GLOBAL SURVEILLANCE

Cyber Crime and Forensics

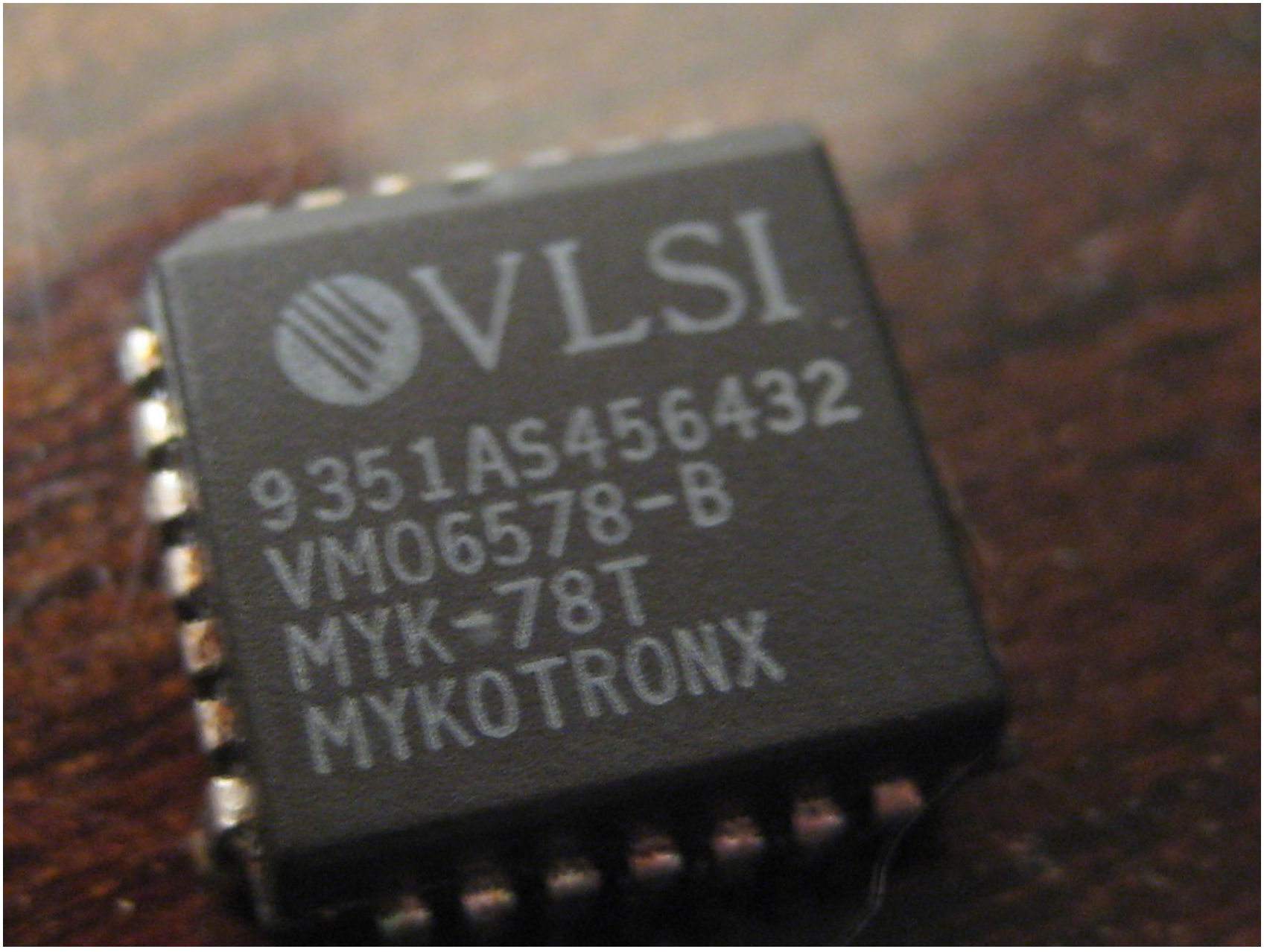
First Revision (2020/21)

Pierre-Philipp Braun <pbraun@nethence.com>

Table of contents

HISTORY & BREACHES

- some history on global surveillance
- acknowledged surveillance
- the state of the art
- infamous use-cases
- when data leaks go in the wrong direction



// wikimedia.org

Clipper chip

- NSA cryptosystem – device cryptographic key + DH + symmetric 80-bit cipher
- key escrow/surrender – some authority can decrypt live(?) and retroactively on demand

Crypto Wars in the 90's

- export control for crypto considered as weapons
- nsa vs. fbi

Situation is now berable e.g.

- NetBSD EXPORT NOTICE got updated[1]

[1] EXPORT NOTICE, <http://ftp.fr.netbsd.org/pub/NetBSD/README.export-control>

PEOPLE AND ORGANIZATIONS

Bruce Schneier
<https://www.schneier.com/>

D. J. Bernstein
<https://cr.yp.to/djb.html>

Electronic Frontier Foundation
<https://www.eff.org/>

FR - La Quadrature du Net
<https://www.laquadrature.net/en/>

- PRISM – record it all[2]
- Snowden leaks classified documents to The Washington Post and The Guardian
- Microsoft, Skype, Google, Yahoo where in the game quite early

Skype acquired by Microsoft on 10 May 2011 – what a coincidence!

[2]Prism slides, <https://www.documentcloud.org/documents/813847-prism>
NSA slides explain the PRISM data-collection program,
<https://wikileaks.org/hackingteam/emails/emailid/224564>

targetted

SUN Microsystems in swizerland[3]

[3]FR - Comment les États-Unis nous espionnent | Temps Présent, <https://youtube.com/watch?v=wRLvO4Z9zB8&feature=share>

2016 - Shadow Brokers

targetted

- got EternalBlue hence Wannacry

Acknowledged surveillance

Testimony of NSA head

we sniff only meta-data

US routers

- US routing advantage
- and what about BGP routers all over the world, which are owned by US companies anyhow? // LAB
- TODO looking glass live link

Do you understand the question about BGP owners and what does it matter?…

==>

1. sniff more *aka eavesdropping*
2. possibly targetted and active mitm *when required*

How does a nation-state great firewall work?…

==> where it happens

- at the ISP-level?
- –and/or– country's internet backbone enter/exit pipes?

==> how it happens

- brutal IP block based on IPs
- brutal IP block based on domain names
- DNS-based

So which one is it?…

==> mainly DNS-based at the ISP-level (at least in Russia)

- built-in ISP's DNS – *and got a blacklist of IPs and hostnames from Roskomnadzor (FEDERAL SERVICE FOR SUPERVISION OF COMMUNICATIONS, INFORMATION TECHNOLOGY, AND MASS MEDIA)*
- passive-transparent DNS for those who *go wild* (only block target domains)
- blocking IPs has too much side-effects (vhosts)

How to check if there's a transparent DNS-proxy in da place?…

==>

- DNSSEC eventually disapears
- you can recursive-query root servers

Domain fronting

Target host/domain appears

- DNS query
- SNI (and certificate's SAN)
- HTTP header

The latter is encrypted and can be mangled. However the hosting or CDN company can DPI and block it (depending if they host the SSL cert or not). Actually the trick they now use is to simply discard the HTTP header and redirect based on SNI only.

LAB // try domainless fronting (no SNI) against some CDN

CDN providers

CDN providers

- cloudflare
- fastly
- akamai
- …

LAB // what CDNs are bult-into the JQuery or other frameworks?

The state of the art

what they can break (targetted, not necessarily global surveillance related)

- this is not esp. related to global surveillance, but rather to targetted attacks
- however they do store loads of data, who knows if there's more than meta-data (PFS?…)

NSA breaks RSA?

The NSA Is Breaking Most Encryption on the Internet
<https://www.schneier.com/blog/archives/2013/09/the_nsa_is_brea.html>

Black Hat USA 2013 - The Factoring Dead: Preparing for the Cryptopocalypse
<https://www.youtube.com/watch?v=33RbRid1deo>

–> somebody cracks MD5 fast @5m30s

–> RSA vs Suite B @40m

NSA “has something” on ECDSA?

- rumors against NIST’s curves

“She laughted”

DEFCON 19: The Dark Side of Crime-fighting, Security, and Professional Intelligence
<https://www.youtube.com/watch?v=XIfrfWgJlsI&t=35m50s>

–> we won’t get free of global intrusion and detection

Infamous use-cases

examples when the big players went too far

iOS Siri

Siri natural language commands and dictation – true people where handling capture samples

Facebook listens 5 seconds

Is Facebook listening and creating conversation-based ads on Instagram? I think so, and I put it to the test using WireShark.
https://amp.reddit.com/r/privacy/comments/7mxn9i/is_facebook_listening_and_creating/

LAB // try to reproduce that test

Windows 10+

Telemetry incl. in the (open-sourced) calculator – *what happens when you paste a password there?*

LAB // sniff Telemetry events

When data leaks in the wrong direction

- Russian intelligence also got leaked – *not mentioning the many time when this happened to the US intelligence*
- NASA leaked by an raspi
- (episode about the Uyghurs in China)

Use their framework

- FB and/or VK – locate users with a developer account // LAB

// Questions on history and breaches?

WAYS TO PRIVACY FOR N00BS

what any person working for CAC40 or some government should know…

Citation of Rob Joyce, head of Tailored Access Operations (TAO) at the NSA[4]

« Cloud computing is really a fancy name for somebody else's computer. »

[4]Disrupting Nation State Hackers, at minute 09:50, <https://www.usenix.org/node/194636>

Remain pseudo-anonymous

While browsing the web or using phone applications

- do not identify yourself on Google and if you do, don't forget to disconnect when finished, and restart your browser to clean-up authentication cookies
- do not identify yourself on YouTube

Protect your privacy

About social networks (organized spyware when authenticated)

- do not use Facebook privately *but for your own of marketing or propaganda*
- *idem* for Twitter
- *idem* for YouTube (Google)
- *idem* for Instagram (Facebook) *and beware of images' meta-data*

Protect your email

Store your message history in a trusted environment

- avoid @gmail.com – *it's never too late to proceed with a migration e.g. through IMAP*
- avoid @live.com @hotmail.com @outlook.com @outlook.fr and other Microsoft services (incl. enterprise domains)

CONSIDER MOVING FROM GMAIL TO *SOMETHING ELSE*

What email hosting providers are there?…

==> a few *supposedly* secure and privacy-friendly email hosting providers

- ProtonMail (Switzerland *but sometimes the americans are there anyway*[5])
- Tutanota (Germany)
- SecMail (secmail.pro) – *need ToR!*
- @yandex.ru or @mail.ru (Russia)
- *other ones worth mentioning?*

[5] FR- Opération Rubicon : Espionnage à l'échelle mondiale | Temps Présent, <https://www.youtube.com/watch?v=SWFlA248spU>
FR - Comment les États-Unis nous espionnent | Temps Présent, <https://www.youtube.com/watch?v=wRLvO4Z9zB8>

And there's always DIY…

- some *local-enough* Cloud / IT outsourcing
- self-hosting on-premises

How to move your message history from one place to anoter?…

==> move your emails out of gmail.com e.g. as such

- connect your IMAP client to both sides
- drag & drop mail folders
- and clean-up (& EXPUNGE)

// Questions on ways to privacy for n00bs?

WAYS TO PRIVACY FOR THE PARANOID

what a computer & network pirate should know

What about the "private browsing" feature in Chrome and Firefox?…

==> not much worth anything, just hides history and cleans-up cookies on-exit

Any idea how to do it right?…

==> VPN providers e.g. Express VPN, NordVPN, Surfshark

==> Tor e.g. Tor Browser (some Firefox fork)

What are VPN providers good for?…

==>

- avoid censorship/blockage e.g. access torrent tracker websites – *bypass transparent DNS proxies*
- **hide your IP**
- avoid to get sniffed/DPI by your ISP
- avoid to get sniffed/DPI by your nation-state

local authorities loose

VPN providers are *mostly* useless – forget to enable the VPN just once –> link is made between your genuine IP and what provider you're using? // LAB sniff a VPN provider session setup and see what meta-data we got

- IP changes but cookies keep identify you
- IP changes but twitter prompts for my credentials within Chromium? // LAB
- IP changes but phone apps identify the device // LAB

LAB // are we using different IPs every time we connect, even when it's on the same country end-point?

GAFA are winning yet again

What is Tor good for?…

- same advantages as for VPN providers (but for free)
- even better, as it's distributed and nobody can trace you back
- also reach `.onion` web sites

Cases where Tor is *mostly* useless

- for daily and casual activity, you need to authentify on many sites anyways
- need to have yet a separate pseudo-identity

LAB // other ways to use Tor than with the Tor Browser?

On american surveillance

- this one really pisses **them** off // TODO find reference
- many exit nodes handled by the NSA // TODO *idem*

Alternatives to Tor // LAB try those out

`freenet`

`i2p`

`GNUnet`

`retroshare`

Why not just your own VPN?…

One could consider OpenVPN or WireGuard but it won't help much unless you got many IP addresses

LAB // do your own VPN –> app for smartphone?

LAB // try to schedule a user-VPN service across multiple IPs in a PoC (and compete with NordVPN)

Messaging/chat apps

- thumbs down for facebook messanger
- thumbs up for Signal and WhatsApp (end-to-end encryption)
- the unknown status of Telegam – *how often do you switch to secure mode?…*

Privacy devices

- Legacy phones
- Rugged-or-custom smartphones without camera
- Hardware-lock on camera and WiFi (Librem phone)
- *And let's not talk about Intel ME vs. Coreboot just yet*

Alternate systems (Android forks)

- LineageOS – *not that easy, will take you about a day*
- …

LAB // root phone and switch to LineageOS, what's not working? GPS? Are there ways to configure and make them work?

Quoting Peter Gutmann[6]

I read encrypted email on a non-network-connected machine

- secret services also cut the network altogether
- PKIX private and DNSSEC private keys are also kept offline
- *aka physical security*

[6]Peter Gutmann, <https://www.cs.auckland.ac.nz/~pgut001/>

Files' meta-data

- jpeg headers – instragram & friends know your location

Your laser printer leaves traces

- Machine Identification Code
- does it really matter, as long as you don't give your ID to the reseller?

Avoid DPI

GoodbyeDPI
https://github.com/ValdikSS/GoodbyeDPI

Another method for bypassing DPI #71
https://github.com/ValdikSS/GoodbyeDPI/issues/71

LAB // try-out, explain and comment GoodbyeDPI

For the webdev

- Beware you're making your users work for Google's AI

LAB // Google capchat/robot-checker alternatives?

// Questions on ways to privacy for the paranoid?

Remind me again, what's the best way to defend & protect?…

==> experiment with the attack

So what would it mean here?…

BECOME BIG BROTHER

what they are – or could be – doing

The Eve I love

Sniff meta-data while being on the path

- IP accounting vs. NetFlow vs. IPFIX // LAB
- collect more meta-data than that (SNI, …) // LAB
- can we track what IP addresses are logging into sites e.g. facebook? // LAB

DEMO // wireshark & show SNI in SSL Client Hello

Heavy bad-ass DPI

- Cisco & others' SSL interception feature – not supposed to happen on the public network
- Blue Coat Systems (Israel) – nation-wide censorship and surveillance e.g Syria
- …

LAB // can cisco & friends' ssl interception be made targetted (catch only a precise victim)?

Assets for DPI (DIY)

Obtaining meta-data by means of Intrusion Detection System (IDS)

- Zeek / Suricata / Snort // LAB

Or sniffing tools e.g.

- just `urlsnarf` and such on a router (clear-text only) // LAB

Consider adding SSL termination for those to be effective.

Enable Wifi for better geo-localization

Does it ring any bells? How do you think it works?…

Hint: no need to be connected to any AP, they just want you to enable Wifi

==> Your favorite spy (smartphones)

Enable Wifi to improve localization…

- Apple & Google keep track of all APs around you
- they could also track what APs you managed to connect to
- and obviously behind what public IPs you are being NATed
- do they also track your friends' supplicant MACs? // LAB

How would you do that on your own?…

- Aircrack-NG's `airodump-ng` output to csv, xml
- (and here comes data science to cross-match people together)

Also worth mentioning

- WifiKill (Android)

Malls can track your movements…

- are all WiFi MAC addresses random now? // LAB on the status of Android
- malls can still track user movements as long as shuffle does not happen too often
- they just can't pin a user the time it comes

LAB // do you have a random MAC on your phone? How fast does it get re-shuffled?

all the things they know… about you!

- Google – search engine / Android / YouTube
- Apple – iOS / MacOS
- Facebook – WhatsApp
- Amazon – *what you read & privkeys*
- Microsoft – Linkedin / **Github**
- Twitter

What does Google know – or could know?

==>

had the wrong item in your clipboard? that's too bad!

- whatever you enter in the search box even though you don't press enter
- from what IP you search and when (even without auth thx to cookies)
- *not mentioning academic studies on how to identify user based on their behavior*
- *nor side-channel attacks such as how the keyboard buttons sound or typing timing*

Logged-in once? That's probably good enough for them!

- IP remains the same – however possibly multiple IPs and users behind
- does Google remind you've been identified before? Check that logout truly clears-out your cookies. Is there something left or is everything is clean? // LAB

Any idea how much money Google spends on lobbying per year?…

==> 25 million dollars

Google will conquer the world one charitable donation at a time <https://theoutline.com/post/6999/google-will-conquer-the-world-one-charitable-donation-at-a-time>

What does YouTube know – or could know?

==>

assuming w/o being authenticated

- what “read more” links you click
- different devices but same IP? – *no cross-referencing/identical content observed, cookie-like seems to be device specific*
- do they go as far as keeping a trace on what video you’re passing your mouse over, as a quick shot on their content?

LAB // method for attempting to check those kinds of things would be to sniff and measure how many bytes are going outbound while doing so, but that’s assuming they’re collecting that meta-data in real-time

What does WhatsApp know – or could know?

- Your logged-in phone and desktop devices
- **YOUR CONTACT LIST**
- Who you talk to, when and where (meta-data)

What else?…

Possibly the weblinks you share with friends and contacts?

- WA does previsualisation and this got handled by the app itself
- possibly outside the end-to-end communication stream…

By the way, what happens when

- you click on a link that was shared to you?
- and when your correspondant clicks on the link you sent?
- does this got handled by the app or simply by the system which opens an app/browser? // LAB

What does Github know – or could know?

==> for the least…

- IP where you auth from
- may store commited and reverted pushup by error of yours that includes critical information
- if you found a vulnerability and study it on github – even with a private repo – before publishing it, they can get it retroactively
- can help cross-match your SSH public key with global meta-data sniffing databases

// Questions on how to think like big brother?

THE LAW

- in Russia
- in France / EU

The law in Russia

- law 912-51 (1993) – government's data protection (secret data, top secret, …)
- federal law 152 (2006) **on personal data**
- federal law 126
- federal law 374
- Yarovaya law (2016 + 2018) – *looks like a prism…*

FEDERAL LAW 152 (2006) **on personal data**

- host personal data of russian citizens
- on servers located on the russian territory

What is meant by `personal data`?

Any **combination** of the following[7]

- name surname
- phone number
- email
- tax
- cards
- address
- birth date
- …

[7]LAW 152, <http://www.consultant.ru/document/cons_doc_LAW_61801/>
ENGLISH, <https://pd.rkn.gov.ru/authority/p146/p164/>
UNDERSTANDABLE VERSION, <https://www.zetasoft.ru/korotko-fz-152/>

So who has to go to jail?…

for public services e.g. Whatsapp

- the user is responsible

for private sector services e.g. a company

- either the CTO or the dedicated employees dealing with the personal data matter are responsible

Штраф – How much?…

==> From 50 000 to 1M+ RUB

1) data should be stored physically in Russia
2) A company should develop information security policies
3) notify the RosComNadzor (Russian government) that company is processing personal data
4) publish the confidentiality policy
5) publish the users agreement
6) Company should collect approval for personal data processing from each user

==> point 4 is publishing what you've designed at point 2

It does not matter whether you are a Russian or foreign company.
Everybody has to comply.

- that is most probably why Linkedin was banned for a while (it is back)
- government negociates with

THE YAROVAYA LAW (2016)

The 2018 update – Telecom operators are required to keep

- voice and messaging traffic for 6 monthes
- internet traffic for 30 days
- nearly impossible (requires too much storage)

// Questions on the law in Russia?

The law in EU

EU regulation took over the CNIL in France (Apr 2016)

General Data Protection Regulation (GDPR)

Règlement Général sur la Protection des Données (RGPD)

GDPR principle for data controllers

Don’t store nor process personal data unless there is a legal basis

1. user consent
2. needed to fulfill a contract with the user
3. comply data controller’s legal duties
4. public interest or official authority
5. “legitimate interests” of a data controller or third party?

Source: wikipedia.org

GDPR data subject's rights

- Information and access (access your own personal data)
- Rectification and erasure (right to be forgotten)
- Right to object and automated decisions (right to object personal data processing for marketing, …)

LAB // what about EULAs and policies we all have to agree without that box to object? do we consent *ipso facto* for third-party marketing altogether?

GDPR penalties

How much?…

==> after multiple warnings

Failing articles 8,11,25,39.41,42,43

- eventually up to 10 million EUR
- up to 2% of the annual worldwide finalcial turnover

Failing articles 5,6,7,9,12,22,58

- eventually up to 20 million EUR
- up to 4% of the annual worldwide finalcial turnover

Data mgmt

there's always a good reason to collect user data, you just need to name one, such as "improve user experience"…

- transparency: tell users what you do with the data
- users' rights to access, modify/correct, erase, stop billing

A commercial opportunity

make 'em trust you

- transparency –> more trust from internal users and/or customers
- users' rights embedded in nice UI/UX –> user's loyalty

RGPD principles

- collect less (only what you need)
- know what you have (inventory of data assets)
- what is collected
- and where

Data assets

- within single or multiple databases
- other kinds of metrics
- *how and where are all those mixed up*

Private data (donnée personnelle)

- direct (name, firstname)
- indirect (phone number, client ID)
- possibly by cross-reference (marketing/surveillance database)

Example solution

In some case of video-based statistics collection (wearing mask? body temperature?)

> *« les images filmées ne sont “ni stockées, ni diffusées” »*

- they got away and didn’t had to apply RGPDs
- now what about functional and advertisment cookies? Could we also avoid the Cookie Consent banner in some cases? Maybe if we don’t do any profiling of any kind? // LAB

finally, any idea why this would be incompatible with blockchain?…

==> CANNOT DELETE, CANNOT GO BACK, DATA IS THERE (supposedly) FOR-EVER

Other laws (projects?) worth mentioning

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>

Loi n° 2016-1321 du 7 octobre 2016 parue au JO n° 235 du 8 octobre 2016
<http://www.senat.fr/dossier-legislatif/pjl15-325.html>

ARTICLE ADDITIONNEL APRÈS ARTICLE 26
<https://www.senat.fr/amendements/2015-2016/535/Amdt_473.html>

LAB // FB picture belongs to them vs. RGPD

LAB // FB cannot delete account vs. RGPD

LAB // restrospective on all the EU vs. GAFAM law suits

// Questions on the law in the EU?

POWERFUL NATION-STATES

- 2016 - Russia blocks Linkedin
- 2018 - Russia blocks Telegram *with drama* (ended 2020)
- 2021 - Russia forces Apple to pre-install gov-approved apps
- 2021 - Top US companies' leaders attend Chinese's development forum (incl. Apple, Tesla, Cisco)

The Telegram blockage

- other services got hit (AWS IP ranges…)
- attempt to change technology for blocking
- debate was about opt-in secure mode – what about non-secure communications?

Facebook vs. law 152

Let's suppose that

- Cassendra cannot be splitted across countries in terms of user's citizenship
- all they can do is negociate and agree to provice a copy of the datasets of users

// Questions on nation-state regulations?

DESKTOP & PHONE SECURITY FOR N00BS

what any person working for CAC40 or some government should also know…

(esp. CEO, CTO and CSOs)

Instant messaging

in order of preference

1. Signal (phone app & desktop)
2. Telegram secret chat (phone app only)
3. WhatsApp (Facebook) although collecting meta-data and contacts, still *good-enough* end-to-end encryption[8]

Avoid

- Telegram – *message history stored on their servers?*
- Skype (Microsoft) – *those ones are always willing to colaborate anyhow*

[8] Beware of URL previews…

Video conference

in order of preference

1. Jitsi Meet
2. Cisco WebEX // LAB study its security status
3. Zoom // LAB attempt PoC/understand some vulnerability from the past

And if you're only two in the virtual room

- Jitsi Meet + end-to-end encryption (Beta as of June 2021)

Login & password dictionary/brute-force mitigations

What's a good password?…

- either some phrase incl. a number and a special character
- –or– 8+ pseudo-random chars incl. a number and special character
- USE ONLY ONCE

Where to store those safely?…

- on a paper book
- simply let your browser save those
- using a web-browser-based password manager add-on
- using a dedicated password manager (desktop / browser / phone)

- **EVENTUALLY** ENABLE 2ND FACTOR AUTHENTICATION
- when it's critical
- when it's a trusted app/provider – don't necessarily give all your phone numbers to GAFAM

Built-in password managers

Chrome & Firefox

- will tell about weak passwords
- will tell about breaches
- will help generate new passwords

Dedicated password managers

- are compatible with Chrome and Firefox by means of plugins
- will also prevent *some* phishing attempts (known hoaxen and targets)
- may work behond web browser applications (esp. on smartphones?)
- dedicated phone app – *ideally only stored there*
- master password can be protected by biometric or face-id

Products

- Dashlane, Keeper, LastPass, 1Password, …

LAB // sniff keystrokes on master password – can we tune the sniffer so it records only e.g. specific application?

Email phishing mitigations

- BEWARE OF WEIRD EMAILS AND LINKS
- BE SUSPICIOUS WHEN ASKED FOR CREDIT CARD INFO OR CREDENTIALS

How to check a link in an email?…

==> Move your mouse over it and look at the status bar

- be it with an MUA or on a webmail
- check there's HTTPS in case it needs to be
- check the domain part
- copy/paste the link to virustotal.com & urlscan.io

RCE & APPSEC mitigations

here again, but this time about viruses

- **BEWARE OF WHAT YOU EXECUTE AND INSTALL ON YOUR COMPUTER** (anti-virus won't do the job so well)
- **UPDATE YOUR WORKSTATION'S OPERATING SYSTEM**
- for once, ENABLE your SYSTEM-FIREWALL without exceptions nor Universal Pulg-and-Play (UPnP)
- and in case you would be infected (you never know), put some sticker on the webcam (ideally one should also cut the microphone)

MITM mitigations

Un-trusted network e.g. airport and restaurants without a PSK (OPN Wi-Fi)

- make sure you're always HTTPS or some end-to-end of some sort
- eventually use a VPN provider e.g. NordVPN, ExpressVPN, Surfshark, …

LAB // try `arpspoof` over Wi-Fi OPN/WEP/WPA

// Questions on desktop / phone security for n00bs?

DESKTOP & PHONE SECURITY FOR THE PARANOID

what a computer & network pirate should also know

…back to password attack mitigations

Technical check-up

Why do we need a strong password?

Why use a password only once?

==> help prevent dictionary & brute-force

- how fast does the service respond to auth attempts?
- does it identify and block brute forces? (eventually enable sshguard)

==> some sites get hacked and badly stored password get leaked

for developers & devops

How to store passwords properly as a web/app service provider?…

==> hash *with some* salt

Check your users' credentials

- Have I Been Pwned?[9]
- download password breaches (BreachCompilation on Torrent)

[9] Have I Been Pwned?, <https://haveibeenpwned.com/>

…back to phishing

Notice weird behaviors

- BE SCARED WHEN ASKED TO ENTER PASSWORD TWICE (getting disconnected / reconnected)
- it may be old-school phishing + redirection (not a clever MITM)

…back to system hardening

- *if only that was a server (cannot easily do that on Ubuntu)*
- overwrite your system binaries once in a while (erase kernel & userland rootkits)

…back to pkix hardening

keep your certificate store clean

- grab the Curl/Mozilla bundle as `/etc/ssl/cacert.pem`
- point `wget`, `curl` and friends against it
- maintain a clean SSL certificate trust-store in your browser – *install `p11-kit` for Firefox*

For the absolute paranoid above-human

- run your own DNSSEC validating-resolver LOCALLY // LAB does the chain-of-trust also validates when going through a forwarder?
- disable phone camera completely[10] // LAB cannot be reverted, really?
- disable Intel Management Engine (ME) with `me_cleaner`[11] // LAB

[10] Permanently Disable Camera for Android, <http://disablecamera.com/>

[11] corna / me_cleaner, <https://github.com/corna/me_cleaner>

…back to mobile phone security

- ROOT YOUR PHONE // BONUS
- run alternate phone OS // LAB

…back to Email Security

- enforce STARTTLS
- validate MX certificates – *won't work for some destinations*

// Questions on desktop / phone security for the paranoid?

Tips & Tricks

a little bit of practice

Generate pseudo-random passwords incl. special character and with variable length

```
pwgen --capitalize --numerals --symbols --ambiguous \
      1$(( $RANDOM % 10 ))
```

That's all folks

LABS

Become a lawyer

- Review some EULAs and terms of use

Tune your browser like hell[12]

- play with p11-kit and validate your CA bundle
- DIY Firefox compartmentalization
- GNU Icecat

Become paranoid

- Play with neflabs software[13]

---

[12] Enabling Custom Trust-store in Mozilla Products, <https://pub.nethence.com/desktop/mozilla-p11>
Running firefox a bit more safely - HOWTO, <https://lists.dragonflybsd.org/pipermail/users/2015-August/228324.html>

[13] fuck the surveillance state, <https://neflabs.com/menu/>

Sniff and discuss communication protocols

- WhatsApp, Web WhatsApp, Skype, Telegram, Signal

Become big brother

- grab meta-data with Zeek
- PoC IP accounting or NetFlow / IPFIX

This is the end