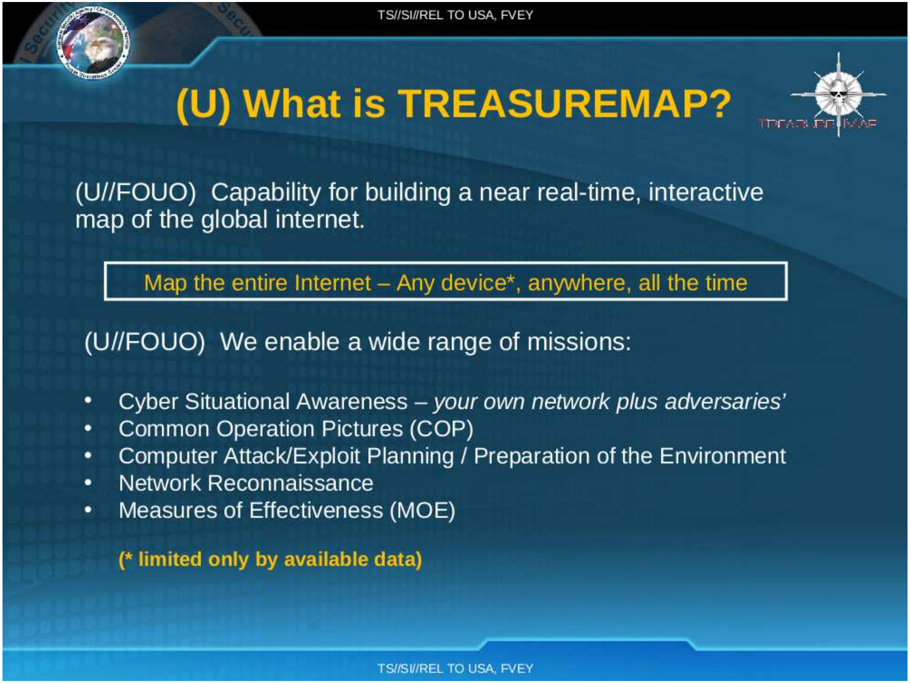


TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Where is X-KEYSCORE?

“Google for global tcpdump” –Jacob Appelbaum

Treasuremap



TS//SI//REL TO USA, FVEY

(U) What is TREASUREMAP?

(U//FOUO) Capability for building a near real-time, interactive map of the global internet.

Map the entire Internet – Any device*, anywhere, all the time

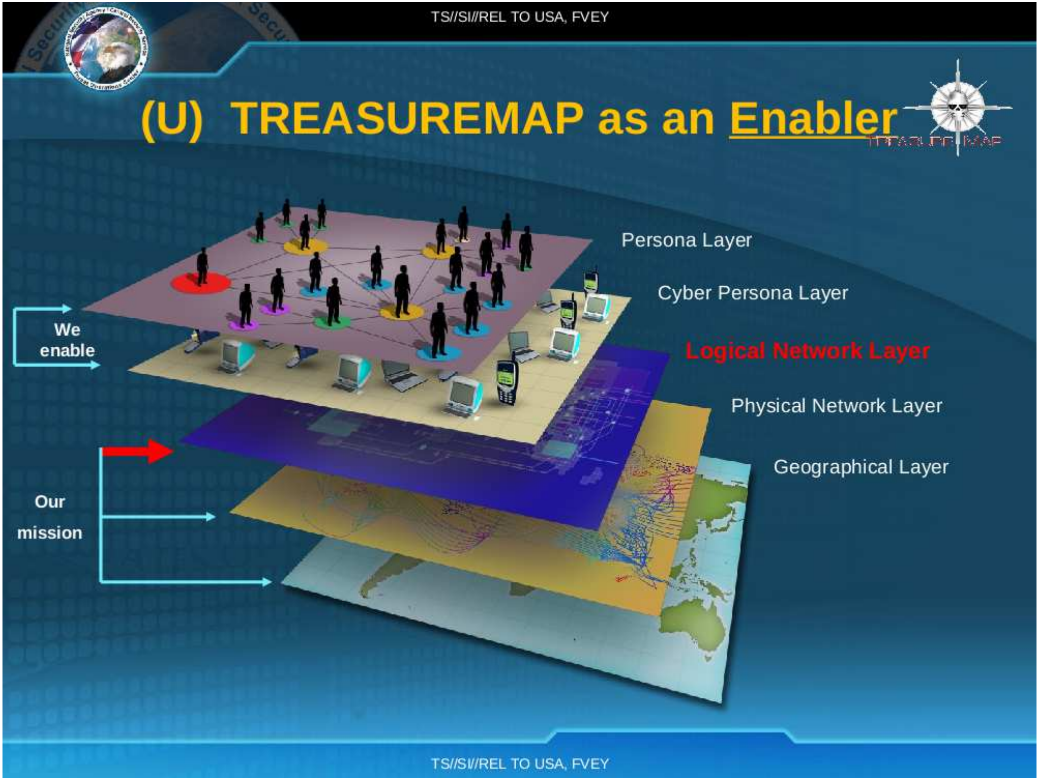
(U//FOUO) We enable a wide range of missions:

- Cyber Situational Awareness – *your own network plus adversaries'*
- Common Operation Pictures (COP)
- Computer Attack/Exploit Planning / Preparation of the Environment
- Network Reconnaissance
- Measures of Effectiveness (MOE)

(* limited only by available data)

TS//SI//REL TO USA, FVEY

If X-KEYSCORE is NSA's Google, Treasuremap is their Google Maps.



(U) TREASUREMAP as an Enabler

Persona Layer

Cyber Persona Layer

Logical Network Layer

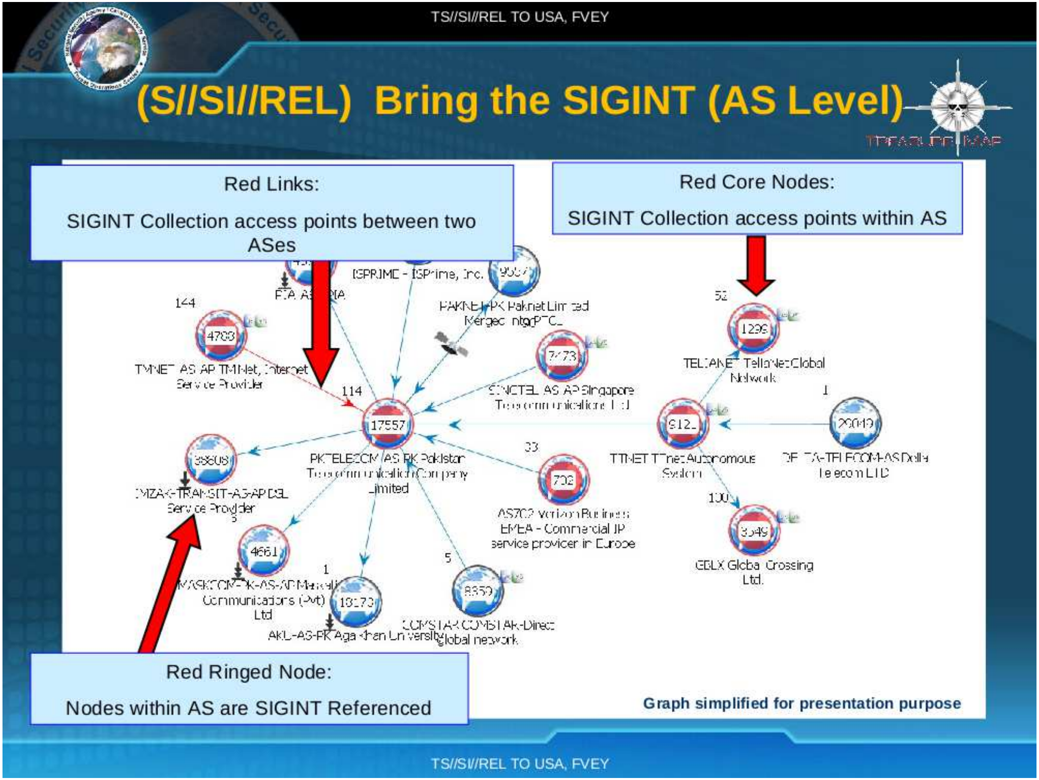
Physical Network Layer

Geographical Layer

We enable

Our mission

(S//SI//REL) Bring the SIGINT (AS Level)


TREASURE MAP
ISPRIME - ISPrime, Inc.
9557
FTA-AS ...IA
144
4788
TMNET-AS-AP TM Net, Internet Service Provider
PAKNET-PK Paknet Limited Merged into PTCL
7473
SINGTEL-AS-AP Singapore Telecommunications Ltd
114
17557
PKTELECOM-AS-PK Pakistan Telecommunication Company Limited
38508
IMZAK-TRANSIT-AS-AP DSL Service Provider
3
4661
MASKCOM-PK-AS-AP Maskall Communications (Pvt) Ltd
1
18173
AKU-AS-PK Aga Khan University
5
8359
COMSTAR COMSTAR-Direct Global network
33
702
AS702 Verizon Business EMEA - Commercial IP service provider in Europe
52
1299
TELIANET TeliaNet Global Network
1
9121
TTNET TTnet Autonomous System
29049
DELTA-TELECOM-AS Delta Telecom LTD
100
3549
GBLX Global Crossing Ltd.

Red Links:

SIGINT Collection access points between two ASes

Red Core Nodes:

SIGINT Collection access points within AS

Red Ringed Node:

Nodes within AS are SIGINT Referenced

Graph simplified for presentation purpose

The GCHQ's HACIENDA

- HACIENDA is one of the programs feeding the TREASUREMAP
- There are many others.

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

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 [redacted]
  - At NSA, contact [redacted]
  - At DSD, contact [redacted]

NETWORK ANALYSIS CENTRE

[redacted]

UK TOP SECRET STRAP1
TOP SECRET//COMINT//REL FVEY

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

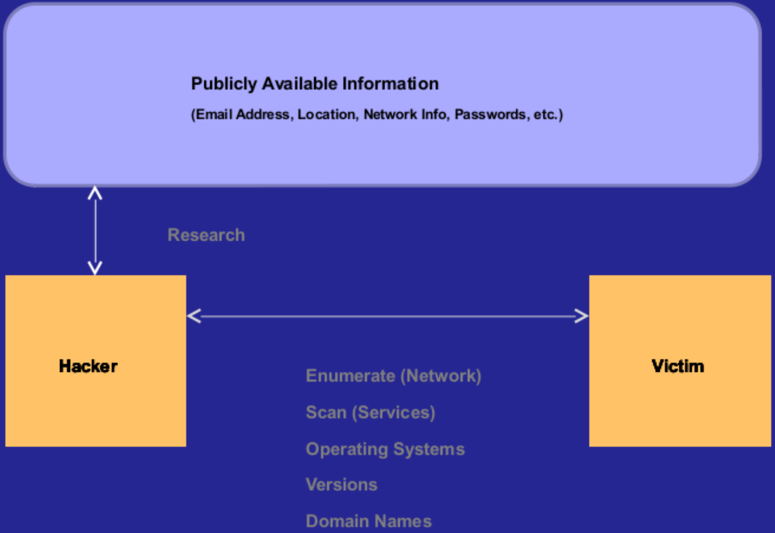
Step 3

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)

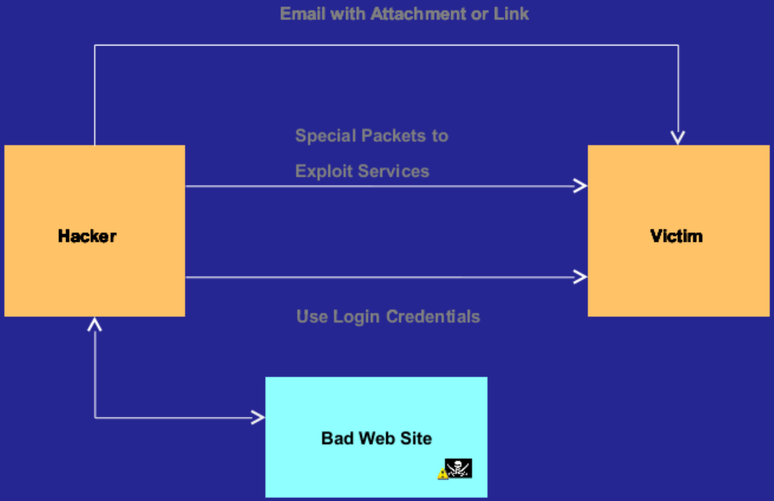
Operating Systems

Versions

Domain Names

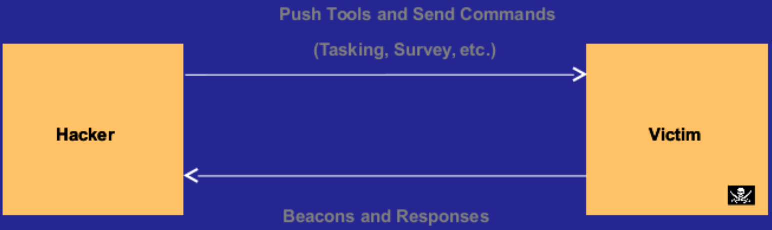
Reconnaissance Infection Command and Control Exfiltration

Infection



Reconnaissance Infection Command and Control Exfiltration

Command and Control



Push Tools and Send Commands

(Tasking, Survey, etc.)

Hacker

Victim

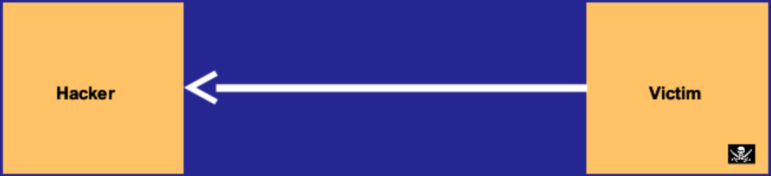
Beacons and Responses

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

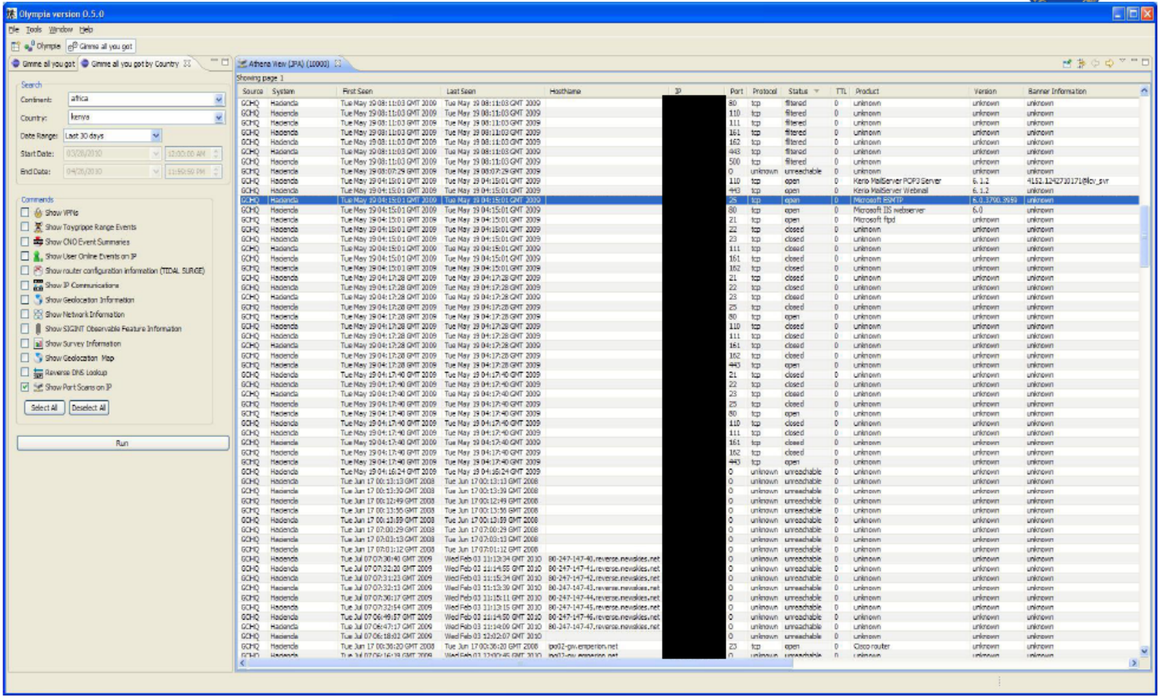
How is it used?

- 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

[redacted]
[redacted]
[redacted]
[redacted]



Search

Continent: africa

Country: kenya

Date Range: Last 30 days

Start Date: 03/26/2010 12:00:00 AM

End Date: 04/26/2010 11:59:59 PM

Commands

- ☐ Show VPNs
- ☐ Show Toygrippe Range Events
- ☐ Show CNO Event Summaries
- ☐ Show User Online Events on IP
- ☐ Show router configuration information (TIDAL SURGE)
- ☐ Show IP Communications
- ☐ Show Geolocation Information
- ☐ Show Network Information
- ☐ Show SIGINT Observable Feature Information
- ☐ Show Survey Information
- ☐ Show Geolocation Map
- ☐ Reverse DNS Lookup
- ☑ Show Port Scans on IP

Showing page 1

Source	System	First Seen	Last Seen	HostName	IP	Port	Protocol	Status	TTL	Product	Version	Banner Information
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	80	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	110	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	111	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	161	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	162	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	443	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	500	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:07:29 GMT 2009	Tue May 19 08:07:29 GMT 2009		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	110	tcp	open	0	Kerio MailServer POP3 Server	6. 1.2	4152.1242710171@lcv_svr
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	443	tcp	open	0	Kerio MailServer Webmail	6. 1.2	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	25	tcp	open	0	Microsoft ESMTP	6.0.3790.3959	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	80	tcp	open	0	Microsoft IIS webserver	6.0	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	21	tcp	open	0	Microsoft ftpd	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	22	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	23	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	111	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	161	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	162	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	21	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	22	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	23	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	25	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	80	tcp	open	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	110	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	111	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	161	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	162	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	443	tcp	open	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	21	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	22	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	23	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	25	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	80	tcp	open	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	110	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	111	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	161	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	162	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	443	tcp	open	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:16:24 GMT 2009	Tue May 19 04:16:24 GMT 2009		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:13:13 GMT 2008	Tue Jun 17 00:13:13 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:13:39 GMT 2008	Tue Jun 17 00:13:39 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:12:49 GMT 2008	Tue Jun 17 00:12:49 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:13:56 GMT 2008	Tue Jun 17 00:13:56 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:13:59 GMT 2008	Tue Jun 17 00:13:59 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 07:00:29 GMT 2008	Tue Jun 17 07:00:29 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 07:03:13 GMT 2008	Tue Jun 17 07:03:13 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 07:01:12 GMT 2008	Tue Jun 17 07:01:12 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:30:40 GMT 2009	Wed Feb 03 11:13:34 GMT 2010	80-247-147-40.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:32:20 GMT 2009	Wed Feb 03 11:14:55 GMT 2010	80-247-147-41.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:31:23 GMT 2009	Wed Feb 03 11:15:34 GMT 2010	80-247-147-42.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:32:13 GMT 2009	Wed Feb 03 11:13:39 GMT 2010	80-247-147-43.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:30:17 GMT 2009	Wed Feb 03 11:15:11 GMT 2010	80-247-147-44.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:32:54 GMT 2009	Wed Feb 03 11:13:15 GMT 2010	80-247-147-45.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 06:49:57 GMT 2009	Wed Feb 03 11:14:50 GMT 2010	80-247-147-46.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 06:47:17 GMT 2009	Wed Feb 03 11:14:09 GMT 2010	80-247-147-47.reverse.nevakies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 06:18:02 GMT 2009	Wed Feb 03 12:02:07 GMT 2010		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:36:20 GMT 2008	Tue Jun 17 00:36:20 GMT 2008	ipo02-gw.emperion.net	[redacted]	23	tcp	open	0	Cisco router	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 06:16:19 GMT 2009	Wed Feb 03 12:00:45 GMT 2010	ipo02-gw.emperion.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown

- BUT, network analysis still manual!

[redacted]

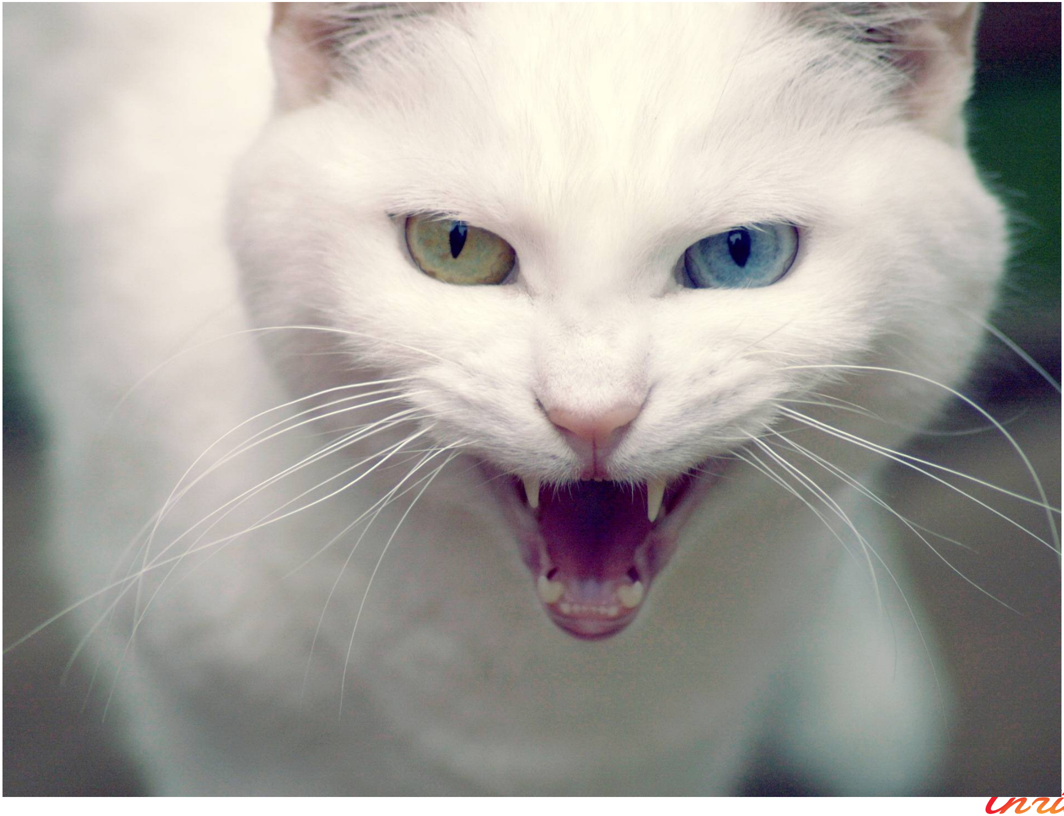
- [redacted] GSM provider
- NSA TAO requested assistance gaining access to the network
- Network analysis using OLYMPIA:
  - DNS query to determine IP address
  - IP address to network range
  - Network range to port scan
  - Are there any vulnerable devices in that range?
- Duration: < 5 minutes

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]

Cat break



Knocking down the HACIENDA[1]

Idea: protect administrative services via port knocking

[1] Joint work with Julian Kirsch

Knocking down the HACIENDA[1]

Idea: protect administrative services via port knocking

- Use stealthy knock ⇒ SilentKnock

[1] Joint work with Julian Kirsch

Knocking down the HACIENDA[1]

Idea: protect administrative services via port knocking

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

[1] Joint work with Julian Kirsch

Knocking down the HACIENDA[1]

Idea: protect administrative 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

[1] Joint work with Julian Kirsch

Knocking down the HACIENDA[1]

Idea: protect administrative 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
- Implement: `https://gnunet.org/knock`
- Standardize: TCP Stealth (IETF draft)

[1] Joint work with Julian Kirsch

ISN Calculation

- Destination IP address IP_d
- Destination port P_d
- TCP timestamp T

- Pre-Shared Key S
- Hash functions h, h'
- Payload p

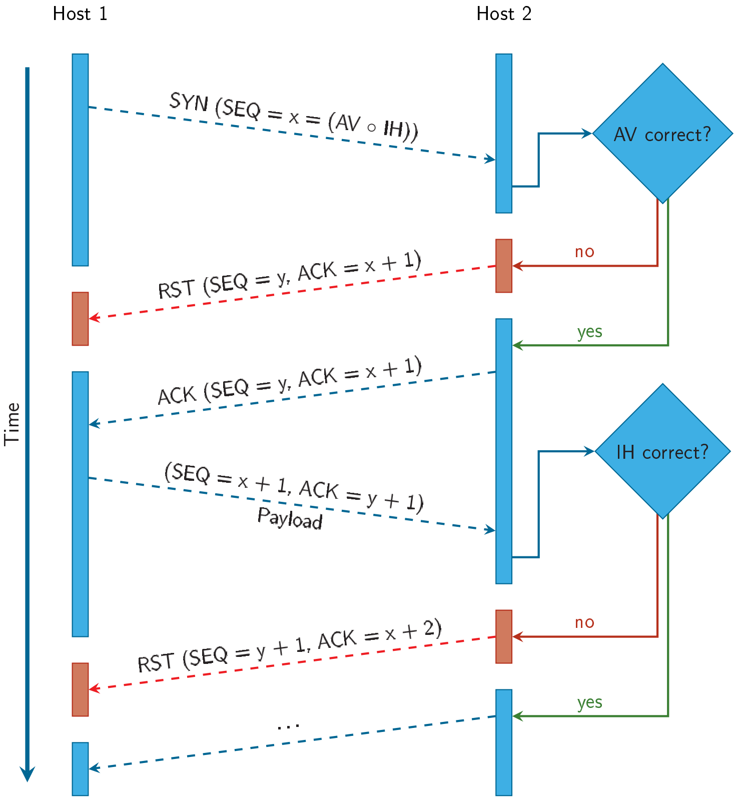
TCP Payload Integrity Protector IH

$\mathrm{IH} := h'(S \circ p)$

Authentication Security Token AV

$\mathrm{AV} := h((IP_d, P_d, T, \mathrm{IH}), S)$

- $\mathrm{ISN} := \mathrm{AV} \circ \mathrm{IH}$


Host 1
Host 2
Time
SYN (SEQ = x = (AV ∘ IH))
AV correct?
no
RST (SEQ = y, ACK = x + 1)
yes
ACK (SEQ = y, ACK = x + 1)
IH correct?
(SEQ = x + 1, ACK = y + 1)
Payload
no
RST (SEQ = y + 1, ACK = x + 2)
yes
...

Oh, but wait!

"Why should I care?"

Oh, but wait!

"Why should I care?"

"We'll all be terrorists for the last 15 minutes of our lives." –JA

A Matter of Life and Death: History Lesson — Irak War

Katharine Gun leaked memo from NSA agent Frank Koza in 2003 about an American effort to monitor the communications of six delegations to the United Nations who were undecided on authorizing the Iraq War and who were being fiercely courted by both sides:

> “As you’ve likely heard by now, the Agency is mounting a surge particularly **directed at the UN Security Council (UNSC)** members (minus US and GBR of course) for insights as to how to membership is reacting to the on-going debate RE: Iraq, plans to vote on any related resolutions, what related policies/negotiating positions they may be considering, alliances/dependencies, etc — the whole gamut of information that could give US policymakers an edge in **obtaining results favorable to US goals** or to head off surprises. In RT, that means a QRC surge effort to revive/create efforts **against** UNSC members Angola, Cameroon, Chile, Bulgaria and Guinea, as well as extra focus on Pakistan UN matters.”

A Matter of Life and Death: History Lesson — Copenhagen

> (TS//SI//REL) Analysts here at NSA, as well as our Second Party partners, will continue to provide policymakers with unique, timely, and valuable insights into key countries' preparations and goals for the conference, as well as deliberations within countries on climate change policies and negotiating strategies. A late November report detailed China's efforts (...). Another report provided advance details of the Danish proposal and their efforts to launch a "rescue plan" to save COP-15.
> (TS//SI//REL) Given such large participation (...), leaders and negotiating teams from around the world will undoubtedly be engaging in intense lastminute policy formulating; (...) – details of which are of great interest to our policymakers. (...), signals intelligence will undoubtedly play a significant role in keeping our negotiators as well informed as possible throughout the 2-week event.

Deputy SINIO for Economics and Global Issues (S17): "UN Climate Change Conference in Copenhagen – Will the Developed and Developing World Agree on Climate Change?", 7.12.2009.

A Matter of Life and Death: History Lesson — Copenhagen

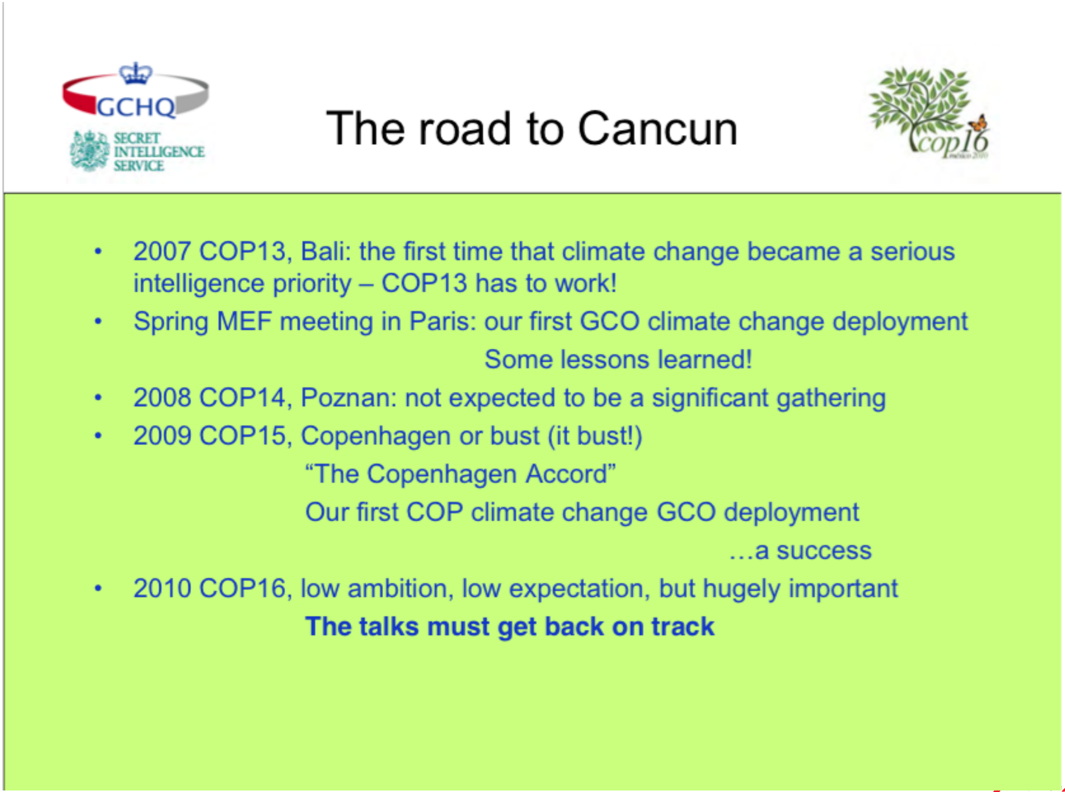
> Low targets, goals dropped: Copenhagen ends in failure.

The Guardian, 19.12.2009

> “They simply sat back, just as we had feared they would if they knew about our document,” one source said. “They made **no constructive statements**. Obviously, if they had known about our plans since the fall of 2009, it was in their interest to simply wait for our draft proposal to be brought to the table at the summit... I was often completely taken aback by what they knew.”

Russia Times: “NSA spied on Copenhagen UN climate summit – Snowden leak”, 30.1.2014

A success?


GCHQ
SECRET INTELLIGENCE SERVICE
cop16
méxico 2010

The road to Cancun

- 2007 COP13, Bali: the first time that climate change became a serious intelligence priority – COP13 has to work!
- Spring MEF meeting in Paris: our first GCO climate change deployment

  Some lessons learned!
- 2008 COP14, Poznan: not expected to be a significant gathering
- 2009 COP15, Copenhagen or bust (it bust!)

  "The Copenhagen Accord"

  Our first COP climate change GCO deployment

  …a success
- 2010 COP16, low ambition, low expectation, but hugely important

  The talks must get back on track

Technical Cooperation

Bloomberg reports:

- US companies provide internal information to US secret services
- Companies from software, banking, communications hardware providers, network security firms
- Including technical specifications and **unpatched software vulnerabilities**
- In return, these **US companies** are given **access to intelligence information**
- Partners include: Microsoft, Intel, McAfee

We cannot trust any infrastructure provider.

Not Just Mass Surveillance

- ORBing is untargeted active attack
- Compromising standards and institutions also documented
- Full extent yet unknown

Not Just Mass Surveillance

- ORBing is untargeted active attack
- Compromising standards and institutions also documented
- Full extent yet unknown

- What might spy agencies do if they are not from “friendly”, “democratic” and “liberal” allied states?
- How can research help secure networks to avoid totalitarianism?

⇒ DÉCENTRALISÉ

Not Just Mass Surveillance

- ORBing is untargeted active attack
- Compromising standards and institutions also documented
- Full extent yet unknown

- What might spy agencies do if they are not from “friendly”, “democratic” and “liberal” allied states?
- How can research help secure networks to avoid totalitarianism?

  ⇒ DÉCENTRALISÉ

- How can we even just stop mass surveillance?

Encryption to the Rescue?

Centralised Internet infrastructure is easily controlled:

- Number resources (IANA)
- Domain Name System (Root zone)
- DNSSEC root certificate
- X.509 CAs (HTTPS certificates)
- Major browser vendors (CA root stores!)

Encryption to the Rescue?

Centralised Internet infrastructure is easily controlled:

- Number resources (IANA)
- Domain Name System (Root zone)
- DNSSEC root certificate
- X.509 CAs (HTTPS certificates)
- Major browser vendors (CA root stores!)

Encryption will not help if PKI is compromised!

The GNU Name System[2]

Properties of GNS

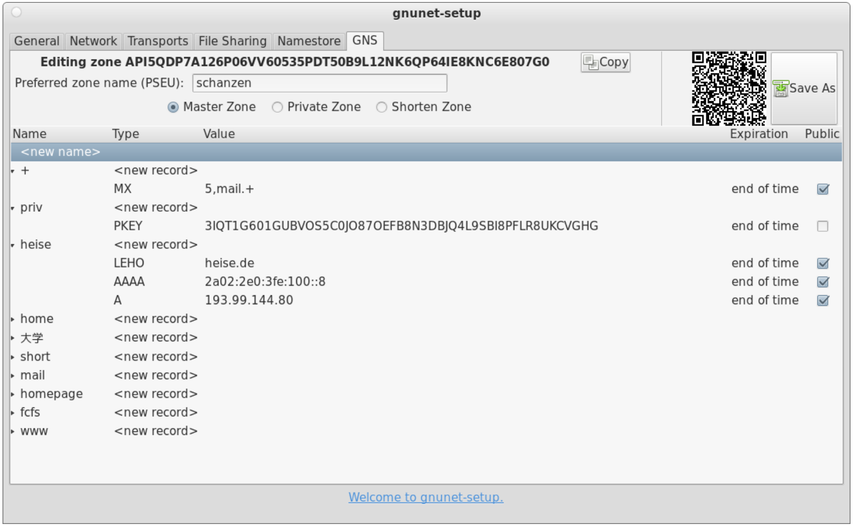
- Decentralised name system with secure memorable names
- Delegation used to achieve transitivity
- Also supports globally unique, secure identifiers
- Achieves query and response privacy
- Provides alternative public key infrastructure
- Interoperable with DNS

New applications enabled by GNS

- Name services hosted in P2P networks
- Name users in decentralised social networking applications

[2] Joint work with Martin Schanzenbach and Matthias Wachs

Zone management: like in DNS



gnunet-setup

General | Network | Transports | File Sharing | Namestore | GNS

Editing zone API5QDP7A126P06VV60535PDT50B9L12NK6QP64IE8KNC6E807G0 Copy

Preferred zone name (PSEU): schanzen

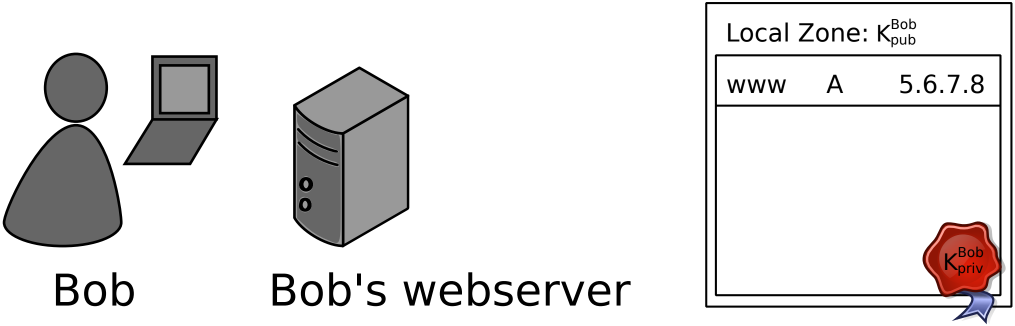
● Master Zone ○ Private Zone ○ Shorten Zone

Save As

Name	Type	Value	Expiration	Public
<new name>				
▾ +	<new record>			
	MX	5,mail.+	end of time	☑
▾ priv	<new record>			
	PKEY	3IQT1G601GUBVOS5C0JO87OEFB8N3DBJQ4L9SBI8PFLR8UKCVGHG	end of time	☐
▾ heise	<new record>			
	LEHO	heise.de	end of time	☑
	AAAA	2a02:2e0:3fe:100::8	end of time	☑
	A	193.99.144.80	end of time	☑
▸ home	<new record>			
▸ 大学	<new record>			
▸ short	<new record>			
▸ mail	<new record>			
▸ homepage	<new record>			
▸ fcfs	<new record>			
▸ www	<new record>			

Welcome to gnunet-setup.

Name resolution in GNS



Bob

Bob's webserver

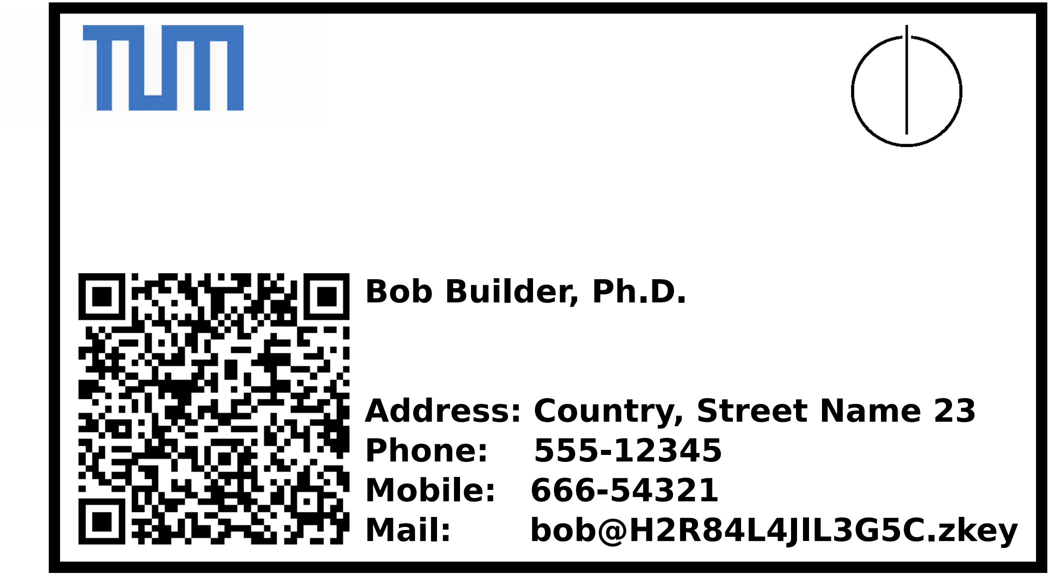
Local Zone: K_{pub}^{Bob}

www	A	5.6.7.8

K_{priv}^{Bob}

- Bob can locally reach his webserver via **www.gnu**

Secure introduction

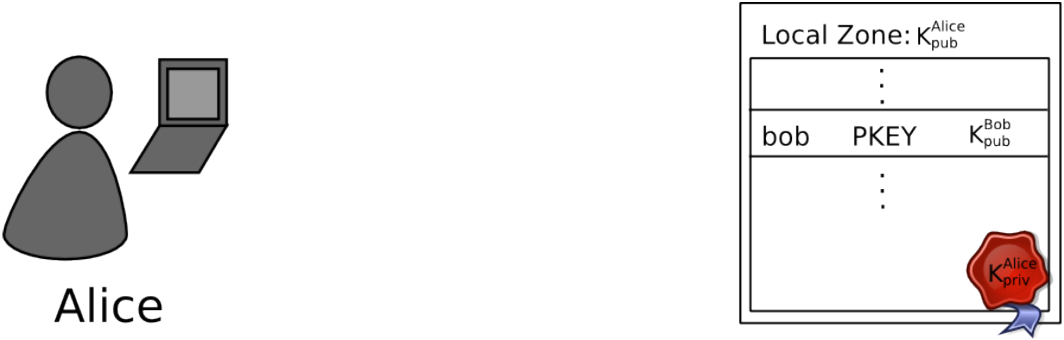


Bob Builder, Ph.D.

Address: Country, Street Name 23
Phone: 555-12345
Mobile: 666-54321
Mail: bob@H2R84L4JIL3G5C.zkey

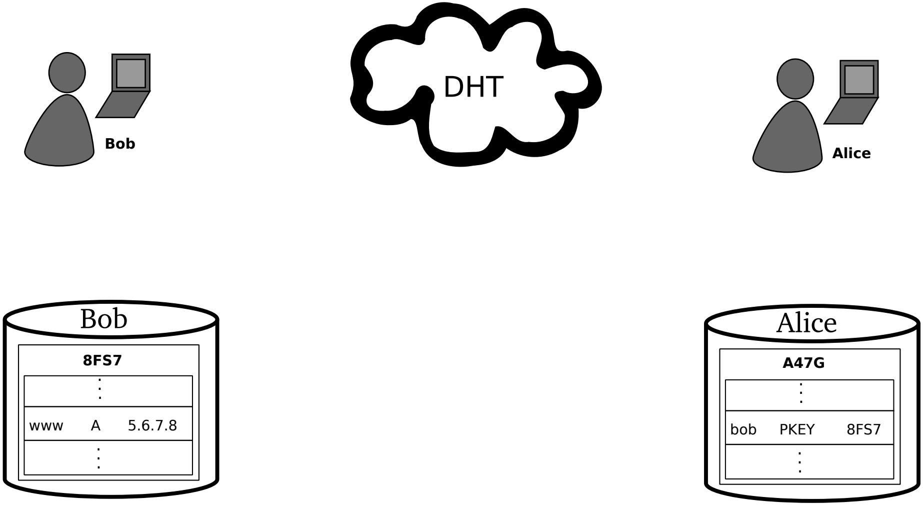
- Bob gives his public key to his **friends**, possibly via QR code

Delegation



- ▶ Alice learns Bob's public key
- ▶ Alice creates delegation to zone K_{pub}^{Bob} under label **bob**
- ▶ Alice can reach Bob's webserver via **www.bob.gnu**

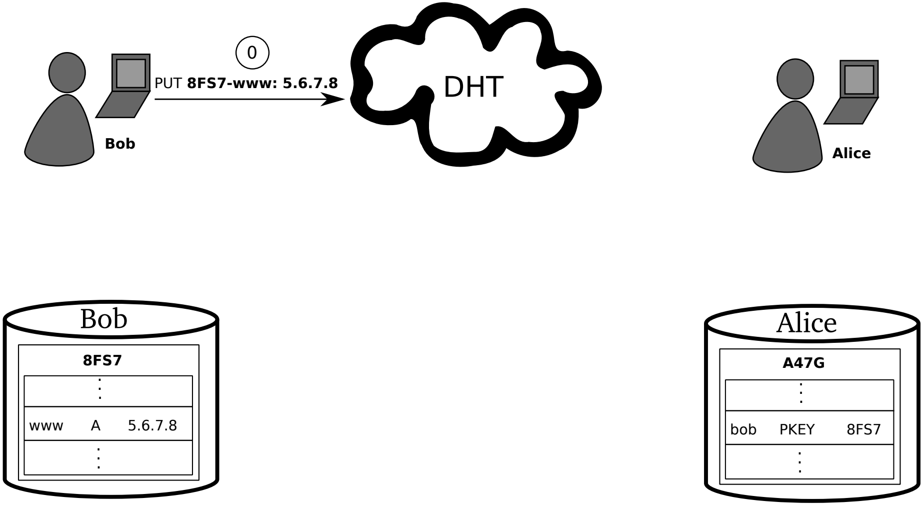
Name resolution



8FS7		
⋮		
www	A	5.6.7.8
⋮		

A47G		
⋮		
bob	PKEY	8FS7
⋮		

Name resolution



0

PUT **8FS7-www: 5.6.7.8**

DHT

Bob

Alice

Bob

8FS7

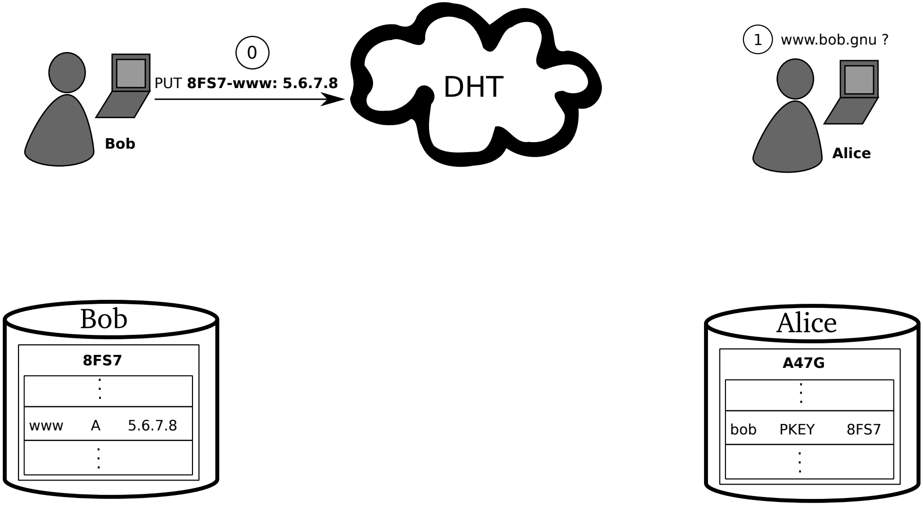
	⋮	
www	A	5.6.7.8
	⋮	

Alice

A47G

	⋮	
bob	PKEY	8FS7
	⋮	

Name resolution



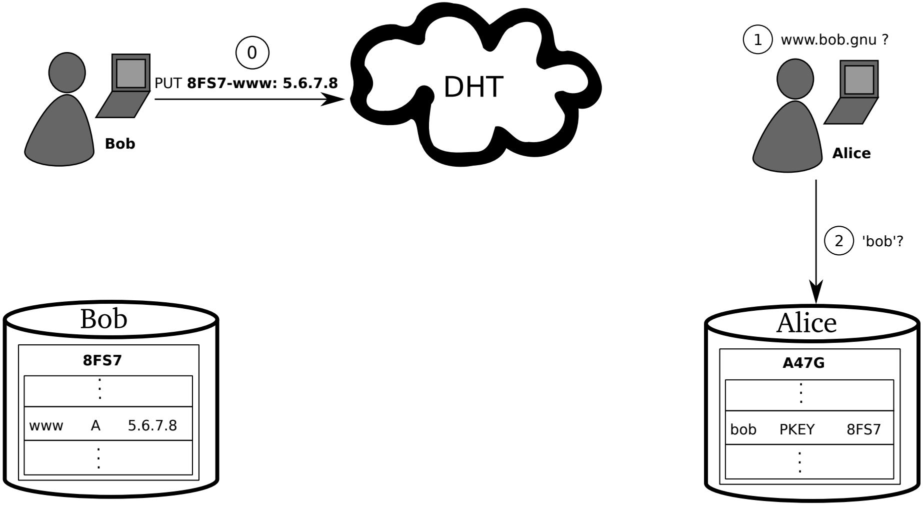
8FS7

	⋮	
www	A	5.6.7.8
	⋮	

A47G

	⋮	
bob	PKEY	8FS7
	⋮	

Name resolution



0 PUT **8FS7-www: 5.6.7.8**

DHT

1 www.bob.gnu ?

Bob

Alice

2 'bob'?

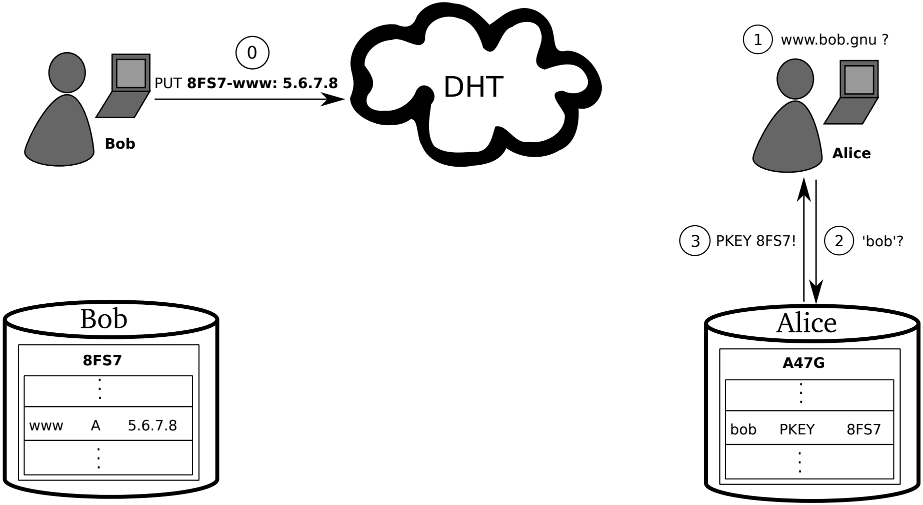
Bob

8FS7		
	⋮	
www	A	5.6.7.8
	⋮	

Alice

A47G		
	⋮	
bob	PKEY	8FS7
	⋮	

Name resolution



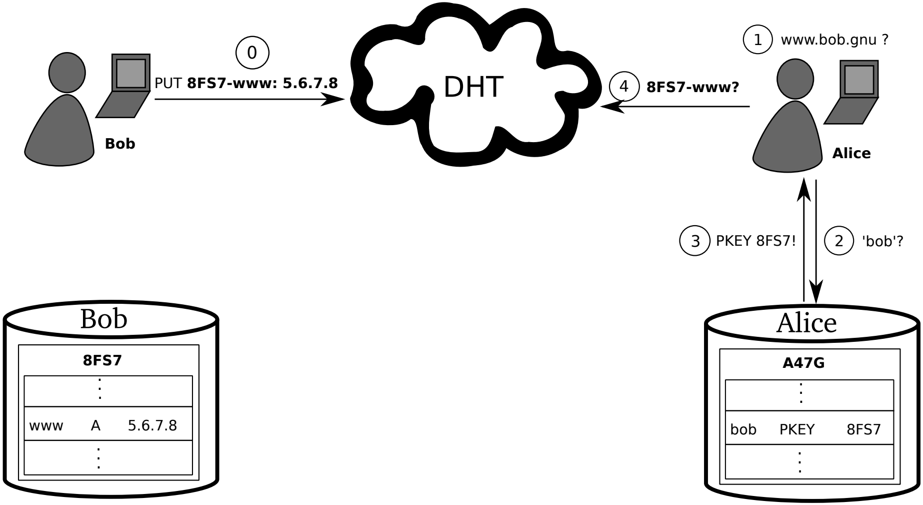
8FS7

	⋮	
www	A	5.6.7.8
	⋮	

A47G

	⋮	
bob	PKEY	8FS7
	⋮	

Name resolution



0 PUT **8FS7-www: 5.6.7.8**

DHT

Bob

Alice

1 www.bob.gnu ?

2 'bob'?

3 PKEY 8FS7!

4 **8FS7-www?**

Bob

8FS7

⋮

www	A	5.6.7.8

⋮

Alice

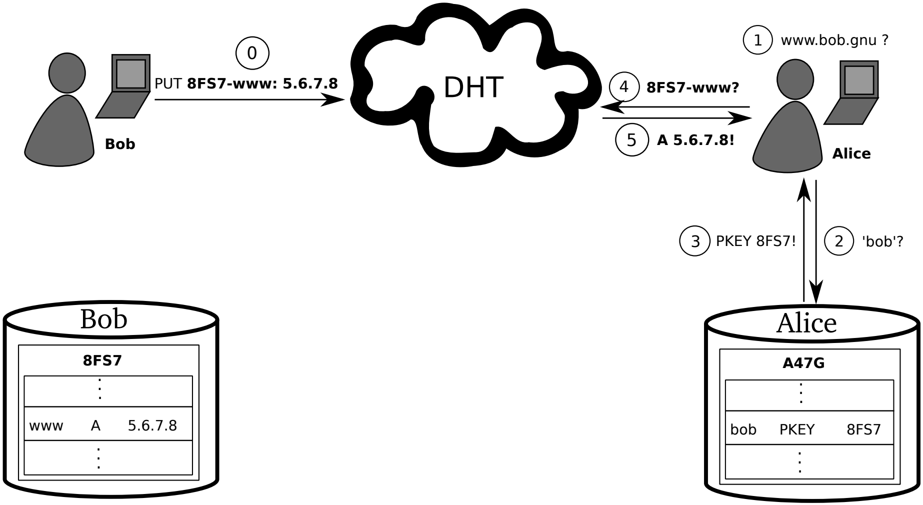
A47G

⋮

bob	PKEY	8FS7

⋮

Name resolution



Bob

8FS7

	⋮	
www	A	5.6.7.8
	⋮	

Alice

A47G

	⋮	
bob	PKEY	8FS7
	⋮	

Query privacy: terminology

G generator in ECC curve, a point

n size of ECC group, $n := |G|$, n prime

x private ECC key of zone ($x \in \mathbb{Z}_n$)

P public key of zone, a point $P := xG$

l label for record in a zone ($l \in \mathbb{Z}_n$)

$R_{P,l}$ set of records for label l in zone P

$q_{P,l}$ query hash (hash code for DHT lookup)

$B_{P,l}$ block with encrypted information for label l in zone P published in the DHT under $q_{P,l}$

Query privacy: cryptography

Publishing records $R_{P,l}$ as $B_{P,l}$ under key $q_{P,l}$

$$
\begin{align}
h &:= H(l, P) \tag{1} \\
d &:= h \cdot x \mod n \tag{2} \\
B_{P,l} &:= S_d(E_{HKDF(l,P)}(R_{P,l})), dG \tag{3} \\
q_{P,l} &:= H(dG) \tag{4}
\end{align}
$$

Query privacy: cryptography

Publishing records $R_{P,l}$ as $B_{P,l}$ under key $q_{P,l}$

$$
\begin{aligned}
h &:= H(l, P) && (1)\\
d &:= h \cdot x \mod n && (2)\\
B_{P,l} &:= S_d(E_{HKDF(l,P)}(R_{P,l})), dG && (3)\\
q_{P,l} &:= H(dG) && (4)
\end{aligned}
$$

Searching for records under label l in zone P

$$
\begin{aligned}
h &:= H(l, P) && (5)\\
q_{P,l} &:= H(hP) = H(hxG) = H(dG) \Rightarrow \texttt{obtain } B_{P,l} && (6)\\
R_{P,l} &= D_{HKDF(l,P)}(B_{P,l}) && (7)
\end{aligned}
$$

Oh, but wait!

So now we have a decentralised PKI, we can encrypt...

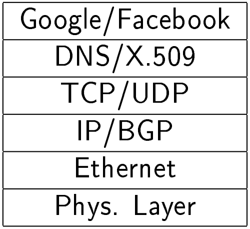
Didn't we forget something?

- Guardian: “The PRISM program allows the intelligence services direct access to the companies’ servers.”
- Cooperating providers: Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple

- Guardian: “The PRISM program allows the intelligence services direct access to the companies’ servers.”
- Cooperating providers: Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple
- PRISM enables real-time surveillance and access to stored content
- Data collected: E-mails, instant messages, videos, photos, stored data (likely files), voice chats, file transfers, video conferences, log-in times, and social network profiles
- Tiny part of NSA: $20 M budget

Context: The Vision

Internet



Google/Facebook

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Phys. Layer

Context: The Vision

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

Context: The Vision

Internet	
Google/Facebook	
DNS/X.509	
TCP/UDP	
IP/BGP	
Ethernet	CORE (OTR)
Phys. Layer	HTTPS/TCP/WLAN/...

Context: The Vision

Internet	
Google/Facebook	
DNS/X.509	
TCP/UDP	
IP/BGP	R^5N DHT
Ethernet	CORE (OTR)
Phys. Layer	HTTPS/TCP/WLAN/...

Context: The Vision

Internet	
Google/Facebook	
DNS/X.509	
TCP/UDP	CADET
IP/BGP	R^5N DHT
Ethernet	CORE (OTR)
Phys. Layer	HTTPS/TCP/WLAN/...

Context: The Vision

Internet	
Google/Facebook	
DNS/X.509	**GNU Name System**
TCP/UDP	CADET
IP/BGP	R^5N DHT
Ethernet	CORE (OTR)
Phys. Layer	HTTPS/TCP/WLAN/...

Context: The Vision

Internet

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

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

Context: The Vision

Internet	*GNUnet*
Google/Facebook	Applications
DNS/X.509	**GNU Name System**
TCP/UDP	CADET
IP/BGP	R^5N DHT
Ethernet	CORE (OTR)
Phys. Layer	HTTPS/TCP/WLAN/...

DÉCENTRALISÉ Mission

To Design and Build a Decentralised GNU Network
for Privacy and Security

DÉCENTRALISÉ Mission

To Design and Build a Decentralised GNU Network
for Privacy and Security

... and deploy incremental fixes on the Internet if applicable.

DÉCENTRALISÉ Research and Development Agenda

Make decentralised systems:

- faster, more scalable
- easier to develop, deploy and use
- easier to evolve and extend
- secure (privacy-preserving, censorship-resistant, available, ...)

by:

- designing secure network protocols
- implementing secure software following and evolving best practices
- creating tools to support developers
- evaluating the system in the real world

DÉCENTRALISÉ Plans

Focus: Secure Decentralised Networking

- DISSENT — Social networking for dissenters (or journalists)
- PRIVATEER — Anti-PRISM H2020 submission (TUM, UiO, OII, FSFE, CEA, CIJ)
- REUTERS — news distribution (related: Anne-Marie Kermarrec & GOSSPLE)
- TALER — Taxable Anonymous Libre Electronic Reserves
- SMC — voting, resource allocation, constraint solving, optimization

Edge: Defense in Depth

- Secure programming
- System security
- Operational security
- Useable security

Conclusion

- Decentralization is necessary:
  - Centralised infrastructure is a juicy target for crackers
  - Centralised computation enables totalitarian control
  - Centralised data storage enables mass surveillance (PRISM)

Conclusion

- Decentralization is necessary:
  - Centralised infrastructure is a juicy target for crackers
  - Centralised computation enables totalitarian control
  - Centralised data storage enables mass surveillance (PRISM)
- Decentralization creates challenges for research:
  - Privacy-enhancing network protocol design
  - Secure software implementations
  - Software engineering and system architecture
  - Programming languages and tool support
  - Usability and operational security

Do you have any questions?

References:

- Julian Kirsch. *Improved Kernel-Based Port-Knocking in Linux*. **Master's Thesis (TUM)**, 2014.
- Matthias Wachs, Martin Schanzenbach and Christian Grothoff. *A Censorship-Resistant, Privacy-Enhancing and Fully Decentralised Name System*. **13th International Conference on Cryptology and Network Security (CANS)**, 2014.
- Matthias Wachs, Martin Schanzenbach and Christian Grothoff. *On the Feasibility of a Censorship Resistant Decentralised Name System*. **6th International Symposium on Foundations & Practice of Security**, 2013.
- 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. s
- Bart Polot and Christian Grothoff. *CADET: Confidential Ad-Hoc Decentralised End-to-End Transport*. **MedHocNet**, 2014.
- Gabor Toth. *Design of a Social Messaging System Using Stateful Multicast*. **Master's Thesis (UVA)**, 2013.
- Nathan Evans and Christian Grothoff. *R^5N. Randomized Recursive Routing for Restricted-Route Networks*. **5th International Conference on Network and System Security**, 2011.