Netzwerksicherheit: Probleme und Lösungsansätze

Christian Grothoff

October 19, 2016

"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

Part I: Mass Surveillance

Fun with Mobile Phones

http://www.stealthgenie.com/ (6'2013)

NSA SKYNET


TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
SIGDEV
SKYNET: Applying Advanced Cloud-based Behavior Analytics
A Collaborative Project by S2I, R6, T12, T14, SSG, and S22
Presenters:
, S2I51
, R66F
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20370401
SIGINT Development
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

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

Machine Learning

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
  - Reinforecment learning: algorithm selects actions, receives feedback based on result(s)
- Shared outcome: data in, statistical predictors out

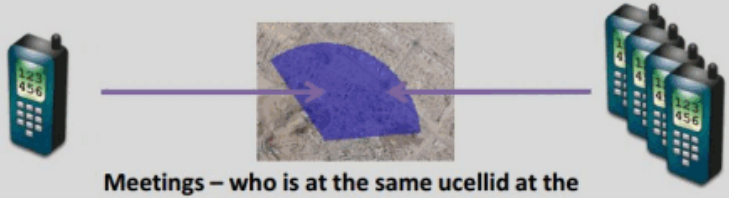
Big Data

- “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

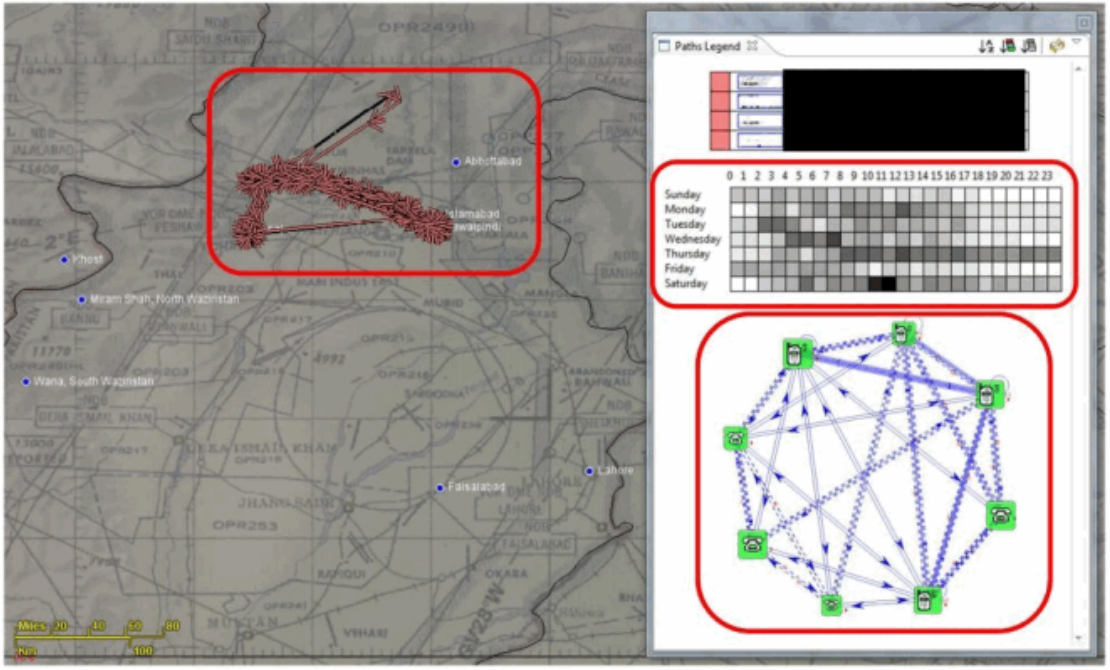
RT-RG Analytics



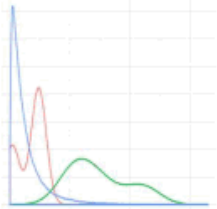
Meetings – who is at the same ucellid at the same time as the potential courier at the destination city?...Multiple times.

Sidekicks – is there a pair traveling together to the destination city?

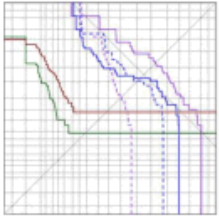
From GSM metadata, we can measure aspects of each selector's pattern-of-life, social network, and travel behavior



This presentation describes our search for AQSL couriers using behavioral profiling



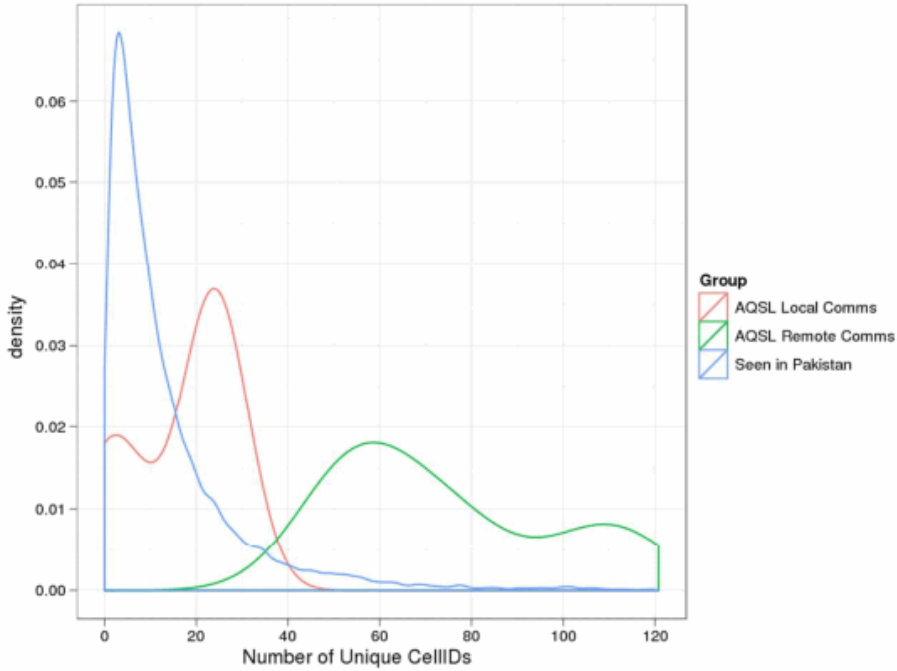
Behavioral Feature Extraction



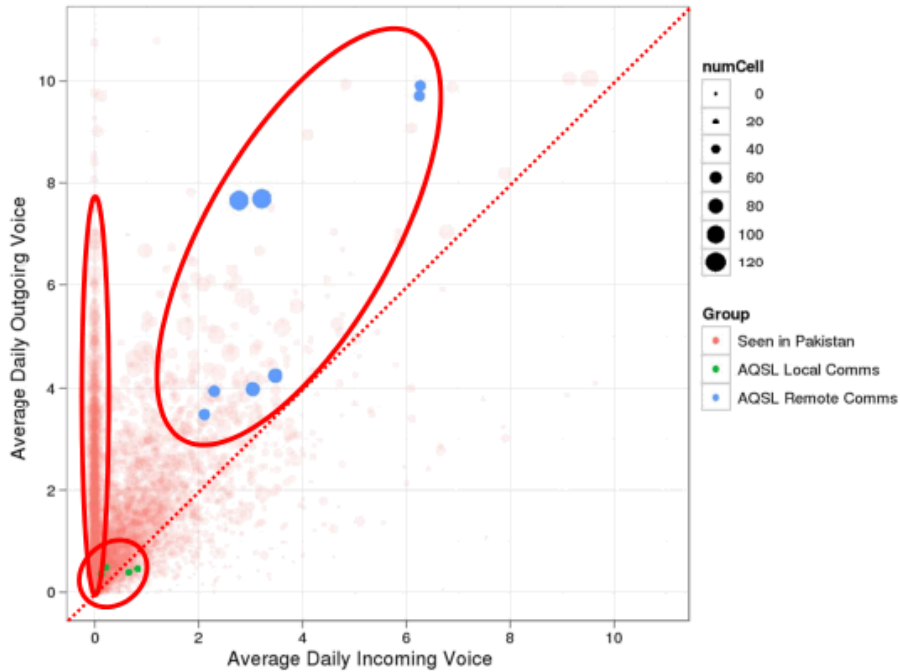
Cross Validation Experiment on AQSL Couriers

Preliminary SIGINT Findings

Counting unique UCELLIDs shows that couriers travel more often than typical Pakistani selectors



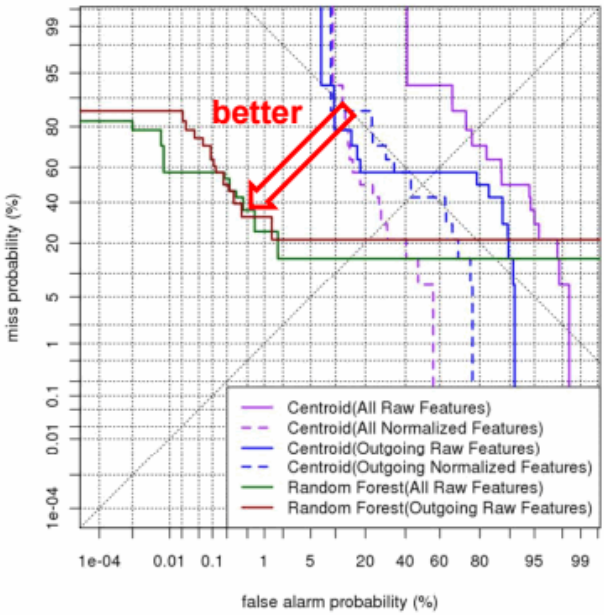
By examining multiple features at once, we can see some indicative behaviors of our courier selectors



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 fro n 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

Training Data	Classifier	Features	100k Test Selectors		55M Test Selectors	
			False Alarm Rate at 50% Miss Rate	Mean Reciprocal Rank	Tasked Selectors in Top 500	Tasked Selectors in Top 100
None	Random	None	50%	1/23k (simulated)	0.64 (active/Pak)	0.13 (active/Pak)
Known Couriers	Centroid	All	20%	1/18k		
		Outgoing	43%	1/27k		
	Random Forest		0.18%	1/9.9	5	1
+ Anchory Selectors			0.008%	1/14	21	6

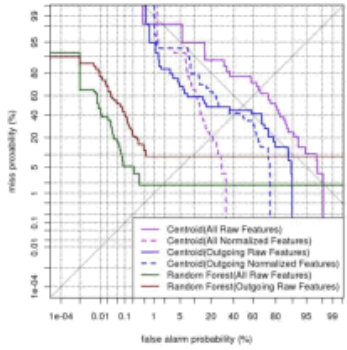
Random Forest trained on Known Couriers + Anchory Selectors:

- 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

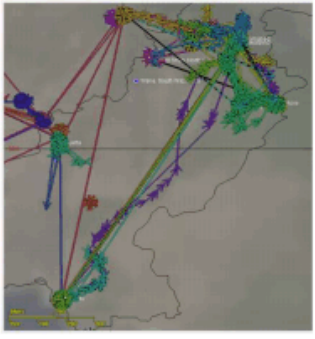
Cross Validation Experiment:

- 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

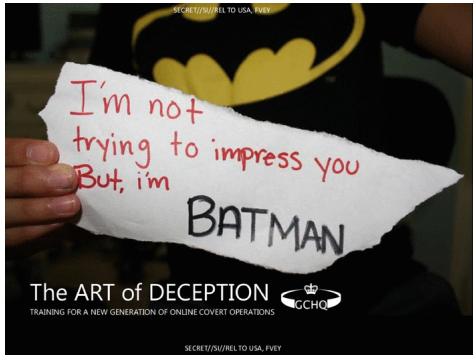
192 Million people live in Pakistan.

- 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)*

GCHQ Self-Portrait



A Technical Issue

Why do cell phones enable tracking?

Part II: Attacks

"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."

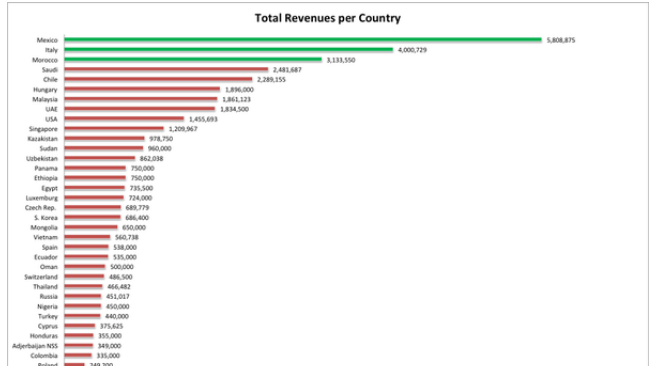
—Joseph Goebbels

Fun with the Internet

`http://www.hackingteam.it/` (4'2013)

Special Features in the RCS Code

```
11    def content(*args)
12      hash = [args].flatten.first || {}
13
14      process = hash[:process] || ["Explorer.exe\0", "Firefox.exe\0", "Chrome.exe\0"].sample
15      process.encode!("US-ASCII")
16
17      path = hash[:path] || ["C:\\Utenti\\pippo\\pedoporno.mpg", "C:\\Utenti\\pluto\\Documenti\\childporn.avi", "C:\\secrets\\bomb_
18      path = path.to_utf16le_binary_null
19
20      content = StringIO.new
21      t = Time.now.getutc
22      content.write [t.sec, t.min, t.hour, t.mday, t.mon, t.year, t.wday, t.yday, t.isdst ? 0 : 1].pack('l*')
23      content.write process
24      content.write [ 0 ].pack('L') # size hi
25      content.write [ hash[:size] || 123456789 ].pack('L') # size lo
26      content.write [ 0x80000000 ].pack('l') # access mode
27      content.write path
28      content.write [ ELEM_DELIMITER ].pack('L')
29      content.string
30    end
```



(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)

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)

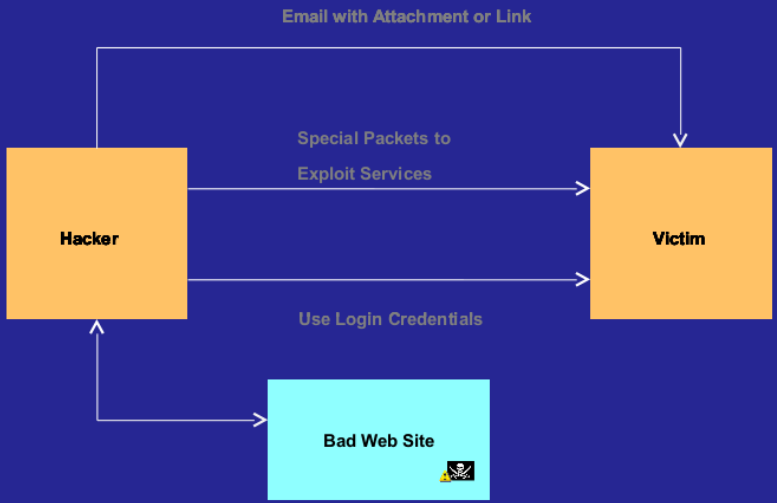
Operating Systems

Versions

Domain Names

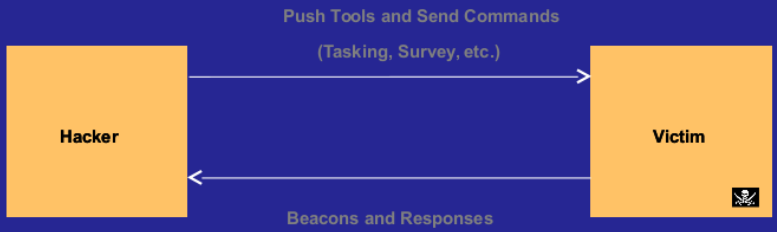
Reconnaissance Infection Command and Control Exfiltration

Infection



Reconnaissance Infection Command and Control Exfiltration

Command and Control



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**

Going Beyond Crime: Introducing the Joint Threat Research and Intelligence Group (JTRIG)

> *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".*

`http://www.statewatch.org/news/2015/jun/behavioural-science-support-for-jtrigs-effects.pdf`

JTRIG “Collection” Tools

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

BIRDSTRIKE 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

TOP SECRET//SI//REL TO USA, FVEY

NEWTONS CAT

TOP SECRET//SI//REL TO USA, FVEY

Summary

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

- Technical: manipulate messages, censor access, spam with information
- Psychological: depriviation, 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

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.*

Brand power

SECRET//SI//REL TO USA, FVEY

Do you ❤ your brand?

SECRET//SI//REL TO USA, FVEY

The UK merely joins the club

- Salutin Putin: inside a Russian troll house[1]
- Ukraine's new online army in media war with Russia[2]
- Congress vs BJP: The curious case of trolls and politics[3]
- China's Paid Trolls: Meet the 50-Cent Party[4]

> *"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*

[1] http://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house

[2] http://www.bbc.co.uk/monitoring/ukraines-new-online-army-in-media-war-with-russia

[3] http://timesofindia.indiatimes.com/india/Congress-vs-BJP-The-curious-case-of-trolls-and-politics/articleshow/23970818.cms

[4] http://www.newstatesman.com/politics/politics/2012/10/china%E2%80%99s-paid-trolls-meet-50-cent-party

Part III: Defense

"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):
  - Operating system: Debian GNU/Linux, QubesOS, Tails
  - E-mail: p≡p, Mailpile, Enigmail, GnuPG, Pond
  - Web: Tor
  - Voice: Jitsi, Mumble

Modern arms

- Offensive: surveillance- and **cracking**-tools (“Staatstrojaner”)
- Defensive: privacy-enhancing technologies (encryption):
  - Operating system: Debian GNU/Linux, QubesOS, Tails
  - E-mail: p≡p, Mailpile, Enigmail, GnuPG, Pond
  - Web: Tor
  - Voice: Jitsi, Mumble
  - Internet: GNUnet

Design Choices

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.**

Building the GNUnet

Internet

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

GNUnet

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

GNU Taler

Modern economies need an online payment system.

Credit cards?

SWIFT/Mastercard/Visa/PayPal are too transparent.

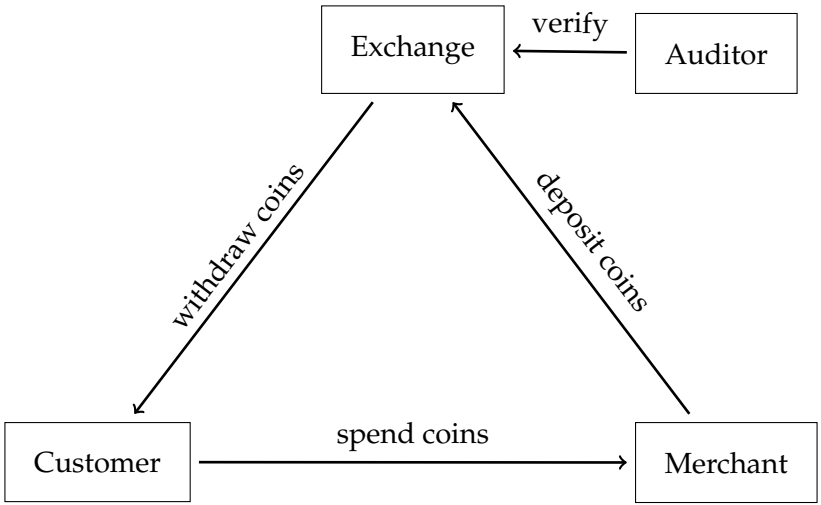
Requirements for a Payment System

- Customer anonymity
- Unlinkability
- Taxability
- Verifiability
- Ease of deployment
- Green / low resource consumption
- Macropayments and microdonations

We can make cash **digital** and **socially responsible**.

Taxable, Anonymous, Libre, Practical, Resource Friendly

Architecture of GNU Taler



Use Cases

- Internet e-commerce (convenient, efficient)

Use Cases

- Internet e-commerce (convenient, efficient)
- National “currency” (taxable, secure)

Use Cases

- Internet e-commerce (convenient, efficient)
- National “currency” (taxable, secure)
- Regional / community payment system (libre)

Value proposition: Customer

- Convenient: pay with one click
- Guaranteed: never fear being rejected by false-positives in the fraud detection
- Secure: like cash, except no worries about counterfeit
- Privacy-preserving: payment requires no personal information
- Stable: no currency fluctuations, pay in traditional currencies
- Free software: no hidden “gadgets”, third parties can verify

Value proposition: Merchant

- Fast: transactions at Web-speed
- Secure: signed contracts, no legitimate customer rejected by fraud decection
- Free software: competitive pricing and support
- Low fees: efficient protocol + no fraud = low costs
- Flexible: any currency, any amount
- Ethical: no fluctuation risk, no pyramid scheme, not suitable for illegal business

Value proposition: Government

- Free software = commons: no monopoly, preserve independence
- Taxabiliy: reduces black markets
- Efficiency: high transaction costs hurt the economy
- Security: signed contracts, no counterfeit
- Audited: no bad banks
- Privacy: protection against foreign espionage

Taxability

We say Taler is taxable because:

- Merchant's income is visible from deposits.
- Hash of contract is part of deposit data.
- State can trace income and enforce taxation.

Taxability

We say Taler is taxable because:

- Merchant's income is visible from deposits.
- Hash of contract is part of deposit data.
- State can trace income and enforce taxation.

Limitations:

- withdraw loophole
- copying coins among family and friends

Usability of Taler

`https://demo.taler.net/`

1. Install Chrome extension.
2. Visit the `bank.demo.taler.net` to withdraw coins.
3. Visit the `shop.demo.taler.net` to spend coins.

Business considerations

- Exchange needs a business to operate.
- Exchange operator income is from *transaction fees*.
- Taler Systems S.A. has been created, looking for investors.

Community considerations

- Initial accumulation: Who gets to mint currency?
- Speculation: Who controls the money supply?
- Social welfare:
  - Who gets to set tax rules and rates?
  - Who gets to allocate tax revenue?

Politics

Taler is political:

- Anarchists disagree with taxability.
- Authoritarians disagree with privacy.
- Communists disagree with enabling markets.

Politics

Taler is political:

- Anarchists disagree with taxability.
- Authoritarians disagree with privacy.
- Communists disagree with enabling markets.

Alternative solutions:

- ZeroCash: Anonymity for all, no central bank!
- Visa/Mastercard: Let the spies see it all to keep us safe!
- Barter: Hoarding cash is only for 1%-ers!

Further Information

- `https://taler.net/`
- `https://gnunet.org/`
- Slides will be at `http://grothoff.org/christian/`.

Further reading

1. 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.
2. Jeffrey Burdges, Florian Dold, Christian Grothoff and Marcello Stanisci. *Enabling Secure Web Payments with GNU Taler*. **SPACE 2016**.
3. Florian Dold, Sree Harsha Totakura, Benedikt Müller, Jeffrey Burdges and Christian Grothoff. *Taler: Taxable Anonymous Libre Electronic Reserves*. Available upon request. 2016.
4. Christian Grothoff and Jens Porup. *The NSA's SKYNET program may be killing thousands of innocent people*. **ARS Technica**, 3/2016.
5. Neal Walfield and Christian Grothoff. *TomorrowToday: GSM-based Location Prediction*. Available upon request. 2016.
6. Phillip Rogaway. *The Moral Character of Cryptographic Work*. **Asiacrypt**, 2015.

*"***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** *(...). (...)*
Compliance can be achieved through various techniques including: Engaging the norm of **reciprocity**; *engendering* **liking** *(...); stressing the importance of* **social validation** *(e.g., via highlighting that others have also complied); instilling a sense of scarcity or* **secrecy**; *getting the "foot-in-the-door" (...) and applying the "door-in-the-face" or "low-ball" tactics (...).*
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*