WELCOME TO THE

WORLD's MOST POWERFUL SECURED PHONE

About The Company

WIMI Defence GMBH -Munich provides truly secure phones, tablets and laptops — Eliminates tracking; unbreakable, end-to-end encryption; prevents hacking and blocks WIFI and GSM interception and both over-the-air and baseband attacks.

VISION

Our Vision is to be your First Choice for Most Secure Mobile,Tablet & Laptop Security and Crypto call services.

Mission

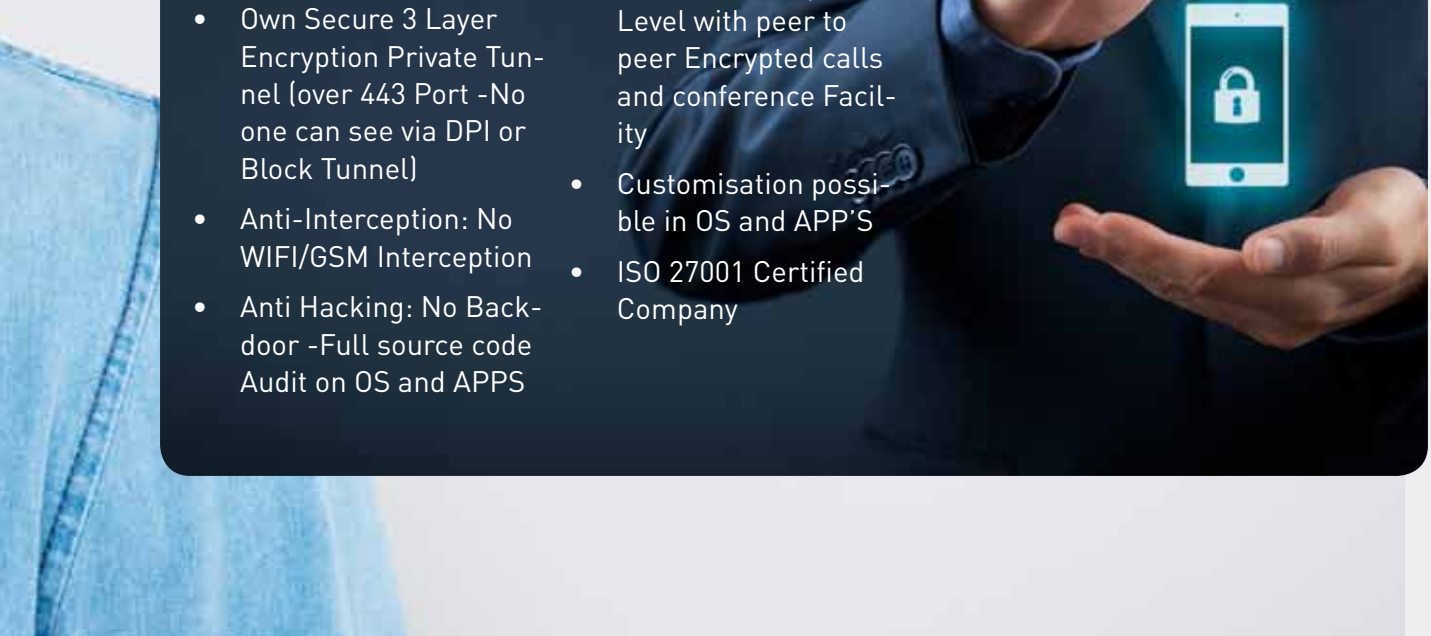
WIMI designs M100 Secure phone, the most secure phone in the world to Bring inspiration and innovation to every business and Government in the world.

Because Normal Smartphones can't Resolve Below Critical Mobile Security Problem

- GSM Geo Location -SS7 Attacks
- Fake Base Station, IMSI cather, GSM Active Interception
- Silent SMS or Remote Attacks by Binary SMS
- Femtocell Attack, SIM Cloning , Firmware over the air attack
- SIM Toolkit attack , SMS Fuzzing
- GSM Passive Interception
- Operating System Attacks
- Zero day Exploits , Trojan, Virus, Malware's
- NFC, Bluetooth, GPS Attacks
- Forensic Data Extraction -Phone
- PIN unlock -To Get Data
- Remote Access, Data Leakage
- Meta data, Encryption Weakness
- MITM, WIFI Interception, IP Injection

Our Secured Phone offer below Uniqueness and Benefits

- Own Secure Harden Operating system with Base band, TCP, APP Firewall
- Own Secure 3 Layer Encryption Private Tunnel (over 443 Port -No one can see via DPI or Block Tunnel)
- Anti-Interception: No WIFI/GSM Interception
- Anti Hacking: No Backdoor -Full source code Audit on OS and APPS
- Anti-Location: No GSM or Data Location tracking
- No Servers: Top Sec Level with peer to peer Encrypted calls and conference Facility
- Customisation possible in OS and APP'S
- ISO 27001 Certified Company



Values Statement

- Clients Establish lasting relationships and exceed expectations.
- Employees Foster a culture where our employees are valued.
- Quality Continuously strive to achieve excellence at all levels.
- Teamwork Work together, sharing knowledge, talents, and skills.
- Integrity Use good judgment and strive to do what is right.

WIMI SECURE OS Overview

WIMI OS is an Android variant modified to further increase the security of the stock Android build. It is based directly on the AOSP (Android Open Source Project), for reason of having a stable and robust base, with predictable updates, with the downside of supporting a limited number of devices.

The current version supports the Nexus 5, 5X and 9 range of devices

WIMI OS built-in security features

- Protection against zero-day exploits and malware
- The following features belong to the kernel of the OS and are aimed at protecting the user against malware targeting zero-day exploits, and make the system more` robust in order to better protect it against attacks aimed at taking control of the execution flow of the device through various programming techniques like modifying return pointers, creating runnable code at runtime, executing code from data sections or exploiting the buffer overflow scenario.

Bootloader security

- The bootloader of the device has been locked and flashing the device while in recovery mode is not allowed as developer options were removed alltogether, both from settings menu as well as from kernel with factory defaults being removed as well, the device cannot be restored to factory OS.
- Protection against cloning the OS device has been added by preventing ADB (Android Debug Bridge) access to the device.

Exec-based spawning model

Launching an application in Android is based on the "Zygote" mechanism : having a process that pre-loads all Java class modules at start-up, so that when a new application is launched the "Zygote" process executes a fork() call and proceeds on running the application code directly. This breaks Address Space Layout Randomization (ASLR) as each application will have the same layout offsets.

3 WIMI OS improves on this mechanism by adding an exec() call after fork(), so that the address space is randomized for each newly launched application, thus hardening the system against exploitation.

Encryption and authentication

Full disk encryption is enabled by default on all supported devices. Encryption password can be separate from the lockscreen password, thus allowing for a simple unlock method to be used on the lockscreen(pin or password), while having a strong pass phrase for the encryption.

To discourage brute force methods, when the encryption password if used, the lockscreen will force a reboot after 5 failed unlocking attempts.

The maximum password length has been increased from 16 characters to 32 characters. Separate passwords can be set up for encryption and decryption.

Networking

- Interfaces are assigned a random MAC address every time they are brought up. Wireless MAC addresses are randomized during scanning, in order to avoid tracking the device as it moves from one AP connection to another.
- The hostname is randomized by default ar boot time. This behavior can be disabled, in which case the persistent hostname based on ANDROID_ID will be used instead.

Improved security settings and defaults

Certain Android default settings have been modified or removed altogether for increased security/privacy:

- Location tagging is disabled by default for the camera app;
- EXIF data for taken pictures has been removed;
- Passwords are hidden by default;
- Sensitive notifications are hidden by default on the lockscreen;
- Factory reset option is removed;
- Developer options are removed from settings;
- The option to install apps from unknown sources is no longer present;
- Creation of new users is disabled;
- Tracking-prone device capabilities are disabled : GPS, NFC and Bluetooth.

Also, Google Play services and the Google apps suite have been removed from the build, as well as all the dependencies on the Google account. Default Browser app has also been removed and replaced with a more secure one.

The Unbreakable Encryption

Nobody wants to break the Encryption. Because they can't. They hack Device so WIMI solution applies 4 encryption levels that are on TopSecure-level compliant.

Each End to End Encryption Crypto Call use Random Encryption +Key each time within a dedicated VPN-Tunnel . To prove this, we offered a bounty to any hacker who cracks our security. Experts from MIT, Stanford and 240 other institutions tried. No one succeeded. The encryption of voice and data, combining the Cryptographic parameters are of exceptionally high standards. AES 256 bits, Authentication ECDSA 384 Bits, Key exchange Diffie-Hellman ECDH 384 Bits. Mark the clean implementation of random number generation through different entropy generators.

WIMI Defence GmbH

Stefan-George-Ring 29 81929 Munich Germany

Email: sales@wimidefence.com

www.wimidefence.com