IMSI catchers, source wiretapping and mobile security
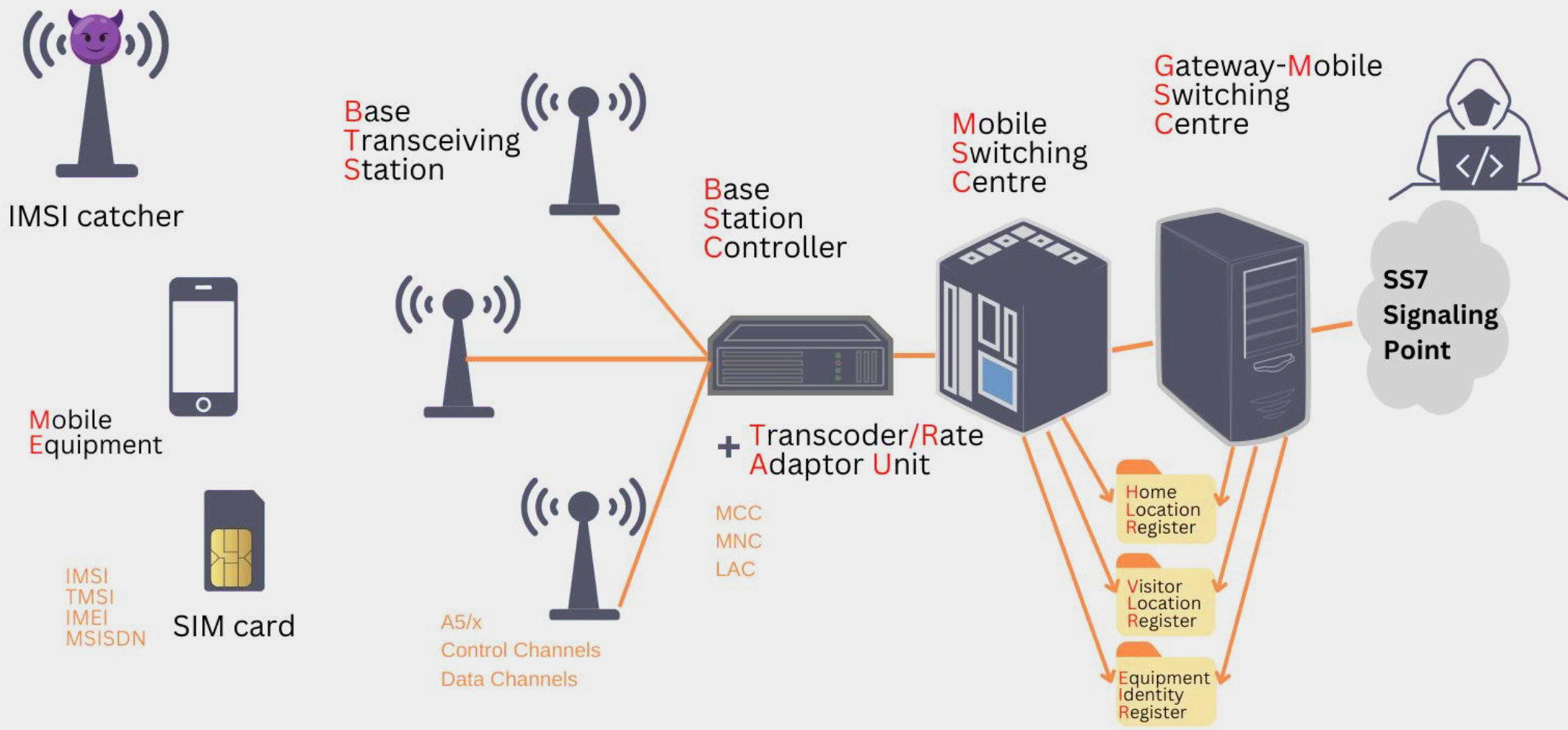
Some technical and legal aspects of the interception of electronic communications in mobile networks.

Matej Kovačič
https://telefoncek.si

Some GSM basics...

BTS are grouped in large logical unit (controlled by one or more BSC's – Base Station Controllers) - **Location Area**. Each LA is assigned a Location Area Identity (LAI).

The Location Area Identity (LAI) uniquely identifies a Location Area (LA) within a mobile network. It consists of the Mobile Country Code (MCC), the Mobile Network Code (MNC) and the Location Area Code (LAC).

All base stations in one Location Area are under control of the same network control equipment, so user's mobile phone can easily switch between base stations.

However, when a mobile phone is **moved** into a different Location Area, things get a little more complex...

Some GSM basics...

When a mobile phone is turned on, it **automatically checks which base stations are available nearby**.

After logging into the network (so called IMSI attach), mobile phone **sends its identification** data to the network (IMEI and IMSI number). Then goes into so called **idle mode**.

When logged in, the network assigns a TMSI number to it.

Then the mobile phone **minimizes its activities**, but regularly observes signal strength of the base station it is connected to, and also nearby base stations.

It periodically also reports that it is still present in the network (so called Periodic Location Update).

Some GSM basics...

When a mobile phone finds out that it has been moved to a different Location Area, **it will notify the network** about its presence with a so called **Location Update**.

However, via SDCCH (Stand-alone Dedicated Control Channel) it reports **its TMSI** number only!

So an external observer can only see that mobile phone with a given TMSI has been moved into a new Location Area, and **cannot** identify its IMSI number, which is the real identity of a mobile user in a mobile network (and can be linked to mobile phone number (MSISDN) and IMEI number.

Why IMSI number is important?

IMSI number is the **main unique identifier** of user in a mobile network.

Mobile phone transmits its IMSI number to mobile network **on very limited occasions**.

Usually its **TMSI number is used** (which protects user identity on the network).

Law enforcement agency needs an **identifiable telecommunication endpoint** for lawful interception.

If the target is using a mobile phone without subscription, law enforcement does not have an identifiable telecommunication endpoint – they do not know which phone they should eavesdrop!

Since people are dependent on mobile phones, IMSI catchers can be used to identify people.

How does IMSI catcher work?

IMSI catcher first **falsely presents itself** as a base station of a legitimate mobile network.

It then **transmits fake Location Area Code** to nearby mobile phones (lying about location).
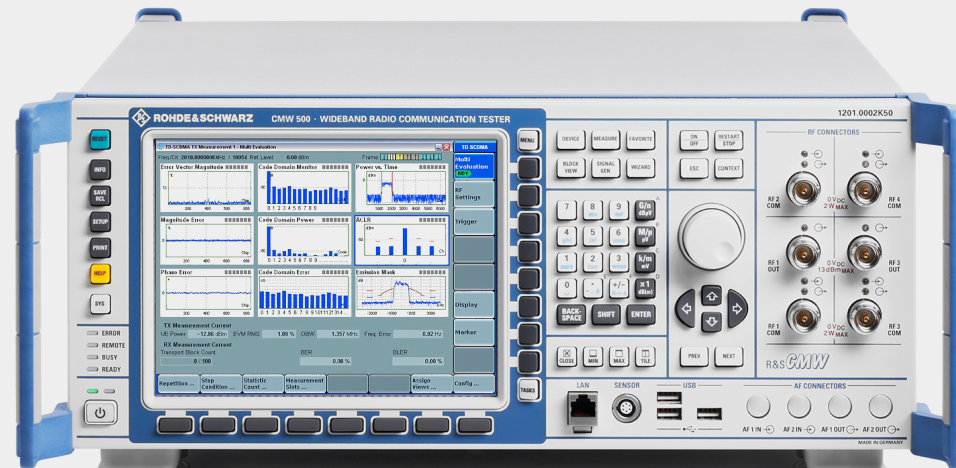
Mobile phone responds with a Location Update to the IMSI catcher and sends it its TMSI number.

Then IMSI catcher responds that mobile phone's TMSI **has expired** and **requests re-authentication**.

Mobile phone now sends its IMSI and IMEI number to the IMSI catcher.

How does IMSI catcher work?

IMSI catcher now got what it wanted, so it responds that it cannot accept the mobile phone connection (sends so called Location Update Reject). Mobile phone is now directed back to a original network operator. This usually takes about several seconds.


However, sometimes mobile phone is not directed back to the original network...

How police gets IMSI number of a target?

In vicinity of a target it performs a measurement and gets all IMSI numbers of **all nearby** mobile phones.

When the target phone is moved to another location, police repeats the process and obtains a **new list** of IMSI numbers.

With the **intersection** of these measurements the IMSI number of a target device is identified.

What else can be done with them?

The capabilities of IMSI catchers vary from model to model.

IMSI catcher can reveal exact location of a mobile phone.

It can offer network connectivity to mobile phone and performs man-in-the-middle attack.
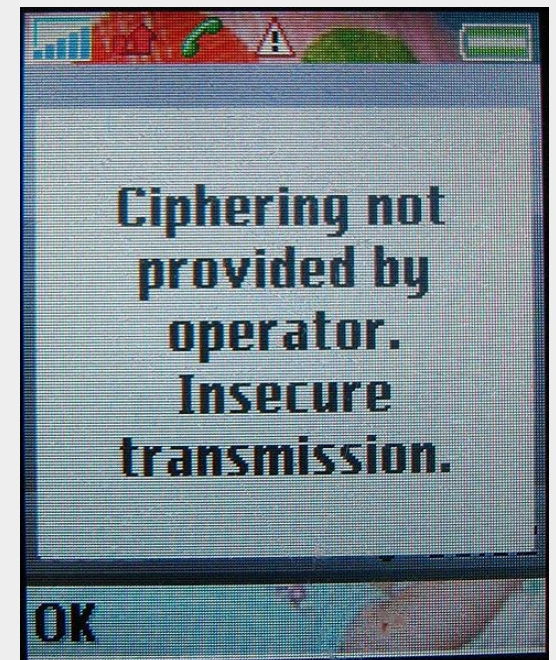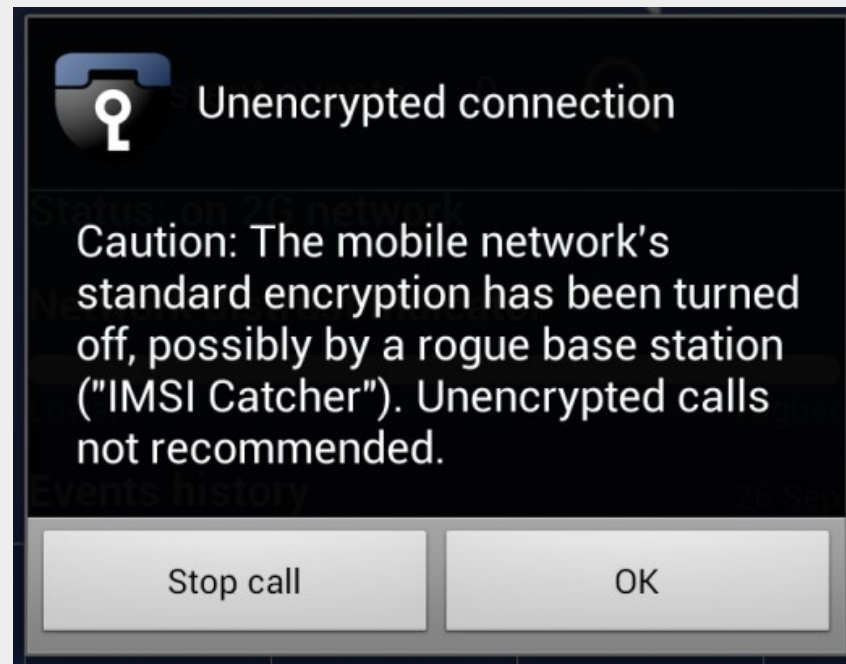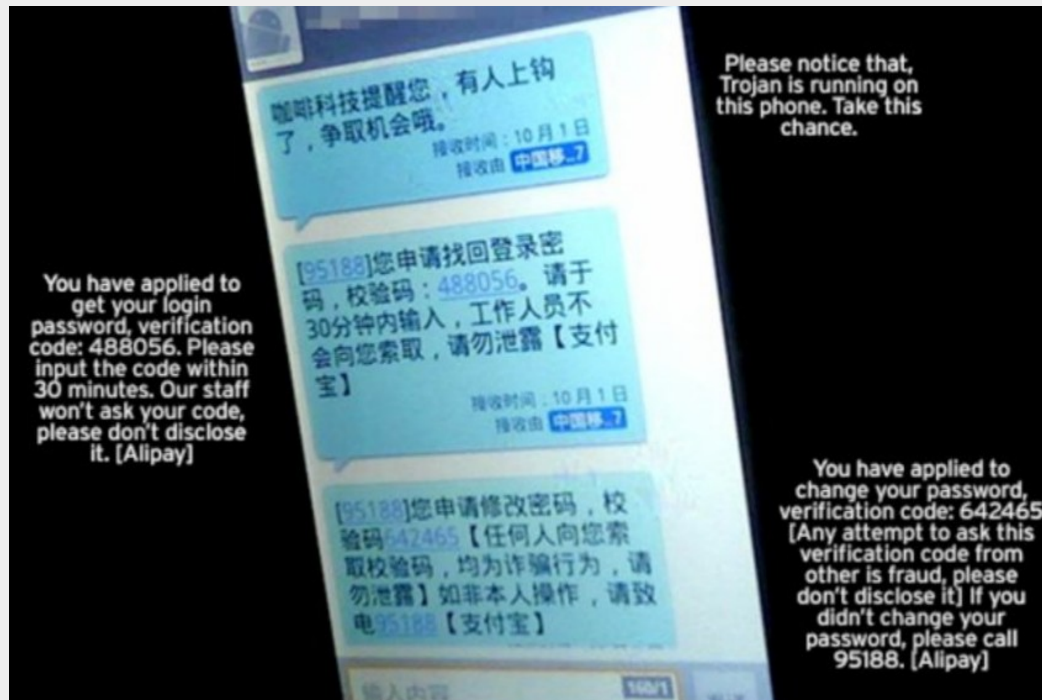
What else can be done with them?

Mobile phones should show warnings about possible MITM attacks, but this is not clearly visible, does not happen or could be suppressed..
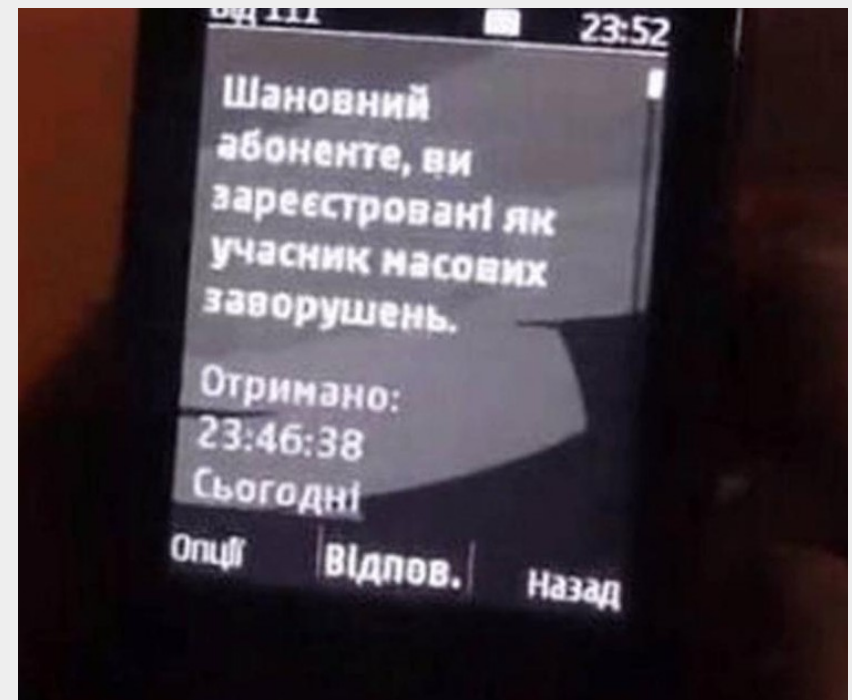
What else can be done with them?

IMSI catcher can initiate calls and send SMS messages to a target phone bypassing the network.


Chinese SPAM messages.

Ukraine – SMS message to protesters in 2014.

What else can be done with them?

IMSI catcher can isolate a single mobile phone from the network.

It can disable the mobile phone (until reboot) or drain its battery.

With a so called "silent call" IMSI catcher can switch the microphone on the mobile phone on. Mobile phone is then turned into a bugging device.
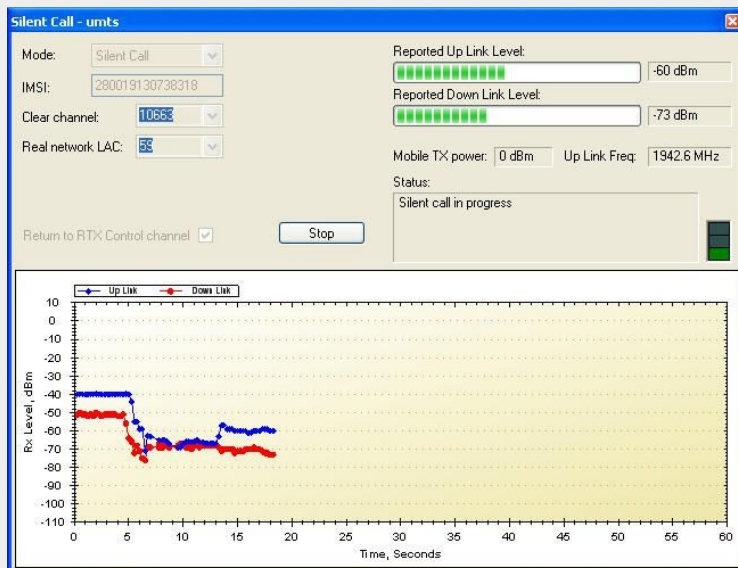
UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- X

IN THE MATTER OF AN APPLICATION OF   :
THE UNITED STATES OF AMERICA FOR
AUTHORIZATION TO CONTINUE TO   :
INTERCEPT ORAL COMMUNICATIONS   APPLICATION FOR AN
OCCURRING AT (i) THE SEATING AREA   :   ORDER AUTHORIZING THE
INSIDE BRUNELLO TRATTORIA, 227 EAST   INTERCEPTION OF ORAL
MAIN STREET, NEW ROCHELLE, NEW YORK   :   COMMUNICATIONS_____
10801; (ii) THE SEATING AREA INSIDE
MARIO'S RESTAURANT, 2342 ARTHUR   :
AVENUE, BRONX, NEW YORK 10458;
(iii) THE SEATING AREA INSIDE   :
AGOSTINO'S RESTAURANT, 969 BOSTON
POST ROAD, NEW ROCHELLE, NEW YORK   :
10801; AND (iv) THE SEATING AREA
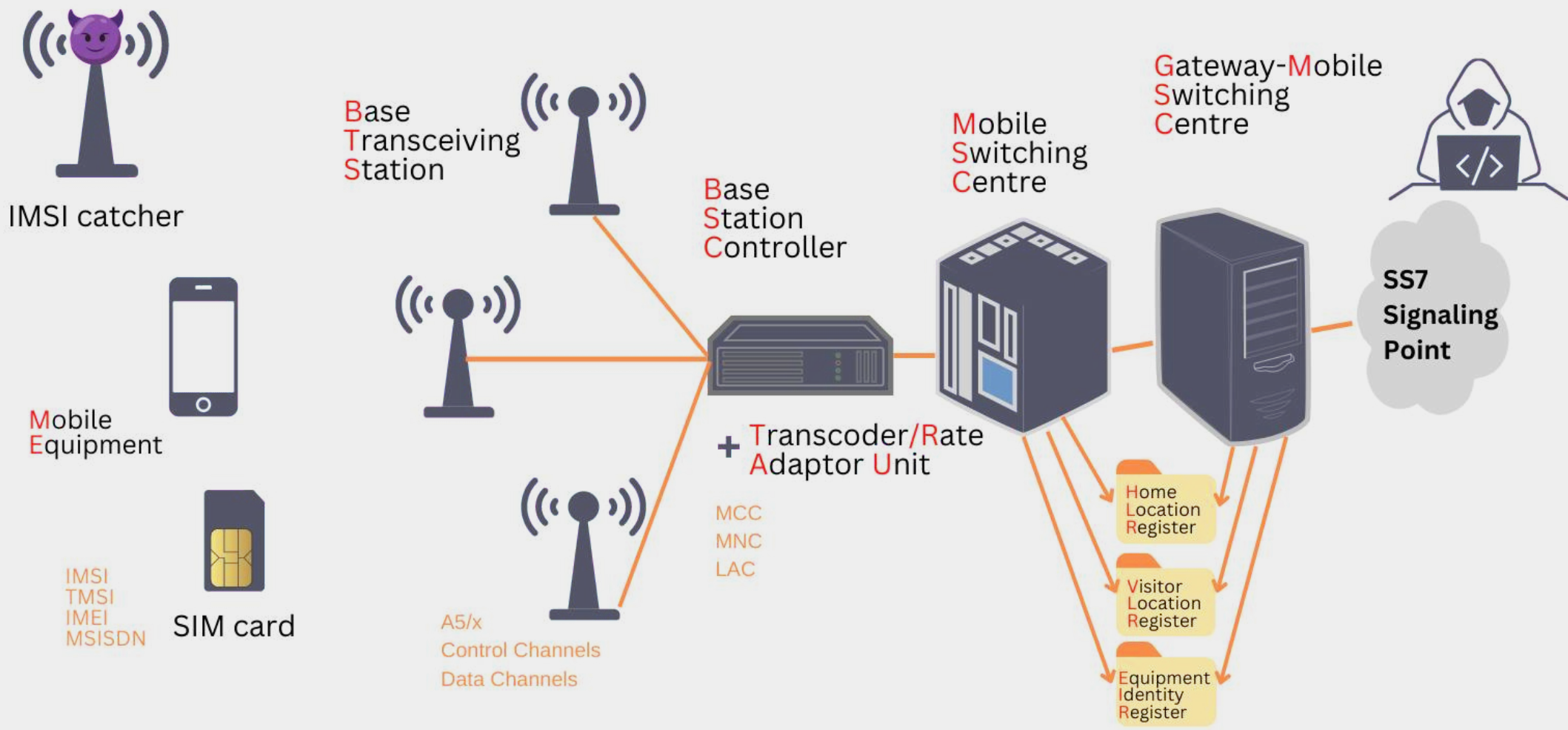INSIDE THE MARINA RESTAURANT, WRIGHT   :
ISLAND MARINA, 290 DRAKE AVENUE, NEW

What else can be done with them?

IMSI catcher can attack radio (baseband) processor and install malware into the mobile phone (and bypass all security mechanisms).

Only a few special telephones have mechanisms to detect this behaviour... and some are using so called baseband isolation.

IMSI catcher

Mobile **E**quipment

IMSI
TMSI
IMEI
MSISDN

SIM card

Base **T**ransceiving **S**tation

Base **S**tation **C**ontroller

+ **T**ranscoder/**R**ate **A**daptor **U**nit

MCC
MNC
LAC

A5/x
Control Channels
Data Channels

Mobile **S**witching **C**entre

Gateway-**M**obile **S**witching **C**entre

SS7 Signaling Point

Home **L**ocation **R**egister

Visitor **L**ocation **R**egister

Equipment **I**dentity **R**egister

IMSI catcher on the network
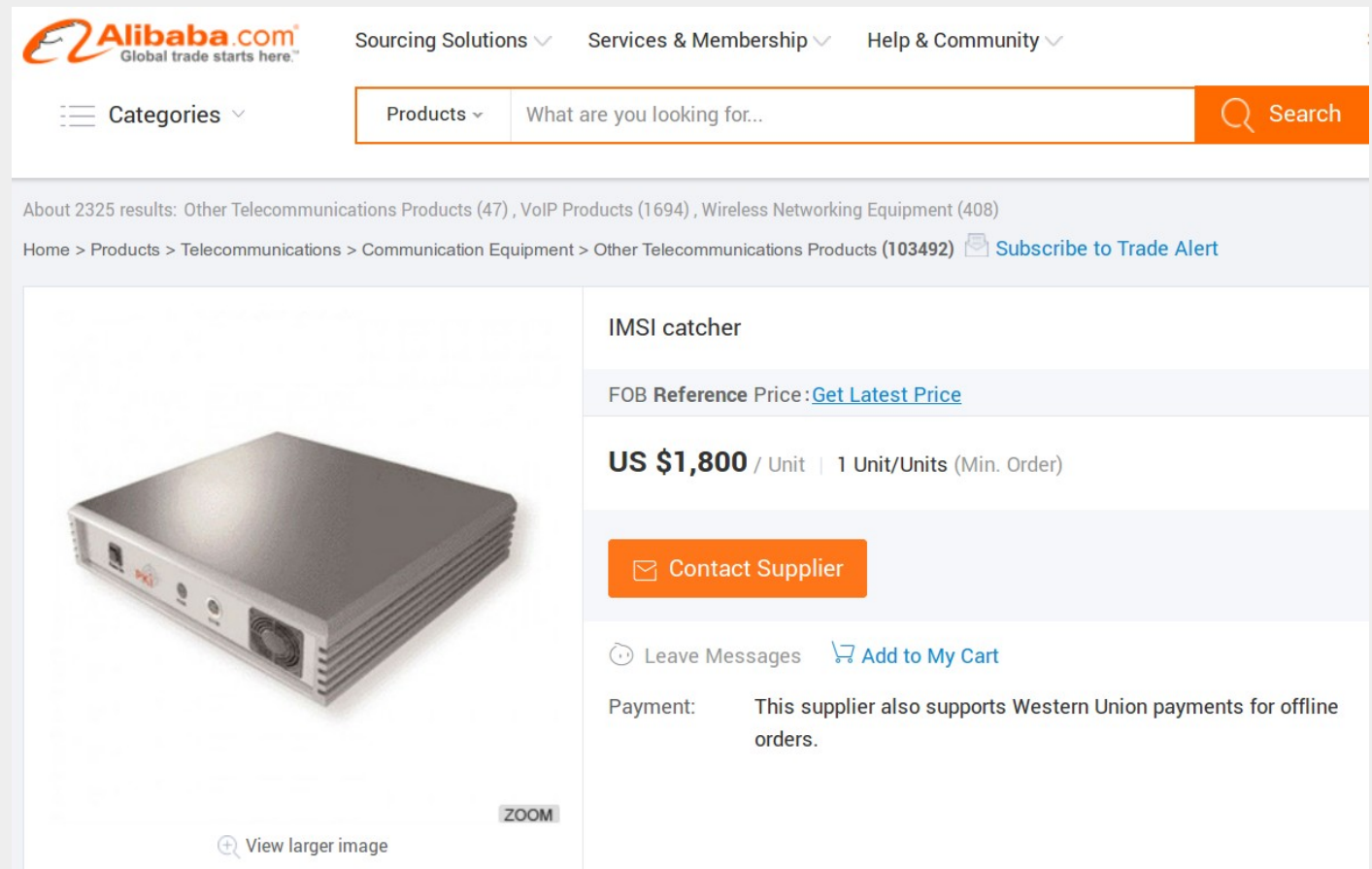
Can I have one?
:-)

You can buy professional equipment...

You can buy them on the Internet...

IMSI catchers are not only accessible to law enforcement agencies, but also to criminals. Prices are not so high...

Or you can build your own...

Hardware costs around 300 EUR, software is freely available on the Internet.
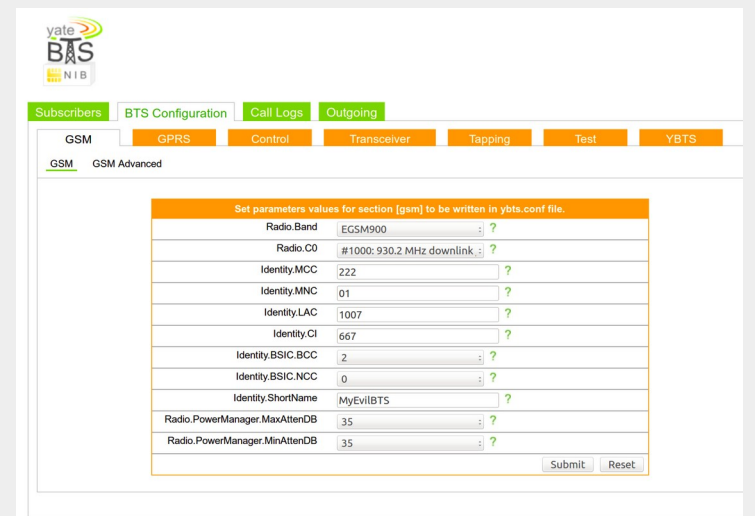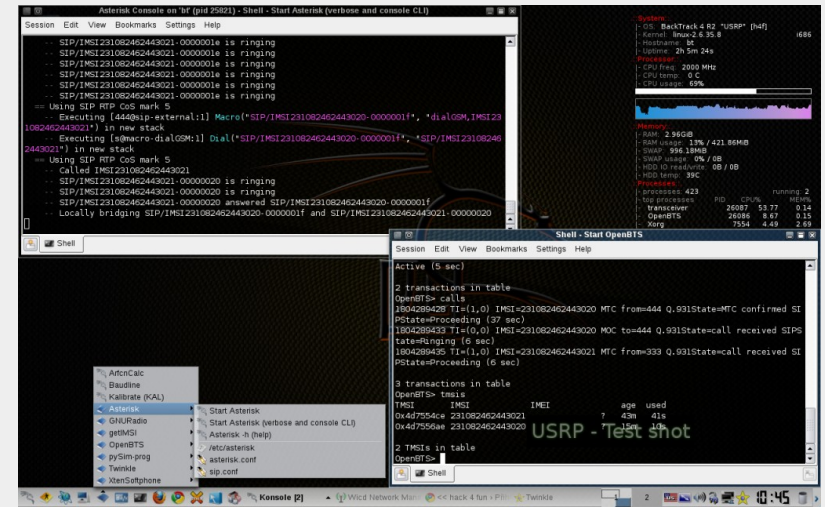
Or you can build your own...

Passive IMSI catcher (for ~40 EUR).
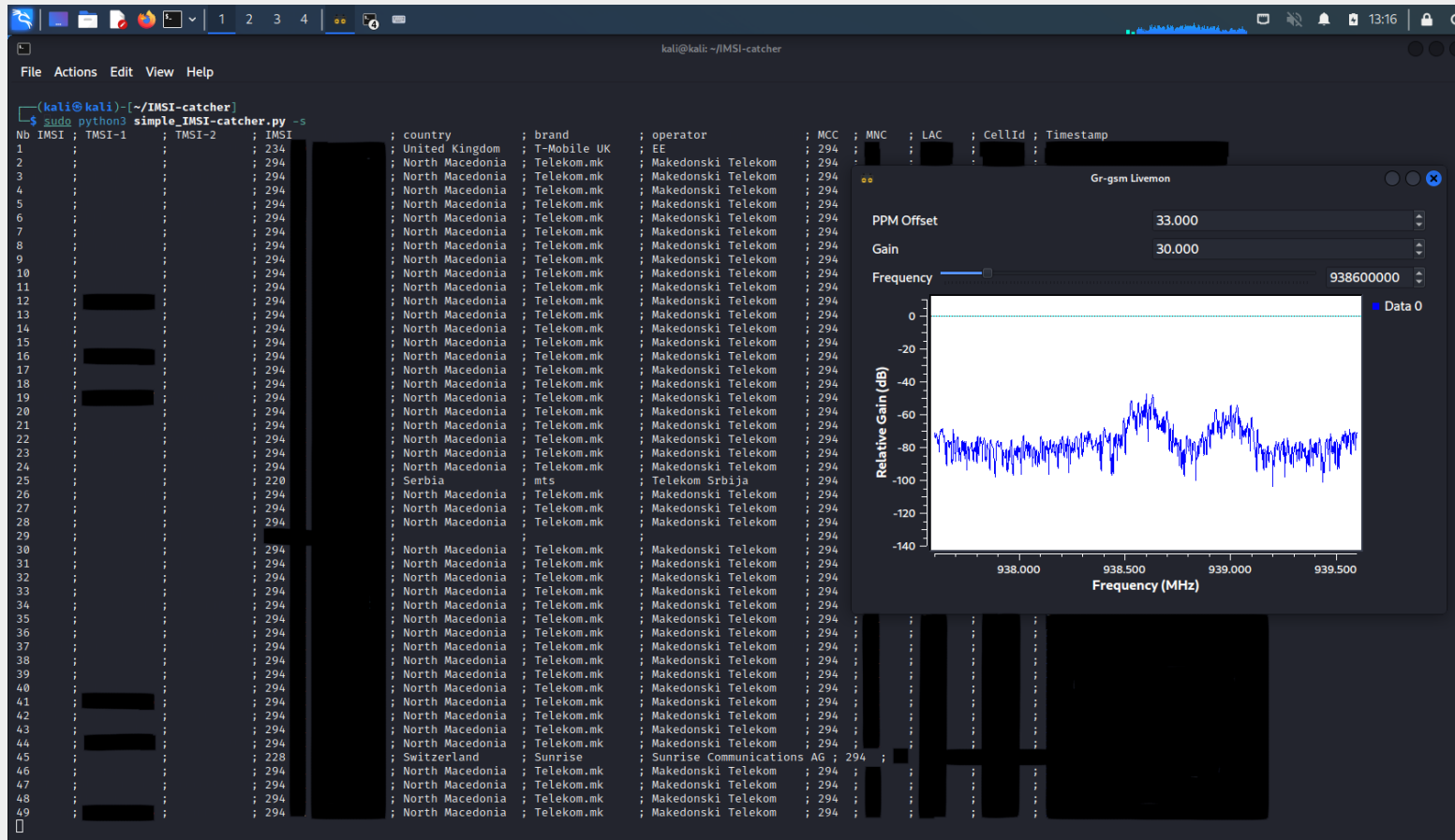
A passive IMSI catcher **does not** transmit radio signals, **does not** interfere with cellular networks in any way, and **can not** perform a man-in-the-middle attack between a phone and a mobile base station.

Legal aspects of IMSI catchers

Passive or active attack?

Important question with legal consequences is:

- is IMSI catcher a "**passive device**", which just present itself as a base station and "tricks" nearby mobile phones to reveal their data to it by themselves…

- …or, is there an **active attack** on the mobile phones going on?

In legal terms: are we talking about **covert observation** or **intrusion into communication privacy**?

Passive or active attack?

In fact mobile phone transmits IMSI and IMEI numbers to mobile networks on very limited occasions.

Even more, mobile networks communicate with mobile phone via pseudoanonymous identity – TMSI number. TMSI number was explicitly introduced in order to protect user's identity from external observers.

IMSI catcher actually **forces mobile phones** to reveal their identity (IMSI and IMEI number) by abusing network protocol.

So it is an **active attack**. It is a measure similar to eavesdropping, which **requires high judicial standards** (i.e. court order) – at least in countries adhering to the rule of law.

It is an intrusion into communication privacy.

Legal aspects of IMSI catchers

Principle of proportionality and indiscriminate collection of data (of innocent bystanders)

Monitoring and intercepting communications

Monitoring and intercepting traffic data

IMSI and IMEI data: personal data

Location tracking

IMSI catchers and...

- the right to privacy

- freedom of expression

- freedom of assembly and association

Further reading: IMSI catchers legal analysis, June 2020, privacyinternational.org.

IMSI catchers: Slovenian case study

IMSI catchers in Slovenia

July 12th, 2004

Deputy director general of police signed a proposal for the purchase of the first IMSI catcher. Document was later obtained by Access to Public Information Act.

August 26th, 2004

Deputy director general of police denies for media that police knows about "*techniques that allow illegal wiretapping*".

August 30th, 2004

After session of parliamentary Commission for Supervision of Intelligence and Security Services, director general of police denies that "*the equipment for eavesdropping without the operator's knowledge*" has been legally imported in Slovenia.

IMSI catchers in Slovenia

September 6th, 2004

Police signed contract for purchasing first IMSI catcher (GI2 – GSM Identity Interrogator). Copy of contract was obtained by Access to Public Information Act.

February 20th, 2006

Police asks General Prosecutors's Office whether a measure of secret surveillance under article 149a of Criminal Procedure Act would be an appropriate legal basis for the use of IMSI catcher for the gathering of IMSI and IMEI numbers (secret surveillance shall be permitted by the state prosecutor on the basis of a written order).

March 21th, 2006

General Prosecutors's Office supports that legal interpretation and distributes the document to all prosecutors. Document was not marked as classified and was later obtained by Access to Public Information Act.

IMSI catchers in Slovenia

June 26th, 2006

Policice prepares proposal for the purchase plan of an upgrade of IMSI catcher and training for its use. Copy of the document was obtained by Access to Public Information Act.

July 17th, 2008

Police for newspaper Mladina: "*The police do not disclose the technical means, tactics and methodology of their operation for implementation of covert investigative measures*".

October 28th, 2009

Police buy second IMSI catcher (Nethawk FONE). Copy of the document was obtained by Access to Public Information Act.

IMSI catchers in Slovenia

December 10th, 2010

Police opens tender for upgrade of an IMSI catcher and training of its use.

March 1st, 2011

Contract for upgrade of an IMSI catcher and training is signed. Copy of document was obtained by Access to Public Information Act.

Total price for both devices, upgrades and training: **1.351.362,24 EUR**.

IMSI catchers in Slovenia

January 18th, 2012

Lawyer Roman Završek officially asks ministry of interior if police owns an "IMSI catcher" device.

February 21th, 2012

Police denies answer claiming this is classified information. Lawyer appeals to Information Commissioner

April 25th, 2012

Information Commissioner rejects the complaint.

IMSI catchers in Slovenia

November 27th, 2012

Deputy director general of police confirms the existence of IMSI catcher for national radio, but denies that police is actually using it.

January 7th 2013

Deputy director of police for newspaper Večer confirms that police is using IMSI catcher, but only for searching missing persons and when there is kidnapping. However, he denied using device for obtaining the telephone numbers of suspects.

April 4th, 2013

Ministry of interior officially confirms existence of IMSI catcher to media and its use for obtaining IMSI and IMEI numbers.

IMSI catchers in Slovenia

April 2013

Information Commissioner starts inspection procedure against police because of IMSI catcher use.

April 19th 2013

Minister of interior confirms existence of two IMSI catchers for media.

December 2014

On-line portal Slo-Tech obtains documents about purchase and use of IMSI catchers. Documents show that police used the device more than 300 times between 2006 and 2012, mostly for obtaining telephone numbers of suspects and for various crimes, including drug trafficking, etc.

Legal aspects

First IMSI catcher was **purchased in September 2004**.

Till March 2006 device was not used, because police opinion has presumably been that for using the device legal ground is needed.

In March 2006, General Prosecutor's Office supports legal interpretation that using IMSI catcher is a measure of secret surveillance under article 149a of Criminal Procedure Act.

For using these measures (secret surveillance) **no court order is needed**, but **written order of state prosecutor** is sufficient.

Meanwhile, deputy director general of police in January 2013 stated for media that "*Article 148 of Criminal Procedure Act … does not allow using the device for obtaining telephone numbers of suspects*".

Legal aspects

In 2013 there has been prepared new Criminal Procedure Act, but legal provisions to allow and regulate the use of IMSI catchers were later left out.

The the opinion from several legal experts in 2013:

- There is no a priori opposition to the use of IMSI catcher devices.

- Using IMSI catcher presents a covert acquisition of personal data from the person to whom this data relates. IMSI and other identification numbers enable the individualization of SIM card and the mobile terminal, which are personal data of the user.

- The use of an IMSI catcher - even if it is not directly used to monitor communication - can still mean an invasion of communication privacy.

Legal aspects

- Legally, the most sensitive in this context is the nature and amount of data that police officers can collect with such devices. The use of the IMSI catcher is **completely unfocused during the data collection phase** - because it collects IMSI and IMEI data from **all** mobile devices in its working area.

- The implementation of this measure cannot be focused during the data collection phase. Focusing occurs only at the stage of **processing** of the collected data.

- This means that the police collects the personal data of an indefinite number of persons who, in this context, act as a means to achieve the goal, i.e. identification of one or more means of communication of the suspect.

Legal aspects

- Therefore the use of the IMSI catcher dangerously interferes with the very core of human dignity of persons who are not suspects or defendants.

- Technical devices of this type are mobile, small, hidden and therefore extremely difficult to control. The use of the IMSI catcher in itself does not enable control by third parties (e.g. the operator, who must ensure indelible recording of intrusions into personal privacy).

"Opinion on proposal of ZKP-M" by dr. Primož Gorkič, dr. Katja Šugman Stubbs, dr. Ciril Keršmanc, dr. Aleš Završnik, 23. 12. 2013

Legal aspects

The German Federal Constitutional Court exempted the use of the IMSI catcher from the sphere of protection of communication privacy, since in their opinion the IMSI catcher should interfere only with communication between devices (BVerfG, 2 BvR 1345/03 of 22.8.2006).

In Slovenia the opinion from legal experts in 2013 stated that "*due to the technological capabilities of such devices, such an approach is no longer adequate*".

"Opinion on proposal of ZKP-M" by dr. Primož Gorkič, dr. Katja Šugman Stubbs, dr. Ciril Keršmanc, dr. Aleš Završnik, 23. 12. 2013

Legal aspects

In 2016 police indirectly confirmed that there is **no clear legal grounds** for using IMSI catchers.

In the same year the government prepared new Criminal Procedure Act with clear legal grounds for using IMSI catchers.

Principles:

- The permissible purposes of using the IMSI catcher should be limited to the identification of a specific mobile device or to the more precise location of mobile device.

Legal aspects

- The police should not be allowed to carry out "eavesdropping" with IMSI catcher (both passive (deciphering existing traffic) or active (i.e. man-in-the-middle attack)), as well as other advanced investigative actions.

- Police should only obtain data for identifying the communication device (IMEI number) and data about mobile identity (IMSI number), but not other data about nearby mobile phones. Acquired data belonging to third parties, should be discarded.

- Strict audit trail should be kept.

The **legislation has been adopted in March 2019**.

Legal aspects

In **July 2019** Constitutional Court of the Republic of Slovenia **temporary withhold the implementation of law** (at the proposal of (left-wing) Left party and (right-wing) Slovenian Democratic Party).

The applicants claimed that the legislation which regulates the use of IMSI catchers presents a severe and disproportionate invasion of privacy.

The proponents disputed Article 150a of the Criminal Procedure Act, but did not propose temporary withholding its implementation. However, the Constitutional Court did that ex officio.

Legal aspects

To this date Constitutional Court of the Republic of Slovenia did not decided on the constitutionality of law even they concluded that they "*will treat the case with absolute priority*".

After more than 18 years of legal controversy using IMSI catchers and more than 1.3 million EUR taxpayer's money spend, **there is still no clear legal grounds** for using these devices in Slovenia.

Source wiretapping
(lawful interception at the source)

The problem...

Capabilities Development Risk Matrix (U)

| Impact > to production Use Risk v	TRIVIAL Loss/lack of insight to small aspect of target communications, presence	MINOR Loss/lack of insight to significant aspect of target communications, presence	MODERATE Loss/lack of insight to large component of target communications, presence	MAJOR Loss/lack of insight to majority of target communications, presence	CATASTROPHIC Near-total loss/lack of insight to target communications, presence
Current Highest Priority Target Use	Document tracking	Fivewes, Facebook chat presentation	Mail.ru, TeamViewer, Join.me	OTR, Tor, Smartphones, Zoho.com webmail, TrueCrypt	Tor+ Trilight Zone + Cspace + ZRTP VoIP client on Linux
Current Operational Target Use					
Current Low Priority/Previous Higher Priority Target Use					
Technical Thought Leader Recommendations, Experimentatio					

Things become "*catastrophic*" for the NSA at level five – when, for example, a subject uses a combination of Tor, another anonymization service, the instant messaging system CSpace and a system for Internet telephony (voice over IP) called ZRTP. This type of combination results in a "*near-total loss/lack of insight to target communications, presence*," the NSA document states. (Der Spiegel)

Source wiretapping

The use of encryption means that wiretapping on the network is not useful any more.

So law enforcement and intelligence agencies started to use data interception tools **on devices** (computers, mobile phones) for eavesdropping.

These tools are in fact a special software (malware, trojan, spyware), which could be installed on the target device and can **wiretap at the source** (before data are encrypted).
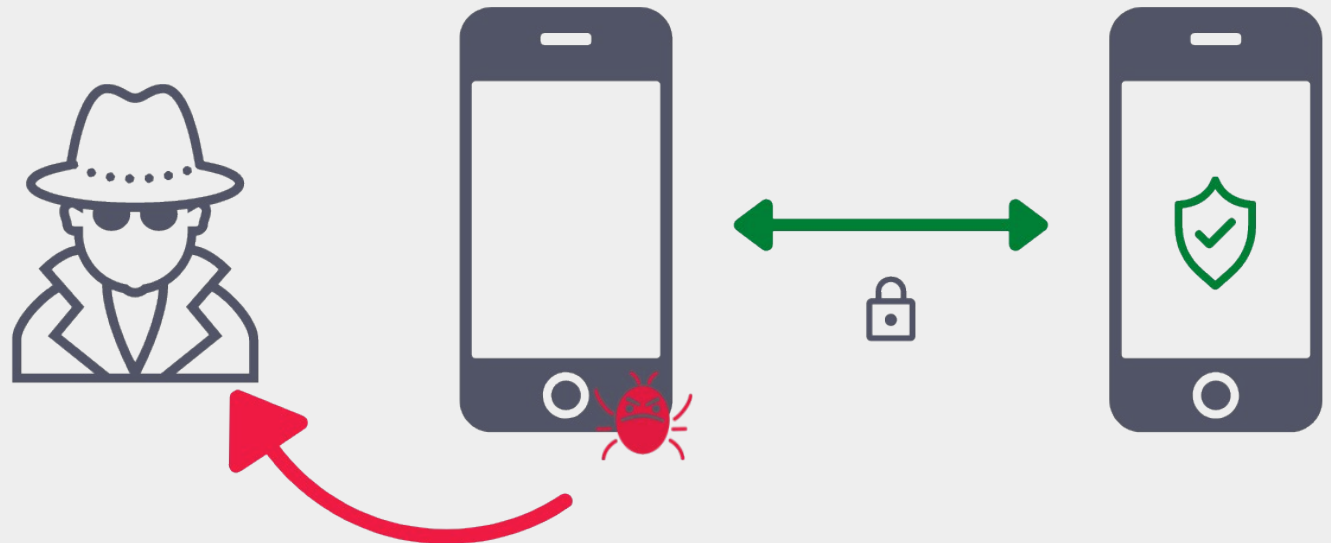
Source wiretapping

One of the first tools for source wiretapping was Germany's "Staatstrojaner" used for spying and monitoring VoIP applications and messengers on computers and mobile devices.

In 2011 the tool has been reverse engineered and analysed. Findings:

- the Trojan can activate microphone and camera;

- can monitor screen;

- can access files on the device;

- can receive uploads of arbitrary programs from the Internet and execute them remotely;

Source wiretapping

In 2008 the German Federal Constitutional Court has found the use of Trojans to be justified if there is a concrete risk to a legal interest of paramount importance.

However court order is required for installation and use of such tools.

Today the market for such tools is well developed and there are several spyware cyberweapons available (for instance FinFisher, Pegasus, Predator, Black Cube, Blue Hawk CI, BellTroX, Cytrox107, Predator, Candiru, Subzero/KNOTWEED, etc.).

And many of these tools is being used to target activists, journalists, government officials, executives...

Cyberweapons
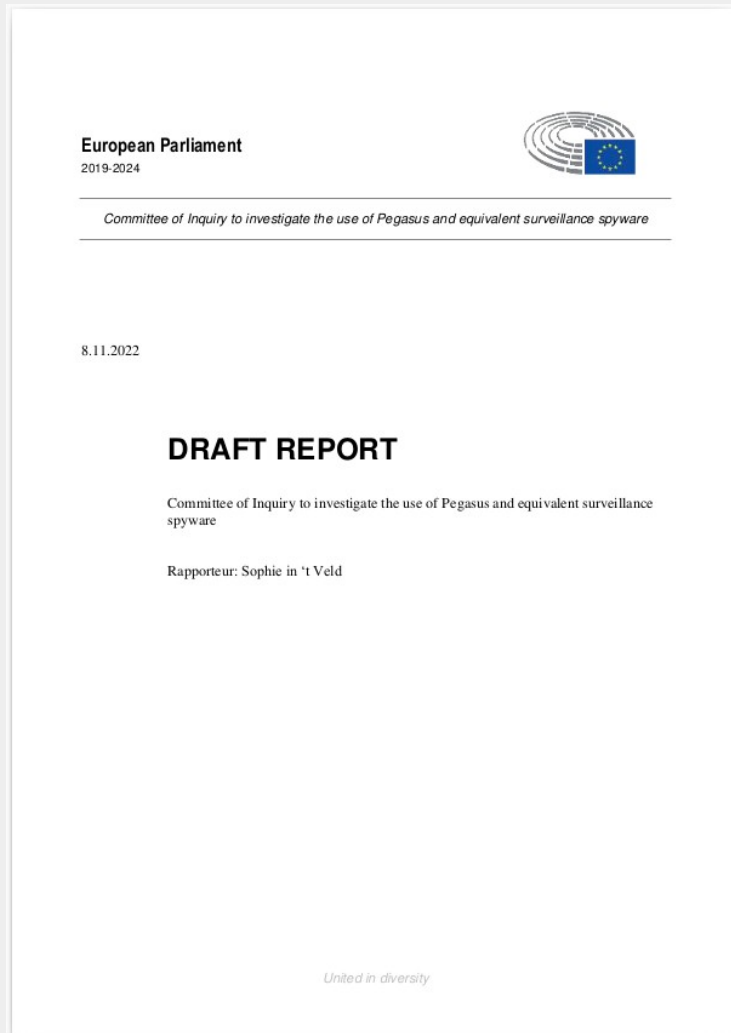

Source: Citizen Lab
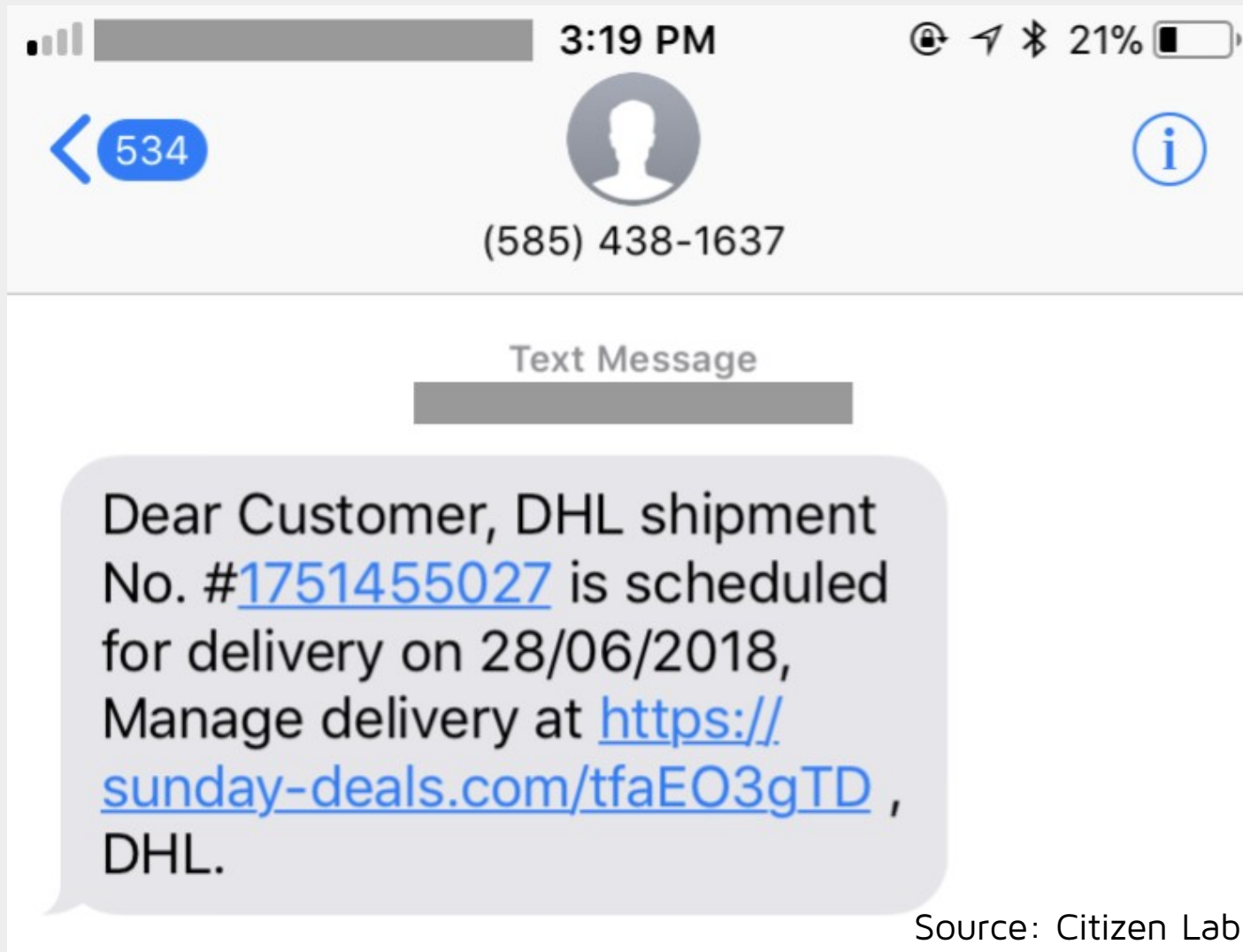
Some spyware tools require that user clicks on a link (or opens a message,...), while others can perform zero-click infection.

Cyberweapons

»This spyware tool is designed to secretly turn mobile phones - both with Android and iOS operating systems - into 24-hour surveillance devices, as it grants complete and unrestricted **access to all sensors and information of the targeted device**. It can read, send or receive messages that should be end-to-end encrypted, download stored photos, collect passwords, hear and record voice or video calls as, among other things, it has full access to the phone's camera, microphone, and geolocation module.«

Pegasus and surveillance spyware. Report for European Parliament, May 2022.

Cyberweapons

European Parliament
2019-2024

Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware

8.11.2022

DRAFT REPORT

Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware

Rapporteur: Sophie in 't Veld

United in diversity

European Parliament 2019-2024 Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware 8.11.2022 DRAFT REPORT Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware

Spyware is not a mere technical tool, used ad hoc and in isolation. **It is used as integral part of a system.** In principle its use is embedded in a legal framework, accompanied by the necessary safeguards, oversight and scrutiny mechanisms, and means of redress. The inquiry shows that these safeguards are often weak and inadequate. That is mostly unintentional, but in some cases, the system has – in part or in whole – been bent or designed purposefully to serve as a tool for political power and control. **In those cases, the illegitimate use of spyware is not an incident, but part of a deliberate strategy.**

Source: PEGA draft report, published November 8th 2022

Cyberweapons in Slovenia

In 2013 there were attempts to include legal basis for source wiretapping in Criminal Procedure Act, however they were not successful.

In September 2014 Slovenian police has been in communication with Hacking Team regarding their trojan RCS (Galileo). Hacking Team also prepared a demo for Slovenian police.

However, at that time Slovenia was still missing a government and there were no legislation covering use of such tools, so the deal with the police has not been closed.

Cyberweapons in Slovenia

In 2015 Hacking Team has been hacked and around 400 GB of their internal data has been published...

Cyberweapons in Slovenia

Leaked e-mail messages also revealed that (allegedly) Slovenian Intelligence and Security Agency has also been interested in the purchase in October 2013. The deal was supposed to be made through Israeli company *NICE Systems* and their Serbian partner *TERI Engineering*. Representative of Israeli company NICE systems mentioned, that Slovenian partner already has approved budget for buying trojan software.

On November 15th 2013, the adopted budget for Slovenian Intelligence and Security Agency contained a relatively high item for "investments in technical resources" (SIGINT) in the amount of EUR 1.490.000 EUR.

0803 Obveščevalno-varnostna dejavnost					**13.548.689**
080301 Obveščevalno varnostna dejavnost					*13.022.328*
Ukrepi					11.532.328
(1524) 1524-11-0001 HUMINT in SIGINT	01.01.11	31.12.15			11.532.328
1524-13-S001 INVESTICIJE					1.490.000
(1524) 1524-11-0002 SIGINT - tehnični viri	01.01.11	31.12.17	13.409.484	72,6%	1.490.000

Source: https://slo-tech.com/novice/t649095/0

Cyberweapons in Slovenia

In 2015 CitizenLab published an analysis of their Internet scanning for FinFisher proxies...

FINFISHER SPYWARE
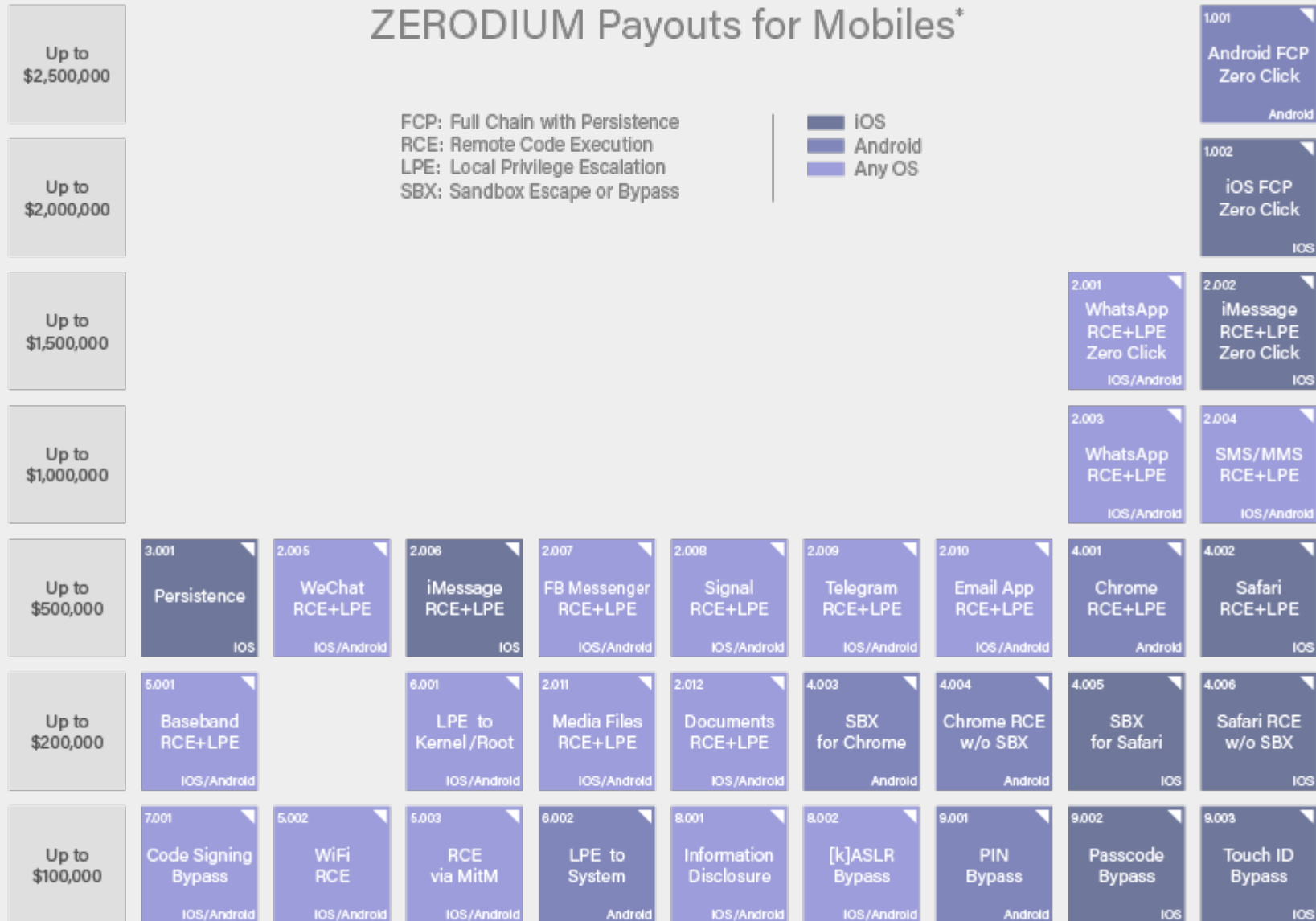Suspected Government Users In 2015

Citizen Lab 2015
Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto & Sarah McKune

Cyberweapons

ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

- iOS
- Android
- Any OS

Up to $2,500,000									1.001 Android FCP Zero Click — Android
Up to $2,000,000									1.002 iOS FCP Zero Click — iOS
Up to $1,500,000								2.001 WhatsApp RCE+LPE Zero Click — iOS/Android	2.002 iMessage RCE+LPE Zero Click — iOS
Up to $1,000,000								2.003 WhatsApp RCE+LPE — iOS/Android	2.004 SMS/MMS RCE+LPE — iOS/Android
Up to $500,000	3.001 Persistence — iOS	2.005 WeChat RCE+LPE — iOS/Android	2.006 iMessage RCE+LPE — iOS	2.007 FB Messenger RCE+LPE — iOS/Android	2.008 Signal RCE+LPE — iOS/Android	2.009 Telegram RCE+LPE — iOS/Android	2.010 Email App RCE+LPE — iOS/Android	4.001 Chrome RCE+LPE — Android	4.002 Safari RCE+LPE — iOS
Up to $200,000	5.001 Baseband RCE+LPE — iOS/Android		6.001 LPE to Kernel/Root — iOS/Android	2.011 Media Files RCE+LPE — iOS/Android	2.012 Documents RCE+LPE — iOS/Android	4.003 SBX for Chrome — Android	4.004 Chrome RCE w/o SBX — Android	4.005 SBX for Safari — iOS	4.006 Safari RCE w/o SBX — iOS
Up to $100,000	7.001 Code Signing Bypass — iOS/Android	5.002 WiFi RCE — iOS/Android	5.003 RCE via MitM — iOS/Android	6.002 LPE to System — Android	8.001 Information Disclosure — iOS/Android	8.002 [k]ASLR Bypass — iOS/Android	9.001 PIN Bypass — Android	9.002 Passcode Bypass — iOS	9.003 Touch ID Bypass — iOS

2019/09 © zerodium.com

The problem?

»We can't choose a world where the US gets to spy but China doesn't, or even a world where governments get to spy and criminals don't.

We need to choose, as a matter of policy, communications systems that are secure for all users, or ones that are vulnerable to all attackers.

It's security or surveillance.«

Bruce Schneier: Cyberweapons Have No Allegiance, February 25, 2015

The backdoor dilemma

»Adding backdoors will only exacerbate the risks. As technologists, we can't build an access system that only works for people of a certain citizenship, or with a particular morality, or only in the presence of a specified legal document. If the FBI can eavesdrop on your text messages or get at your computer's hard drive, so can other governments. So can criminals. So can terrorists.«

Bruce Schneier. 2016. Security vs. Surveillance.

Countermeasures?

Mobile security hardening

In 2012 the U.S. National Security Agency (NSA) released the specifications for a new, super-secure smartphone for use by government officials. It was based on Android operating system and VoIP technology...
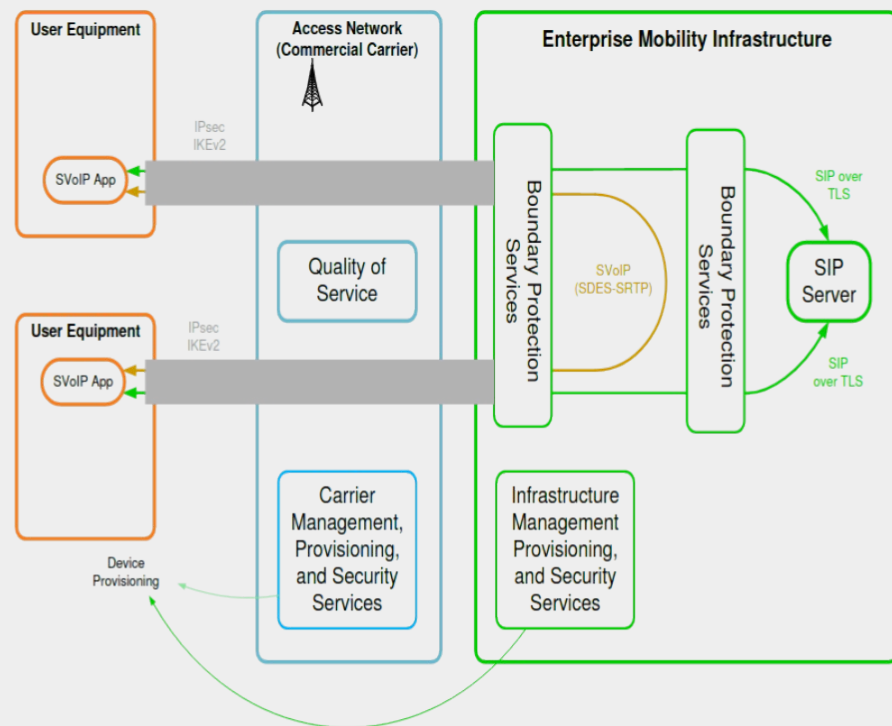

Figure 6-1 Basic Secure VoIP Architecture

Source: Mobility Capability Package - Secure VoIP Version 1.1, February 27th 2012, NSA (page 91).

Mobile security hardening

Security hardened mobile phone

- Hardware security module.

- Thoroughly tested & security certified hardware.

- Hardened OS and user applications.

- Advanced sandboxing.

- Baseband isolation.

- Perfect blending in with other mobile phone users.

- Zero learning required by average users (zero learning curve).
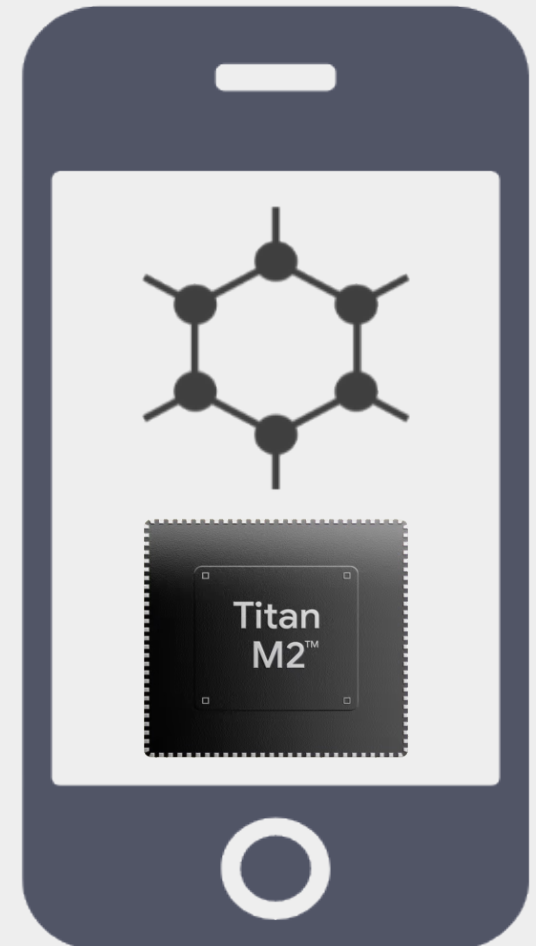
Mobile security hardening

Hardware attestation

- Attestation is the mechanism in which software verifies the authenticity and integrity of the hardware and software of a device.

- With hardware attestation malware infection can be detected.
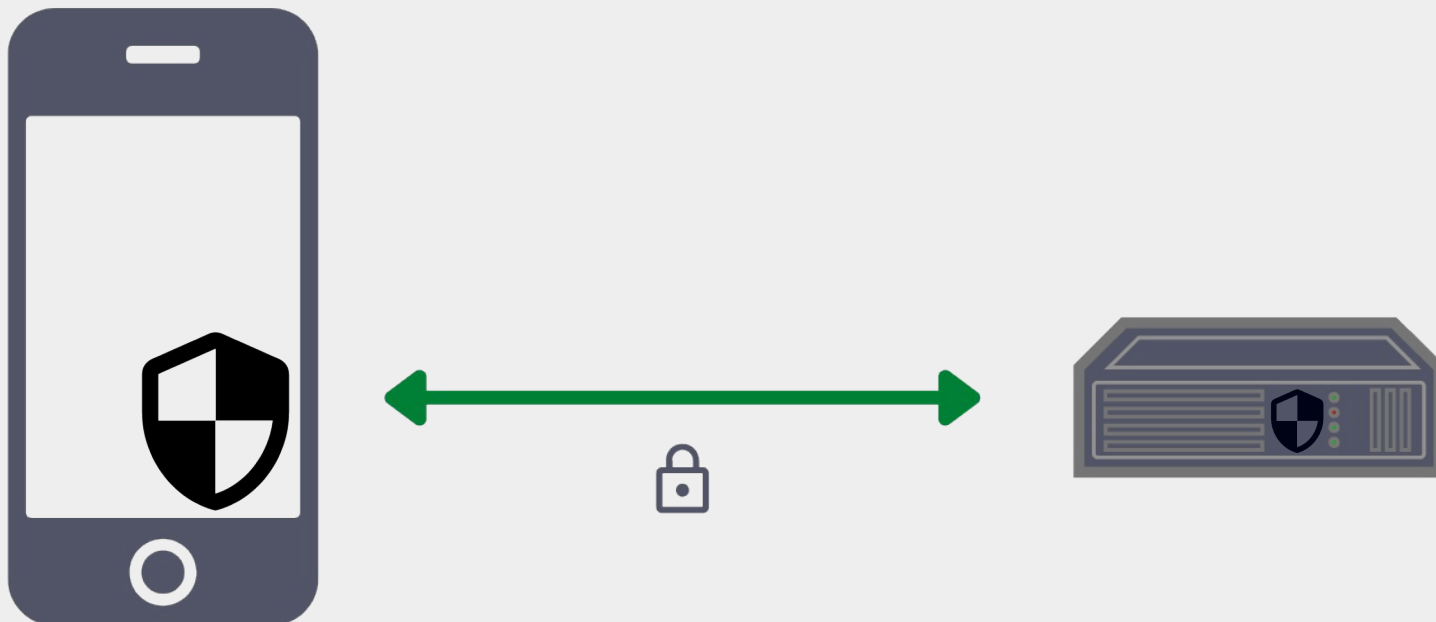
Mobile security hardening

E2E encrypted messenger, audio and video communications

- End-to-end encryption.

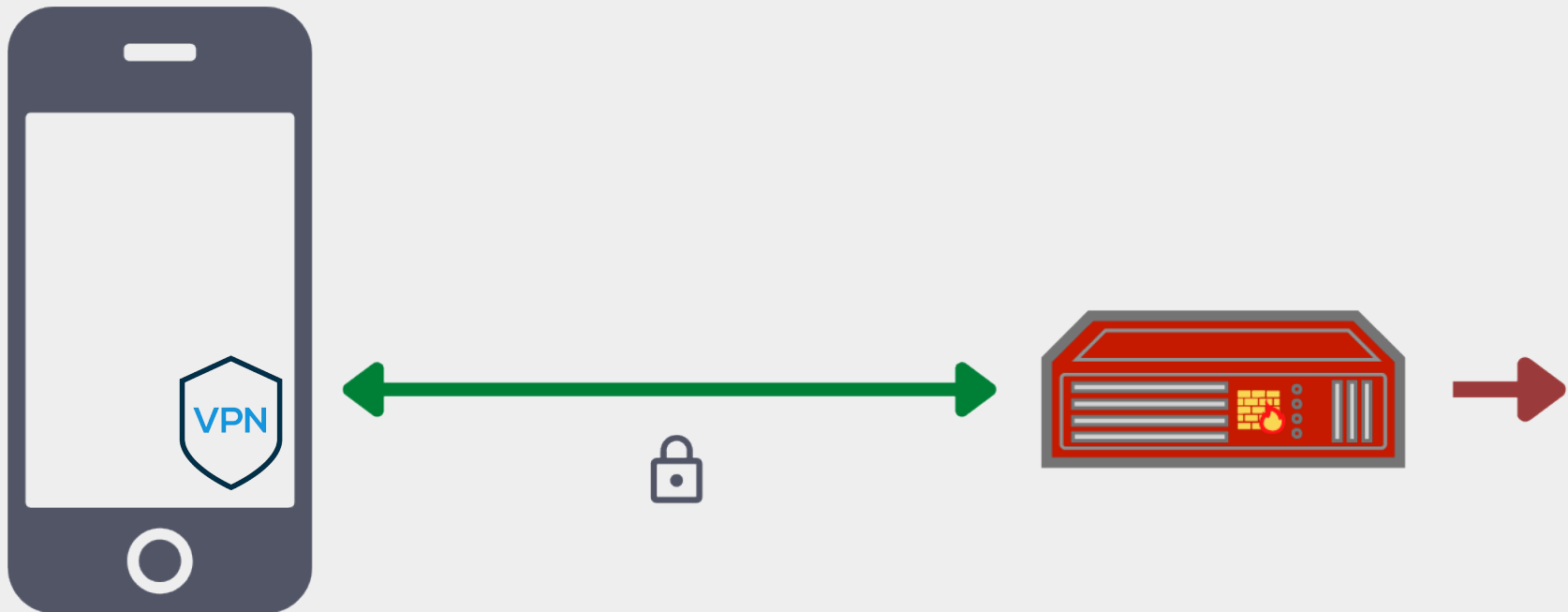- Audited and expert community accepted application.
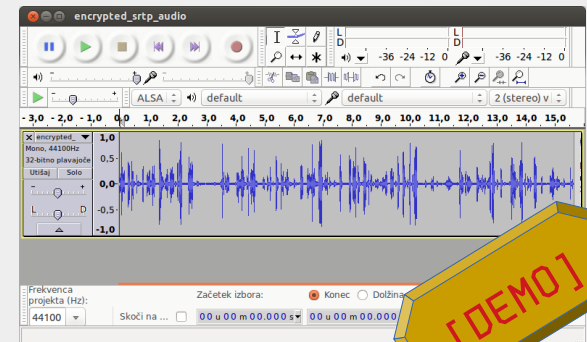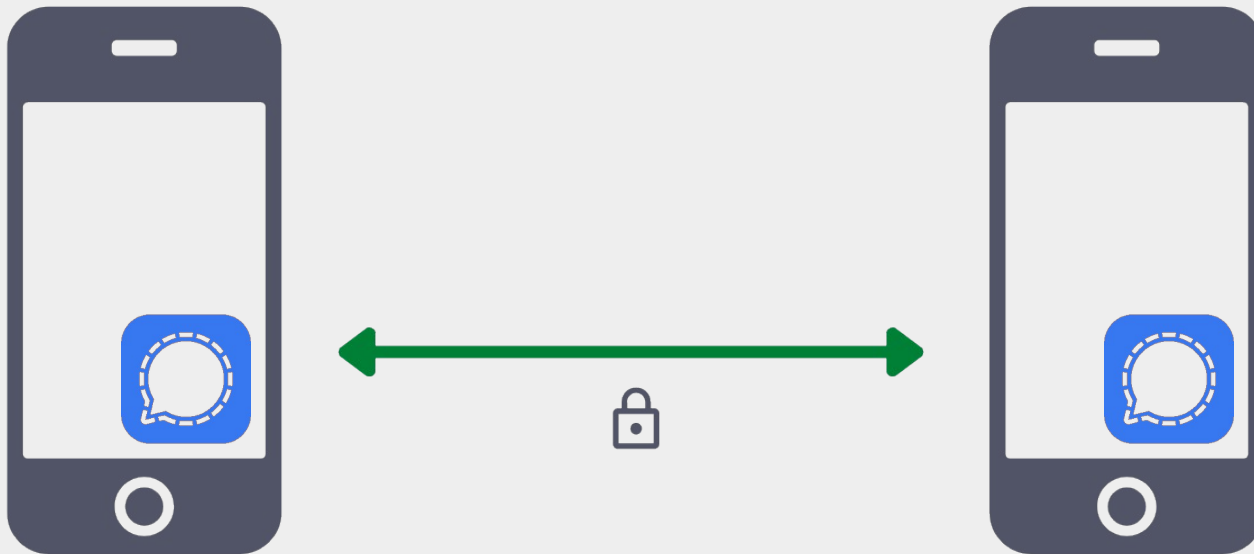
Mobile security hardening

Network traffic protection

VPN.

Security gateway with advanced intrusion detection/prevention system.

Mobile security hardening

Infrastructure security

- Infrastructure monitoring and notifications.
- Network vigilance.
- Incident response.
- Secure mobile devices management.
- Technology for rapid deployment of the whole infrastructure.
- Versioning (tracking changes) of the whole infrastructure.
- Fast reconstructing in case infrastructure gets compromised.
- On premises infrastructure (i. e. cloud free).
- Open source technologies.

Questions?

Прашања?

Matej Kovačič

https://telefoncek.si

Some further reading...

Matej Kovačič. 2022. Crash course on cybersecurity: a manual for surviving in a networked world. ISBN: 978-961-7025-24-8 (PDF)

The book tries to explain the complex area of cybersecurity in an understandable way, to help to grasp the essential information on how to protect yourself and/or your company from cyberattacks and to provide technologically neutral advice for the implementation of protection against cyberattacks.

The book is available under a Creative Commons license and PDF is freely available online.

Matej Kovačič

CRASH COURSE ON CYBERSECURITY

A manual for surviving in a networked world

University of Nova Gorica Press | 2022