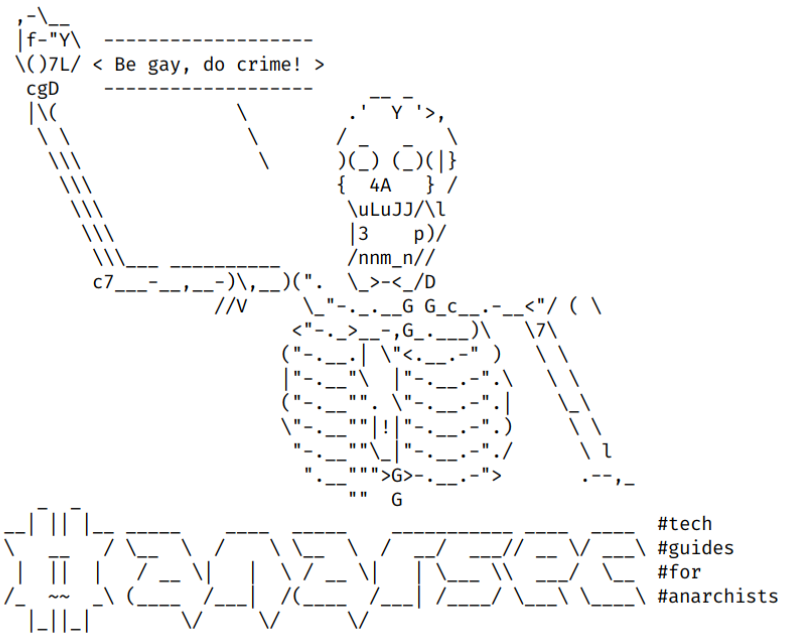
There are several different options for end-to-end encrypted communication, each with different trade-offs. This article provides an overview and installation instructions for Tails, Qubes OS, and GrapheneOS.



Encrypted Messaging for Anarchists

Series: Defensive

This version of the zine was last edited on 2024-04-19. Visit anarsec.guide to see whether it has been updated since.

The dagger symbol † on a word means that there is a glossary entry for it. Ai ferri corti.

AnarSec is a resource designed to help anarchists navigate the hostile terrain of technology — defensive guides for digital security and anonymity, as well as offensive guides for hacking. All guides are available in booklet format for printing and will be kept up to date.

Defensive

Tails

- Tails for Anarchists
- Tails Best Practices

Qubes OS

- Qubes OS for Anarchists

Phones

- Kill the Cop in Your Pocket
- GrapheneOS for Anarchists

General

- Linux Essentials
- Remove Identifying Metadata From Files
- Encrypted Messaging for Anarchists
- Make Your Electronics Tamper-Evident

Offensive

Coming soon

Contents

There are several different options for end-to-end encrypted† communication, each with different trade-offs. This article provides an overview and installation instructions for Tails, Qubes OS, and GrapheneOS. Before proceeding, let's go over a few concepts to help you distinguish between the different options.

- **End-to-end encryption** means (in theory) that only you and the person you are communicating with can read messages. However, not all encryption† is created equal. The quality of the encryption is determined by the *encryption protocol* used and how it's implemented at the software level.
- **Metadata protection** means that the message *metadata*† (the data about the data) is obscured. Even if the message itself is encrypted, metadata can reveal who is communicating with whom, when, how often, the sizes of any files that may have been transferred, and so on. Metadata exposure is a major concern[1].
- **Peer-to-peer** means that the messages do not pass through a centralized server.
- **Tor** is an anonymity network†. Some applications route your messages through Tor by default.

For a more in-depth look at these various considerations, we recommend The Guide to Peer-to-Peer, Encryption, and Tor: New Communication Infrastructure for Anarchists[2]. This text criticizes Signal for not being peer-to-peer and not using Tor by default, and goes on to compare Signal, Cwtch, and Briar.

Since anonymous public-facing projects such as counter-info websites interact with unknown (i.e. untrusted) contacts, they need more from encrypted communication than people using applications for private communication. These additional needs include:

- That anyone can contact the project
- Resiliency to correlation attacks†

[1] docs.cwtch.im/security/risk#threat-model
[2] notrace.how/resources/#pet-guide

VoIP (Voice over Internet Protocol)

Google Voice is a well-known and insecure VoIP service; this technology routes your calls over the Internet (as Signal does) instead of using standard cell tower transmission. Unlike Signal, VoIP allows you to receive calls from anyone, not just other Signal users. The advantage of using VoIP for calls over a data plan is that you can create different numbers for different activities (one for bills, one for signing up for a Signal account, etc.), and you never need to turn off Airplane mode. The advantage of using a data plan instead is that you can use it away from Wi-Fi, at the cost of geolocation (i.e. it will be possible for your service provider and possibly other parties to know where your device is at any given time).

Synchronous communication

Unlike asynchronous communication†, both parties must be online at the same time. This does not require servers for the communication and is often referred to as "peer to peer".

Tor network

Tor[129] (short for The Onion Router) is an open and distributed network that helps defend against traffic analysis. Tor protects you by routing your communications through a network of relays run by volunteers around the world: it prevents someone monitoring your Internet connection from learning what sites you visit, and it prevents the operators of the sites you visit from learning your physical location.

Every website visited through the Tor network passes through 3 relays. Relays are servers hosted by different people and organizations around the world. No single relay ever knows both where the encrypted connection is coming from and where it is going. An excerpt from a leaked top-secret NSA assessment calls Tor "the King of high secure, low latency Internet anonymity" with "no contenders for the throne in waiting". The Tor network can be accessed through the Tor Browser on any operating system. The Tails† operating system forces every program to use the Tor network when accessing the Internet.

For more information, see Tails for Anarchists[130] and Privacy Guides[131]. To understand the limitations of Tor, see the Whonix documentation[132].

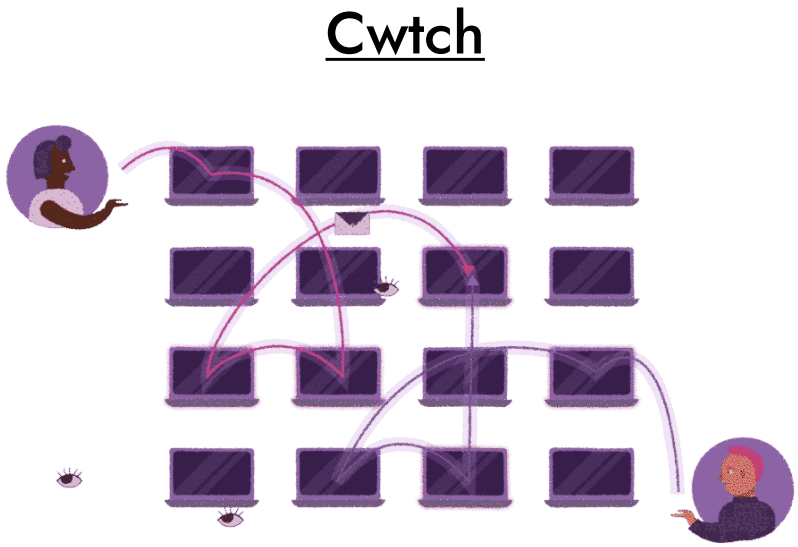
[129] torproject.org/
[130] anarsec.guide/posts/tails/#tor
[131] privacyguides.org/en/advanced/tor-overview/
[132] whonix.org/wiki/Warning

- Resiliency to exploits†
- For multiple project members to be able to access the same messages

The following recommendations for encrypted messaging are listed in order of highest to lowest metadata protection.

TL;DR

- Cwtch for text communication
- SimpleX Chat or Signal for voice/video calls
- PGP Email for anonymously-run public projects



- **Mediums**: Text
- **Metadata protection**: Yes (strong)
- **Encryption protocol**: Tor Onion Services (v3) + Tapir[3]
- **Peer-to-peer**: Yes
- **Tor**: Yes

[3] docs.cwtch.im/security/components/tapir/authentication_protocol

Cwtch is our preference for text communication by a long shot. Cwtch is designed with metadata protection in mind; it's peer-to-peer, uses the Tor network, and stores all data locally on the device, encrypted.

Like all peer-to-peer communication, Cwtch requires *synchronous*† communication, meaning that both people must be online at the same time. However, its server feature also allows *asynchronous*† communication by providing offline delivery:

> "Cwtch contact to contact chat is fully peer to peer, which means if one peer is offline, you cannot chat, and there is no mechanism for multiple people to chat. To support group chat (and offline delivery) we have created untrusted Cwtch servers which can host messages for a group. [...] the server has no way to know what messages for what groups it might be holding, or who is accessing it."

Cwtch servers enable group communication through untrusted infrastructure — these servers are "untrusted" because the protocol is designed to be secure against a malicious Cwtch server[4]. Once the server exists, contacts can be invited to use it. For asynchronous direct messaging, create a group chat with only two people.

Any Cwtch user can turn the app on their phone or computer into a server to host a group chat, though this is best for temporary needs like an event or short-term coordination, as the device must remain powered on for it to work. Fortunately, Anarchy Planet[5] runs a public server that is suitable for long-term groups.

Asynchronous conversations on Cwtch need to be started from a synchronous conversation — in other words, you need to be online at the same time as your contact to invite them to a group, and then you no longer need to be online at the same time. This "first contact" dynamic is not unique to Cwtch, but is present in all peer-to-peer

[4] docs.cwtch.im/security/components/cwtch/server
[5] anarchyplanet.org/chat.html#cwtch

Operating system (OS)

The system software that runs your device before any other software. Some common examples include Windows, macOS, Linux, Android, and iOS. Linux and some versions of Android are the only open-source options on this list.

Physical attacks

A physical attack is a situation where an adversary first gains physical access to your device through loss, theft, or confiscation. For example, your phone may be confiscated when you cross a border or are arrested. This is in contrast to a remote attack†.

For more information, see Making Your Electronics Tamper-Evident[124], the Threat Library[125], the KickSecure documentation[126], and Defend Dissent: Protecting Your Devices[127].

Remote attacks

By remote attack, we mean that an adversary would access the data on your phone or laptop through an Internet or data connection. There are companies that develop and sell the ability to infect your device (usually focusing on smartphones) with malware[111] that would allow their customer (your adversary, be it a corporate or state agent) to remotely access some or all of your information. This is in contrast to a physical attack†.

For a more detailed look, see Defend Dissent: Protecting Your Devices[128].

[124] anarsec.guide/posts/tamper
[125] notrace.how/threat-library/techniques/targeted-digital-surveillance/physical-access.html
[126] kicksecure.com/wiki/Protection_Against_Physical_Attacks
[127] open.oregonstate.education/defenddissent/chapter/protecting-your-devices/
[128] open.oregonstate.education/defenddissent/chapter/protecting-your-devices/

Exploit

An exploit is designed to take advantage of a vulnerability[111]. Even worse (or better, depending on whether you are the attacker or the target) are zero-day exploits[111].

Forward secrecy

Forward secrecy (FS, also known as "Perfect Forward Secrecy") combines a system of long-term keys and session keys to protect encrypted communications from future key compromise. An attacker who can record every encrypted message (man-in-the-middle[111]) won't be able to decrypt those messages if the keys are compromised in the future. Modern encryption protocols such as TLS[111] 1.3 and the Signal Protocol provide FS. For more information, see Anonymous Planet[121].

Metadata

Metadata is data that provides information about other data. For example, a JPG file contains the actual image (data) but it may also contain metadata such as the date the file was created, the type of camera, GPS coordinates, and so on. Metadata can be valuable to attackers (to find appropriate exploits for outdated software the target is using), government agencies (to collect information about people to create social graphs), and other parties (to target location-based advertising). Whenever you use a computer, you are likely leaving metadata behind.

For more information, see Remove Identifying Metadata From Files[122] and Defend Dissent: Metadata[123].

[121] anonymousplanet.org/guide.html#forward-secrecy
[122] anarsec.guide/posts/metadata
[123] open.oregonstate.education/defenddissent/chapter/metadata/

applications. In the future, Cwtch plans to improve this with hybrid groups[6]. Until hybrid groups are implemented, you will need to establish your asynchronous Cwtch conversations by using a second channel to set a time when you will both be online.

You can learn more about how to use Cwtch with the Cwtch Handbook[7].

Note

Briar[8] is another application that works in a similar way (with peer-to-peer and Tor), using the Bramble Transport Protocol[9] (BTP). Briar's main distinguishing feature is that it continues to work even when the underlying network infrastructure is down[10]. It was audited in 2017[11]. Unfortunately, Briar Desktop does not yet work with Tails or Qubes-Whonix because it cannot use the system Tor[12]. Unlike Cwtch, to connect to a contact on Briar, you both have to add each other first. You can either exchange `briar://` links or scan a contact's QR code if they are nearby. Briar Mailbox[13] allows asynchronous communication.

OnionShare[14] has a chat feature that creates an ephemeral peer-to-peer chat room that is routed over the Tor network. The metadata protection works in the same way as Cwtch; it uses the Tor network as a shield and stores everything (ephemerally) locally on the device running OnionShare. OnionShare doesn't implement any chat encryption on its own — it relies on the Tor onion service's encryption. Cwtch and Briar both have more features (including the additional Tapir and BTP encryption protocols). The only advantage of OnionShare is that it is installed on Tails by default.

[6] docs.cwtch.im/blog/path-to-hybrid-groups/
[7] docs.cwtch.im/
[8] briarproject.org

For Anonymous Public-facing Projects

Need #1: That anyone can contact the project

Anyone can connect to a public Cwtch account when it's online. If the account is offline, it's not currently possible to establish first contact, though this will be supported in the future.

Need #2: Resiliency to correlation attacks

Real-time messaging applications are particularly susceptible to end-to-end correlation attacks because of the ability of an adversary, once they know their target's ID on the messaging platform, to trigger incoming network traffic on the target's side by sending them messages on the platform (when the target is online). "Appear Offline Mode" in Cwtch allows a user to selectively connect to trusted contacts and groups, while appearing offline to everyone else. An issue[15] is open to further address this.

Content padding exists[16] to frustrate correlation attacks via message size.

Need #3: Resiliency to exploits

A vulnerability in any application can be targeted with exploits — a severe vulnerability can allow an adversary to hack your system, such as by permitting Remote Code Execution[17]. Cwtch libraries are written in memory-safe languages (Go and Rust) and Cwtch does fuzz testing[18]

[9] code.briarproject.org/briar/briar/-/wikis/A-Quick-Overview-of-the-Protocol-Stack

[10] briarproject.org/how-it-works/

[11] code.briarproject.org/briar/briar/-/wikis/FAQ#has-briar-been-independently-audited

[12] code.briarproject.org/briar/briar/-/issues/2095

[13] briarproject.org/download-briar-mailbox/

[14] docs.onionshare.org/2.6/en/features.html#chat-anonymously

[15] git.openprivacy.ca/cwtch.im/cwtch-ui/issues/712

[16] docs.cwtch.im/security/components/tapir/packet_format

[17] en.wikipedia.org/wiki/Arbitrary_code_execution

[18] openprivacy.ca/discreet-log/07-fuzzbot/

subject, see Thirteen Years of Tor Attacks[116] and the design proposal on information leaks in Tor[117].

Encryption

Encryption is the process of scrambling a message so that it can only be unscrambled (and read) by the intended parties. The method you use to scramble the original message, or *plaintext*, is called the *cipher* or *encryption protocol*. In almost all cases, the cipher is not intended to be kept secret. The scrambled, unreadable, encrypted message is called the ciphertext and can be safely shared. Most ciphers require an additional piece of information, called a *cryptographic key*, to encrypt and decrypt (scramble and unscramble) messages.

For more information, see symmetric cryptography[111], asymmetric cryptography[111], or Defend Dissent: What is Encryption?[118]

End-to-end encryption (e2ee)

Data is encrypted† as it travels from one device to another — endpoint to endpoint — and cannot be decrypted by any intermediary. It can only be decrypted by the endpoints. This is different from "encryption at rest", such as Full Disk Encryption[111], where the data stored on your device is encrypted when the device is turned off. Both are important!

For more information, check out Encrypted Messaging for Anarchists[119], and Defend Dissent: Protecting Your Communications[120].

[116] github.com/Attacks-on-Tor/Attacks-on-Tor#correlation-attacks

[117] spec.torproject.org/proposals/344-protocol-info-leaks.html

[118] open.oregonstate.education/defenddissent/chapter/what-is-encryption/

[119] anarsec.guide/posts/e2ee

[120] open.oregonstate.education/defenddissent/chapter/protecting-your-communications/

Appendix: Glossary

Asynchronous Communication

Unlike synchronous communication†, both parties do not need to be online at the same time. This relies on some sort of server to store messages until the message recipients come online. This is the type of messaging that most people are familiar with (email, Signal, etc.).

Command Line Interface (CLI)

The "command line" is an all-text alternative to the graphical "point and click" tool that most of us are more familiar with; the Command Line Interface (CLI) allows us to do some things that a Graphical User Interface (GUI) does not. Often, either a GUI or a CLI would work, and which you use is a matter of preference. For example, in Tails†, you can verify the checksum[111] of a file using either a GUI (the GtkHash program) or a CLI command (`sha256sum`).

For more information, see Linux Essentials[112]. The Tech Learning Collective's "Foundations: Linux Journey" course on the command line[113] is our recommended introduction to using the CLI/terminal.

Correlation Attack

An end-to-end correlation attack is a theoretical way that a global adversary could break the anonymity of the Tor network†. For more information, see Protecting against determined, skilled attackers[114] and Make Correlation Attacks More Difficult[115]. For research papers on the

[111] anarsec.guide/glossary

[112] anarsec.guide/posts/linux/#the-command-line-interface

[113] techlearningcollective.com/foundations/linux-journey/the-shell

[114] anarsec.guide/posts/tails-best/#2-protecting-against-determined-skilled-attackers

[115] anarsec.guide/posts/tails/#make-correlation-attacks-more-difficult

to find bugs. See the Security Handbook[19] to learn more. For public-facing project accounts, we recommend against enabling the "file sharing experiment" or the "image previews and profile pictures experiment" in the settings.

Need #4: For multiple project members to be able to access the same messages

If a project has multiple members, all of them should be able to access the same messages independently. Currently, this is not possible with Cwtch.

Installation

Cwtch Installation on GrapheneOS

Install Cwtch the same way you would install any app that doesn't require Google Services[20] (we don't recommend F-Droid).

Cwtch Installation on Tails

Cwtch support for Tails is very new and not thoroughly tested.

- Start Tails with an Adminstration Password.
- Download Cwtch for Linux[21] with Tor Browser
- According to our Tails Best Practices[22], personal data should be stored on a second LUKS USB and Persistent Storage should not be enabled. Extract the folder with the file manager (right click, select "Extract"), then move the `cwtch` folder to such a "personal data" LUKS USB.
- Run the install script
  - In the File Manager, enter the `cwtch` directory you just moved, so that you can see a file named "install-tails.sh". Right click in the File Manager and select "Open in Terminal"
  - Run `./install-tails.sh` and enter the Administration Password when prompted.

[19] docs.cwtch.im/security/intro

[20] anarsec.guide/posts/grapheneos/#how-to-install-software

- You can now launch Cwtch from the “Activities” overview.
- With Persistent Storage disabled, profile data must be restored from backup every session you need to install Cwtch. Export your profile when you are done using Cwtch, copy it to the “personal data” LUKS USB, and import it again the next time you install Cwtch.
  - Alternatively, you can backup `/home/amnesia/.cwtch` to the “personal data” LUKS USB, and copy it back to `/home/amnesia/` before you open Cwtch during your next session, in order to also persist configuration settings. “Show Hidden Files” will need to be enabled in the File Manager.
- When a new version of Cwtch is released, you will have to update manually. Download the new version, extract it, and replace the `cwtch` folder.

Cwtch Installation on Qubes-Whonix

Cwtch on Whonix does not guarantee Tor Stream Isolation[23] from other applications in the same qube, so we will install it in a dedicated qube. Cwtch is installed in an App qube, follow the installation instructions[24].

SimpleX Chat

[21] cwtch.im/download/#linux
[22] anarsec.guide/posts/tails-best/#using-a-write-protect-switch
[23] anarsec.guide/posts/qubes/#whonix-and-tor
[24] docs.cwtch.im/docs/platforms/whonix/

moderating a sketchy website, researching for actions, reading articles that may be criminalized, etc.). Tails runs from a USB drive and is designed with the anti-forensic property of leaving no trace of your activity on your computer, as well as forcing all Internet connections through the Tor network†. See Tails for Anarchists[104] and Tails Best Practices[105].

Operating system†: Qubes OS has better security than Tails for many use cases, but has a steeper learning curve and no anti-forensic features. However, it is accessible enough for journalists and other non-technical users. Basic knowledge of using Linux is required — see Linux Essentials[106]. Qubes OS can even run Windows programs such as Adobe InDesign, but much more securely than a standard Windows computer. See Qubes OS for Anarchists[107].

See When to Use Tails vs. Qubes OS[108]. We do not offer “harm reduction” advice for Windows or macOS computers, as this is already widespread and gives a false sense of privacy and security.

Encrypted Messaging

See Encrypted Messaging for Anarchists[109]

Storing Electronic Devices

See Make Your Electronics Tamper-Evident[110].

[104] anarsec.guide/posts/tails/
[105] anarsec.guide/posts/tails-best/
[106] anarsec.guide/posts/linux
[107] anarsec.guide/posts/qubes/
[108] anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os
[109] anarsec.guide/posts/e2ee/
[110] anarsec.guide/posts/tamper/

the purposes of incrimination[98] and network mapping[99]. Our goal is to obscure the State's visibility into our lives and projects. Our recommendations are intended for all anarchists, and they are accompanied by guides to put the advice into practice.

We agree with the conclusion of an overview of targeted surveillance measures in France[100]: "So let's be clear about our responsibilities: if we knowingly bring a networked device equipped with a microphone and/or a camera (cell phone, baby monitor, computer, car GPS, networked watch, etc.) close to a conversation in which "private or confidential words are spoken" and must remain so, even if it's switched off, we become a potential state informer..."

You may also be interested in the Threat Library's "Digital Best Practices"[101].

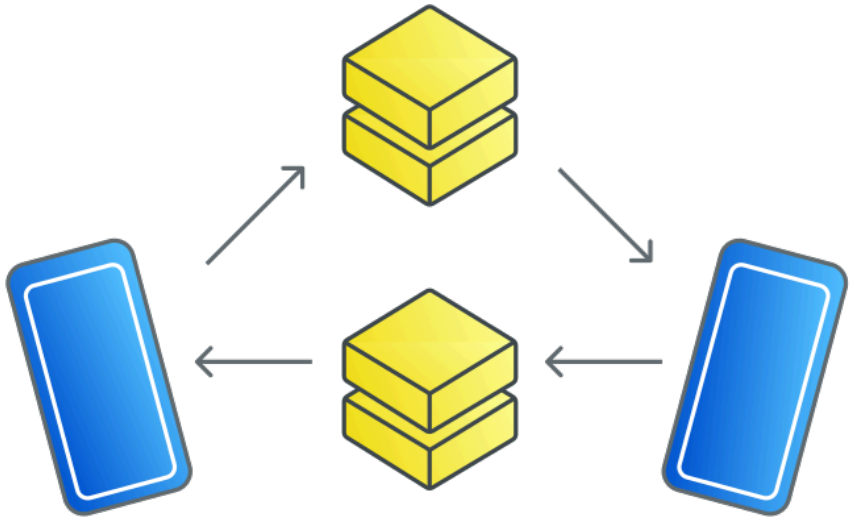
Your Phone

> **Operating system†**: **GrapheneOS** is the only reasonably secure choice for cell phones. See GrapheneOS for Anarchists[102]. If you decide to have a phone, treat it like an "encrypted landline" and leave it at home when you are out of the house. See Kill the Cop in Your Pocket[103].

Your Computer

> **Operating system†**: **Tails** is unparalleled for sensitive computer use (writing and sending communiques,

[98] notrace.how/threat-library/tactics/incrimination.html
[99] notrace.how/threat-library/techniques/network-mapping.html
[100] actforfree.noblogs.org/post/2023/07/24/number-of-the-day-89502-preventive-surveillance-measures-france/
[101] notrace.how/threat-library/mitigations/digital-best-practices.html
[102] anarsec.guide/posts/grapheneos/
[103] anarsec.guide/posts/nophones/



- **Mediums**: Video call, voice call, text
- **Metadata protection**: Yes (Moderate)
- **Encryption protocol**: SimpleX Messaging Protocol[25], audited (2022[26]), and SimpleX File Transfer Protocol[27]
- **Peer-to-peer**: No
- **Tor**: Not default

SimpleX Chat allows voice and video calls, but this inherently provides less metadata protection[28]. As a design choice to facilitate asynchronous communication, SimpleX Chat is not peer-to-peer — it uses decentralized servers that anyone can host[29] and does not rely on any centralized component. Servers do not store any user information (no user profiles or contacts, or messages once they are delivered), and

[25] simplex.chat/docs/protocol/simplex-chat.html
[26] simplex.chat/blog/20221108-simplex-chat-v4.2-security-audit-new-website.html
[27] simplex.chat/blog/20230301-simplex-file-transfer-protocol.html
[28] mastodon.social/@sarahjamielewis/112311305534271974
[29] simplex.chat/docs/server.html

primarily use in-memory persistence. To understand what a server can and cannot see, read the threat model[30].

Since SimpleX requires that users place some trust in the SimpleX servers[31], **we recommend prioritizing Cwtch over SimpleX Chat for text communication with other anarchists, and using SimpleX Chat or Signal for voice and video calls**. Unlike Signal, SimpleX Chat doesn't require a phone number or smartphone.

If SimpleX is served with a warrant, their privacy policy[32] is quite specific. Servers have the records of the message queues[33] and any undelivered encrypted messages[34] — no data is stored that links the queues or messages to particular users, and the data which is stored is not very useful without access to the user's device.

SimpleX Chat will work with Tor if used on an operating system that forces it to, such as Whonix or Tails. However, voice and video calls generally don't work very well over Tor regardless of which application you use.

You can learn more about how to use SimpleX Chat with their guide[35]. Make sure to set a database passphrase[36].

For Anonymous Public-facing Projects

Need #1: That anyone can contact the project

[30] github.com/simplex-chat/simplexmq/blob/stable/protocol/overview-tjr.md#simplex-messaging-protocol-server

[31] github.com/simplex-chat/simplexmq/blob/stable/protocol/overview-tjr.md#trust-in-servers

[32] github.com/simplex-chat/simplex-chat/blob/stable/PRIVACY.md

[33] github.com/simplex-chat/simplex-chat/blob/stable/PRIVACY.md#connections-with-other-users

[34] github.com/simplex-chat/simplex-chat/blob/stable/PRIVACY.md#messages-and-files

[35] simplex.chat/docs/guide/readme.html

[36] simplex.chat/docs/guide/privacy-security.html#database-passphrase

Applications we do not recommend

We do *not* recommend:

- **Telegram**: Telegram has no end-to-end encryption for group chats, and it is opt-in for one-on-one chats. The encryption doesn't use established protocols, and has had cryptographers describe it as "the most backdoor-looking bug I've ever seen"[89].
- **Matrix/Element**: Matrix has a problem that is inherent in federated networks — terrible metadata leakage[90] and data ownership[91]. It has no forward secrecy, the Element client has a large attack surface, and there is a long list of other issues[92]. What's more, the developers are very friendly with various national police agencies[93].
- **XMPP Clients**: Regardless of the client, an XMPP server will always be able to see your contact list[94]. Additionally, server-side parties (e.g., administrators, attackers, law enforcement) can inject arbitrary messages, modify address books, log passwords in cleartext[95] and act as a man-in-the-middle[96].

Appendix: Recommendations

As anarchists, we must defend ourselves against police and intelligence agencies that conduct targeted digital surveillance[97] for

[89] words.filippo.io/dispatches/telegram-ecdh/

[90] anarc.at/blog/2022-06-17-matrix-notes/#metadata-handling

[91] anarc.at/blog/2022-06-17-matrix-notes/#data-retention-defaults

[92] telegra.ph/why-not-matrix-08-07

[93] element.io/blog/bundesmessenger-is-a-milestone-in-germanys-ground-breaking-vision/

[94] coy.im/documentation/security-threat-model/

[95] web.archive.org/web/20211215132539/https://infosec-handbook.eu/articles/xmpp-aitm/

[96] notes.valdikss.org.ru/jabber.ru-mitm/

[97] notrace.how/threat-library/techniques/targeted-digital-surveillance.html

Anyone can send a message to a public email account regardless of whether the recipient is online or offline.

Need #2: Resiliency to correlation attacks

Email is not a real-time messaging application — this means that it is not particularly susceptible to end-to-end correlation attacks via time.

No content padding exists to frustrate correlation attacks via message size in email protocols, but if you access the mail servers through Tor then the traffic is padded.

Need #3: Resiliency to exploits

A vulnerability in any application can be targeted with exploits — a severe vulnerability can allow an adversary to hack your system, such as by permitting Remote Code Execution[87]. Email can be accessed through webmail (via Tor Browser) or through a client like Thunderbird — these have different attack surfaces. For example, a Cwtch developer found an exploit to turn Thunderbird into a decryption oracle[88] when it displays messages with HTML.

We recommend using Thunderbird (which is available in Tails and Qubes-Whonix by default) with the setting to display email as "Plain Text" rather than as HTML: **View → Message Body As → Plain Text**. Most webmail will not function with Tor Browser in "Safest" mode.

Need #4: For multiple project members to be able to access the same messages

If a project has multiple members, all of them should be able to access the same messages independently. This is straight forward with email, if all project members have the email password and the private PGP key.

[87] en.wikipedia.org/wiki/Arbitrary_code_execution

[88] pseudorandom.resistant.tech/disclosing-security-and-privacy-issues-in-thunderbird.html

Unlike the one-time invitation links that are normally used by SimpleX Chat and shared through a separate channel, you also have a long term address[37] that can be published online so that anyone can connect to you. We recommend against enabling "Auto-accept".

Need #2: Resiliency to correlation attacks

Real-time messaging applications are particularly susceptible to end-to-end correlation attacks because once an adversary knows their target's ID on the messaging platform, they can trigger incoming network traffic on the target's side by sending them messages on the platform (when the target is online). An issue[38] is open to address this. Message "mixing" is also planned[39].

Content padding exists[40] to frustrate correlation attacks via message size.

Need #3: Resiliency to exploits

A vulnerability in any application can be targeted with exploits — a severe vulnerability can allow an adversary to hack your system, such as by permitting Remote Code Execution[41]. For public-facing project accounts, we recommend that you set SimpleX Chat preferences to only allow text (prohibiting voice messages and attachments).

Need #4: For multiple project members to be able to access the same messages

If a project has multiple members, all of them should be able to access the same messages independently. Currently, this is not possible with SimpleX Chat.

[37] simplex.chat/docs/guide/app-settings.html#your-profile-settings

[38] github.com/simplex-chat/simplex-chat/issues/3197

[39] github.com/simplex-chat/simplex-chat#privacy-and-security-technical-details-and-limitations

[40] github.com/simplex-chat/simplex-chat#privacy-and-security-technical-details-and-limitations

[41] en.wikipedia.org/wiki/Arbitrary_code_execution

Installation

SimpleX Chat Installation on GrapheneOS

Install SimpleX Chat the same way you would install any app that doesn't require Google Services[42] (we don't recommend F-Droid). If you're using a VPN (as we recommend[43]) then the default relay for calls is redundant and can be turned off to improve call quality: **Settings → Audio & video calls**, disable **Always use relay**

SimpleX Chat Installation on Tails

- Tails does *not* need an Administration Password to run an AppImage package.
- Download the AppImage[44] with Tor Browser
- According to our Tails Best Practices[45], personal data should be stored on a second LUKS USB and Persistent Storage should not be enabled. Copy the .AppImage file to such a "personal data" LUKS USB.
- Make the AppImage executable
  - In the File Manager, right-click "Properties". Under "Permissions", enable "Executable as Program".
- You can now launch SimpleX Chat by double-clicking the AppImage file.
- In **Settings → Network & Servers**, enable "Use SOCKS proxy (port 9050)" (to configure SimpleX Chat to go through Tor[46]). You can now create a SimpleX address.
- With Persistent Storage disabled, configuration and profile data must be restored from backup every session you use SimpleX Chat. Export your database (**Settings → Database passphrase & export**) when you are done using SimpleX Chat, copy it to the "personal data" LUKS USB, and import it again the next time you use SimpleX Chat.
  - Alternatively, you can backup `/home/amnesia/.local/share/simplex` to the "personal data" LUKS USB, and copy it back to `/`

[42] anarsec.guide/posts/grapheneos/#how-to-install-software
[43] anarsec.guide/posts/grapheneos/#how-to-install-software

forward secrecy†. The goal of forward secrecy is to protect past sessions from future key or password compromises. It maintains the secrecy of past communications even if the current communication is compromised. This means that an adversary could decrypt all past PGP messages in one fell swoop. When you also consider the metadata exposure inherent in email, PGP simply doesn't meet the standards of modern cryptography. For a more technical critique, see The PGP Problem[81] and Stop Using Encrypted Email[82]. Privacy Guides[83] agrees that "email is best used for receiving transactional emails [...], not for communicating with others." **We recommend that anarchists still using PGP email use Cwtch groups instead.**

There is an exception: for anonymous public-facing projects, we still recommend using PGP email because it is currently the best option that meets the additional needs required by a public account. Use a radical server[84] that doesn't require an invite code. You can learn more about how to use PGP email with the Riseup Guide to Encrypted Email[85].

> **Note**
>
> PGP is used for another purpose outside of communication: verifying the integrity and authenticity of files. For this use case, see our explanation[86].

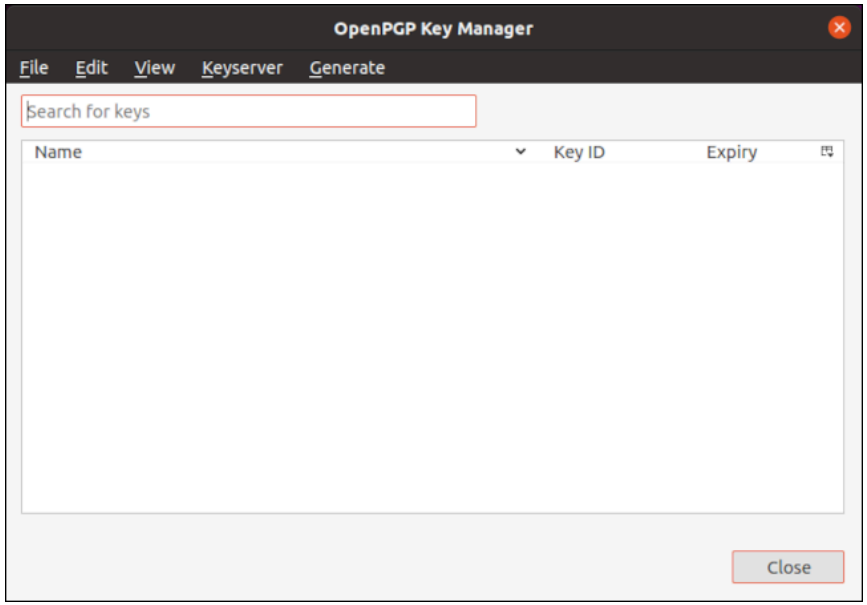
For Anonymous Public-facing Projects

Need #1: That anyone can contact the project

[81] latacora.micro.blog/2019/07/16/the-pgp-problem.html
[82] latacora.micro.blog/2020/02/19/stop-using-encrypted.html
[83] privacyguides.org/en/basics/email-security/
[84] riseup.net/en/security/resources/radical-servers
[85] riseup.net/en/security/message-security/openpgp
[86] anarsec.guide/posts/tails-best/#appendix-gpg-explanation

Templates. Signal Desktop on Flathub is community maintained[78], not official, which is a security consideration[79].

PGP Email



- **Mediums**: Text
- **Metadata protection**: No
- **Encryption protocol**: RSA[80] or ed25519, no forward secrecy
- **Peer-to-peer**: No
- **Tor**: Not default

PGP (Pretty Good Privacy) is not so much a messaging platform as it is a way to encrypt messages on top of existing messaging platforms (in this case, email). PGP email does not have the encryption property of

[77] micahflee.com/2021/11/introducing-qube-apps/
[78] github.com/flathub/org.signal.Signal
[79] kicksecure.com/wiki/Install_Software#Flathub_Package_Sources_Security
[80] blog.trailofbits.com/2019/07/08/fuck-rsa/

`home/amnesia/.local/share` before you open SimpleX during your next session. "Show Hidden Files" will need to be enabled in the File Manager.

- When a new version of SimpleX Chat is released, you will have to update manually. Download the new version and replace the .AppImage file.

SimpleX Chat Installation on Qubes-Whonix

SimpleX Chat on Whonix does not guarantee Tor Stream Isolation[47] from other applications in the same qube, so we will install it in a dedicated qube. SimpleX Chat is installed in an App qube, not a Template (because it is an AppImage).

- Download the AppImage[48] using Tor Browser in a disposable Whonix qube.
- Create an App qube[49] with the Template `whonix-workstation-17` and networking `sys-whonix`.
- Copy the file to your new App qube
- Make the AppImage executable
  - In the File Manager, right-click "Properties". Under "Permissions", enable "Allow this file to run as a program".
- You can now launch SimpleX Chat by double-clicking the AppImage file.
- When a new version of SimpleX Chat is released, you will have to update manually. Download the new version and replace the .AppImage file.

Signal

[44] simplex.chat/downloads/#desktop-app
[45] anarsec.guide/posts/tails-best/#using-a-write-protect-switch
[46] tails.net/doc/persistent_storage/additional_software/index.en.html#index5h2
[47] anarsec.guide/posts/qubes/#whonix-and-tor
[48] simplex.chat/downloads/#desktop-app
[49] anarsec.guide/posts/qubes/#how-to-organize-your-qubes

- **Mediums**: Video call, voice call, text
- **Metadata protection**: Yes (Moderate)
- **Encryption protocol**: Signal Protocol, audited (2017[50])
- **Peer-to-peer**: No
- **Tor**: Not default

The Signal Protocol has a moderate amount of metadata protection; sealed sender[51], private contact discovery[52], and the private group system[53]. Message recipient identifiers are only stored on Signal's servers for as long as it takes to deliver each message. As a result, if Signal is served with a warrant, they will only be able to provide[54] the time of account creation and the date of the account's last connection to the Signal servers. Still, Signal relies on the Google Services Framework (though it's possible to use Signal without it), and the sealed sender metadata protection applies only to contacts (by default).

[50] en.wikipedia.org/wiki/Signal_Protocol
[51] signal.org/blog/sealed-sender/
[52] signal.org/blog/private-contact-discovery/
[53] signal.org/blog/signal-private-group-system/
[54] signal.org/bigbrother/

- Go to **Applications menu → Qubes Tools → Qube Manager**
- Clone whonix-workstation-17 and name it something like whonix-workstation-17-signal.
  - We do this to avoid adding attack surface to the base Whonix Workstation template. If you also install other messaging applications, they could share a cloned template with a name like whonix-workstation-17-e2ee
- Open a Terminal in the new Template: **Applications menu → Template: whonix-workstation-17-signal: Xfce Terminal**
- Run the commands in the Signal installation guide[75] to install Signal Desktop in the Template.
  - Note that the layout of the Signal installation guide is a bit confusing for users unfamiliar with the command line; `wget` and `cat` are separate commands, but `echo` in #2 is a command so long that it takes two lines (which is why the second line is indented).
  - Template qubes require a proxy for `wget`. Before running the command, create a configuration file at `~/.wgetrc` in the Template, with the following contents:

```
use_proxy = on
http_proxy = 127.0.0.1:8082
https_proxy = 127.0.0.1:8082
```

- Create an App qube[76] with the Template `whonix-workstation-17-signal` and networking `sys-whonix`.
- In the **Settings → Applications** tab of the new App qube, you may need to click "Refresh applications" for Signal to show up. Move Signal to the Selected column and press "OK".
- Updates will be handled by **Qubes Update** as you would expect.

Alternative method

You can install Signal Desktop in a Whonix Workstation App qube using Qube Apps[77] and not need to bother with

[75] signal.org/download/linux/
[76] anarsec.guide/posts/qubes/#creating-qubes

turned off: **Settings → Privacy → Advanced**, disable **Always relay calls**

Molly-FOSS[67] is a fork of Signal with hardening and anti-forensic features available on Android — we recommend it over Signal, and trusting the Molly team is made easier by its reproducible builds[68]. Follow the instructions for installing software that isn't available in the Play Store[69]. You can migrate from an existing Signal account[70]. Turn on database encryption.

Signal Installation on Tails

About.Privacy maintains a guide[71] for installing Signal Desktop on Tails. There is a guide for registering an account from Tails without a smartphone (using Signal-cli), and another guide for if you already have a Signal account.

Some of the Signal Configuration and Hardening Guide[72] also applies to Signal Desktop.

Signal Installation on Qubes-Whonix

Signal Desktop on Whonix is not guaranteed to have Tor Stream Isolation[73] from other applications in the same qube, so we will install it in a dedicated qube. Signal Desktop is installed in a Template, not an App qube (because it is available as a .deb from a third party repository).

Some of the Signal Configuration and Hardening Guide[74] also applies to Signal Desktop.

[67] blog.privacyguides.org/2022/07/07/signal-configuration-and-hardening/#molly-android

[68] github.com/mollyim/mollyim-android/tree/main/reproducible-builds

[69] anarsec.guide/posts/grapheneos/#software-that-isn-t-on-the-play-store

[70] github.com/mollyim/mollyim-android#compatibility-with-signal

[71] 0xacab.org/about.privacy/messengers-on-tails-os/-/wikis/HowTo

[72] blog.privacyguides.org/2022/07/07/signal-configuration-and-hardening/

[73] anarsec.guide/posts/qubes/#whonix-and-tor

[74] blog.privacyguides.org/2022/07/07/signal-configuration-and-hardening/

Signal is not peer-to-peer; it uses centralized servers that we must trust. Signal will work with Tor if used on an operating system that forces it to, such as Whonix or Tails.

Signing up for a Signal account is difficult to do anonymously. The account is tied to a phone number that the user must retain control of — due to changes in "registration lock"[55], it is no longer sufficient to register with a disposable phone number. An anonymous phone number can be obtained on a burner phone or online[56] and must be maintained as long as you're using it, which takes some technical know-how and money, limiting the amount of people who will do this.

Another barrier to anonymous registration is that Signal Desktop will only work if Signal is first registered from a smartphone. For users familiar with the command line†, it is possible to register an account from a computer using Signal-cli[57]. The VoIP† account used for registration would have to be obtained anonymously.

These barriers to anonymous registration mean that Signal is rarely used anonymously. This has significant implications if the State gains physical† or remote† access to the device. One of the primary goals of State surveillance of anarchists is network mapping[58], and it's common for them to gain physical access to devices through house raids[59] or arrests. For example, if police bypass your device's authentication[60], they can identify Signal contacts (as well as the members of any groups you are in) simply by their phone numbers, if those contacts haven't changed their settings to hide their phone number.

In a recent repressive operation in France against a riotous demonstration[61], the police did exactly that. Police got physical access

[55] blog.privacyguides.org/2022/11/10/signal-number-registration-update/

[56] anonymousplanet.org/guide.html#getting-an-anonymous-phone-number

[57] 0xacab.org/about.privacy/messengers-on-tails-os/-/wikis/HowTo#signal

[58] notrace.how/threat-library/techniques/network-mapping.html

[59] notrace.how/threat-library/techniques/house-raid.html

[60] notrace.how/threat-library/techniques/targeted-digital-surveillance/authentication-bypass.html

[61] notrace.how/resources/#lafarge

to suspects' phones during arrests and house raids, remote access through spyware, and then identified Signal contacts and group members. These identities were added to the list of suspects who were subsequently investigated.

The risk of a compromised device aiding the police in network mapping is partly mitigated by the username feature[62] — use it to prevent a Signal contact from being able to learn your phone number. In **Settings → Privacy → Phone Number**, set both **Who can see my number** and **Who can find me by number** to **Nobody**. We recommend that you select a profile name and photo that won't be useful for establishing your identity. For voice and video calls, Signal reveals the IP address of both parties by default, which could also be used to identify Signal contacts. If you aren't using Signal from behind a VPN or Tor, then in **Settings → Privacy → Advanced**, enable **Always relay calls** to prevent this.

A private company that sells spyware to governments has a product called JASMINE that is marketed to deanonymize Signal users[63], based on the analysis of metadata.

> In its targeted interception mode — which starts from a single target — JASMINE has claimed it is able to identify communicating parties in encrypted but peer-to-peer applications […] the JASMINE documentation explicitly claims support for identifying the IP addresses of participants in encrypted apps such as WhatsApp and Signal during voice and video calls where peer-to-peer connections are also used for calling by default.
>
> The JASMINE documentation also explains that by analysing encrypted traffic "events" for a whole country — in mass interception mode — JASMINE has the ability to correlate and identify the participants in encrypted group chats on messaging apps.

[62] signal.org/blog/phone-number-privacy-usernames/

[63] securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products

A similar surveillance product would not work against Cwtch because it uses Tor by default. Without a Tor or VPN proxy, an adversary can see that you are connecting to Signal servers which is what enables this type of timing correlation attack. Although it is possible to configure Signal to use a VPN or Tor, it is opt-in so most people will not use it like this.

Signal was designed to bring encrypted communication to the masses, not for an anarchist threat model. Because it's very difficult to register for Signal anonymously, and because you must first install Signal on a phone to use it on a computer, **we recommend prioritizing Cwtch over Signal for text communication with other anarchists, and using SimpleX Chat or Signal for voice and video calls.** For the same reasons, Signal is not well-suited for anonymous public-facing projects.

Installation

Signal Installation on GrapheneOS

We recommend the Signal Configuration and Hardening Guide[64]. As noted above, unless you are familiar with the Command Line Interface[†], Signal needs to be registered on a smartphone before it can be connected to a computer. Install Signal the same way you would install any app that doesn't require Google Services[65] (we don't recommend F-Droid). If you are using Signal from behind a VPN (as we recommend[66]) then a relay for calls is redundant and should be

[64] blog.privacyguides.org/2022/07/07/signal-configuration-and-hardening/

[65] anarsec.guide/posts/grapheneos/#how-to-install-software

[66] anarsec.guide/posts/grapheneos/#how-to-install-software