GrapheneOS security

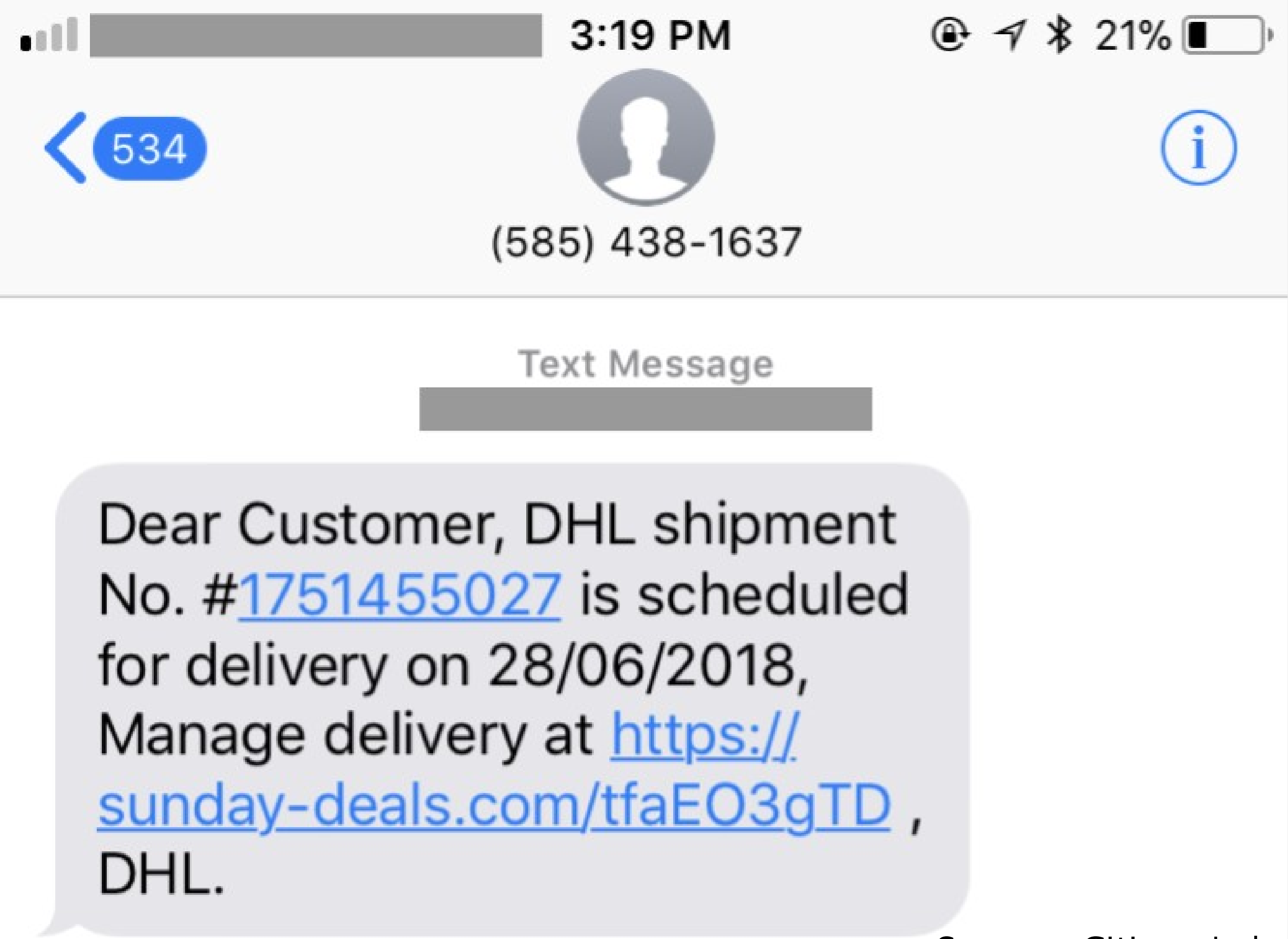
Making your mobile highly resistant to mobile spyware and other cyberweapons.

Matej Kovačič
https://telefoncek.si

Balkan Cybersecurity Days

Ohrid, May 16th, 2023

The problem



[redacted] 3:19 PM 21%

534

(585) 438-1637

Text Message

[redacted]

Dear Customer, DHL shipment No. #1751455027 is scheduled for delivery on 28/06/2018, Manage delivery at https://sunday-deals.com/tfaEO3gTD , DHL.

Source: Citizen Lab

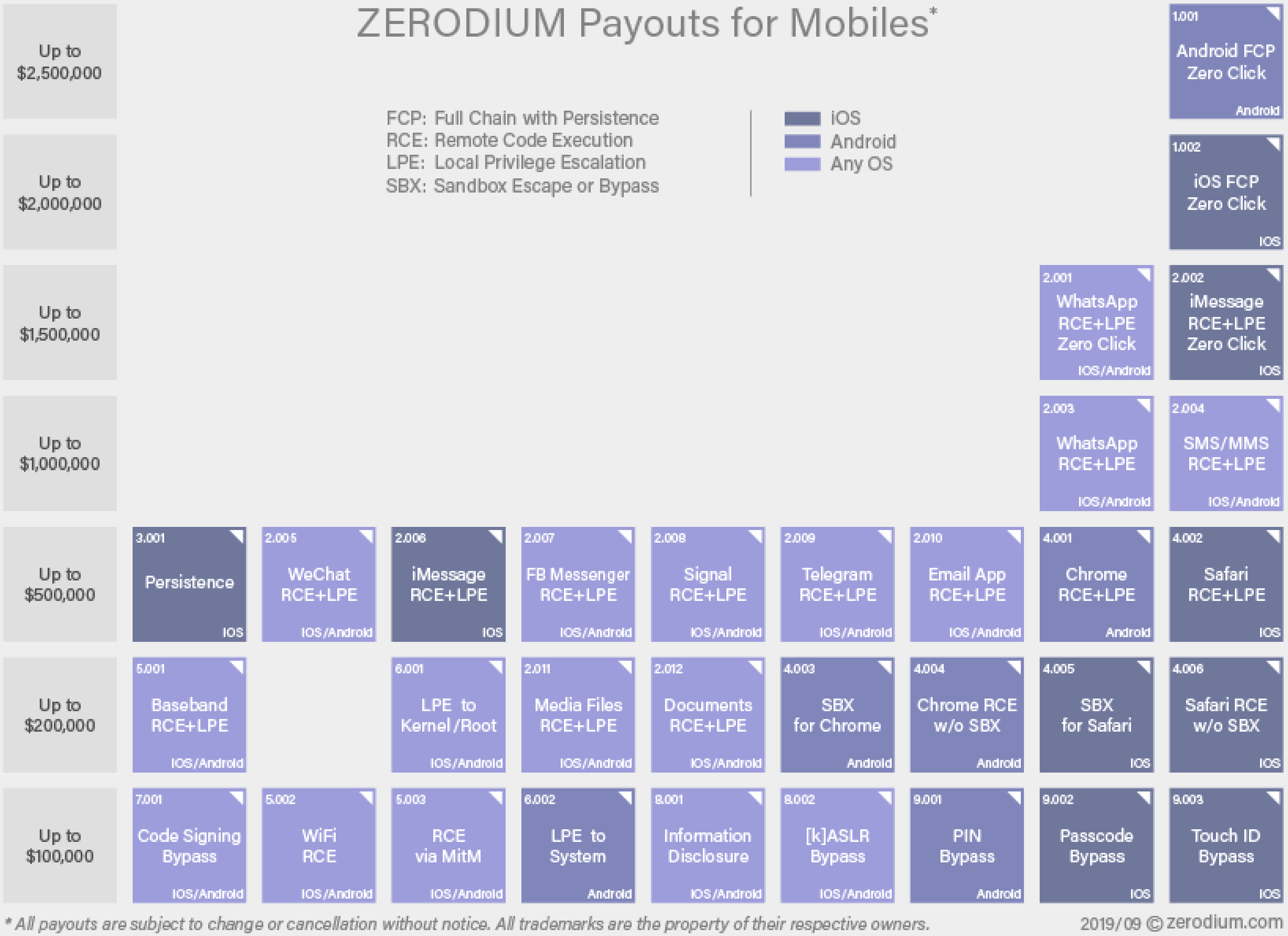
Some spyware tools require that user clicks on a link (or opens a message,...), while others can perform zero-click infection.

The problem

»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.

The problem



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

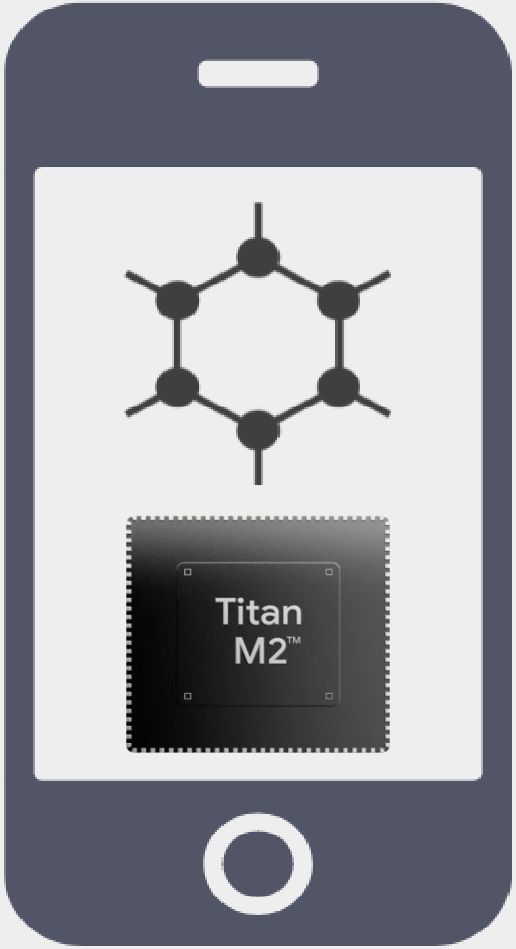
* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com

Solution

Security hardened mobile phone

- Hardware security module.
- Tested & security certified hardware.
- Hardened OS and user applications.
- Advanced sandboxing.
- Baseband isolation.
- Privacy improvement features.
- Perfect blending in with other mobile phone users.
- Zero learning required by average users (zero learning curve).



Hardware Security Module: Titan M2

- Has been developed by Google and is part of Pixel 6 and Pixel 7 series smartphones.
- Based on the RISC-V CPU architecture, contains its own memory and cryptographic accelerator and runs its own operating systems (microkernel).
- Isolation inside the processor - every cryptographic task has an isolated file system on its internal secure flash.
- Is housed in a secure package that makes it difficult to access the internal components.
- It has hardened protection against side-channel attacks like power analysis and voltage fluctuations.

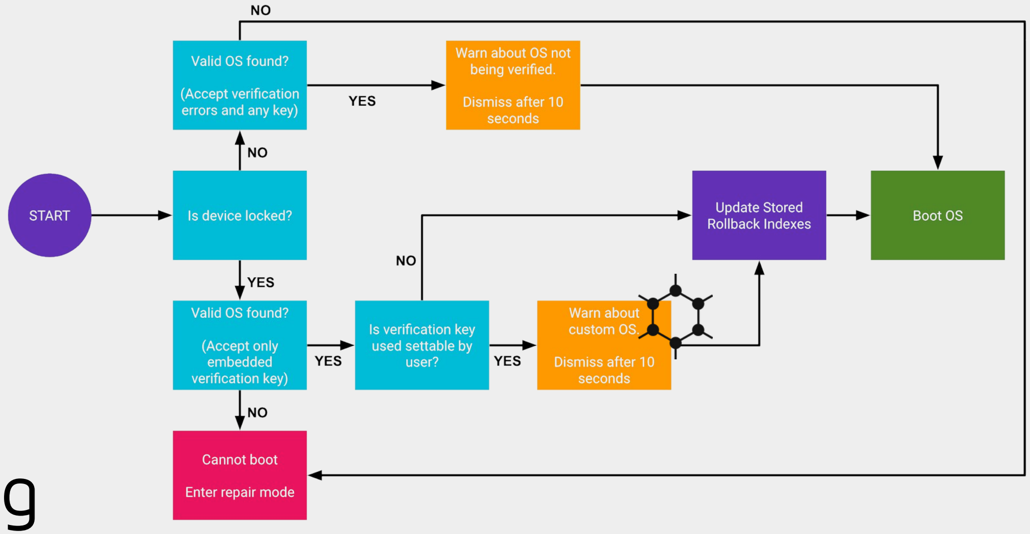
Hardware Security Module: Titan M2

- Prevents changing or updating the chip’s firmware without the device’s pattern or PIN.
- Titan M2 has passed the highest hardware vulnerability assessment (AVA_VAN.5) by an independent and accredited evaluation lab.
- It is heavily utilized by GrapheneOS for providing security.

Titan M2 offers a secure environment which is completely physically separated from the main processor. This security design is offering much more isolated and secure environment as “classic” Trusted Execution Environment solutions.

Hardware Security Module: Titan M2

Titan M2 is providing critical security services: **verified boot**, hardware-based key storage and attestation services.


NO
Valid OS found?
(Accept verification errors and any key)
YES
Warn about OS not being verified.
Dismiss after 10 seconds
NO
START
Is device locked?
Update Stored Rollback Indexes
Boot OS
NO
YES
Valid OS found?
(Accept only embedded verification key)
YES
Is verification key used settable by user?
YES
Warn about custom OS.
Dismiss after 10 seconds
NO
Cannot boot
Enter repair mode

- **Verified boot**: Titan M2 chip communicates with the bootloader in order to ensure that mobile phone will load and run the correct operating system. This is preventing an attacker to install his own, maliciously modified operating system on your device, or that an attacker would be able to roll back the operating system on your mobile phone to an older, potentially unsafe version. Also, Titan M2 chip is also preventing malicious attempts to unlock the bootloader.

Hardware Security Module: Titan M2

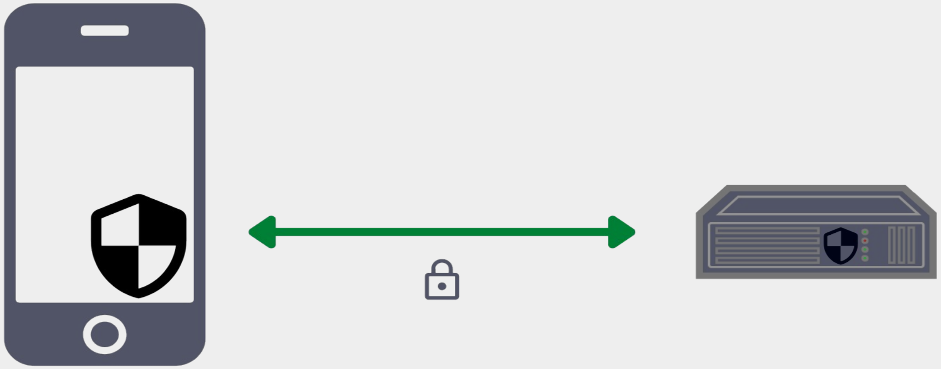
Titan M2 is providing critical security services: verified boot, **hardware-based key storage** and attestation services.

- **Secure storage of the encryption keys**: After booting, mobile phone can not be unlocked with biometrics. Titan M2 is storing the decryption keys, and will unlock the internal phone storage only if user will enter the correct PIN or password. If an attacker try to tamper the operating system and perform brute force attack, the chip will limit the number of attempts at the hardware level.
- Titan M2 chip also supports StrongBox, the technology that is offering a safe storage space for cryptographic keys used by third-party apps.

Hardware Security Module: Titan M2

Titan M2 is providing critical security services: verified boot, hardware-based key storage and **attestation services**.

- **Attestation services**: Attestation is a mechanism to prove the trustworthiness, and to verify that there has been no tampering with the operating system and that the bootloader is locked. It can detect persistent malware infection.
- Titan M2 supports hardware-based attestation, security verification and monitoring of the GrapheneOS via attestation service.
- Hardware attestation can significantly increase the chances of detecting a potentially compromised mobile device.



Operating system security

- **Verified boot**.
- **Attack surface reduction**.
- **Exploit mitigation** (hardened compiler toolchain, hardened kernel, filesystem access hardening, built-in defence against memory corruption, using hardened memory allocator,...).
- **Sandboxing and isolation** (isolating applications or other specific software components (for instance media codecs or browser renderers), so that they can access only certain resources within a system).
- **Fortifying the kernel** and other base operating system components (using latest LTS Linux kernel).

Operating system security

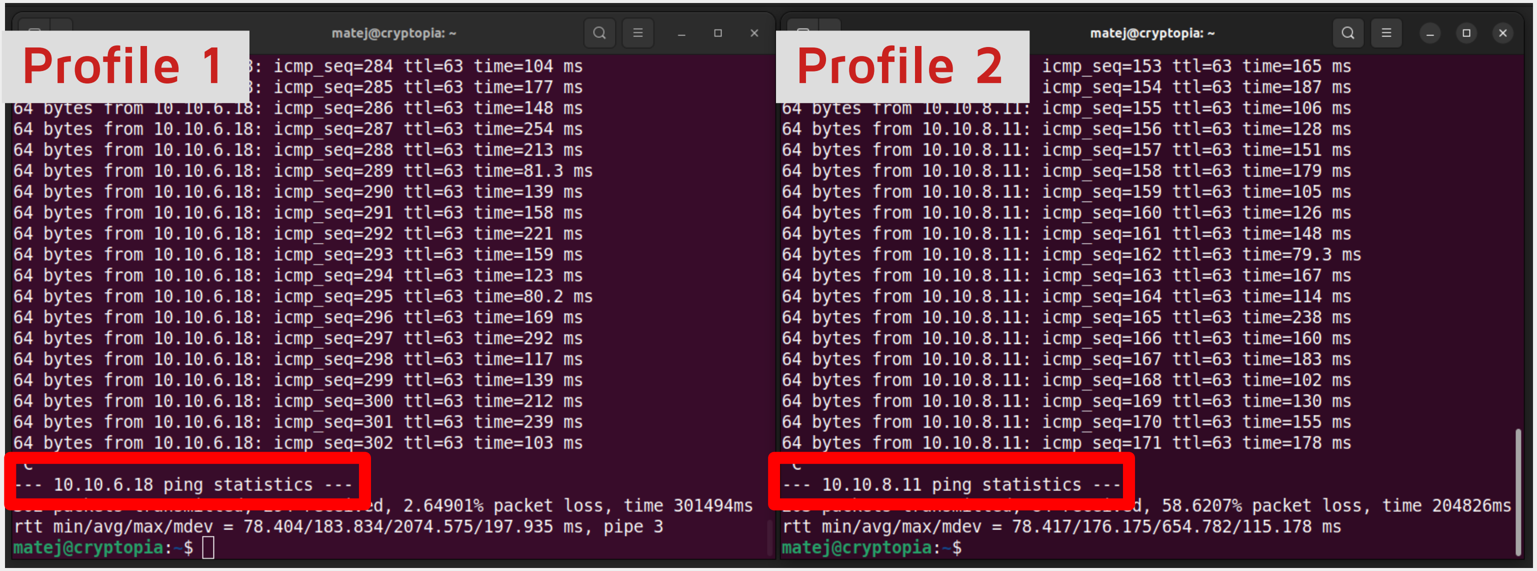
- **Hardened** default web browser (Vanadium), hardened WebView, hardened and sandboxed PDF Viewer.
- Integration of Google service in **nonivasive way** (compatibility layer providing the option to install and use the official releases of Google Play, but Google services are sandboxed).
- **Multiple isolated user profiles** (isolated workspaces with their own instances of applications, application data and profile data).
- Hardware supported **filesystem-based disk encryption** (metadata are also encrypted, each user profile is encrypted with their own unique, randomly generated disk encryption key).

Operating system security

- **Networks** are treated as inherently unsafe place and even hostile environment!
- **Isolated baseband** (WiFi, GPS, Bluetooth, NFC, etc.).
- Disabling 2G, enabling LTE-only mode, Wi-Fi only mode, per-connection MAC randomization (enabled by default).
- PIN scrambling.
- Longer passwords (by default 64 characters long passwords are supported).
- Fingerprint unlock in GrapheneOS permits only 5 attempts total, after that, unlocking is possible only by entering the correct PIN code.
- No telemetry.

Operating system security

- **Encrypted backups**.
- **Advanced and fine grained permissions** (network permission toggle, sensors permission toggle, advanced storage permissions with so called highly restricted mode).
- **“Always-on” VPN** to prevent leaking.
- Separate network settings for **different profiles**.



Profile 1

```
: icmp_seq=284 ttl=63 time=104 ms
: icmp_seq=285 ttl=63 time=177 ms
64 bytes from 10.10.6.18: icmp_seq=286 ttl=63 time=148 ms
64 bytes from 10.10.6.18: icmp_seq=287 ttl=63 time=254 ms
64 bytes from 10.10.6.18: icmp_seq=288 ttl=63 time=213 ms
64 bytes from 10.10.6.18: icmp_seq=289 ttl=63 time=81.3 ms
64 bytes from 10.10.6.18: icmp_seq=290 ttl=63 time=139 ms
64 bytes from 10.10.6.18: icmp_seq=291 ttl=63 time=158 ms
64 bytes from 10.10.6.18: icmp_seq=292 ttl=63 time=221 ms
64 bytes from 10.10.6.18: icmp_seq=293 ttl=63 time=159 ms
64 bytes from 10.10.6.18: icmp_seq=294 ttl=63 time=123 ms
64 bytes from 10.10.6.18: icmp_seq=295 ttl=63 time=80.2 ms
64 bytes from 10.10.6.18: icmp_seq=296 ttl=63 time=169 ms
64 bytes from 10.10.6.18: icmp_seq=297 ttl=63 time=292 ms
64 bytes from 10.10.6.18: icmp_seq=298 ttl=63 time=117 ms
64 bytes from 10.10.6.18: icmp_seq=299 ttl=63 time=139 ms
64 bytes from 10.10.6.18: icmp_seq=300 ttl=63 time=212 ms
64 bytes from 10.10.6.18: icmp_seq=301 ttl=63 time=239 ms
64 bytes from 10.10.6.18: icmp_seq=302 ttl=63 time=103 ms

--- 10.10.6.18 ping statistics ---
                         ed, 2.64901% packet loss, time 301494ms
rtt min/avg/max/mdev = 78.404/183.834/2074.575/197.935 ms, pipe 3
matej@cryptopia:~$
```

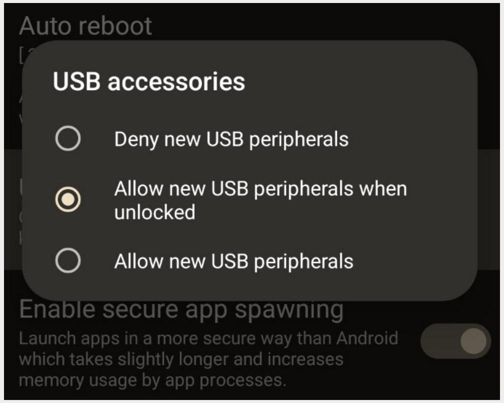
Profile 2

```
icmp_seq=153 ttl=63 time=165 ms
icmp_seq=154 ttl=63 time=187 ms
64 bytes from 10.10.8.11: icmp_seq=155 ttl=63 time=106 ms
64 bytes from 10.10.8.11: icmp_seq=156 ttl=63 time=128 ms
64 bytes from 10.10.8.11: icmp_seq=157 ttl=63 time=151 ms
64 bytes from 10.10.8.11: icmp_seq=158 ttl=63 time=179 ms
64 bytes from 10.10.8.11: icmp_seq=159 ttl=63 time=105 ms
64 bytes from 10.10.8.11: icmp_seq=160 ttl=63 time=126 ms
64 bytes from 10.10.8.11: icmp_seq=161 ttl=63 time=148 ms
64 bytes from 10.10.8.11: icmp_seq=162 ttl=63 time=79.3 ms
64 bytes from 10.10.8.11: icmp_seq=163 ttl=63 time=167 ms
64 bytes from 10.10.8.11: icmp_seq=164 ttl=63 time=114 ms
64 bytes from 10.10.8.11: icmp_seq=165 ttl=63 time=238 ms
64 bytes from 10.10.8.11: icmp_seq=166 ttl=63 time=160 ms
64 bytes from 10.10.8.11: icmp_seq=167 ttl=63 time=183 ms
64 bytes from 10.10.8.11: icmp_seq=168 ttl=63 time=102 ms
64 bytes from 10.10.8.11: icmp_seq=169 ttl=63 time=130 ms
64 bytes from 10.10.8.11: icmp_seq=170 ttl=63 time=155 ms
64 bytes from 10.10.8.11: icmp_seq=171 ttl=63 time=178 ms

--- 10.10.8.11 ping statistics ---
                         d, 58.6207% packet loss, time 204826ms
rtt min/avg/max/mdev = 78.417/176.175/654.782/115.178 ms
matej@cryptopia:~$
```

Operating system security

- Proxying to network services (NTP, PSDS, connectivity check,...).
- USB blocking by default.
- Autoreboot feature (automatic rebooting the device after N hours of not unlocking any user profile, making sure every logged in user profile ends up fully back at rest when not using the device).
- Location is default off, even for Camera.
- Option to turn the microphone and camera off.



Auto reboot

USB accessories

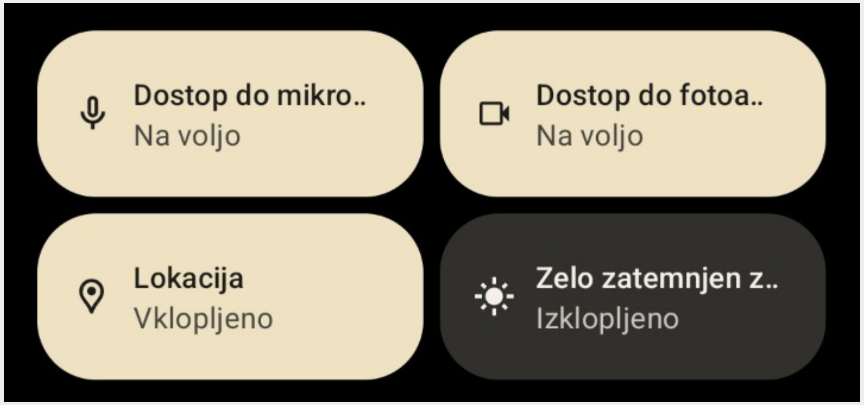
○ Deny new USB peripherals

◉ Allow new USB peripherals when unlocked

○ Allow new USB peripherals

Enable secure app spawning

Launch apps in a more secure way than Android which takes slightly longer and increases memory usage by app processes.



Dostop do mikro..
Na voljo

Dostop do fotoa..
Na voljo

Lokacija
Vklopljeno

Zelo zatemnjen z..
Izklopljeno

Operating system security

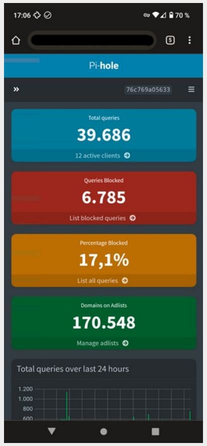
Zero learning curve and perfect blending with other users:

- Looks and feels like ordinary Android (but with some additional settings).
- Integration of Google service (but in nonivasive way, and Google services are sandboxed).
- Almost all applications are working (but Google Pay/Wallet is not).
- NFC and NFC payments are working.
- Some applications behave a little bit strange (for instance: does not auto start after reboot), but this can be solved »manually«.
- Image quality of GrapheneOS’ Camera app is very nearly on par with Google's Camera app.
- eSIM is working (but has to be enabled first).
- Very stable.

Additional security hardening

Network traffic protection

- VPN.
- Security gateway with DNS filtering, advanced intrusion detection/prevention system and network vigilance.



17:06 70 %

[redacted]

Pi-hole

76c769a05633

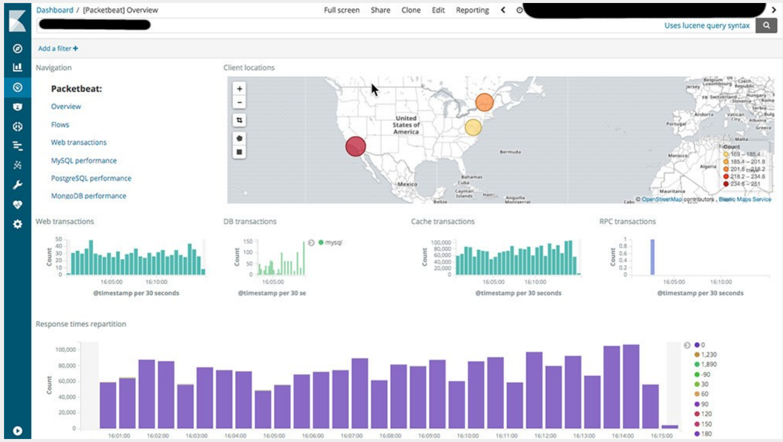
Total queries
39.686
12 active clients

Queries Blocked
6.785
List blocked queries

Percentage Blocked
17,1%
List all queries

Domains on Adlists
170.548
Manage adlists

Total queries over last 24 hours



Dashboard / [Packetbeat] Overview

Full screen Share Clone Edit Reporting

[redacted]

[redacted]

Uses lucene query syntax

Add a filter +

Navigation

Packetbeat:

Overview

Flows

Web transactions

MySQL performance

PostgreSQL performance

MongoDB performance

Client locations

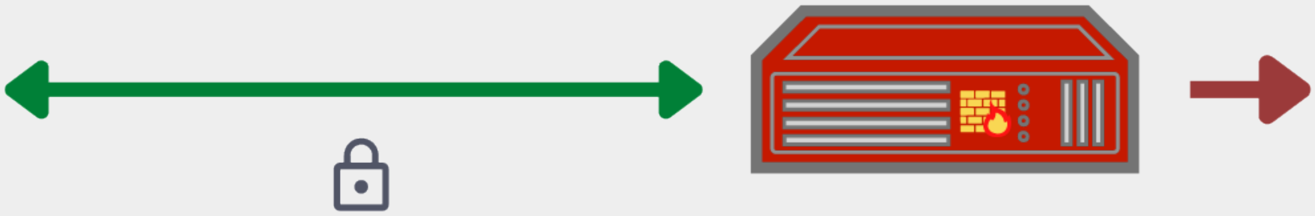
Web transactions

DB transactions

Cache transactions

RPC transactions

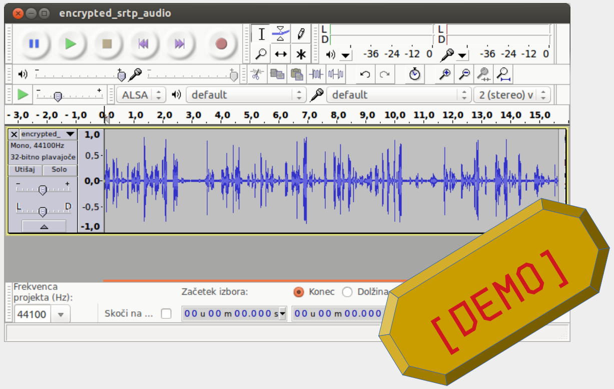
Response times repartition



Additional security hardening

E2E encrypted messenger

- End-to-end encryption!
- Audited and expert community accepted application.
- Text chat, voice, and video calls.
- Group chat and file sharing.
- Centralized (Signal) or decentralized (Matrix) network?
- Cloud or on premises?
- Integration with other services?
- Location sharing for emergency situations or coordination among members of a group?



Use cases

Different scenarios:

- ✓ Work profile and home profile.
- ✓ Two Signal installations with two different phone numbers.
- ✓ One profile with always-on VPN and the other without VPN.
- ✓ Special user profile with Tor.*
- ✓ Block network access for a specific application only.
- ✓ Microphone mute and camera off on important meetings.
- ✓ Wi-Fi device only to avoid user tracking.
- ✓ ...

Advanced security use cases

Questions about security:

- ***What about IMSI Catchers?***
  All networks should be treated as hostile environment. IMEI detection. Airplane mode.
- ***Using encrypted SMS?***
  An attacker can see traffic data. Adoption of encrypted SMS tools is very low and this would make you and your contact stand out from the crowd. Anonymisation!
- ***What if radio firmware gets compromised?***
  Baseband isolation via IOMMU. Rebooting the phone restores firmware into a known good state.

Advanced security use cases

Questions about security:

- ***What about plausible deniability/hidden profiles?*** It is possible to determine if the ciphertext contains a hidden volume encrypted to a different key. Better, however unhandy option is to create and store an encrypted backup somewhere, factory reset your device before taking it through “checkpoint”, and then download and restore your backup once you're through.

- ***What about forensic extraction of data?*** Forensic tools can extract the contents of the SSD of an unlocked phone. Cellphone unlocking systems that offer lock bypasses usually involve an exploit on the enclave itself to bypass rate limiting. Solution: Titan M2 and long passwords.

Advanced security use cases

Questions about security:

- ***What about interoperability of the applications?*** Apps installed into the same profile must both be given permission to interoperate. If this functionality is seen as being undesirable, the apps can be installed into different user profiles, which will make it impossible for them to leak information to each other, or peek into other apps' sandboxes.

Questions?

Прашања?

Matej Kovačič

https://telefoncek.si

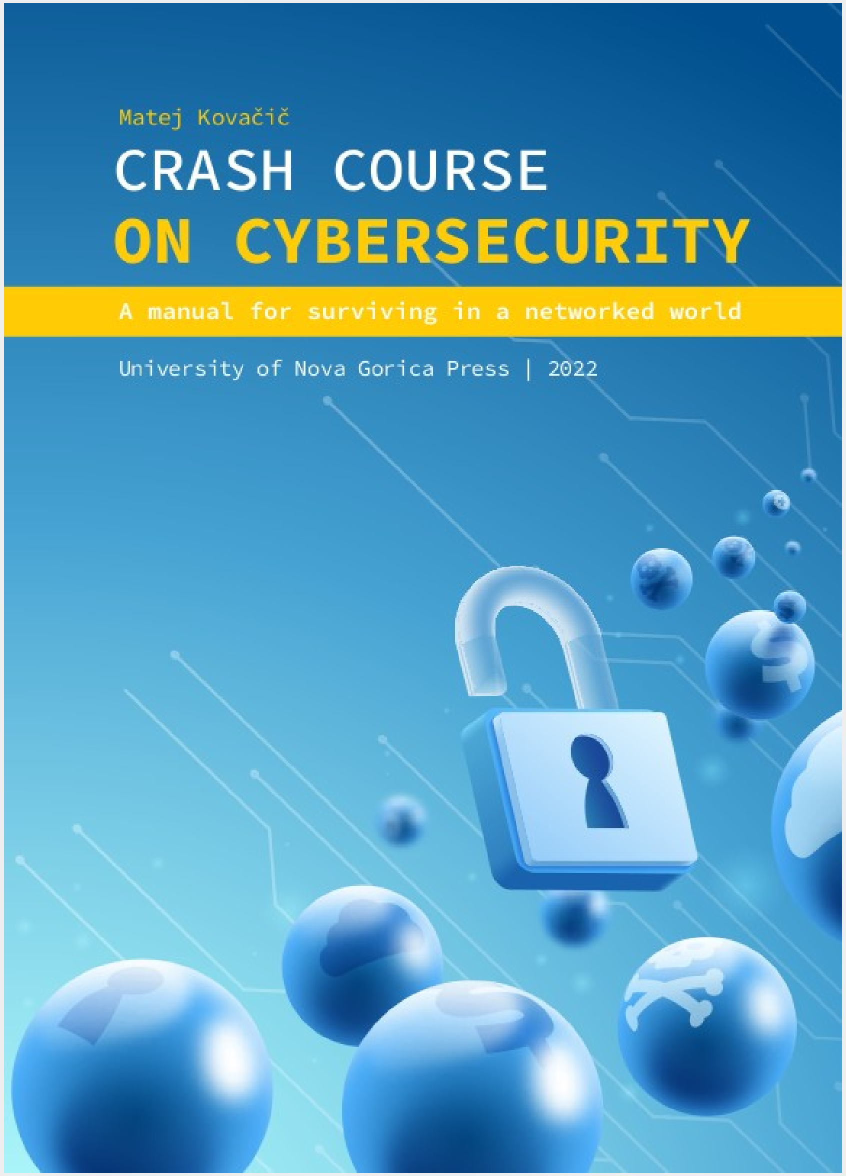
https://1985.systems

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