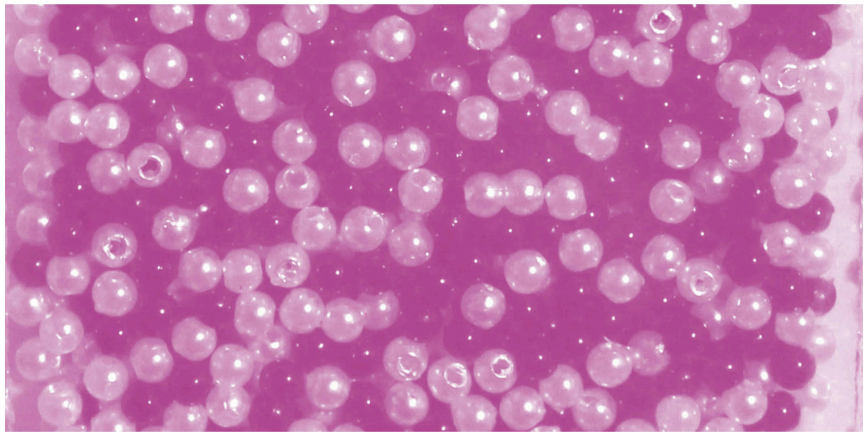
If the police ever have physical access to an electronic device like a laptop, even for five minutes, they can install hardware keyloggers, create images of the storage media, or otherwise trivially compromise it at the hardware, firmware, or software level. One way to minimize this risk is to make devices tamper-evident. As the Threat Library notes, “Tamper-evident preparation is the process of taking precautionary measures to make it possible to detect when something has been physically accessed by an adversary.”

```
 ,-\__
 |f-"Y\  -------------------
 \()7L/ < Be gay, do crime! >
  cgD    -------------------
  |\(                \          __ _
   \ \                \       .'  Y '>,
    \\\                \      / _   _    \
     \\\                      )(_) (_)(|}
      \\\                     {  4A   } /
       \\\                     \uLuJJ/\l
        \\\                    |3    p)/
         \\\___ __________     /nnm_n//
         c7___-__,__-)\,__)(".  \_>-<_/D
                   //V     \_"-._.__G G_c__.-__<"/ ( \
                          <"-._>__-,G_.___)\   \7\
                         ("-.__.| \"<.__.-" )   \ \
                         |"-.__"\  |"-.__.-".\   \ \
                         ("-.__"". \"-.__.-".|    \_\
                         \"-.__""|!|"-.__.-".)     \ \
                          "-.__""\_|"-.__.-"./      \ l
                           ".__"""">G>-.__.-">       .--,_
                              ""  G
   _ _
__| || |__ _____   ____  _____   __________ ____  ____  #tech
\    __    / \__  \  /    \ \__  \  /  __/  ___// __ \/ ___\ #guides
 |  ||  |   / __ \|   |  \ / __ \|   | \___ \\  ___/  \__  #for
/_  ~~  _\ (____  /___|  /(____  /___| /____/ \___\ \____\ #anarchists
  |_||_|        \/     \/      \/
```

Make Your Electronics Tamper-Evident



Series: Defensive

This version of the zine was last edited on 2024-04-18. 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

your phone may be confiscated when you cross a border or are arrested. This is in contrast to a remote attack[66].

For more information, see Making Your Electronics Tamper-Evident[68], the Threat Library[69], the KickSecure documentation[70], and Defend Dissent: Protecting Your Devices[71].

Tor network

Tor[72] (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[73] and Privacy Guides[74]. To understand the limitations of Tor, see the Whonix documentation[75].

[68] anarsec.guide/posts/tamper
[69] notrace.how/threat-library/techniques/targeted-digital-surveillance/physical-access.html
[70] kicksecure.com/wiki/Protection_Against_Physical_Attacks
[71] open.oregonstate.education/defenddissent/chapter/protecting-your-devices/
[72] torproject.org/
[73] anarsec.guide/posts/tails/#tor
[74] privacyguides.org/en/advanced/tor-overview/
[75] whonix.org/wiki/Warning

Contents

If the police ever have physical access† to an electronic device like a laptop, even for five minutes[1], they can install hardware keyloggers, create images of the storage media, or otherwise trivially compromise it at the hardware, firmware, or software level. One way to minimize this risk is to make devices tamper-evident. As the Threat Library notes[2], "Tamper-evident preparation is the process of taking precautionary measures to make it possible to detect when something has been physically accessed by an adversary."

'Evil maid' attacks[3] work like this: an attacker gains temporary access to your encrypted† laptop or phone. Although they can't decrypt your data, they can tamper with your laptop for a few minutes and then leave it exactly where they found it. When you return and enter your credentials, you have been hacked. The attacker may have modified data on your hard drive[4], replaced the firmware, or installed a hardware component such as a keylogger.

"Defense in depth" means that there are multiple layers of security that an adversary must bypass in order to succeed. This article will cover tamper-evident laptop screws, storage and firmware, as well as physical intrusion detection.

Tamper-Evident Laptop Screws

Let's start with your laptop. For a seal to effectively alert you to intruders, it must be impossible to remove and replace without leaving a trace, and it must also be unique—otherwise, the adversary could simply replicate the seal and you'd never know they'd been there. Glitter nail polish creates a unique pattern that is impossible to replicate, and if you take a photo of this pattern, you can use it to

[1] vice.com/en/article/a3q374/hacker-bios-firmware-backdoor-evil-maid-attack-laptop-5-minutes

[2] notrace.how/threat-library/mitigations/tamper-evident-preparation.html

[3] en.wikipedia.org/wiki/Evil_maid_attack

[4] media.ccc.de/v/gpn20-32-poc-implementing-evil-maid-attack-on-encrypted-boot

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[66], asymmetric cryptography[66], or Defend Dissent: What is Encryption?[67]

Full Disk Encryption (FDE)

FDE means that the entire disk is encrypted† until a password is entered when the device is powered on. Not all FDE is created equal. For example, the quality of how FDE is implemented on a phone depends not only on your operating system, but also on your hardware (the model of your phone). FDE uses symmetric cryptography[66], and on Linux it typically uses the LUKS specification[66].

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,

[66] anarsec.guide/glossary

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

> can even run Windows programs such as Adobe InDesign, but much more securely than a standard Windows computer. See Qubes OS for Anarchists[62].

See When to Use Tails vs. Qubes OS[63]. 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[64]

Storing Electronic Devices

See Make Your Electronics Tamper-Evident[65].

Appendix: Glossary

Brute-force attack

An attacker who "simply" tries every possible key to access a service or decrypt a file is using "brute force." This process is called a brute-force attack. More powerful computers make brute-force attacks more feasible. Modern cryptographic protocols are designed to force an adversary (who does not have the cryptographic key) to spend (nearly) as much time as it would take to try every possible key to break the code. The parameters of a good protocol are chosen to make this amount of time impractical.

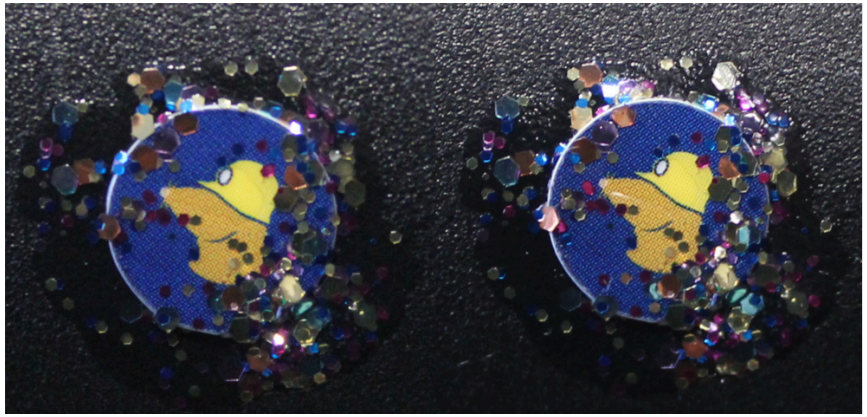
[61] anarsec.guide/posts/linux
[62] anarsec.guide/posts/qubes/
[63] anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os
[64] anarsec.guide/posts/e2ee/
[65] anarsec.guide/posts/tamper/

verify that the nail polish has not been removed and reapplied in your absence, such as during a covert house search[5]. The presentation "Thwarting Evil Maid Attacks[6]" introduced this technique in 2013.

Mullvad VPN created a guide[7] for applying this technique: first apply stickers over the laptop case screws, then apply the nail polish. An independent test[8] noted:

> Attackers without a lot of practice can use a needle or scalpel, for example, to drive under the sticker and push it partially upward to get to the screws relatively easily. The broken areas in the paint could be repaired with clear nail polish, although we did not need to do this in most of our tests. The picture below is a pre-post-comparison of one of our first attempts. Except for 3-4 glitter elements at the top left edge of the sticker, all others are still in the same place. This could be further reduced in subsequent attempts, so we rate this method as only partially suitable. [...] The relevant factor in this process is the amount of elements on the edge of the sticker. In addition, there are special seal stickers available which break when peeled off. They are probably more suitable for this method.

[5] notrace.how/threat-library/techniques/covert-house-search.html
[6] media.ccc.de/v/30C3_-_5600_-_en_-_saal_1_-_201312301245_-_thwarting_evil_maid_attacks_-_eric_michaud_-_ryan_lackey
[7] mullvad.net/en/help/how-tamper-protect-laptop/
[8] dys2p.com/en/2021-12-tamper-evident-protection.html#glitzer-nagellack-mit-aufklebern



For this reason, it is preferable to apply nail polish directly to the screws rather than over a sticker. This direct application is done for NitroKey[9] and Purism[10] laptops. Keep these nuances in mind:

> The screws holes are particularly relevant here. If they are too deep, it is difficult to take a suitable photo of the seal under normal conditions. If the hole is shallow or if it is completely filled with nail polish, there is a risk that if a lot of polish is used, the top layer can be cut off and reapplied after manipulation with clear polish. If the nail polish contains too few elements, they could be manually arranged back to the original location after manipulation if necessary.

[9] docs.nitrokey.com/nitropad/qubes/sealed-hardware
[10] puri.sm/posts/anti-interdiction-update-six-month-retrospective/

You may also be interested in the Threat Library's "Digital Best Practices"[56].

Your Phone

> **Operating system**†: **GrapheneOS** is the only reasonably secure choice for cell phones. See GrapheneOS for Anarchists[57]. 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[58].

Your Computer

> **Operating system**†: **Tails** is unparalleled for sensitive computer use (writing and sending communiques, 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[59] and Tails Best Practices[60].

> **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[61]. Qubes OS

[56] notrace.how/threat-library/mitigations/digital-best-practices.html
[57] anarsec.guide/posts/grapheneos/
[58] anarsec.guide/posts/nophones/
[59] anarsec.guide/posts/tails/
[60] anarsec.guide/posts/tails-best/

should be possible to make tamper-evident, as it requires access to the wires.

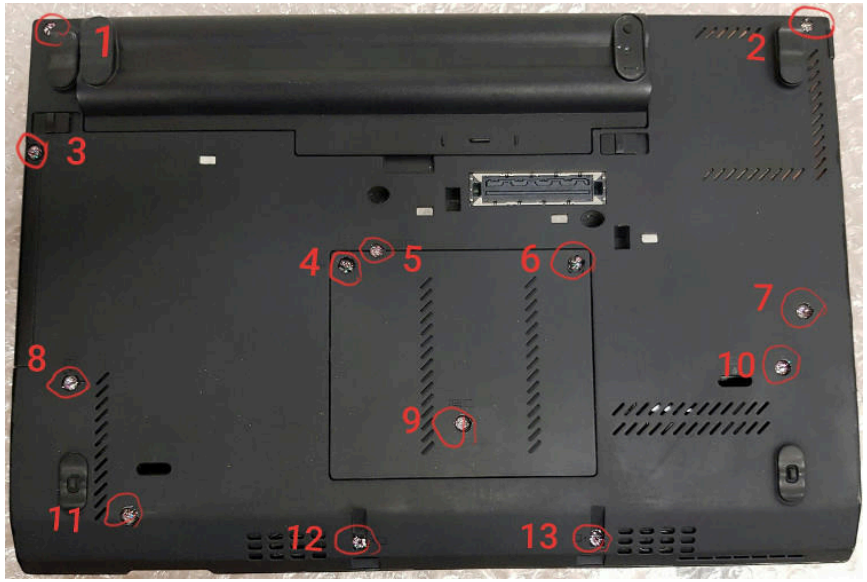
- There are several keypad-based attacks[51], and some can be mitigated with proper operational security.

Appendix: Recommendations

As anarchists, we must defend ourselves against police and intelligence agencies that conduct targeted digital surveillance[52] for the purposes of incrimination[53] and network mapping[54]. 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[55]: "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…"

[44] en.wikipedia.org/wiki/Safe-cracking#Magnet_risk
[45] youtube.com/watch?v=Y6cZrieFw-k
[46] en.wikipedia.org/wiki/Safe-cracking#Safe_bouncing
[47] mosandboo.com/how-to-open-a-safe-without-the-key-or-code/
[48] en.wikipedia.org/wiki/Safe-cracking#Spiking_the_lock
[49] learn.sparkfun.com/tutorials/building-a-safe-cracking-robot
[50] youtube.com/watch?v=vkk-2QEUvuk
[51] en.wikipedia.org/wiki/Safe-cracking#Keypad-based_attacks
[52] notrace.how/threat-library/techniques/targeted-digital-surveillance.html
[53] notrace.how/threat-library/tactics/incrimination.html
[54] notrace.how/threat-library/techniques/network-mapping.html
[55] actforfree.noblogs.org/post/2023/07/24/number-of-the-day-89502-preventive-surveillance-measures-france/



Glitter nail polish was successfully bypassed during a Tamper Evident Challenge in 2018 — the winner explained[11] how they managed to do it. Notably, a brand of nail polish with relatively large pieces of glitter in only two colors was used. It would be difficult to apply this bypass to inset screw holes; if the glitter was applied with a high density of elements, but not too thick, this would also increase the difficulty. Finally, using an adhesive[12] would also make the bypass less feasible.

Verification that the random pattern hasn't changed can be done manually with what astronomers call a "blink comparison". This is used in astronomy to detect small changes in the night sky: you quickly flick between the original photo and the current one, which makes it easier to see any changes. Alternatively, if you have an Android smartphone (either GrapheneOS[13] or a cheap one for

[11] hoodiepony.medium.com/bypassing-the-glitter-nail-polish-tamper-evident-seal-25d6973d617d
[12] dys2p.com/en/2021-12-tamper-evident-protection.html#glitzer-nagellack-mit-klebstoff
[13] anarsec.guide/posts/grapheneos/

intrusion detection[14]), you can use an app called Blink Comparison[15], which makes it less likely that you will miss something. It can be installed like any other app that doesn't require Google Services[16], i.e. not through F-Droid.

The Blink Comparison app encrypts its storage to prevent an adversary from easily replacing the photos, and provides a helpful interface for comparing them. The app helps you take the comparison photo from the same angle and distance as the original photo. Blink Comparison then switches between the two images when you touch the screen, making direct comparison much easier than manually comparing two photos.

In practice

Now that you understand the nuances of applying nail polish to the screws of your laptop case, let's actually do it — if you are going to install Heads firmware[17], do that first so the nail polish doesn't have to be removed and repeated. Before you start, you can also take a picture of the inside of the laptop in case you ever need to check if the internal components have been tampered with despite the nail polish protection (keep in mind that not all components are visible). Use a nail polish that has different colors and sizes of glitter, like the one shown above.

- First, take a photo of the bottom of the computer and use a program like GIMP to number the screws to make it easier to verify. For example, the ThinkPad X230 shown above has 13 screws that need to be numbered so that in the future you know which screw the photo `3.jpg` refers to.
- Apply the glitter nail polish directly to each screw, making sure there are enough glitter elements without it being too thick.

[14] anarsec.guide/posts/tamper/#physical-intrusion-detection
[15] github.com/proninyaroslav/blink-comparison
[16] anarsec.guide/posts/grapheneos/#how-to-install-software
[17] anarsec.guide/posts/tamper/#tamper-evident-software-and-firmware

set up; Auditor runs without interaction and Heads becomes part of your boot process.

Further Reading

- Random Mosaic — Detecting unauthorized physical access with beans, lentils and colored rice[43]

Appendix: Cracking Safes

- Rare-earth magnets[44] can unlock safes that use a solenoid[45] as the locking device in an undetectable manner.
- Safe bouncing[46] is when the locking mechanism can be moved sufficiently by banging or bouncing the safe[47] to open it in an undetectable manner. Safes that use a gear mechanism are less susceptible to mechanical attacks.
- Many safe models have a "management reset code" (also known as a "try-out combination") — if this code is not changed from its default setting the safe can be unlocked in an undetectable manner.
- Spiking[48] is when the wires leading to the reset button, solenoid, or motor can be exposed and spiked with a battery. This should be possible to make tamper-evident, as it requires access to the wires.
- Brute force[†] attacks — trying all possible combinations — are possible if the adversary has time. Dialing mechanisms can be brute-forced with a computerized autodialer[49] that doesn't need supervision[50]. Electronic keypads are less susceptible to brute force if they have a well-designed incremental lockout feature; for example, get it wrong 10 times and you're locked out for a few minutes, 5 more wrong codes and you're locked out for an hour, etc.
- There are several tools that can automatically retrieve or reset the combination of an electronic lock, such as the Little Black Box and Phoenix. Tools like these are often connected to wires inside the lock that can be accessed without damaging the lock or container. This

[43] dys2p.com/en/2021-12-tamper-evident-protection.html

Wrapping Up

With the measures described above, any 'evil maid' would have to bypass:

1) Physical intrusion detection, and
2) The tamper-evident storage, and
3) The tamper-evident glitter nail polish (for an attack that requires opening the laptop), or Heads/Auditor (for a software or firmware attack)

These layers are all important, although they may seem redundant. The expertise and cost required to successfully execute the attack increases significantly with each layer, making it much less likely that an adversary will attempt it in the first place. The best practice is to obtain a fresh device in such a way that it cannot be intercepted[42], and then consistently implement all of these layers from the beginning.

In practice

To summarize, take the following measures every time you leave the house with no one home for a significant amount of time:

1) Put the turned-off devices into tamper-evident storage
2) Take the necessary photos
3) Activate Haven

This may sound tedious, but it can be done in less than a minute if you leave unused devices in storage. When you get home:

1) Start by checking the Haven log
2) Next, verify the tamper-evident storage with Blink Comparison

Laptop screws can be verified when something suspicious happens. Neither Heads nor Auditor require much effort to use properly once

[42] anarsec.guide/posts/tails-best/#to-mitigate-against-physical-attacks

- Once it is dry, take good close-up photos of each screw — either with the Blink Comparison app on a smartphone or with a regular camera. It is a good idea to use lighting that is reproducible, so close the blinds on any windows and rely on the indoor lighting and the camera flash. Number the file names of the photos and back them up to a second storage location.

If you ever need to remove the nail polish to access the inside of the laptop, you can use a syringe to apply the nail polish remover to avoid applying too much and damaging the internal electronics.

Tamper-Evident Storage

You also need a tamper-evident storage solution for all sensitive electronics when you are away from home (laptops, external drives, USBs, phones, external keyboards and mice) — a laptop can be tampered with in ways that don't require removing the screws. Safes are often used to protect valuable items, but they can be bypassed in many ways, and some of these bypasses are difficult to detect (see below[18]). It is not trivial or inexpensive to make a safe tamper-evident, if it can be done at all.

[18] anarsec.guide/posts/tamper/#appendix-cracking-safes

A better and cheaper solution is to implement dys2p's guide[19]:

> When we need to leave a place and leave items or equipment behind, we can store them in a box that is transparent from all sides. Then we fill the box with our colorful mixture so that our devices are covered. The box should be stored in such a way that shocks or other factors do not change the mosaic. For example, the box can be positioned on a towel or piece of clothing on an object in such a way that this attenuates minor vibrations of the environment, but the box cannot slide off it.
>
> For an overall comparison, we can photograph the box from all visible sides and store these photos on a device that is as

[19] dys2p.com/en/2021-12-tamper-evident-protection.html#kurzzeitige-lagerung

is important to protect against the local logs being modified by an intruder. Choose a model with privacy features (e.g. it doesn't function through the cloud) so that the police cannot easily learn the timing of your comings and goings from it. For instance, motionEye OS[39] supports remote notifications for motion detection, but it requires Linux knowledge to set up.

In practice

Haven should be used on a dedicated cheap Android device that is otherwise empty. An older Pixel[40] is a good choice because it is cheap but has good cameras, which is important for both Haven and Blink Comparison — it may even still be supported by GrapheneOS[41]. Make sure that full disk encryption[†] is enabled. If you have a smartphone in addition to the dedicated Haven phone, it should be turned off in the tamper-evident storage — if Haven was running on it instead and was discovered by the intruder, they would now have physical access to the device while it was turned on.

- Place the Haven smartphone in a location that has a line of sight to where an intruder would have to pass, such as a hallway that must be used to move between rooms or to access where the tamper-evident storage is located. It should be plugged in so the battery doesn't die; fairly long cables are available for this purpose.
- Set a countdown to turn Haven on before you leave the house. The Haven app will log everything locally on the Android device. As mentioned above, sending remote notifications is currently broken.
- Check the Haven log when you get home.

[39] github.com/motioneye-project/motioneyeos/wiki/Features
[40] privacyguides.org/android/#google-pixel
[41] grapheneos.org/faq#device-lifetime

Physical Intrusion Detection

Physical intrusion detection[35] is the process of detecting when an adversary enters or attempts to enter a space. As the Threat Library notes:

> A video surveillance system that monitors a space can have the following characteristics:
>
> - The cameras can be motion-activated and send you an alert if they are detected and tampered with.
> - The cameras can be positioned with the space entrances in their line of sight and/or in a discreet location.
> - To prevent the system from monitoring you while you are in the space, you can turn it on just before you leave the space and turn it off as soon as you return.

We recommend employing physical intrusion detection in addition to all of the tamper-evident measures. That way, even if a covert house search doesn't interact with the tamper-evident storage (for example, because the goal is to install covert surveillance devices[36]), you can still find out about it.

Haven is an Android app developed by the Freedom of Press Foundation that uses the smartphone's many sensors — microphone, motion detector, light detector, and cameras — to monitor the room for changes, and it logs everything it notices. Unfortunately Haven is currently unmaintained, remote notifications are broken[37], and it is unreliable on many devices.

Until Haven is fully functional[38], we recommend also using a video surveillance system so that you can receive remote notifications — this

[35] notrace.how/threat-library/mitigations/physical-intrusion-detection.html
[36] notrace.how/threat-library/techniques/covert-surveillance-devices.html
[37] github.com/guardianproject/haven/issues/454
[38] github.com/guardianproject/haven/issues/465

> secure as possible, send it to a trusted person via an encrypted and verified channel, or send it to another device of our own. The next step is to compare the found mosaic with the original one. The app Blink Comparison is ideal for this purpose.
>
> To protect an object from damage, e.g., by staining or by the substance leaking into, say, the ports of a laptop, it can be wrapped in cling film, a bag, or otherwise.

Several colorful mixtures are described: red lentils & beluga lentils[20], yellow peas & white beans[21], etc. For a box that is transparent on all sides and fits a laptop, a small fish tank works well. For longer-term storage, vacuum seals[22] can be used.

This excerpt assumes that we take the cell phone with us, but as discussed elsewhere[23], this has its own security issues and is not recommended. So the smartphone we use to take a picture of the storage will have to stay in the house outside of the storage. As discussed below[24], we recommend that you get a cheap Android phone that only runs an app called Haven when you are out of the house. This device will stay out of storage anyway, so you can use it to take pictures of the storage. Alternatively, if you don't have a dedicated Haven phone but do have a GrapheneOS[25] device, you can use it to take photos of the storage and then hide it somewhere in your house while you're away. If you don't have a phone, you can use a camera. However, cameras don't have encryption, so it's much easier for an

[20] dys2p.com/en/2021-12-tamper-evident-protection.html#rote-linsen-und-belugalinsen
[21] dys2p.com/en/2021-12-tamper-evident-protection.html#gelbe-erbsen-und-wei%C3%9Fe-bohnen
[22] dys2p.com/en/2021-12-tamper-evident-protection.html#laengerfristige-lagerung-oder-versand
[23] anarsec.guide/posts/nophones/#do-you-really-need-a-phone
[24] anarsec.guide/posts/tamper/#physical-intrusion-detection
[25] anarsec.guide/posts/grapheneos/

adversary to modify the photos and you won't be able to use the Blink Comparison app to facilitate the comparison.

In practice

- Once you have placed the bagged electronic devices in the container and covered them with a colorful mixture, take photos using the Blink Comparison app. Optionally, send them to another device of your own (that is currently in storage) via Molly[26] or SimpleX Chat[27]. Close Blink Comparison so that the storage is encrypted.
  - *If you are using a dedicated Haven phone (preferred)*: Set up Haven for physical intrusion detection before leaving, as described below.
  - *If you are using a GrapheneOS phone*: Turn off the device and hide it somewhere. If the phone is found and the firmware or software is modified, Auditor will notify you.
- When you return, use Blink Comparison to verify the mosaic with new photos.
  - Optionally, if you sent the photos to yourself on Molly/SimpleX Chat, once your devices are out of storage you can verify that they don't differ from the reference photos saved in Blink Comparison. However, the Blink Comparison encryption makes it very unlikely that these reference photos were modified in your absence.

Tamper-Evident Software and Firmware

So far, we have only looked at making hardware compromise tamper-evident. It is also possible to make software and firmware tamper-evident. This is required for "defense in depth" — to trust an electronic

[26] anarsec.guide/posts/e2ee/#signal
[27] anarsec.guide/posts/e2ee#simplex-chat

device, you must trust the hardware, firmware, and software. Software or firmware compromise can occur remotely[28] (over the Internet) as well as with physical access, so it is especially important because the other measures won't necessarily detect it. Tamper-evident firmware is compatible with our recommendations (*Appendix: Recommendations*): Qubes OS or Tails on laptops, or GrapheneOS on a smartphone.

For GrapheneOS, Auditor[29] is an app that allows you to be notified if firmware or operating system software has been tampered with — you will receive an email when Auditor performs a remote attestation.

For Tails or Qubes OS, Heads[30] can do the same before you enter your boot password (on supported devices[31]). However, installing Heads is advanced, though using it is not. Keep the Heads USB security dongle with you when you leave the house, and have a backup hidden at a trusted friend's house in case it ever falls into a puddle. For more information, see Tails Best Practices[32].

If Auditor or Heads ever detects tampering, you should immediately treat the device as untrusted. Forensic analysis[33] may be able to reveal how the compromise occured, which helps to prevent it from happening again. You can get in touch with a service like Access Now's Digital Security Helpline[34], though we recommend not sending them any personal data.

[28] anarsec.guide/posts/tails-best#2-running-tails-on-a-computer-with-a-compromised-bios-firmware-or-hardware
[29] anarsec.guide/posts/grapheneos/#auditor
[30] osresearch.net/
[31] osresearch.net/Prerequisites#supported-devices
[32] anarsec.guide/posts/tails-best/#to-mitigate-against-remote-attacks
[33] notrace.how/threat-library/mitigations/computer-and-mobile-forensics.html
[34] accessnow.org/help