The Internet: We deserve a GNU one!

Christian Grothoff

June 2, 2018

“The means of defense against foreign danger historically have become the instruments of tyranny at home.” –James Madison
The Internet Architecture Model

Design theory: “rough consensus and running code”

- Application Protocols
- Transport Protocols (TCP/UDP)
- Internet Protocol (IP)
- Network Protocols

The IETF culture requires that new layers provide a protocol specification and at least two or three running implementations.

Likely, the four layer model will not grow in complexity (unless the internet does first.)
1. **Internet communication must continue despite loss of networks or gateways.**

2. The Internet must support multiple types of communications service.

3. The Internet architecture must accommodate a variety of networks.

4. The Internet architecture must permit *distributed management* of its resources.

5. The Internet architecture must be cost effective.

6. The Internet architecture must permit host attachment with a low level of effort.

7. **The resources used in the internet architecture must be accountable.**
Mass Surveillance
(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)
“Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.”

—Bundesverfassungsgericht zum Volkszählungsurteil
Legitimizing Surveillance
Legitimacy

Effective governance uses the appearance of legitimacy to justify their actions:
- Voting legitimizes sham democracies
- Laws legitimize the executive protecting the status quo
Legitimacy

Effective governance uses the appearance of legitimacy to justify their actions:

- Voting legitimizes sham democracies
- Laws legitimize the executive protecting the status quo
- Strategy of tension (counter insurgency tactics) legitimizes the deep state
Effective governance uses the appearance of legitimacy to justify their actions:

▶ Voting legitimizes sham democracies
▶ Laws legitimize the executive protecting the status quo
▶ Strategy of tension (counter insurgency tactics) legitimizes the deep state

Italian terrorist Vincenzo Vinciguerra explained about the strategie of tension in Italy:

“Man musste Zivilisten angreifen, (...), unschuldige Menschen, unbekannte Menschen, die weit weg vom politischen Spiel waren. Der Grund dafür war einfach. Die Anschläge sollten das italienische Volk dazu bringen, den Staat um größere Sicherheit zu bitten. Diese politische Logik liegt all den Massakern und Terroranschlägen zu Grunde, welche ohne richterliches Urteil bleiben, weil der Staat sich ja nicht selber verurteilen kann.”

Commercial tools: The crime fighting genie!

Warum ist Überwachung gerechtfertigt?

"Wir sind die Guten." —Die Anstalt
Risks of Mass Surveillance
Societal control technology: Analytics

SKYNET: Applying Advanced Cloud-based Behavior Analytics

A Collaborative Project by S2I, R6, T12, T14, SSG, and S22

Presenters: S2i51, R66F
Statistics

- mathematical techniques for drawing general conclusions from data samples
- means, medians, distributions, samples, significance, bias
- resulting aggregates may have meaning, or not
- no hard assurances about individual inputs, only probabilities
We have too much (statistical) data for humans to determine which ones have meaning, so:

- Ask computer to figure out which inputs matter!
- Different techniques:
  - Supervised learning: given example inputs and desired outputs, derive “general rule”
  - Unsupervised learning: find hidden structure in data
  - Reinforcement learning: algorithm selects actions, receives feedback based on result(s)
- Shared outcome: data in, statistical predictors out
Big Data

- “big” = too large for “standard” methods
- uses parallel-processing (CPU and data storage) – “Cloud”
- focus on decision-making based on quantitative information
- commercially use: model customers to increase sales
Cloud Analytic Building Blocks

- Travel Patterns
  - Travel phrases (Locations visited in given timeframe)
  - Regular/repeated visits to locations of interest
- Behavior-Based Analytics
  - Low use, incoming calls only
  - Excessive SIM or Handset swapping
  - Frequent Detach/Power-down
  - Courier machine learning models
- Other Enrichments
  - Travel on particular days of the week
  - Co-travelers
  - Similar travel patterns
  - Common contacts
  - Visits to airports
  - Other countries
  - Overnight trips
  - Permanent move
RT-RG Analytics

Meetings – who is at the same cellid at the same time as the potential courier at the destination city?...Multiple times.

Sidekicks – is there a pair traveling together to the destination city?
From GSM metadata, we can measure aspects of each selector’s pattern-of-life, social network, and travel behavior.
This presentation describes our search for AQSL couriers using behavioral profiling

Behavioral Feature Extraction

Cross Validation Experiment on AQSL Couriers

Preliminary SIGINT Findings
Counting unique UCELLIDs shows that couriers travel more often than typical Pakistani selectors.
By examining multiple features at once, we can see some indicative behaviors of our courier selectors.
Statistical algorithms are able to find the couriers at very low false alarm rates, if we’re allowed to miss half of them.

Random Forest Classifier

- 7 MSISDN/IMSI pairs
- Hold each pair out and then try to find them after learning how to distinguish remaining couriers from other Pakistanis (using 100k random selectors here)
- Assume that random draws of Pakistani selectors are nontargets
- 0.18% False Alarm Rate at 50% Miss Rate
We’ve been experimenting with several error metrics on both small and large test sets

<table>
<thead>
<tr>
<th>Training Data</th>
<th>Classifier</th>
<th>Features</th>
<th>100k Test Selectors</th>
<th>55M Test Selectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Random</td>
<td>None</td>
<td>False Alarm Rate at 50% Miss Rate</td>
<td>Mean Reciprocal Rank</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>50%</td>
<td>1/23k (simulated)</td>
</tr>
<tr>
<td>Known Couriers</td>
<td>Centroid</td>
<td>All</td>
<td>20%</td>
<td>1/18k</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>43%</td>
<td>1/27k</td>
</tr>
<tr>
<td>+ Anchory Selectors</td>
<td>Random Forest</td>
<td>Outgoing</td>
<td>0.18%</td>
<td>1/9.9</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.008%</td>
<td>1/14</td>
</tr>
</tbody>
</table>

Random Forest trained on Known Couriers + Anchory Selectors:

- 0.008% false alarm rate at 50% miss rate
- 46x improvement over random performance when evaluating its tasked precision at 100
Preliminary results indicate that we’re on the right track, but much remains to be done.

Cross Validation Experiment:
- Random Forest classifier operating at 0.18% false alarm rate at 50% miss
- Enhancing training data with Anchory selectors reduced that to 0.008%
- Mean Reciprocal Rank is ~1/10

Preliminary SIGINT Findings:
- Behavioral features helped discover similar selectors with “courier-like” travel patterns
- High number of tasked selectors at the top is hopefully indicative of the detector performing well “in the wild”
192 Million people live in Pakistan.
▶ 0.18% of the Pakistani population = 343,800 innocent citizens
▶ 0.008% of the Pakistani population = 15,280 innocent citizens
192 Million people live in Pakistan.

- 0.18% of the Pakistani population = 343,800 innocent citizens
- 0.008% of the Pakistani population = 15,280 innocent citizens

This is with half of AQSL couriers surviving the genocide.

“We kill based on metadata.”

—Michael Hayden (former NSA & CIA director)
The NSA mathematician’s presentation only gives the percentages.
The NSA mathematician’s presentation only gives the percentages.

Compartmentalization is an unconscious psychological defense mechanism used to avoid cognitive dissonance, or the mental discomfort and anxiety caused by a person’s having conflicting values, cognitions, emotions, beliefs, etc. within themselves.
"Angela Merkel lässt sich sehr stark von der Meinungsforschung leiten. Das zeigen Umfragen im Auftrag des Bundespresseamtes, die der SPIEGEL ausgewertet hat. Sätze der Demoskopen schafften es fast wortgleich in eine Regierungserklärung."

http://www.spiegel.de/politik/deutschland/angela-merkel-meinungsforscher-beeinflussen-arbeit-der-kanzlerin-html
"Angela Merkel lässt sich sehr stark von der Meinungsforschung leiten. Das zeigen Umfragen im Auftrag des Bundespresseamtes, die der SPIEGEL ausgewertet hat. Sätze der Demoskopen schafften es fast wortgleich in eine Regierungserklärung."

http://www.spiegel.de/politik/deutschland/angela-merkel-meinungsforscher-beeinflussen-arbeit-der-kanzlerin.html

"Germany is a digitally failed state." —Sasha Lobo
Surveillance is just step 1

Let’s look at how the US professionals do it...
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.)

Hacker
Enumerate (Network)
Scan (Services)
Operating Systems
Versions
Domain Names

Victim

Reconnaissance  Infection  Command and Control  Exfiltration
Infection

Email with Attachment or Link

Special Packets to Exploit Services

Hacker

Victim

Use Login Credentials

Bad Web Site

Reconnaissance  Infection  Command and Control  Exfiltration
Command and Control

Push Tools and Send Commands
(Tasking, Survey, etc.)

Beacons and Responses

Reconnaissance  Infection  Command and Control  Exfiltration
Exfiltration

Exfil using known and custom protocols
(Known: HTTP, SMTP, ICMP, FTP, etc)

Hacker

Victim

Reconnaissance  Infection  Command and Control  Exfiltration
Exfiltration is just step 4...

Let’s look at how the IT professionals do it...
```python
def content(*args):
    hash = [args].flatten.first || {}

    process = hash[:process] || ["Explorer.exe\0", "Firefox.exe\0", "Chrome.exe\0"][].sample
    process.encode!("US-ASCII")

    path = hash[:path] || ["C:\\Utenti\\pippo\\pedoporno.mpg", "C:\\Utenti\\pluto\\Documenti\\childporn.avi", "C:\\secrets\\bomb\n"
    path = path.to_utf16le_binary_null

    content = StringIO.new
    t = Time.now.getutc
    content.write [t.sec, t.min, t.hour, t.mday, t.mon, t.year, t.wday, t.yday, t.isdst ? 0 : 1].pack('l*')
    content.write process
    content.write [ 0 ].pack('L') # size hi
    content.write [ hash[:size] || 123456789 ].pack('L') # size lo
    content.write [ 0x80000000 ].pack('L') # access mode
    content.write path
    content.write [ ELEM_DELIMITER ].pack('L')
    content.string
```

State Surveillance: Benefits and Risks
That was fun, let’s scale it up

Let’s look at how the UK professionals do it...
2.3 (...) Generally, the language of JTRIG’s operations is characterised by terms such as “discredit”, promote “distrust”, “dissuade”, “deceive”, “disrupt”, “delay”, “deny”, “denigrate/degrade”, and “deter”.

EFFECTS: Definition

• “Using online techniques to make something happen in the real or cyber world”

• Two broad categories:
  - Information Ops (influence or disruption)
  - Technical disruption

• Known in GCHQ as Online Covert Action

• The 4 D’s: Deny / Disrupt / Degrade / Deceive
Discredit a target

- Set up a honey-trap
- Change their photos on social networking sites
- Write a blog purporting to be one of their victims
- Email/text their colleagues, neighbours, friends etc
Discredit a company

- Leak confidential information to companies / the press via blogs etc
- Post negative information on appropriate forums
- Stop deals / ruin business relationships
“3.2 Theories and research in the field of social psychology may prove particularly useful for informing JTRIG’s effects and online HUMINT operations. The following topics would be particularly relevant for social influence:

▶ Social cognition (including social perception and attribution)
▶ Attitudes
▶ Persuasive communications
▶ Conformity
▶ Obedience
▶ Interpersonal relationships
▶ Trust and distrust
▶ Psychological profiling

In addition, the application of social psychological ideas to marketing and advertising would be useful.” —Behavioural Science Support for JTRIG’s Effects and Online HUMINT Operations (2011)

Mirroring
People copy each other while in social interaction with them.
- body language
- language cues
- expressions
- eye movements
- emotions

Accommodation
Adjustment of speech, patterns, and language towards another person in communications
- People in conversation tend to converge
- Depends on empathy and other personality traits
- Possibility of over-accommodation and end up looking condescending

Mimicry
adoption of specific social traits by the communicator from the other participant

Question: Can I game this?
DISRUPTION
Operational Playbook

- Infiltration Operation
- Ruse Operation
- Set Piece Operation
- False Flag Operation
- False Rescue Operation
- Disruption Operation
- Sting Operation
Identifying & Exploiting fracture points

Things that push a group together:
- Shared opposition
- Shared ideology
- Common beliefs

Tension

Things that pull a group apart:
- Personal power
- Pre-existing cleavages
- Competition
- Ideological differences

State Surveillance: Benefits and Risks
10 Principles for Influence

- The Time Principle
- The Deception Principle
- The Dishonesty Principle
- The Herd Principle
- The Consistency Principle
- The Reciprocity Principle
- The Need and Greed Principle
- The Social Compliance/Authority Principle
- The Distraction Principle
- The Flattery Principle
The Distraction principle

“While you are distracted by what retains your interest, hustlers can do anything to you and you won’t notice.”
—Frank Stajano, Paul Wilson, UCAM-CL-TR-754
The Herd principle

“Even suspicious marks will let their guard down when everyone next to them appears to share the same risks. Safety in numbers? Not if they’re all conspiring against you.”
—Frank Stajano, Paul Wilson, UCAM-CL-TR-754
“Anything illegal you do will be used against you by the fraudster, making it harder for you to seek help once you realize you’ve been had.”
—Frank Stajano, Paul Wilson, UCAM-CL-TR-754
The Deception principle

“Things and people are not what they seem. Hustlers know how to manipulate you to make you believe that they are.”
—Frank Stajano, Paul Wilson, UCAM-CL-TR-754
The Need and Greed principle

“Your needs and desires make you vulnerable. Once hustlers know what you really want, they can easily manipulate you.”
—Frank Stajano, Paul Wilson, UCAM-CL-TR-754
The Time principle

“When you are under time pressure to make an important choice, you use a different decision strategy. Hustlers steer you towards a strategy involving less reasoning.”
—Frank Stajano, Paul Wilson, UCAM-CL-TR-754
The Social Compliance principle / Authority

“Society trains people not to question authority. Hustlers exploit this ‘suspension of suspiciousness’ to make you do what they want.”
—Frank Stajano, Paul Wilson, UCAM-CL-TR-754

This is related to Cialdini’s principle of persuasion on Authority:

“People respect authority. They want to follow the lead of real experts. Business titles, impressive clothing, and even driving an expensive, high-performing automobile are proven factors in lending credibility to any individual.” —Dr. Robert Cialdini
Reciprocity

“The implication is you have to go first. Give something: give information, give free samples, give a positive experience to people and they will want to give you something in return.” —Dr. Robert Cialdini
“People do not like to back out of deals. We’re more likely to do something after we’ve agreed to it verbally or in writing. People strive for consistency in their commitments. They also prefer to follow pre-existing attitudes, values and actions.” —Dr. Robert Cialdini
Liking — The Flattery Principle (?)

“People prefer to say ‘yes’ to those they know and like.” —Dr. Robert Cialdini
JTRIG “Collection” Tools

**AIRWOLF**  Youtube profile, command and video *collection*.

**BIRDSKITE**  Twitter monitoring and profile *collection*.

**SPRING BISHOP**  **Find** *private* photographs of targets on Facebook.

**FUSEWIRE**  Provides 24/7 *monitoring* of forums for target postings/online activity. Also allows *staggered postings* to be made.

**BIRDSONG**  Automated *posting* of Twitter updates.

**SYLVESTER**  Framework for *automated interaction* / alias management on online social networks.
JTRIG “Effects” Capabilities

**CLEAN SWEEP**  **Masquerade** Facebook wall posts for individuals or entire countries

**BOMB BAY** is the capability to **increase** website hits/rankings.

**UNDERPASS**  **Change outcome** of online polls

**GESTATOR**  **amplification** of a given message, normally video, on popular multimedia websites.

**PITBULL** enabling **large scale delivery** of a tailored message to users of instant messaging services.

**BADGER**  **mass delivery** of email messaging to support an information operations campaign.

**WARPATH**  **mass delivery** of SMS messages to support an information operations campaign.

**CANNONBALL**  is the capability to **send repeated** text messages to a single target.

**BURLESQUE**  is the capability to **send spoofed** SMS text messages.

**SCRAPHEAP CHALLENGE**  **Perfect spoofing** of emails from Blackberry targets.
JTRIG “Effects” Capabilities

CHINESE FIRECRACKER overt brute login attempts against online forums.
TORNADO ALLEY delivery method that can silently extract and run an executable on a target’s machine.
SWAMP DONKEY silently locate files and encrypt them on a target’s machine.
ANGRY PIRATE permanently disables target’s account on their computer.
PREDATORS FACE Targeted denial of service against Web servers.
ROLLING THUNDER Distributed denial of service using P2P.
SILENT MOVIE Targeted denial of service against SSH servers.
VIPERS TONGUE silently denial of service calls on a Satellite or GSM phone.
NEWTONS CAT
The world is interdisciplinary

- Marketing
- Politics
- Psychology
- Computer science
- Statistics
- Warfare
- Gamification
- Espionage
Five-Eye Victims

- United Nations
- European Union
- UK (listed by GCHQ as an operations area!)
- Argentina (Falklands)
- Zimbabwe ("regime change")
- Africa (listed by GCHQ as a "country")
- Leaders of colonies (Hollande, Sarkozy, Merkel)
- Amnesty International
- Greenpeace
- Journalists (Spiegel, Wikileaks)
- Terrorists (Sebastian Hahn)
- Occupy activists
Five-Eye Victims

- United Nations
- European Union
- UK (listed by GCHQ as an operations area!)
- Argentina (Falklands)
- Zimbabwe (“regime change”)
- Africa (listed by GCHQ as a “country”)
- Leaders of colonies (Hollande, Sarkozy, Merkel)
- Amnesty International
- Greenpeace
- Journalists (Spiegel, Wikileaks)
- Terrorists (Sebastian Hahn)
- Occupy activists
- plus 9:10 unintended targets

\[\text{\textsuperscript{1}} \text{http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html}\]
Summary

GCHQ paid to train 150+ staff to perform a range of criminal acts:

- Technical: manipulate messages, censor access, spam with information
- Psychological: deprivation, emotional distress, deception, abuse of authority with victims in other countries but also domestic to further UK political agenda:
  - overthrow governments
  - stiffle dissent
  - provide economic advantages
The UK merely joins the club

- Salutin Putin: inside a Russian troll house
- Ukraine’s new online army in media war with Russia
- Congress vs BJP: The curious case of trolls and politics
- China’s Paid Trolls: Meet the 50-Cent Party

“Das ist das Geheimnis der Propaganda; den, den die Propaganda fassen will, ganz mit den Ideen der Propaganda zu durchtränken, ohne dass er überhaupt merkt, dass er durchtränkt wird.”

—Joseph Goebbels

“Propaganda techniques include: Using stereotypes; substituting names/labels for neutral ones; censorship or systematic selection of information; repetition; assertions without arguments; and presenting a message for and against a subject.”

—TOP SECRET JTRIG Report on Behavioural Science

http://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house
http://www.bbc.co.uk/monitoring/ukraines-new-online-army-in-media-war-with-russia
http://www.newstatesman.com/politics/politics/2012/10/china%E2%80%99s-paid-trolls-meet-50-cent-party
Legitimacy (Reprise)

So what about transnational organized crime?
So what about transnational organized crime?

Let’s start with the worst.
Terrorism

- A terrorist is someone who uses violence to create fear to achieve political objectives.
Terrorism

- A terrorist is someone who uses violence to create fear to achieve political objectives.

States

- Leaders of states have political objectives.
Terrorism

- A terrorist is someone who uses violence to create fear to achieve political objectives.

States

- Leaders of states have political objectives.

State Terrorism

- A state using violence to achieve political objectives.
- States may use violence abroad or domestically.
Terrorism

▶ A terrorist is someone who uses violence to create fear to achieve political objectives.

States

▶ Leaders of states have political objectives.

State Terrorism

▶ A state using violence to achieve political objectives.
▶ States may use violence abroad or domestically.

“To initiate a war of aggression [...] is the supreme international crime, only different from other war crimes in that it contains within itself the accumulated evil of all the others. To initiate a war of aggression is a crime that no political or economic situation can justify.”

–Declaration of the Nuremberg War Crimes Tribunal, 1945.
Violence

- Kinetic violence is old-fashioned (but still used).
Violence

- Kinetic violence is old-fashioned (but still used).
- Throwing entire countries into economic disarray and despair (fiscal waterboarding, overthrowing governments, causing civil war) is more cost-effective.
Violence

▶ Kinetic violence is old-fashioned (but still used).
▶ Throwing entire countries into economic disarray and despair (fiscal waterboarding, overthrowing governments, causing civil war) is more cost-effective.
What NOT to do.
Grundzüge von SCION

▶ Isolation des ISP-Zusammenschlusses nach Aussen
▶ “Security” (für DNS, BGP)
▶ Privacy ist kein Designziel
▶ Migration auf Level ISP, keine Änderungen beim Endnutzer
Wenn im Zuge der NSA-Affäre über ein “Schlandnetz” gesprochen werde, sei dieser Umbau zu einem nationalen Internet ohne Umgehungsmöglichkeiten für den Einzelnen eine Ausprägung des tiefen Staates. Neben dieser Verstaatlichung und der “Militarisierung des Internet” werde eine Strategie der “Cyber-Counterinsurgency” entwickelt: Hierbei geht es darum, das Netz als äußerst bedrohlich darzustellen, um die Zustimmung der Bevölkerung zu einschneidenden technischen Maßnahmen zu gewinnen. –Andreas Lehner
Geldspielgesetz

- Pretext
- Netzwerkzensur
- Technische Umsetzung
⇒ Schritt 1 für das Swissnet!
What to do?
“When governments fear the people, there is liberty. When the people fear the government, there is tyranny. The strongest reason for the people to retain the right to keep and bear arms is, as a last resort, to protect themselves against tyranny in government.”

—Thomas Jefferson
Modern arms

- Offensive: surveillance- and cracking-tools (“Staatstrojaner”)
- Defensive: privacy-enhancing technologies (encryption)
Supreme Alternatives Advertising
Let’s do something about it!
Design Choices for a Civil Network!

Internet Design Goals (David Clark, 1988)

1. Internet communication must continue despite loss of networks or gateways.
2. The Internet must support multiple types of communications service.
3. The Internet architecture must accommodate a variety of networks.
4. The Internet architecture must permit distributed management of its resources.
5. The Internet architecture must be cost effective.
6. The Internet architecture must permit host attachment with a low level of effort.
7. The resources used in the internet architecture must be accountable.

GNUnet Design Goals

1. GNUnet must be implemented as free software.
2. The GNUnet must only disclose the minimal amount of information necessary.
3. The GNUnet must be decentralised and survive Byzantine failures in any position in the network.
4. The GNUnet must make it explicit to the user which entities must be trustworthy when establishing secured communications.
5. The GNUnet must use compartmentalization to protect sensitive information.
6. The GNUnet must be open and permit new peers to join.
7. The GNUnet must be self-organizing and not depend on administrators.
8. The GNUnet must support a diverse range of applications and devices.
9. The GNUnet architecture must be cost effective.
10. The GNUnet must provide incentives for peers to contribute more resources than they consume.
# Let’s Implement It!

## Internet

<table>
<thead>
<tr>
<th>Google</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS/X.509</td>
</tr>
<tr>
<td>TCP/UDP</td>
</tr>
<tr>
<td>IP/BGP</td>
</tr>
<tr>
<td>Ethernet</td>
</tr>
<tr>
<td>Phys. Layer</td>
</tr>
</tbody>
</table>
Let's Implement It!

**Internet**

<table>
<thead>
<tr>
<th>Google</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS/X.509</td>
</tr>
<tr>
<td>TCP/UDP</td>
</tr>
<tr>
<td>IP/BGP</td>
</tr>
<tr>
<td>Ethernet</td>
</tr>
<tr>
<td>Phys. Layer</td>
</tr>
</tbody>
</table>

| HTTPS/TCP/WLAN/... |
Let’s Implement It!

### Internet

<table>
<thead>
<tr>
<th>Layer</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td></td>
</tr>
<tr>
<td>DNS/X.509</td>
<td></td>
</tr>
<tr>
<td>TCP/UDP</td>
<td></td>
</tr>
<tr>
<td>IP/BGP</td>
<td></td>
</tr>
<tr>
<td>Ethernet</td>
<td></td>
</tr>
<tr>
<td>Phys. Layer</td>
<td></td>
</tr>
<tr>
<td><strong>CORE (OTR)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>HTTPS/TCP/WLAN/...</strong></td>
<td></td>
</tr>
</tbody>
</table>
Let's Implement It!

<table>
<thead>
<tr>
<th>Internet</th>
<th>Google</th>
<th>DNS/X.509</th>
<th>TCP/UDP</th>
<th>IP/BGP</th>
<th>Ethernet</th>
<th>Phys. Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let's Implement It!

### Internet

<table>
<thead>
<tr>
<th>Level</th>
<th>Components</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>DNS/X.509</td>
<td>CADET (Axolotl+SCTP)</td>
</tr>
<tr>
<td>TCP/UDP</td>
<td>IP/BGP</td>
<td>R5N DHT</td>
</tr>
<tr>
<td>IP/BGP</td>
<td>Ethernet</td>
<td>CORE (OTR)</td>
</tr>
<tr>
<td>Ethernet</td>
<td>Phys. Layer</td>
<td>HTTPS/TCP/WLAN/...</td>
</tr>
</tbody>
</table>
Let’s Implement It!

<table>
<thead>
<tr>
<th>Internet</th>
<th>GNU Name System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>CADET (Axolotl+SCTP)</td>
</tr>
<tr>
<td>DNS/X.509</td>
<td>$R^5N$ DHT</td>
</tr>
<tr>
<td>TCP/UDP</td>
<td>CORE (OTR)</td>
</tr>
<tr>
<td>IP/BGP</td>
<td>HTTPS/TCP/WLAN/...</td>
</tr>
<tr>
<td>Ethernet</td>
<td></td>
</tr>
<tr>
<td>Phys. Layer</td>
<td></td>
</tr>
</tbody>
</table>
## Internet

<table>
<thead>
<tr>
<th>Google</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS/X.509</td>
<td>GNU Name System</td>
</tr>
<tr>
<td>TCP/UDP</td>
<td>CADET (Axolotl+SCTP)</td>
</tr>
<tr>
<td>IP/BGP</td>
<td>$R^5N$ DHT</td>
</tr>
<tr>
<td>Ethernet</td>
<td>CORE (OTR)</td>
</tr>
<tr>
<td>Phys. Layer</td>
<td>HTTPS/TCP/WLAN/...</td>
</tr>
</tbody>
</table>
Let’s Implement It!

<table>
<thead>
<tr>
<th>Internet</th>
<th>GNUnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>Applications</td>
</tr>
<tr>
<td>DNS/X.509</td>
<td>GNU Name System</td>
</tr>
<tr>
<td>TCP/UDP</td>
<td>CADET (Axolotl+SCTP)</td>
</tr>
<tr>
<td>IP/BGP</td>
<td>$R^5N$ DHT</td>
</tr>
<tr>
<td>Ethernet</td>
<td>CORE (OTR)</td>
</tr>
<tr>
<td>Phys. Layer</td>
<td>HTTPS/TCP/WLAN/...</td>
</tr>
</tbody>
</table>
Applications (being) built using GNUnet

- Anonymous and non-anonymous file-sharing
- IPv6–IPv4 protocol translator and tunnel
- GNU Name System: censorship-resistant replacement for DNS
- Conversation: secure, decentralised VoIP
- SecuShare, a social networking application
- GNU Taler: privacy-preserving payments
- ...

State Surveillance: Benefits and Risks
Modern economies need a currency.
Motivation

Modern economies need an online payment system.
Credit cards?

SWIFT/Mastercard/Visa are too transparent.
ZeroCoin/ZeroCash is a decentralized online currency
Designs offer fully decentralized transactions with full anonymity
ZeroCoin/ZeroCash is a decentralized online currency
Designs offer fully decentralized transactions with full anonymity

Is society ready for an anarchistic economy?
We can make cash **digital** and socially responsible.

〈Taler〉

Taxable, Anonymous, Libre, Practical, Resource Friendly
Architecture of GNU Taler

- **Exchange**
  - verify

  - withdraw coins

  - deposit coins

  - spend coins

- **Customer**

- **Merchant**

- **Auditor**
More tools and technologies exist

- Tor
- GnuPG
- OTR+XMPP
- Pond
- I2P
- ...

State Surveillance: Benefits and Risks
“Obedience is a direct form of social influence where an individual submits to, or complies with, an authority figure. Obedience may be explained by factors such as **diffusion of responsibility**, perception of the authority figure being **legitimate**, and **socialisation** (...). (...) Conversely, efforts to reduce obedience may be effectively based around **educating** people about the **adverse consequences of compliance**; encouraging them to **question authority**; and exposing them to **examples of disobedience**.”

—TOP SECRET JTRIG Report on Behavioural Science
Conclusion

- Computers have no sense of ethics.
- Code is stronger than law.

⇒ We need to be careful about which technology we adopt.
Conclusion

- Computers have no sense of ethics.
- Code is stronger than law.

⇒ We need to be careful about which technology we adopt.

We SHOULD:

- accept it as *positive* that law-enforcement cannot solve/prevent all crimes
- consider the economic and social *benefits* of having private information
- deploy technological systems that encode our ethical principles
Conclusion

- Computers have no sense of ethics.
- Code is stronger than law.

⇒ We need to be careful about which technology we adopt.

We SHOULD:
- accept it as *positive* that law-enforcement cannot solve/prevent all crimes
- consider the economic and social *benefits* of having private information
- deploy technological systems that encode our ethical principles

**AND**

We MUST defund the deep state and end its wars.
Questions?

Find more information at:

▶ [http://www.taler.net/](http://www.taler.net/)
▶ Slides will be at [http://grothoff.org/christian/](http://grothoff.org/christian/).