Threats

- Public-Chargers
- Forensics
- Phishing
- Silent-Sms
- Shoulder-Surfing
- Meta-Data
- Data-Dogs
- Radio-Cell-Interrogation
- Mobile-Communication
- Network-Surveillance
- Logger
- Imsi-Catcher
- Dangerous-Files

Public-Chargers

> [!toc] Table of Contents

Public “chargers” can be found, for example, in public transportation, cafés, libraries, airports, shopping malls, etc.

Of course, a distinction must be made here between simple power outlets and USB charging ports.

The worst thing that can happen with normal power outlets is that your own charger breaks. Apart from that, your own charger is only good for charging and can't really do anything else.

It's a different story with USB charging sockets. For years, there have been increasing cases of manipulated charging sockets that contain not only a power source but also entire microprocessors that attempt to access the connected device. This could allow malware to be installed, memory to be accessed, and so on.

Fortunately, all (mobile) operating systems are now equipped with protective measures and ask users whether the connected “device” should be given access to the mobile phone. If you are charging you phone somewhere and a warning pops up on your device, this should make you suspicious.

> [!warning] Attention {static}
>
> A simple USB port with the classic 5 volts power supply is not recognized by any mobile phone as a “device” that should be given any rights!

This can also be prevented by only using USB cables without “data lines” for charging. These are cables that cannot be used to transfer data. You can usually test this yourself on your own computer. If you cannot access your mobile phone with the USB cable, then this USB cable most likely only has two wires: positive and negative. No data can be transferred via these wires.

So, be careful with USB charging sockets, as they may have been tampered with! Unlike tampered power outlets, where your own charger is still plugged in, a tampered power supply can seriously damage your device.

It is therefore advisable to avoid these sockets. If you have to use one, it is best to:

1. only use two-wire USB cables

2. use sockets where you have seen someone charge a mobile phone before without it being thrown off afterwards.

Forensics

> [!toc] Table of Contents

Introduction

Forensics is a collective term for fields of work in which “criminal acts” are systematically investigated. In short: **when cops try to find evidence**.

Relevant subfields

Many forensic measures pose relevant threats to activists. These include:

- **Forensic linguistics**: Examines written language to identify the author of a text, for example. *Relevant for anonymous letters of confession, instructions, etc.*.
- **Physical forensics**: Examines fiber traces, DNA, tire or shoe prints, and fingerprints, among other things, to identify people who were present at a specific “crime scene” or who used a specific tool, for example. *Relevant for anonymous actions*.
- **Digital forensics**: Examines data on IT systems such as cell phones, PCs, servers, printers, etc.

> [!warning] {static}
>
> Digital forensics is almost always a threat, as digital devices store an enormous amount of information!

Digital Forensics

E.g. in the words of the German Federal Police Office:

"*In addition to traditional evidence such as files (paper), images, tools, or weapons, digital evidence is playing an increasingly important role in criminal investigations. Evidence includes data*

carriers in countless formats: PCs, e-book readers, printers, chip cards, optical media, mobile phones/smartphones, and SIM cards."

There are many things that can unexpectedly become (digital) evidence. Another thing that one should keep in mind is that digital forensic investigators can often restore files that were "deleted" a long time ago, which is why encrypting and securely deleting your stuff is so important.

Look at our countermeasure article about deleting data securely for more information on how to securely delete data and why it is so important.

> [!technical] How does a digital forensic investigation work?
>
> A forensic investigation is usually requested by prosecutors or courts and carried out by a “forensic expert.” Usually, the cops carry out the forensic analysis.
>
> Many forensic tools are offered to the authorities by external companies, e.g. Cellebrite for mobile phone forensics.
>
> Laptops and data carriers are usually not examined directly. Instead, an “image,” i.e., a copy, of the data carrier/hard drive is made, which is then examined. This is to ensure that no digital evidence has been falsified or corrupted.

Physical Forensics

We will not go into detail about physical forensics here. In general, classic forensic methods used in criminal investigations may also be relevant for activists. These include tracing:

- Fiber traces
- Shoe prints
- Fingerprints
- DNA
- *and more*

It is very difficult not to leave any physical traces. Physical forensic analysis is usually very time-consuming and costly. Nevertheless, individual case studies show that confused cops have ordered this even for minor offenses, even for simple ad busting actions.

Phishing

> [!toc] Table of Contents

Phishing via email or text message is generally more commonly associated with scams, but government actors also often use phishing to infect targets with malware.

> [!warning] {static}
>
> **In fact, phishing is one of the most common reasons for data leakage.**

There are a few things to keep in mind here. One-click malware, where users have to proactively click on a link or download something in order for their device to be infected, is much cheaper than zero-click solutions, where devices can be infected without any further action on the part of the user.

In addition, phishing attacks are relatively difficult to trace. If the phishing is discovered, it usually remains unclear who is behind the attack, which puts the attacker in a fairly secure position.

Being caught secretly bugging someone's home is much riskier and alerts those affected. Phishing, on the other hand, ends up in all of our inboxes all the time and hardly arouses any suspicion.

Here is an example of fake links created through the clever use of Unicode characters. Can you spot the difference between the links? Which link leads to which page?

> [!example] Example 1 {static}
>
> - https://codeberg.org/esc-it/esc-it.org/releases/tag/@esc-it.org
> - https://codeberg.org/esc-it/esc-it.org/releases/tag/@esc-it.org

As an exception, just for learning purposes, you can now click on the two links to see what happens. Was your guess correct?

The first link does not lead to codeberg.org but to esc-it.org. The @ symbol is used as a username. This should not work if there is a / before the @, but the first link contains Unicode characters that are not “normal” slashes.

Some browsers even display a warning for the incorrect link, as shown here in Firefox:

A pop-up in Firefox warns that we are about to log in to a website that does not require login. This c

Chromium, for example, does not display such a warning.

What is noticeable about the links is that there is a domain at the end (...@<esc-it.org>). However, this is not a clear sign of a fake and is becoming increasingly difficult to detect with ever-changing top-level domains. Here is an example with a ".zip" extension, so it could be either a .zip file or a .zip domain:

Warning: The first link leads to a domain *(1312.zip)* that does not belong to us. This means that we do not know what happens there. Therefore, please do not visit this link unless you know exactly what you are doing.

> [!example] Example 2 {static}
>
> - https://codeberg.org/esc-it/esc-it.org/releases/tag/@v1312.zip
> - https://codeberg.org/esc-it/esc-it.org/releases/tag/v1312.zip

Here, too, the first link does not lead to a zip file on codeberg.org, but the second link does. No warning appears here either, because the domain does not yet exist.

> [!info] Conclusion {static}
>
> - Do not click on suspicious links
> - Question the origin of the link. Could it be that this "address" is sending me exactly this link?
>   - Better safe than sorry - search for the page using verifiable methods. Save original links in your password managers, in bookmarks in your browser, or use search engines.
> - If in doubt, type the links manually.
> - However, this will not help if the link itself is fake. [systeml1.org] for example will again lead you to the wrong website. Refer back to the point above to determine the correct URL.

Silent-Sms

> [!toc] Table of Contents

SMS is the protocol by which standard text messages are delivered to your cell phone; a “silent” SMS message would deliver a "message" to the phone without you being aware of it 1. In other words, you wouldn't see a text message or notice anything at all on your phone.

However, this creates traceable data traffic for mobile operators, as the SMS (and later also its confirmation of receipt) is forwarded to its destination via all the necessary mobile phone cells. The path taken by the SMS can then be evaluated by the authorities, allowing locations to be determined with an accuracy of up to a few meters.

> [!question] How to protect against it? {static}
>
> Don't let your phone receive SMS, by either:
>
> - taking out you SIM card
> - turning on airplane mode
> - shutting your phone off

There have been some apps floating around over time, that promised to detect silent SMS. The problem with those is, that:

1. The mobile modems, e.g. the chips that actually receive the SMS, are technical black boxes to the public - we can't tell what they are really doing.
2. For most apps, your phone has to be *rooted*, which we strongly advice against. While it enables more user freedom, rooting breaks the fundamental security mechanisms of your mobile operating system.

on Central/Eastern European map Illustration of the sending of a silent SMS and the receipt of its rep

Silent SMS - Application

How often law enforcement uses Silent SMS may very a lot, mostly depending on the country. As with many other threats we describe here, we don't have a lot of concrete numbers about the

usage of those techniques. What is sure is that it's a very cheap technique, which can be easily used by most authorities without further ado.

In Germany for example, the federal authorities (which don't include the regional ones) send between 200.000 - 400.000 silent SMS per year.

Shoulder-Surfing

> [!toc] Table of Contents

Shoulder surfing is when someone secretly looks over your shoulder to see what you are doing or typing on your cell phone, laptop, notepad etc.

> [!warning] Warning {static} Be especially careful when entering passwords!

After all, even the best password is useless if it falls into the wrong hands. First and foremost, it is important to be aware of the increasing use of video surveillance. Do not enter passwords in front of cameras!

If you have ever tried shoulder surfing yourself, you will have noticed that there are places and situations that are particularly conducive to it.

In crowded lecture halls, for example, you can practically see the screens and keyboards of at least three people in front of you.

On public transportation, seats that are not directly behind the target person but diagonally behind them are particularly suitable. If the bus is extremely crowded, it is not even noticeable when someone is leaning over your cell phone while you are typing.

In such situations, it is important to not just mindlessly type your passwords, but to first evaluate the following:

- Is the potential danger of should surfing real, or is it exaggerated?
- Is it worth the risk to type in my password anyway, or can I wait/find a better place?

Meta-Data

> [!toc] Table of Contents

Here we describe what metadata is and where it can be found. If you just want to know how to clean metadata from files, check out our recommendations.

The data behind the data

Metadata in communication

Imagine you are writing a message to someone or talking to a friend on the phone. You might think, “As long as no one knows the content, everything is fine!” - but that's not entirely true.

Even without knowing the content, a lot can be found out about you from the metadata.

Metadata is data about your data. In lots of messengers for example, it can reveal:

- Who is communicating with whom
- When and how often you are in contact
- Where you sent a message from
- Which app or device you are using

Metadata can be used to deduce habits and how your everyday life usually looks like.

Contact networks can also be identified in the same way: If person A is in contact with person B, and person B always immediately writes to C after receiving a message from A, then C is also connected to A.

IP addresses and location data also belong to the category of metadata. In 2024, for example, several high-ranking intelligence officials from major NATO countries were identified using a commercially available data set because they had used apps and devices that collected their location data and sold it to so-called data brokers. *(Entire series of articles in german on netzpolitik.org)*

It is therefore important to avoid metadata wherever possible.

According to Mike Kuketz, Briar is a role model in this regard: “The metadata generated during use is obfuscated in such a way that it is impossible to trace who was in contact with whom.”

Signal is also rather sparing with metadata. Matrix, email, and Delta Chat, on the other hand, require a lot of metadata to function properly. This metadata is then stored on all servers with which communication takes place.

This does not mean that these messengers do not have their advantages, but the disadvantage of metadata should be kept in mind.

> [!technical] Details about SMTP metadata
>
> Delta Chat uses the old SMTP email protocol. For those who want to delve deeper into metadata in SMTP, here are a few resources:
>
> - Delta Chat
> - Email

Metadata in files

Even simple files often contain metadata. A photo taken with a smartphone, for example, may even contain the location where the photo was taken *(if the settings are poorly chosen)*. In addition, the device model, date, time, and similar information are often included.

PDFs, Word, Excel, and similar files also usually contain a lot of metadata that reveals the device and operating system used for editing, the creation or editing date, user name of editor, and similar information.

This becomes a particular problem when files are uploaded somewhere, as the metadata is also uploaded and can then be viewed by anyone who downloads the file.

> [!tip] {static}
>
> - GrapheneOS's Camera e.g. doesn't store any meta data on photos you take with it, by default.
> - Our recommendations include a list of tools for cleaning metadata.

Metadata on paper

Yes, unfortunately, even printed paper contains metadata, known as printer dots. These are tiny yellow dots that some color laser printers use to leave information about the printer model and print date, which are not visible to the naked eye.

Such dots were presumably used to identify the US whistleblower Reality Winner.

Until 2017, the civil rights organization Electronic Frontier Foundation had compiled and maintained a list of such color printers. However, this has since been discontinued because all color laser printers now leave detectable traces in one form or another.

> [!warning] Warning {static}
>
> Therefore, in highly sensitive cases, no (high resolution) photos of original documents should be uploaded. In our recommendations, we describe a possible alternative.

Data-Dogs

> [!toc] Table of Contents

> [!info] TL;DR {static}
>
> Data dogs, similar to drug detection dogs, are specially trained to sniff out certain metals that are used in electronics and thus in storage media such as USB sticks.

The following is an automated translation from this german article under the Creative Commons BY-NC-SA 4.0 license from netzpolitik.org, as it explains the topic quite well:

The irresistible smell of hard drives

“Data storage detection dogs” are increasingly being used in house searches. They can smell smartphones, hard drives, and even SIM cards. However, the police are keeping their training methods under wraps.

Everyone has heard of police dogs that search for drugs or explosives. There are also dogs that sniff out banknotes in the hunt for tax evaders. At the end of the last decade, a new type of training was added: dogs that sniff out storage media – and the German state of Saxony was a pioneer in this field. In the case of mass child abuse at a campsite in Lüdge,1 Germany's only “data storage detection dog” at the time was deployed. As a result, the North Rhine-Westphalia police also trained such dogs and presented “Odin,” “Jupp,” and “Ali Baba” on social media. 1 A small town in Westphalia.

There are several inquiries about data storage detection dogs on the transparency platform FragdenStaat. There, one could have learned more about how the police train dogs to find CDs, hard drives, memory cards, USB sticks, smartphones, and SIM cards. Apparently, storage media have their own unique smell that dogs can recognize when they are conditioned to do so. However, the NRW (North Rhine-Westphalia) police have classified the training of the dogs as “classified information” and redacted it extensively, so instead we have to rely on media outlets such as zooroyal (a German YouTube channel) and their reporting on the “furry noses.”

A report in the Süddeutsche Zeitung (a German newspaper) states that searching for data carriers is much more difficult than searching for drugs, which simply smell stronger than standard hard drives. The Saxony-Anhalt police (the police force of the German state of Saxony-Anhalt) also write in a presentation that data carriers release hardly any odor molecules.

The Saxon service dog handler told the newspaper at the time that the dog could smell the chemicals used to manufacture the storage media. He even had the impression that his dog could find lithium-ion batteries faster than cell phones with chrome-nickel batteries and assumed that “Artus” could smell lithium.

Because the storage devices being sought give off so little odor, the “tracking work” requires “a high level of endurance and physical exertion” from the service dog, according to the documents from Saxony-Anhalt. For this reason, this training “requires focused, objective tracking behavior on the part of the service dog.”

Reward: bite sleeve

The North Rhine-Westphalia police reveal on their website how the search is conducted: “When Hank [the dog] hears the command ‘Track!’, he begins to search. If he remains motionless, Peter Baumeister [dog handler] knows that he has found something. As a reward, Hank gets his favorite toy: a bite sleeve.”

According to this, the additional training of a tracking dog to become a data storage tracking dog takes 20 days, which the dog completes together with its handler. After the training, the handler can then call themselves a “data storage tracking dog handler.” A word that could hardly sound more German.

Radio-Cell-Interrogation

> [!toc] Table of Contents

To understand this chapter, it is necessary to understand the basic concepts of the mobile network, in particular the connection and authentication process between mobile phones and cell-phone towers. We have attempted to illustrate this in the article Mobile communications.

> [!warning] {static}
>
> Cell data is very easily accessible to the authorities and is regularly used in investigations.

Radio cell inquiry is a measure that law enforcement agencies regularly use in their investigations. Thereby, the authorities request phone cell data that is of interest to the case, usually directly from the mobile operators.

Map symbolically showing how mobile phone cells are distributed in a city

How to protect against radio cell inquiries?

Don't let your phone connect to the radio cells. Ergo, turn your phone of, or at least, put it into airplane mode. With airplane mode, bear two things in mind:

- when you take out your SIM card, but don't put your phone into airplane mode, it may still try to connect to cell-phone towers for making emergency calls.
- not all devices truly shut off cell-phone communication when put into airplane mode.

> [!info] {static}

> To be 100% sure that no cell phone data is gathered - don't take your phone with you.

What is requested in radio cell inquiries?

Radio cell inquiries collect the following data for the period and “location” (i.e., a specific area that may be covered by several mobile phone cells) inquired about:

- Logged-in phone numbers
- Time stamps of:
  - Dial-in/dial-out of devices
  - Outgoing and incoming calls
  - Voicemail messages
  - Sent/received text messages

Radio cell inquiries are often made before, during, and after demonstrations. This can reveal which devices were present at the protest and were they were before and after it. This information can be potentially used to identify protesters, especially when their phone numbers are registered to their names or when the route they took to the demonstration can compromise their identity.

Which devices were at which location at time X, by radio cell inquiry

In addition, radio cell inquiries can be used to create movement profiles over a larger area by looking at the entry and exit times of individual devices at the respective mobile phone cells:

Route of device through city visible through FZA

Statistics on radio cell inquiries

For almost all countries in the world we may very well assume that every single phone number ends up in a radio cell inquiry, more or less regularly. Although clear statistics are quite rare the case of the 18th and 19th of February 2011 in Dresden, Germany is a well documented example: Surrounding several public protests on those days, the authorities collected: `"96.072 Verkehrsdatensätze, 257.858 Rufnummern und 40.732 Bestandsdaten"` .

Mobile-Communication

> [!toc] Table of Contents

First, some basic information about threats in the field of mobile communications needs to be explained. This article focuses on how a single cell phone communicates with the mobile network in the form of a cell phone tower (colloquially: antenna mast). The terms IMSI and IMEI (and sometimes TMSI) appear frequently and are also briefly explained here.

Who owns cell phone towers?

Cell phone towers are operated by mobile phone providers. Accordingly, the respective mobile phone providers also control the data traffic passing through these towers. In the image below, the different colors symbolize different providers (in Germany), such as Telekom, Vodafone, O2, etc.

Map symbolically showing how cell phone towers are distributed in a city

IMSI: SIM identifier

Every SIM card has a unique identifier, the International Mobile Subscriber Identity, or IMSI for short. Due to the registration requirement for SIM cards in most European countries, the SIM card is usually uniquely assigned to an identity. The authorities can easily request this information from mobile phone providers and do so very regularly.

Authorities can ask the providers which phone numbers belong to a certain person. This can also work in the other direction, for example asking who the owner of number 0123456789 is. Those inquiries are very cheap for authorities and are regularly used on a massive scale.

IMEI: Device identifier

Mobile phone modems (i.e., the chip in your cell phone that can connect to the mobile network) also have a unique number, the International Mobile Equipment Identity, or IMEI for short. These IMEIs are usually 15 digits long and globally unique. The structure is as follows:

- The first 8 digits are, to put it simply, type-specific. For example, all Google Pixel 7a devices have the following 8 digits: 35917382
- The next 8 digits are serial numbers
- *The last digit is for error correction*

picture of IMEI sets of different models from same and different vendors next to each other.

> [!technical] How is it ensured that these numbers are unique?
>
> Since many different companies produce such mobile communications modems, it is necessary for them to coordinate with each other. Otherwise, with thousands of modems produced every day, numbers would quickly be assigned multiple times.
>
> This is handled by the **GSMA** (Global System for Mobile Communications Association). The name speaks for itself.
>
> - So if a manufacturer wants to launch a new model, they go to the GSMA and ask for a “number space,” the first 8 digits. They can then name all chips produced for this model with this number space, i.e., assign IMEIs.
> - The serial numbers are used to distinguish individual devices of the same model.
> - Error correction is a bit of black magic and can really be ignored here.

> [!detail] EIR: (Equipment Identity Register)
>
> However, the standard also provides for “whitelists.” This would mean that all IMEIs produced are recorded and only those recorded are allowed to participate in the network. This would then be a significant security risk if a cell phone is purchased with traceable payment methods.
>
> Examples of modem manufacturers: Qualcomm, Huawei, ZTE, Sierra Wireless, Netgear, Alcatel, TP-Link

The IMEI therefore makes every mobile device identifiable.

If a device can be used with multiple SIM cards at the same time (regardless of whether these are two physical SIM cards or one e-SIM and one physical SIM card), it also has the corresponding number of IMEIs.

However, it is often quite easy to establish a connection between these two IMEIs:

- The serial numbers are often simply incremented *(except for error correction)*
- If two IMEIs are always in the same place, this can be correlated
- The manufacturers and retailers know the correlation between the two IMEIs
- If an EIR is involved, these two IMEIs are also linked to each other in the EIR. So if one of the two IMEIs is known, the second one can also be found in the EIR.

The IMEIs cannot be changed easily. In many countries, manipulating them is a criminal offense. It also requires special hardware, which is most likely to be obtained from China.

> [!tip] Tip {static}
>
> There are some mobile routers that can be flashed with a special operating system named blue merle. Blue Merle can be used to change the routers IMEIs and can also be configured to only use TOR.

Problems when buying cell phones

So if you buy a phone in a store and pay with a card, the store will have a link between your card and the IMEI(s) of your phone. As a result, authorities may be able to trace the IMEIs assigned at the factory to specific devices by querying sellers and device manufacturers.

And if the cell phone was purchased using your own identity, this association also may exist. However, we do not yet know whether and how often authorities query this association.

> [!abstract] Conclusion: IMEI {static}
>
> - Identifier of a device, not the SIM card
> - Globally unique (by factory default)
> - Transmitted to mobile network providers when connected to a mobile network (see Authentication)

Authentication

Schematic representation of the authentication process between SIM and cell phone tower

- If the mobile phone detects the signal of a cell phone tower, it tries to “knock” on it with a kind of “Hello” to see if the tower is even reachable and, if so, tells it that it would like to log into the network: "I want to log in!"

- If the radio cell receives this message, it first asks for the identity of the mobile phone to ensure that it has the right to log in: "Who are you?"
- The mobile phone then sends the IMSI of its SIM card to prove that it has the right to connect. At the same time, it also sends the IMEI of its mobile modem (i.e., of the mobile phone).
  - A Telekom cell phone tower would therefore reject a Vodafone SIM card and tell it that it does not have the right to use the Telekom network.
- This completes the authentication process and a connection can be established. The purpose of the TMSI is secondary here and has therefore been removed for simplification.
- According to the standard, such connections can only be established in “encrypted” form.

  You can read why this is in missing quota.

> [!technical] What is the TMSI?
>
> If a connection were simply established, anyone nearby with the appropriate hardware (e.g., software-defined radios starting at €20) could see which cell phones are currently logged into the network with which SIM cards and how much they are communicating.
>
> To prevent this from happening, the procedure goes one step further: The cell phone tower gives the cell phone a TMSI (Temporary Mobile Subscriber Identifier). From now on, the mobile phone uses this TMSI for identification, but only in this session. If the mobile phone logs out of this tower at some point and logs back in later, the entire procedure starts again and a new TMSI is assigned.
>
> If you are still wondering why the mobile phone needs to identify itself again after the initial authentication: Sent packets always need recipients (and senders), of course. So that your mobile phone can be found again during a connection to a website, for example, in order to present the content to you, “the network” must of course know which device you are.

Both the IMSI and the IMEI are transmitted during authentication with the mobile network. This creates traceable data for mobile phone providers that enable a unique assignment between IMSI and IMEI, i.e., cell phone and SIM card.

Therefore you should be aware of this risk when using a mobile phone that has previously been used with another SIM card, which in turn allows conclusions to be drawn about your own identity.

In addition, the mobile phone may also have ended up in a Geofence warrant with another SIM card.

Network-Surveillance

> [!toc] Table of Contents

Monitoring of traffic data

This is usually what is meant when people talk about telecommunications surveillance in general. Here, the authorities force service providers to explicitly monitor your connections and to forward all recorded traffic data to the authorities. This requires a court order.

This is possible because normal telephone connections, i.e., landlines, voice calls, text messages, and (last but not least) voicemail messages, are only **transport encrypted**.

Transport encryption

With transport encryption, virtually every participant in the chain of transmission of a message is given the right to open and read the message.

For example, if you write a normal email, the email is first sent to the mail server with transport encryption. No one can read it in between. However, the mail server can open and scan the email. They usually do this because how else would your email providers know what belongs in the spam folder? Your mail server then sends the email, again with transport encryption, to the mail server of the email recipient. This server can also unpack and scan the email. The mail server then sends the email again, encrypted, to the recipient.

A schematic representation of a MITM attack by the police using transport encryption

This is basically how it works with voice calls and SMS as well.

This shows that email providers/mobile phone providers, who always have the right to read your traffic, are the ideal point of attack for the authorities. There, they can knock on the door (with a court order) and demand all your data traffic. That is why it is so important to use end-to-end encryption!

Logger

> [!toc] Table of Contents

Loggers are devices that can be used to ‘log’ or record something. Two types of loggers are relevant to us here: keyloggers and screen loggers.

Keyloggers

Keyloggers are devices that basically record all keystrokes on your keyboard. They are placed between the keyboard and the computer and look like normal USB adapters:

Keylogger next to keyboard

Keylogger between laptop and keyboard

They can send every single keystroke to an attacker in real time via radio/WiFi/LTE. The problem with this is obvious.

These keyloggers are available for very little money and are easy to obtain, making them very simple to use even for amateurs. There are even keyloggers that look like normal cables, see for example the O.MG Cable.

More advanced attackers (e.g., government agencies) can also install keyloggers in the keyboards themselves by unscrewing the keyboard and installing a small keylogger circuit board directly on the keyboard's electronics. Or they can simply replace the keyboard with a manipulated one. This would not be noticeable on the USB port alone, of course.

Screenloggers

Screen loggers work on the same principle as keyloggers. An adapter-like device is plugged between the display and the PC (depending on the connection used: VGA, HDMI, DisplayPort, etc.) and can then record the entire image transmission and send it to the attacker via radio/WiFi/LTE.

> [!warning] {static}
>
> Be careful with
>
> - publicly accessible PCs
> - other PCs that are not always under observation (your own office, for example)

It should also be noted that “key loggers” and “screen loggers” can also refer to software loggers. However, these are nothing more than viruses and describe a completely different threat than the ones discussed here.

Imsi-Catcher

> [!toc] Table of Contents

An IMSI catcher, also known as Cell-Site Simulator or "Stingray", is a surveillance device that "masquerade as legitimate cell-phone tower, tricking phones within a certain radius into connecting to the device rather than a tower" 1.

In general, standard telecommunication works as follows:

1. End devices, such as your phone, log in to the cell-phone tower with the strongest signal.
2. Upon receiving a request from your device, the tower performs an “Identity Request”
3. Your device then authenticates themselves with their IMSI + IMEI, and receive a TMSI from the tower.

IMSI catchers abuse the above to track the location of cell phones and gather data from nearby devices without the users' knowledge.

A rough distinction can be made between passive and active IMSI catchers:

- **Passive IMSI catchers** simply wait for clients to attempt to authenticate themselves with their identifiers at the cell-phone tower. This allows detailed information to be collected about who or how many people are present at a demonstration, for example. Clients do not notice the deception due to the GSM protocol.
- **Active IMSI catchers** do not just wait for the client's synchronization request. They instead give your device a TMSI (comparable to a local IP) and establish a legitimate connection to a real cell-phone tower on the device's behalf. This allows full-fledged 'machine-in-the-middle attacks' to be carried out.

What security vulnerability is being exploited here?

The problem lies in the authentication between the phone and the cell-phone tower. The phone must verify itself to the tower (as shown below) with its unique identifiers (IMSI, IMEI) to prove that it has the right to use the mobile network.

However, the cell-phone tower does **not** authenticate itself to the phone. Therefore, the phone can never know for sure whether it is actually communicating with a normal, commercial cell-tower or with a clone, operated by the authorities.

Active IMSI catcher - system

IMSI catcher schematic

Why is communication between the phone and the police unencrypted?

The answer can be found in the vulnerability in the communication protocol during authentication described above. By taking certain steps, the IMSI catcher can force the phone to use an old mobile phone standard (usually 2G) during the authentication process. This downgrade is possible in order to use the existing 2G infrastructure in situations where modern standards (3G/4G) do not provide reception. 2G is often somewhat more resistant in terms of territorial coverage than the more modern standards. The 2G standard, on the other hand, has long been obsolete and is not recommended for security reasons. Apart from government agencies, even private individuals can very quickly decrypt 2G “encrypted” communications and read/listen to them. For this reason, we classify this communication as “unencrypted” in practice.

> [!technical] Why is communication between police and mobile phone cells encrypted?
>
> To counteract so-called “eavesdropping,” i.e., being listened in on, the cell-phone towers of the new standards only accept communications that have been encrypted with their respective standard. To ensure that your phone does not notice that it is actually connected to a malicious tower, the IMSI catcher must also establish a real working connection to the legitimate mobile network. To do this, it must re-encrypt the connection to the cell-phone tower.

Practical threats

> [!warning] This means: {static}

> - Cell phones with private SIM cards and IMEI numbers can be identified and located
> - “Anonymous” SIM cards and cell phones are not necessarily anonymous

It should be noted that this poses a potential risk if an “anonymous” cell phone is reused. In connection with radio cell inquiries, it may be possible to create and contextualize movement profiles of these devices.

A potential example scenario could look like this:

You use your action cell phone at several actions/demonstrations, preferably in different cities or states. During these demonstrations, you (and therefore your IMSI+IMEI) end up in cell-phone inquiries multiple times. At first, no one can do anything with this information except say that this device was present at all of these events. However, you might walk past IMSI catchers at further demonstrations and be checked or filmed. Over time, this could establish a correlation between you and the device.

Hardware for professional IMSI catchers in Germany and the surrounding area usually comes from Rhode&Schwarz. Their devices are known and popular worldwide, not only with law enforcement agencies. This state-of-the-art technology is also correspondingly expensive, with prices in the 4-5 digit range.

However, simple passive IMSI catchers can also be implemented with ~€25 SDR dongles (software-defined radios). These are only capable of reading existing traffic, but not of setting up a fake radio cell and carrying out actual MITM attacks.

Recommendation

We recommend reading this article from the Electronics Frontier Foundation, which introduces Rayhunter. A software, that can be flashed onto specific types of mobile routers to detect present IMSI-Catchers.

Sources

- https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks

- SnoopSnitch talk: https://media.ccc.de/v/ber15-5-detecting_imsi-catchers_and_other_mobile_network_attacks, although the app itself does not work.

Dangerous-Files

Note: For a better browsing experience we give the "answer" here at the beginning. See below for a more detailed explanation of this threat.

What file types can be dangerous

Although none of the listed file types are malicious per se, they are often used by attackers to "hide" malware. Most commonly:

- LibreOffice:
  - `.odt`: Text documents (Writer)
  - `.ods`: Spreadsheets (Calc)
  - `.odp`: Presentations (Impress)
  - `.odg`: Drawings (Draw)
  - `.odb`: Databases (Base)
- Microsoft Office:
  - `.docx`: Word documents
  - `.xlsx`: Excel spreadsheets
  - `.pptx`: PowerPoint presentations
- `.pdf`: PDF's
- even image formats like `.gif` have reportedly been exploited, also on mobile devices.

> [!tip]
>
> It is recommended to avoid the above "complex" file types if they are not necessary. If you still have to open such a file from an untrusted source, we recommend using Dangerzone.
>
> Use text files and markup languages like markdown if possible instead.

Why this matters

> [!note] It is a matter of security culture to reconsider if it's really necessary to send an invitation text as a PDF or a draft of a press release as Word document. If it is enough to use the possibilities, that safe markup languages like markdown give you, them use just them.

Markdown is even compatible to collaborative tools like e.g. Nextcloud.

In many contexts we see that people are kind of ashamed of sending plain text invitations for example. They feel that they owe their friends some more effort than just text. While this shows a pretty nice property of friendship, we also have to talk about the problems that this brings along and that it might be worth it to break this behavior down towards a more conscious approach.

What is a file type

Different programs expect their files to have a specific format. They expect the files to follow a pattern that the program recognizes to function correctly.

Each file type is typically identified by a specific extension (such as `.odf`, `.pdf`, `.jpg`), which signals to the operating system what program should open it and how it should behave. For example, if you click on a file that ends with `.pdf`, the operating system knows that is has to open the file with a PDF reader and not with you music player.

How can files be dangerous

Consider a simple text file (not a word document, but a simple plain text file!). A normal text file contains, no surprise, text, which is nothing else than characters, like "A", "a", ";", "/" and so on. Those text file can be read and displayed from simple programs like Gnome's "gedit", Windows notepad, and so on. They are not capable of advanced features, such as calculating tables, like Excel, or LibreCalc.

More advanced programs like Excel, PowerPoint, or modern PDF viewers are capable of much more advanced features. PDF viewers for example can display interactive forms, that you can fill out right inside the PDF viewer. They can have drop-down menus and more.

> [!caution] This means, that your PDF viewer, PowerPoint, Excel etc. are able to **execute additional code**, that is delivered inside the file they are processing.

While this is necessary to use the full feature set of the program, the capability to execute additional code can expose severe security risks.

You probably all heard about viruses being distributed through PDFs. This is exactly what is exploited here:

> [!note] An attacker can smuggle some malicious code inside the PDF. You open the PDF with your PDF viewer. The PDF viewer detects some code and thinks: "Ah, I have to execute this, so that the user has the full functionality of this file" and executes the code, which can then perform malicious actions such as stealing your data and sending it to the attacker.