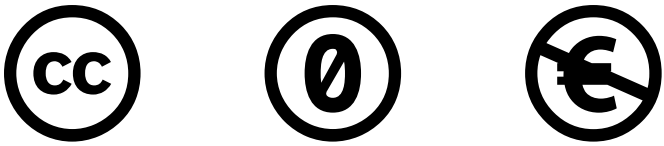

AN ACTIVIST'S GUIDE TO
INFORMATION SECURITY



1 An Activist's Guide to Information Security

This guide aims to be a concise overview on information security for anyone in emancipatory struggles against structures of power. It represents assembled knowledge and best practices from personal experience, conversations with hackers and fellow activists, hacker conferences, and university courses on computer security and cryptography. Nonetheless, the best security is sharing skills with trusted people.

If you have any corrections, questions or additions, please contact us [1] (email: activist-security riseup net). Our perspective is mostly from western countries, we especially welcome additions about repression and tactics in other places of the world.

2 Table of Contents

3 Introduction
4 Security Culture
5 Physical Security
6 Traditional Communication
6.1 Face to Face Communication
6.2 Letters
6.3 (Mobile) Phones

- Mobile phones themselves are identifiable!
- Location Tracking

- Room Surveillance / “Silent Calls”

7 Digital Base Security

7.1 Encryption and Passwords

7.2 Choose Your Computing Device (Integrity)

- Smartphones
- Laptops and Desktop Computers

7.3 Storage Encryption (Confidentiality)

- Encrypt Your Home Folder
- Encrypt The Whole System
- Use an Encrypted Container
- Android and iOS
- Limitations

7.4 Backup your Data (Availability)

8 Internet Services

8.1 A Word about Web Browsers

8.2 Anonymity

8.3 Email

8.4 Mailing Lists

8.5 Messengers / Chat

8.6 Jabber / XMPP

8.6 Voice / Video Chat

8.7 Blogs, Websites and Social Media

9 Wrapping it Up

9.1 TL;DR:

9.2 Example Setups

3 Introduction

Technological progress has made it next to impossible to defend against a sufficiently powerful attacker (a scary example [2]). Fortunately, most of us don't have the NSA hard on our heals, and local authorities are usually limited in their possibilities (e.g. this article [3] about police cooperation). The trick is to be sufficiently careful while staying functional.

This guide tries to point out the possibilities and their trade-offs. Is split into the following sections:

- **Security Culture** introduces the social side of things.
- **Physical Security** describes securing physical access to information.
- **Traditional Communication** is about the pre-Internet kind.
- **Digital Base Security** discusses building a digital base to communicate from.
- **Internet Services** points out problems with and alternatives to common Internet communication services.

4 Security Culture

- **The need to know principle**: share information only with those who need it.
- Establish a culture where people realize when not to ask curious questions and don't take offense when information is not shared with them.

- It is not necessary to know who is in which group and participated in which action - don't brag about it and stop others if they do. You can't accidentally reveal something you don't know.
- Do not keep unnecessary information (e.g. meeting minutes) and keep your house clean of incriminating material. Also, do not make pictures on actions, not even pixelated ones, they may incriminate people anyway (source [4]).
- Do not connect pseudonyms with their public information (e.g., if possible, do not store people's activist email addresses with their name or group).
- Don't let paranoia paralyze you: try to keep a realistic assessment of the threat model and don't suspect people to be snitches just because they don't conform to subcultural norms.

5 Physical Security

While few of our homes can successfully resist a police raid, measures can be taken to fend off fascist thugs or rogue state agents.

Obscurity: It can be useful to live at a place not registered as your official address, and without obvious subcultural symbols on the outside. Still, be prepared for sufficiently motivated forces of darkness to find and attack your home.

Passive defense: Protecting a home from the evils on the outside necessarily means forming an in-group. A reasona-

ble front door and handpicked distribution of keys go a long way. Barred ground level and basement windows and anti-splinter films on the glass offer additional reinforcement.

Active defense: An alarm horn and a lighting system on the outside may mainly help against physical attacks, but they can also buy valuable time in case of a police raid.

Process: Have a short guide on dealing with police raids and your lawyers' (mobile) numbers on the inside of the front door and next to the landline phone, if you still have one.

In some jurisdictions, having people's private rooms marked with their name may help to argue against a search when it is only against specific residents. However, it obviously also reveals the inhabitants' names to visitors and does only point out the existing legal situation to police who often ignore it anyway.

Be aware that the police and state agencies may be allowed to legally stop and search you outside your home, and that you may even be detained for refusing to hand over passwords to your devices in some jurisdictions (source [5]).

6 Traditional Communication

With a reasonably safe home, let's relax and see what our comrades were up to, shall we?

6.1 Face to Face Communication

Modern technology enables the surveillance of the spoken word from far away and even microphone-unfriendly places such as swimming pools and concert halls can theoretically be surveyed with modern noise-cancelling technology. However, taking a walk is still a fairly secure way of communication, when it is reasonably unlikely that hidden microphones are placed in clothes and accessories (that means no mobile phones, too!). If more security is needed, one can resort to writing on paper in a sight-protected place (e.g. under a blanket).

Closed rooms can be monitored even more easily, thus sensitive meetings in established autonomous centers, alternative house projects, lefty bars and the like are strongly discouraged! Speaking of face to face, modern technology can even "unmask" masked protesters (illustration [6], paper [7]), and video surveillance of common meeting places is another reason to avoid them for sensitive meetings.

6.2 Letters

Hopefully you already figured that relying on the confidentiality of snail mail is a gamble at best (e.g. a German article

about mail surveillance). Code words are a last refuge for the imprisoned and desperate, but history has shown that relying on a secret method (e.g. swapping letters) alone to hide information is easily broken.

6.3 (Mobile) Phones

Most importantly, all information (calls, texts, mobile Internet) exchanged via the (mobile) phone network should be considered captured by state agencies and potentially other enemies. They use ETSI wiretapping interfaces mandatory in all mobile network equipment sold in the EU (and thus available everywhere) (source [8]), but on top of that, other motivated actors can capture data in a local mobile radio cell with a few hundred Euros worth of equipment (source [9]).

6.3.1 Mobile phones themselves are identifiable!

The second most important thing to know about mobile phones is that they have a unique IMEI number, that identifies it in the mobile network. Your phone's IMEI is registered in the operator network together with SIM card. **That means when you put a new SIM card into your old phone, it can be easily linked to your old SIM card.** So for a safe phone, both SIM card and phone need to be acquired and used in a way that does not link them to any other information, i.e. by buying phones with cash and getting pre-registered SIM cards or registering them anonymously providing fake information (where at all possible), for example via TOR (see below). Besi-

des law enforcement, even private corporations may be able to obtain the data your mobile number was registered with (source [10]).

6.3.2 Location Tracking

To work, mobile phones regularly contact the *base station* they are booked into, which locates the phone within a minimum of about 400m from the cell tower in urban areas (source [11]). This information is routinely stored by mobile carriers and therefore available without prior targeted surveillance (source [12]). For users of centralized location services (like Google Maps), the police may be able to obtain extremely accurate long time location profiles from the provider (source [13]).

With targeted surveillance, triangulation and querying data from the phone can locate it down to 50m (source [14]), or even 5m with a GPS-equipped phone (source [15]). To get a more time-accurate location profile, state agencies may use so-called stealth pings / silent SMS to make a mobile phone contact its base station more often (source [16]).

As a last resort, police can use so-called *IMSI-catchers* which pretend to be the strongest network cell available, and then record what phones book into them, potentially even recording calls and text messages (source [17], some real-world examples).

Police have been known to use geodata on all kinds of incidents and extended cell phone surveillance of 10s of people on the most ridiculous accusations, or even deploying IMSI-

catchers on sit-ins against fascist marches, so the technical possibilities are not to be taken lightly.

6.3.3 Room Surveillance / "Silent Calls"

Much controversy exists whether it is possible to tap mobile microphones even when no calls are going on. This [18] article hints the FBI has done it, while this [19] research hints it would be built-in functionality. We *guess* that that this is at maximum used against high profile targets, because if any hicksville cop shop was able to use that, the evidence of it would be better known by now.

Open source mobile operating systems offer no protection against those attacks, because there is usually a direct connection from the microphone to the (always closed source, as to comply with regulations) baseband firmware and it can not reliably be powered off. To make matters worse, mobile phones without SIM card might still pre-register to the strongest network (for emergency services), and there is no way to check if "offline / airplane mode" is actually what it promises to be. On smartphones, malicious apps provide additional surveillance (see *Smartphones* below).

To err on the side of caution, it is advisable to leave your phone at home when visiting a sensitive meeting, or at least take out your phone's battery a good couple of km from the meeting point, because the attendants, (cell tower) location, time and duration of a sensitive meeting can easily be spotted by 30 people switching off their phones simultaneously. Especially when meeting with small groups in densely popu-

lated areas, it might be as good to simply put the powered on mobiles in a location outside hearing distance (the fridge two rooms away, for instance).

It should be noted that mobile phones transmit power status (idle, running) during operation and send goodbye messages to the network when powered off properly (so that creates a different pattern than just ripping out the battery).

We encourage you to build your daily activist routine without even counting on using mobile phones. Mobile phones and SIM cards should be destroyed after the action. where needed for longer-term activist infrastructure, phones and SIM cards in the internal network should be swapped regularly (e.g. every six months) all at once to avoid identification by location or communication patterns.

7 Digital Base Security

Traditional means of communication don't feel so good anymore, so what about the Internet? First we need to find a secure device that we can use it with. When it is about information, security is classically divided into integrity, confidentiality and availability. We will see what they mean in a moment, but before, let's talk about encryption.

7.1 Encryption and Passwords

We won't go into any details here, but the basic idea of digital encryption is that there extremely many possibilities for a

key to some encrypted data. With enough possibilities, it takes too long to try all the keys (a *brute force attack*), although old ways of encryption get broken as computers become faster (for what the NSA supposedly can break, see here [20]). Because humans can't remember huge keys either, computers often use some really slow function to derive the key from a password. This works fine if someone enters the password once or twice, but makes it hard to try all possible passwords. But if your password is *1312* or *revolution* or similar, it may be broken by a *dictonary attack*. One way is to generate a completely random password (howto [21]), write it down on paper, memorize it and destroy the paper after a few days.

If this sounds to complicated or you are afraid of forgetting the password after a vacation or similar, it's best to use one of the following schemes and combine them with *random symbols* for extra security.

Scheme 1: use the first words of a random sentence (**T**his **s**ecurity **g**uide **m**akes **f**or **1** **c**ool *%3* **p**assword**!**).

Scheme 2: simply put a lot of random words together (pineappletelevisionconfusion$2salat).

Even a good password is for nothing if the cops have put a virus on your computer and get the password as you type, which brings us to the next point.

7.2 Choose Your Computing Device

None of today's common devices are completely under your control. Laptops and desktop computers come with

obscure low level software ("*firmware*") that is controlled by the manufacturer[A].

7.2.1 Smartphones

The same is true for tablets; and smartphones or tablets with SIM slots are even worse, because they have closed components that are always also controlled from the mobile network (source [30]) and this control could be abused to access personal data on the device (source [31]). On top of that, smartphones are complex computers which often are not treated to security updates by their manufacturers, making them an easy target for attacks (source [32]). Besides sneaky network attacks, malicious apps are used for surveillance (source [33]) and the wealth of sensors for their environment makes smartphones excellent spying devices, even if you ripped out the microphone (e.g. 1 [34],2 [35]). Moreover, they are designed to collect crazy amounts of information on people by default (scary example: article [36], paper [37]) - information that is more often than not readily available to state agencies with or without request.

Therefore **the use of smartphones for sensitive activist**

[A] Technical background: most Intel-based computers run a software that can control the system remotely in parallel to the normal Operating System (AMT [22]), which can be "disabled" in the manufacturer's firmware but that is closed source, and modern Intel Processors usually only boot signed firmware (Intel Boot Guard), so you will never be able to use alternative firmware like Libreboot [23], and even if you could, there would still be things in your computer that you do not have the source code for (even [24] more [25] technical [26] background [27] here [28]). There have been known cases of malware using AMT (source [29]).

work is strongly discouraged, as even the security of alternative Internet services like Jabber/XMPP is greatly diminished on the vast majority of mobile devices[B]. Yes - we are aware that most people reading this use a smartphone as their primary communication device. If you aim for a halfway decent personal device, the choice really is between Android and iOS, because fringe alternatives like Sailfish OS [38] don't even offer personal data encryption by default yet. Google's reason to make Android is to control a platform for advertising and the collection of data. Apple's iOS has many built-in security features, but Apple's convenience features such as remote wipe come at a pretty high cost of privacy invasion itself, and apart from exceptions [39], the company generally cooperates with state agencies.

Open source versions of Android (like *Replicant* [40], *Copperhead OS* [41] or, more commonly, *Lineage OS* [42]) allow for a Google-free Android, at the cost of loosing many convenient apps, and the general problems with smartphones still apply. They usually require unlocking the *boot loader* of the device so that it is even possible to install an alternative Android on it, which then is something that e.g. the police could also do if they have access to your device for a few hours (discussion [43]). On top of that, whilst the alternative Android variants may provide security updates for old devices where the vendor does not, alternative Android *ROMs* for many devices are actually poorly updated (discussion 1 [44], 2 [45]; overview for Li-

[B] This security analysis illustrates quite well that even without any malicious intend, mobile devices as commonly used are just not very secure.

nageOS [46]).

If necessary, our advice is to best use a tablet **without SIM card slot** (because it can't be controlled from the mobile network), or if you must a smartphone supported by Copperhead OS or well supported by Lineage OS.

7.2.2 Laptops and Desktop Computers

Running as much *Free and Open Source Software* as possible on your laptop or desktop computer gives you a good deal of control back. With proprietary software like Microsoft Windows or Apple's Mac OS, chances are they will support law enforcement in their effort to "fight crime" and break into your computer. With *Linux* or any other open alternative, the program code is exposed to a whole community, making it much harder to mess with. As a side node, the best protection against computer viruses is simply to not download software from random websites and to not open potentially dangerous email attachments from untrusted people. This includes Microsoft Office documents that can be abused for various attacks (source [47]). Antivirus software only offers patchy protection but is itself vulnerable to attacks (source [48].

There are many different bundles of the Linux core with various open source software called *distributions*. If the computer is used for sensitive activist work, Tails [49] is a distribution with a focus on security and anonymity that can be installed alongside another operating system, e.g. another variant of Linux.

For mainly personal use, the following two distributions are less geared towards security, but are relatively easy to install, use and update:

- *Ubuntu Linux* [50] is the base for Linux Mint and a company effort to build a user friendly version of Linux. It is itself based on one of the oldest community distributions, *Debian* [51]. While the company behind it decides its direction, it still has a very strong community around it.

- *Linux Mint* [52] offers one of the most painless ways to get an open system with many probably familiar software like Firefox, VLC player, LibreOffice etc. However, their security policies have attracted some controversies (source [53]) and in the update manager you should select *Optimize stability and security* and regularly select *all* updates (also level 4) in the update manager to be safe. They offer different *Editions* of which *XFCE* is a simple, fast desktop that still runs well on old computers and *Cinnamon* is a bit more fancy.

- *Installation:* Make sure to save all your important data on some ***external*** medium (hard drive or stick) and get support from a computer geek if you can. It is usually possible to install Linux next to Windows (*dual boot*), but **expect the installation to overwrite everything**. To get you started here is a guide to install Ubuntu from a USB drive that should also work with Linux Mint if you just download their files, and here is a video how to to install Linux Mint. But first read the next paragraph…

7.3 Storage Encryption (Confidentiality)

Encrypt your computer! All further advices for software and communication means are not safe if your computer is not safe. **The encryption is intended against attacks on switched off computers only, if the police captures your computer unlocked, they will just copy your data.** A screen lock or suspend mode with a decent password is better than nothing, but the device should be powered down whenever possible. **If the police knocks your door, first run to your computer and press the power button until it switches off.**

There are three major ways to encrypt your data:

7.3.1 Encrypt Your Home Folder

Use this if unsure: only your personal data gets encrypted (including Firefox Bookmarks etc.), but the rest is not.

- ▲ Advantages:
  - △ The computer pretty much works as normal and your personal files are still very safe.
- ▼ Disadvantages:
  - ▽ You should use a long user password, which you will need to type each time the screen is locked.
  - ▽ It is possible to manipulate your programs (e.g. Firefox, GPG) so they reveal your passwords etc.

Howto :
during Linux installation, select "Encrypt my home folder" when creating your user.

7.3.2 Encrypt The Whole System

This means that only a tiny part of your hard drive remains unencrypted and everything else - your programs, etc. - is.

- ▲ Advantages:
  - △ It makes it harder e.g. to put a bad version of Firefox or GPG on your computer.
  - △ You can use a long strong password just for starting the computer and a shorter one for your screen lock.
- ▼ Disadvantages:
  - ▽ You need to start the computer, put in the disk encryption password and then wait for it to come up.
  - ▽ You need to remember two passwords.

Howto:
during Linux installation, at *Installation type* select "Encrypt the new (Linux Mint/Ubuntu) installation for security".

7.3.3 Use an Encrypted Container

An external drive or a very big file ("container") is encrypted and you need to unlock / put files in and out / lock the encryption separately.

- ▲ Advantages:
  - △ Can be used to transfer files between encrypted computers.

- △ Can be used on external hard drives.
- △ Can be used on Windows and Mac OS.
- △ Can be used as an additional secure place that is normally closed on an already encrypted Linux.
- △ Has special features to so that a fake password can show fake files, if you are forced to reveal a password.

▼ Disadvantages:

- ▽ All kinds of temporary files from LibreOffice, Thunderbird email, Firefox surfing profiles etc. are not encrypted.
- ▽ Needs to be opened and closed separately.

Howto :
get Veracrypt [54] and follow the howto [55].

7.3.4 Android and iOS

▷ **Android:** go to *Settings -> Security* and tap *Encrypt Phone* more elaborate howto

7.3.5 Limitations

Your password prompt must come from somewhere and so there's always unencrypted data on your device, data that can be messed with (e.g. replacing your Linux' password prompt with one that sends the password to the police). This can be

made harder with some tricks[C], but remember that the most realistic scenario is a simple police raid.

7.4 Backup your Data (Availability)

If it comes to a police raid (or a simple break-in), an oh-so-amazingly encrypted device will still be taken by the police. To take some of the pressure off yourself, **regularly** stash encrypted copies of your data outside your home, ideally with people that are not close relatives nor active in the same groups.

While we are at it, even public data should not be trusted to IT corporations, as they might just delete [58] or accidentally lose it.

8 Internet Services

So by now we can use a well-secured Laptop behind our locked door to write lengthy security guides, but how do we actually talk to people in a secure way?

Besides the technical aspects below, using alternative service providers offers an additional degree of protection, such as storing data encrypted and refusing to cooperate with the police. A list of alternative tech collectives can be found here [59] and even more here [60] and a list of email providers he-

[C] The only way to prevent this attack is to sign the unencrypted data and let some trusted part check the signature. This can either be done using a TPM, or more readily by using SecureBoot and trusting your manufacturer's firmware (which is what modern Linux distributions do). Some pointers: 1 [56], 2 [57]

re [61]. We recommend finding alternatives to Riseup.net, because their prominent position and the legal situation in the US puts a lot of pressure on a single tech collective, and in early 2017, they have cooperated with the police in two non-emancipatory criminal cases (source [62]). We do not think that there is an urgent need to move existing infrastructure away from Riseup.

8.1 A Word about Web Browsers

Web browsers like Mozilla Firefox or Google Chrome are complex monsters and a lot of web sites out there track their visitors. The Riseup Collective has a compact guide [63] how to use a browser more securely.

8.2 Anonymity

The whole point of the Internet is to connect two computers, like yours with… say *Youtube*. Now for the cat videos to find their way back to you, obviously the computers on the way (*routers*) need to know the Internet address of your connection. The trouble is that if any computer on the way is surveyed by the state, or you access an evil web site like e.g. that of the police, they could track that Internet address back to your physical location, or connect it with other online activity you were doing (like accessing your web mail). There are two ways to avoid this, which for additional security should ideally be combined with each other:

The first method is to use a software called *TOR* [64], or *The Onion Router*. In a nutshell, it works by sending your data in 3 layers of encryption (hence the "onion") over three computers (*TOR nodes*), where the first knows your Internet address and the second node to contact (but not the destination), the second knows nothing (only which the third node will be), and the third node knows the destination, but not the origin. For maximum security, it is best to install Tails [65] on a USB thumb drive and boot Tails on computer instead of the Linux / Windows or whatever operating system you're using normally. This way you have the best chance of having no connection between your anonymous activity and your normal use of the Internet. Second best is to follow the guides (Linux [66], Windows [67], Mac OS X [68]) and strictly only use the TOR Browser when doing anything sensitive.

If you must use a mobile device, there is a software called Orbot [69] for Android devices. On Apple devices, Onion browser [70] offers a at least a minimal TOR-enabled browser.

The second method is simply to use public wifi in places where there are no surveillance cameras. Unfortunately, your computer's wifi has a unique *MAC* address. It can be changed with software in case the wifi stores them (some corporate portals will, to tell if you already acknowledge the Terms of Service, or used up your hour of free Internet), but it is advisable to use this method only for extra security when using TOR (ideally using Tails, which will transmit random MAC address).

8.3 Email

Email is like postcards, assume it is read by transport providers and state agencies. PGP is a way to encrypt (wrap your postcard) email contents, but be aware that the email subject and the fact who is communicating when, with whom and from which computer, are not concealed.

Immerda.ch has is a nice German introduction into how PGP works here [71]. PGP depends on *keys* (special files of which the private key is protected with a password) that, like physical lock and keys, should restrict access to information. Therefore PGP's security depends on a safe key exchange; so make sure you got the right key, e.g. by getting it in person from the recipient.

The Electronic Frontier Foundation's Surveillance Self-Defence guide has a pretty good howto for using PGP (Linux [72], Windows [73], Mac OS X [74]).

You shouldn't use your activist email address on mobile devices at all, but if you must, **make sure your communication partners consent to that** and use K9-Mail [75] with OpenKeychain [76] on Android.

8.4 Mailing Lists

Now if PGP encrypts messages between two people, what about mailing lists? If there is just a small group, people can exchange PGP *public* keys and then everybody can encrypt their message so that every recipient can read it. Unfornately, this gets messy quickly if new people join the list. Therefore,

people came up with a solution that is not as secure, but better than nothing:

Schleuder [77] is a mailing list software that gets its own PGP pair. Everybody then encrypts email to Schleuder's mailing list key and Schleuder decrypts the message, and encrypts and sends it to each list member separately. Of course the downside is that whoever is running Schleuder could get hold of Schleuder's PGP private key and read the encrypted messages. Yet, as Schleuder is a complex beast, it is recommended to use it from a tech collective you trust, like for example Immerda.ch [78].

8.5 Messengers / Chat

TL;DR: don't use the rest and skip down to **Jabber** below, and use **Signal** for outside people (e.g. Journalists) that you can't get to use Jabber.

Skype has a reputation for being encrypted, however they have publicly stated their ability and willingness to hand out information to law enforcement, which they do in required cases. All your written text are stored on the servers of Skype and can be accessed by the police (source [79]).

Since some time, mobile messenger apps based on phone numbers have gained popularity. If you consider using any "secure" messengers on a mobile device, be reminded [80] that communication through the mobile network is vulnerable to eavesdropping and manipulation.

In order to figure out who of your contacts uses the same

application, the apps generally require uploading information on ***all*** of them to their servers (source [81]), but they do so in various degrees from grabbing the whole address book to just uploading an obscured form of the phone numbers. **The privacy implications of this for activist are huge, because one person uploading an anonymous number with the person's real name will ruin their effort.**

Whatsapp is by far the most successful mobile messenger to date, and recently they too claim to support "end to end" encryption (everything is encrypted between you and the people you talk to). However, the source code to their programs is not open. There are issues with their end-to-end encryption, though they appear non-intentional (source 1 [82], 2 [83], 3 [84]). In the past it has been possible for anyone to get profile details for any phone number (source [85]) and people can still snoop on any Whatsapp user's online status (source [86]).

Basically the same holds for **Threema**, as their software is not Open Source either.

Telegram has convinced many boasting with their altruism. They *do* provide the source code of their client, but their encryption is outdated techniques from the 70ies (source [87]), needs to be enabled manually and does not work for group chats. On the other hand, they *do* go all inclusive when they just grab your address book, unlike others not just number but with names (source [88]). Consequently, the German federal police has managed to hack into Group chats (German source).

Now, **Signal** [89]. The folks behind Signal are *a lot* more privacy minded than the rest of the phone number based messenger crowd and they were first to make end-to-end encrypted group chats feasible. Our take is that claims [90] of broken end-to-end encryption are inaccurate and actually based on cracking the individual mobile device, not Signal's encryption itself. Whilst they still technically get to see all the patterns of communication (but not the content) (source [91]), at least their founder comes from a more trustworthy background (source [92]; and he has some pretty funny stories [93], too). Still, the system is centralized and while the software is Open Source, they maintain tight control over their network. Signal is available for iOS and Android. Once one of these apps is registered, a Desktop software can be linked to the app, after which Signal can be used on a laptop or desktop computer without a mobile device. On Android, Signal is also available outside Google Play via `https://signal.org/android/apk/`, but Signal's inventor actively asks alternative software to leave the network (source [94]). People find elaborate ways to get around the need for a phone number (guide [95]). Altogether this makes Signal a good choice for people who use Android or Apple smartphones anyway, but **we wouldn't recommend using a mobile phone and number based plattform for internal group infrastructure.**

8.6 Jabber / XMPP

Enter **Jabber** / XMPP. *Finally, you made it!* ***This is what we currently recommend for sensitive real-time communication.***

Similarly to email, people from many different service providers (see the alternative tech collectives above) can talk to each other. Also similarly to email, per default Jabber offers only very weak encryption. For actual messages, *OTR* exists as a pretty okay encryption method for synchronous (both people online at the same time) communication. However, some caveats apply:

- The fact that two people are communicating is still not concealed, therefore use pseudonyms not linked to other activities.
- OTR commonly uses an authentication system based on things only the other person knows. It is important to make use of it to be sure you're actually talking to the right person. Otherwise if the dark side manages to intimidate your Jabber provider they could pose as your friend/comrade.
- Files sent via Jabber are not encrypted with OTR.
- Audio and video chats in Jabber clients are not encrypted by default.

Some clients support *OMEMO* as a newer alternative to OTR, which can also encrypt group chats and supports asynchronous communication, similar to the popular mobile messengers. With Conversations [96] for Android and ChatSecu-

re [97] for iOS, Jabber can be an alternative to these messengers that evades central control. Unfortunately, not all Jabber servers support stashing your messages when you're offline (see here [98] for an overview). Also, chat software for laptops or desktop computers has been a bit slow to pick up OMEMO. so for the foreseeable future, we recommend sticking to OTR. As an alternative to Pidgin (which is usually featured in the Jabber guides), we recommend installing Gajim [99]

einfachJabber.de [100] has an elaborate German introduction and guides for all kinds of devices and operating systems. English language tutorials can be found at the EFF's Surveillance Self-Defence guide (Linux [101], Mac OS [102], Windows [103]).

8.7 Voice / Video Chat

There are several solutions that are Open Source software, available for multiple computing platforms and offer end to end encryption of audio and video (overview [104]). If you can live with the disadvantages, Signal (see above) seems to be the most practical solution for mobile platforms.

On laptop / desktop computers, if you can get it to work, **Tox** [105] is a pretty amazing, high security and low effort alternative. More traditionally, **Jitsi** [106] enables encrypted calls via either a *SIP* or better yet, a Jabber/XMPP (see above) account. **Ring** [107] seems to be another promising alternative (that we haven't tried yet). **Mumble** [108] is a good solution if you can run your own server and also available via the Systemli tech collective.

A more ad-hoc method involves a technology called *WebRTC* just requires a modern web browser like Firefox or Chrome, with the caveat of trusting some central web site to not be malicous (and the connection to that network not to be manipulated). **pavala.tv** [109] and **meet.jit.si** [110] are two open source based web services for that.

8.8 Blogs, Websites and Social Media

Unless you have a computer security person in your group, you probably shouldn't run your own website, as the forces of evil frequently censor websites or - potentially worse - gather data about who operates them (source [111]). On the other hand, social media corporations will happily hand over data or mess with emancipatory content in a multiple ways (German source). The best alternative is to open a blog at one of the tech collectives, or let a trusted collective operate your website, if you really need a custom one.

9 Wrapping it Up

If this has gotten your head spinning, here is the bottom line.

9.1 TL;DR:

- Do actions with people you trust, be honest with them but don't gossip and brag and don't keep more information than necessary.

- Separate your activist and your bourgeois life's Internet identites as much as possible.
- Have meetings in inconspicuous locations without mobile phones.
- Put Linux on your computer and encrypt your data, learn to use PGP for inter-group email and build a network of Jabber contacts with verified OTR or OMEMO encryption for ad hoc chats.
- Learn to use TOR safely.
- Share skills, teach each other and don't panic.

9.2 Example Setups

- **Laptop / Desktop:** Tails for serious anonymity, encrypted Linux Mint with TOR Browser, Thunderbird+Enigmail for encrypted email, Veracrypt to encrypt external media, Gaijim for Jabber with OMEMO encryption, Signal Desktop if needed.
- **If you must, Smartphone for personal use:** an Android smartphone supported by Copperhead OS or well supported by Lineage OS, with data encryption, Orbot for TOR, Conversations for Jabber with OMEMO if necessary and Signal as a messenger app.

Sources and Links

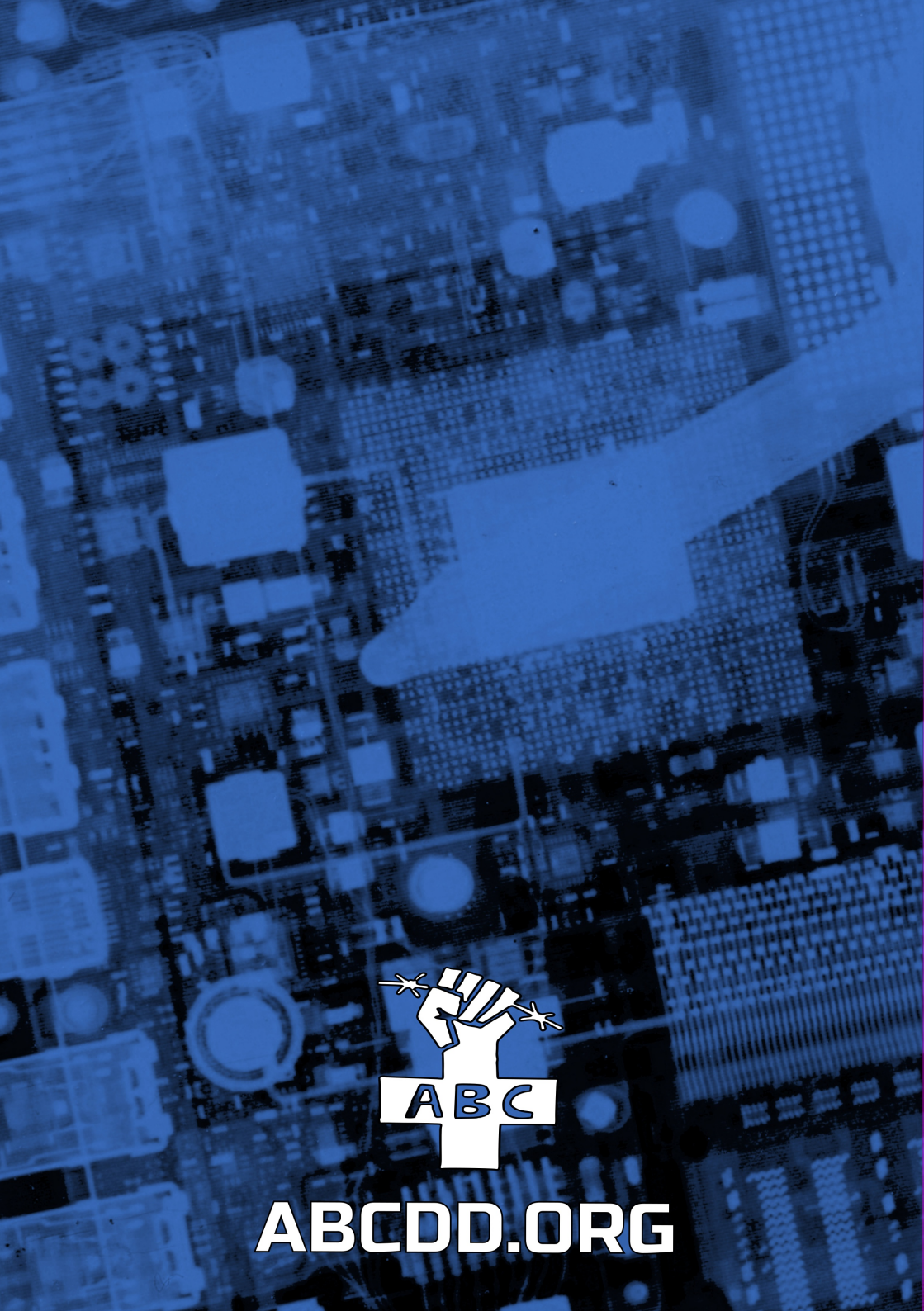
1 https://github.com/activist-security/security-guide
2 https://www.cs.tau.ac.il/~tromer/mobilesc/
3 https://electrospaces.blogspot.de/2017/06/dutch-russian-cyber-crime-case-reveals.html
4 https://www.wired.com/2016/09/machine-learning-can-identify-pixelated-faces-researchers-show/
5 https://theintercept.com/2017/09/23/police-schedule-7-uk-rabbani-gchq-passwords/
6 https://twitter.com/zeynep/status/904683388354867201
7 https://arxiv.org/abs/1708.09317
8 https://en.wikipedia.org/wiki/Lawful_interception
9 https://ferrancasanovas.wordpress.com/cracking-and-sniffing-gsm-with-rtl-sdr-concept/
10 https://medium.com/@philipn/want-to-see-something-crazy-open-this-link-on-your-phone-with-wifi-turned-off-9e0adb00d024
11 https://en.wikipedia.org/wiki/Cell_site#Range
12 http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz
13 https://www.cnet.com/how-to/how-to-delete-and-disable-your-google-location-history/
14 https://en.wikipedia.org/wiki/U-TDOA
15 https://de.wikipedia.org/wiki/GSM-Ortung#cite_note-3GPP43059-3
16 https://en.wikipedia.org/wiki/Short_Message_Service#Silent_SMS
17 https://en.wikipedia.org/wiki/IMSI-catcher
18 http://www.cnet.com/news/fbi-taps-cell-phone-mic-as-eavesdropping-tool/
19 http://www.osnews.com/story/27416/The_second_operating_system_hiding_in_every_mobile_phone
20 https://theintercept.com/2017/05/11/nyu-accidentally-expos

ed-military-code-breaking-computer-project-to-entire-internet/
[21] https://ssd.eff.org/en/node/23/#0
[22] https://en.wikipedia.org/wiki/Intel_Active_Management_Technology
[23] https://libreboot.org/
[24] https://github.com/ptresearch/me-disablement/blob/master/How%20to%20become%20the%20sole%20owner%20of%20your%20PC.pdf
[25] https://embedi.com/blog/bypassing-intel-boot-guard
[26] https://github.com/flothrone/bootguard
[27] https://schd.ws/hosted_files/osseu17/84/Replace%20UEFI%20with%20Linux.pdf
[28] http://blog.ptsecurity.com/2017/08/disabling-intel-me.html
[29] https://www.bleepingcomputer.com/news/security/malware-uses-obscure-intel-cpu-feature-to-steal-data-and-avoid-firewalls/
[30] http://www.osnews.com/story/27416/The_second_operating_system_hiding_in_every_mobile_phone
[31] https://www.tomsguide.com/us/backdoor-samsung-galaxy-devices,news-18470.html
[32] http://www.pcworld.com/article/2953052/security/most-android-phones-can-be-hacked-with-a-simple-mms-message-or-multimedia-file.html
[33] http://www.wthr.com/article/tapping-your-cell-phone
[34] https://mjg59.dreamwidth.org/46952.html
[35] https://crypto.stanford.edu/gyrophone/files/gyromic.pdf
[36] https://www.bleepingcomputer.com/news/security/234-android-applications-are-currently-using-ultrasonic-beacons-to-track-users/
[37] http://christian.wressnegger.info/content/projects/sidechannels/2017-eurosp.pdf
[38] https://sailfishos.org/
[39] https://www.engadget.com/2016/03/28/apple-s-encryption-battle-with-the-fbi-is-over-for-now/

[40] http://www.replicant.us/
[41] https://github.com/copperheados/
[42] https://lineageos.org/
[43] https://www.reddit.com/r/LineageOS/comments/66o5iv/questions_about_security/
[44] https://www.reddit.com/r/Android/comments/6g9imm/the_issue_of_security_in_lineageos/
[45] https://security.stackexchange.com/questions/162798/is-lineageos-more-secure-than-android-vanilla
[46] https://cve.lineageos.org/devices
[47] https://www.thedailybeast.com/this-is-how-cops-trick-dark-web-drug-dealers-into-unmasking-themselves
[48] https://theintercept.com/2015/06/22/nsa-gchq-targeted-kaspersky/
[49] https://tails.boum.org/
[50] http://www.ubuntu.com/desktop
[51] http://www.debian.org
[52] http://www.linuxmint.com/
[53] https://lwn.net/Articles/676664/
[54] https://veracrypt.codeplex.com/releases
[55] https://veracrypt.codeplex.com/wikipage?title=Beginner%27s%20Tutorial
[56] http://blog.hansenpartnership.com/owning-your-windows-8-uefi-platform/
[57] http://kroah.com/log/blog/2013/09/02/booting-a-self-signed-linux-kernel/
[58] http://fusion.net/story/325231/google-deletes-dennis-cooper-blog/
[59] https://www.systemli.org/en/friends.html
[60] https://help.riseup.net/en/security/resources/radical-servers
[61] https://prxbx.com/email/
[62] https://riseup.net/en/about-us/press/canary-statement
[63] https://riseup.net/en/better-web-browsing

[64] https://www.torproject.org/
[65] https://tails.boum.org/
[66] https://ssd.eff.org/en/module/how-use-tor-linux
[67] https://ssd.eff.org/en/module/how-use-tor-windows
[68] https://ssd.eff.org/en/module/how-use-tor-mac-os-x
[69] https://guardianproject.info/apps/orbot/
[70] https://mike.tig.as/onionbrowser/
[71] https://wiki.immerda.ch/index.php/immerda:GnuPGIntroduction
[72] https://ssd.eff.org/en/module/how-use-pgp-linux
[73] https://ssd.eff.org/en/module/how-use-pgp-windows
[74] https://ssd.eff.org/en/module/how-use-pgp-mac-os-x
[75] https://k9mail.github.io/
[76] https://www.openkeychain.org/
[77] http://schleuder2.nadir.org/
[78] https://wiki.immerda.ch/index.php/immerda:NewSchleuderList
[79] https://en.wikipedia.org/wiki/Skype_security#Eavesdropping_by_design
[80] http://news.softpedia.com/news/ss7-attack-leaves-whatsapp-and-telegram-encryption-useless-503894.shtml
[81] https://whispersystems.org/blog/contact-discovery/
[82] https://www.theguardian.com/technology/2017/jan/13/whatsapp-backdoor-allows-snooping-on-encrypted-messages
[83] https://whispersystems.org/blog/there-is-no-whatsapp-backdoor/
[84] http://technosociology.org/?page_id=1687
[85] https://www.lorankloeze.nl/2017/05/07/collecting-huge-amounts-of-data-with-whatsapp/
[86] https://robertheaton.com/2017/10/09/tracking-friends-and-strangers-using-whatsapp/
[87] https://unhandledexpression.com/2013/12/17/telegram-stand-back-we-know-maths/
[88] https://news.ycombinator.com/item?id=6915194
[89] https://signal.org/

[90] https://www.theregister.co.uk/2017/07/14/uk_spookhas_gchq_can_crack_endtoend_encryption_says_australian_ag/?mt=1500021512347
[91] https://en.wikipedia.org/wiki/Signal_(software)#Metadata
[92] https://moxie.org/blog/we-should-all-have-something-to-hide/
[93] https://moxie.org/stories.html
[94] https://github.com/LibreSignal/LibreSignal/issues/37#issuecomment-217211165
[95] https://yawnbox.com/index.php/2015/03/14/create-an-anonymous-textsecure-and-redphone-phone-number/
[96] https://conversations.im
[97] https://chatsecure.org/
[98] https://gultsch.de/compliance_ranked.html
[99] https://gajim.org/
[100] http://www.einfachjabber.de/
[101] https://ssd.eff.org/en/module/how-use-otr-linux
[102] https://ssd.eff.org/en/module/how-use-tor-mac-os-x
[103] https://ssd.eff.org/en/module/how-use-tor-windows
[104] https://en.wikipedia.org/wiki/Comparison_of_VoIP_software
[105] https://tox.chat
[106] https://jitsi.org/
[107] https://ring.cx/en
[108] https://mumble.info
[109] https://palava.tv/
[110] https://meet.jit.si/
[111] https://www.washingtonpost.com/local/public-safety/judge-lets-internet-firm-redact-user-identifying-data-in-information-provided-to-prosecutors-in-rioting-case/2017/10/10/dacf710a-adf2-11e7-9e58-e6288544af98_story.html


ABC
ABCDD.ORG