OCTALAS SECURE

SECURE MOBILE COMMUNICATIONS

Solutions for Secure Communications

www.octalassecure.com

INDEX

OUR PROMISE

THE EVOLVING THREAT LANDSCAPE

Technology emerged as a means to connect people, enable borderless communication, and provide a platform for storing information accessible from anywhere. Over time, it has evolved into our great entertainer and educator, a worldwide social café. Technology is an integral part of our lives, supporting businesses, easing daily communications, and helping us collaborate.

While technology enriches our lives, it also introduces unprecedented risks and challenges that we have never before faced as a global society. Data is now the world's most valuable, yet still unregulated resource, and technology companies are both both the facilitators and exploiters of this asset.

"The data wars have begun," stated Brittany Kaiser in 2019, the former American business development director for Cambridge Analytica, and current whistleblower. This statement is evident in today's news. Today, we see technology being used to transform social movements and psychographics into tools for mass-communication warfare. News headlines are filled with reports of attacks on individuals, organizations, and even entire states—no one is safe. The most significant data breaches have compromised the information of millions of organizations, often without a clear trace of who was responsible.

SECURING THE INTEGRITY OF MOBILE COMMUNICATION

At Octalas Secure, we firmly believe in technology's limitless potential and the capabilities of tomorrow's digital world. However, with this vast digitalization arise challenges that humanity has never before encountered.

We established the company more than 15 years ago to ensure the integrity of technology and the safety of our mobile future. As frontrunners in the innovation race within the mobile communications market, we develop cybersecurity solutions that counter surveillance and data-mining techniques, guaranteeing data safety and confidentiality.

Our ultimate goal is to make mobile security accessible to everyone. We work closely with other organizations to develop custom solutions tailored to address the ever evolving challenges. We are here to protect data, the world's most valuable resource, and ensure that the mobile technologies you use serve your interests solely.

ABSTRACT

THE SECURE WAY TO TECH ENABLEMENT

The capabilities of technology are expanding rapidly. However, this progress also makes surveillance technology more accessible to a wide range of parties and introduces new data collection techniques and attack vectors.

In a digital era where data is the most valuable commodity, our solutions focus on securing the weakest link - mobile devices. We are reshaping mobile technology to shift from an "enablement-at-all-cost" model to "enablement within the limits of security." Octalas Secure is challenging both the security limitations of standard mobile devices and the enablement limitations of current mobile security solutions.

We offer multiple solutions to make mobile cybersecurity as accessible and capable to withstand adversary attacks. Octalas Secure closely monitors and researches trends in digital threats and changes in attackers' techniques. We use this analysis to provide practical, easy-to-use solutions that offer organizations comprehensive data security and communication protection against any mobile threat—physical or digital.

OUR SOLUTIONS FOR SECURE MOBILE COMMUNICATION

We offer multiple solutions to address the need for accessible mobile cybersecurity. Our offerings range from in-house designed hardware to custom Secure OS, encrypted applications for data storage and communication, device management platform, and connectivity solutions.

- **Octa device:** in-house designed hardware with built-in security features.
- **Secure OS:** custom Android-based OS with multiple defense layers.
- **Secure Chat:** end-to-end encrypted messenger.
- **Lunar Control Center:** mobile device management platform.

SECURITY-FIRST HARDWARE

Most encrypted mobile solutions prioritize digital security above all else. However, protection of your data starts from the hardware you are using.

BYOD (Bring Your Own Device) and refurbished solutions often pose a threat as they may have been compromised long before being security-hardened, thus failing to ensure zero-day integrity.

To counter these threats, we have undertaken rigorous efforts to build our own in-house designed custom hardware devices.

PROTECTION AT THE FOUNDATION

PHYSICAL SWITCH

Adversaries utilize spyware software to gain access to a device’s audio and visual inputs through the microphone and cameras, respectively. Additionally, some app store-approved applications listen to devices even when running in the background or not running at all.

Our device is equipped with a cutting-edge switch that disconnects the microphone and cameras at the hardware level. By seamlessly disabling these components, users can be assured that the microphone and cameras are only active when they need them to be.

MANAGED SENSORS

Consumer-grade smartphones introduce broader functionality but that introduces serious security risks.. For example, the device sensors (accelerometer, proximity sensor, gravity field, etc.) offer convenience for users, but also are exploitable by adversaries, giving them more contextual user information.

Users can easily spoof or disable the device’s sensors on a hardware abstraction level. This unique feature allows users to minimize their hardware attack surface through user-tailored configuration.

CONFIGURABLE SWITCH

The device has an additional switch that is configurable by the user based on their preferences. The switch allows easy access to disabling on a OS framework level device sensors such as location, Bluetooth, or all connectivity.

HARDWARE INTEGRITY CHECK

One of the common vector of attacks on hardware is through side-load installation of a compromised Operating System. Without implemented integrity checks at the hardware level, the device can boot a malicious OS and compromise the user.

Our devices utilize a hardware-based device attestation system designed to prevent the device from starting if it has been rooted or jailbroken.

FINGERPRINT UNLOCK

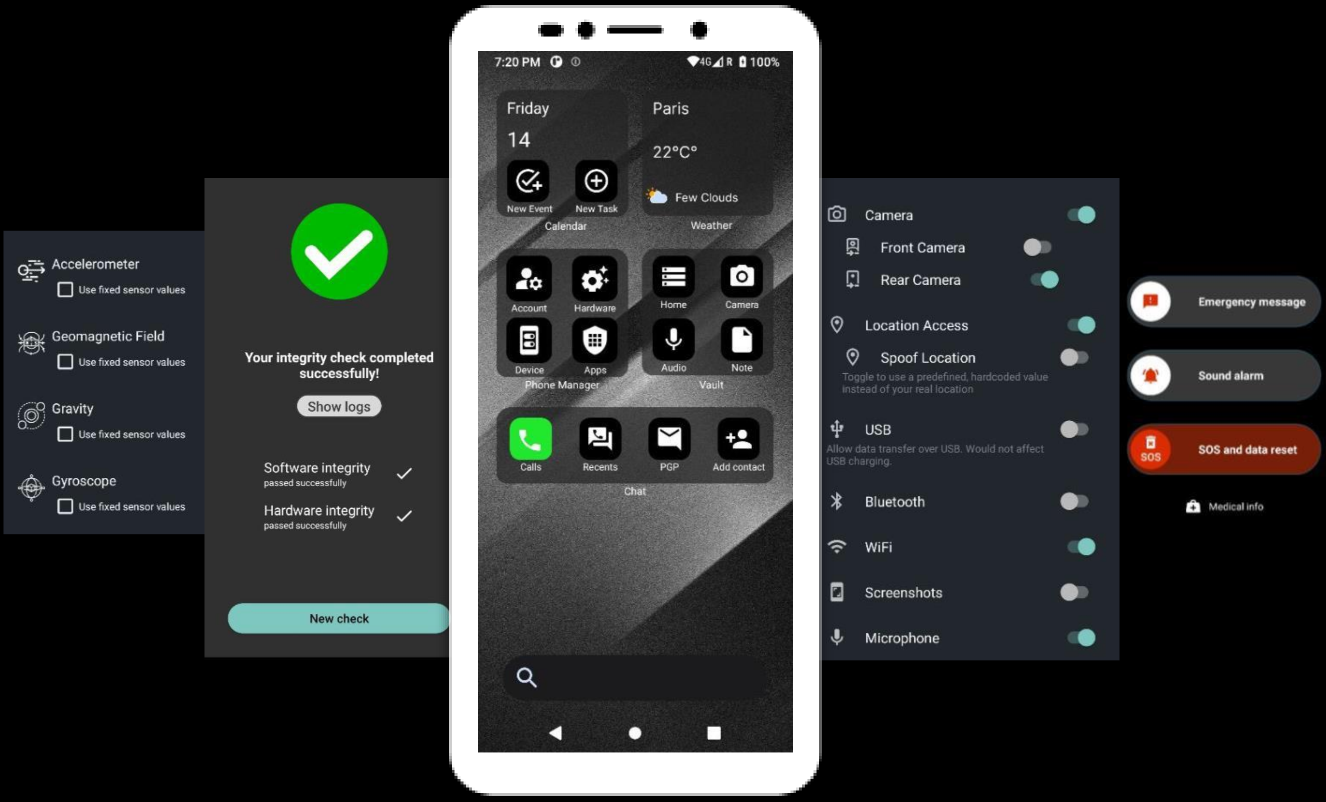
Fingerprint unlock methods have been introduced by smartphone manufacturers since some time ago. While offering convenience, users are rightfully suspicious of the digital protection of their fingerprints. This concern is heightened by the lack of user control over their digital data, including the inability to delete their smartphone account information from the cloud. As a result, many users opt for unlocking their devices via PIN, password, or pattern. Due to the frequency of this action (users unlock their phones over 100 times on average), many opt for simpler PINs, patterns, or passwords, which are easily brute forced by adversaries.

Our devices store the user's fingerprint locally and never share it on the cloud. Combined with the device WIPE feature, users are guaranteed that their fingerprint data will not be accessed by any other organization. The secure fingerprint unlock allows users to set up a very complex password and unlock the phone with a single touch on the fingerprint sensor.

SECURE OS

The threat landscape is evolving. Attacks now exploit multiple endpoints and backdoors rather than using a single attack vector. Consumer-grade operating systems prioritize user experience and extensive functionalities at the cost of thorough security. This makes such solutions easily exploitable by anyone with technical expertise, exposing your data to any third party that desires it. Even if the OS is MDM-managed, it only helps with restricting some inherent vulnerabilities, as the MDM cannot manage system applications or software at a lower OS level.

To address the complexity of modern threats, we have integrated Secure OS into our devices. Secure OS is a custom Android-based operating system that combines multiple defense layers, threat mitigation, and malicious software detection, ready to counter any threat. It offers a simplistic UI and easy-to-use functionalities, ensuring robust security without compromising user experience.



Accelerometer
□ Use fixed sensor values

Geomagnetic Field
□ Use fixed sensor values

Gravity
□ Use fixed sensor values

Gyroscope
□ Use fixed sensor values

Your integrity check completed successfully!

Software integrity ✓
passed successfully

Hardware integrity ✓
passed successfully

Camera
Front Camera
Rear Camera
Location Access
Spoof Location
Toggle to use a predefined, hardcoded value instead of your real location
USB
Allow data transfer over USB. Would not affect USB charging.
Bluetooth
WiFi
Screenshots
Microphone

360-DEGREE PROTECTION

MANAGED ATTACK SURFACE

As a general rule, you cannot be certain of the integrity of third-party applications, regardless of the provider's reputation. App behavior within the mobile ecosystem and the potential for some of its libraries to maliciously abuse standard flows cannot be accurately predicted. Services such as Google Mobile Services (a collection of Google's apps and APIs baked in every consumer-grade android device) utilize embedded location-tracking functionality, which can be exploited.

Users can take charge of their device through our hardware control feature enabling users to manage hardware components and sensors (Wi-Fi, Bluetooth, Location, and more) reducing the attack surface by switching them on and off depending on their needs..

PHYSICAL EXTRACTION SAFE

There are numerous ways to extract data from a mobile device, especially if it is obtained physically. Physical access to a device poses a significant threat as adversaries can files through the USB port using specialized equipment. This method allows attackers to bypass many security measures, gaining access to sensitive information. Especially vulnerable are devices that are protected with simplistic PINs, patterns or passwords (e.g. a 16 digit PIN is cracked in 1 hour)

The device's USB port is modified to allow users to fully control it, including fully disabling all USB port functions (except for charging). The USB port is disabled on a hardware abstraction level, ensuring that it can not be utilized even by the most sophisticated extraction tools.

MULTIPLE DATA WIPE OPTIONS

Even if users are well protected against over-the-air attacks, they can lose control of their data if an adversary forces them to unlock their phone or if they lose possession of the device. To counter these risks, our solutions offer users and administrators multiple methods to wipe all stored data:

- **Anti-Tamper Wipe**: In the event of physical tampering through a way of brute forcing the security lock, the device will enter an automatic wipe flow that will delete all of the user's data and render the account inaccessible.

- **Emergency Center**: Sometimes, critical circumstances require immediate action. The Emergency Center provides users with a one-swipe option to utilize critical functionalities, such as an instantaneous wipe, removing all sensitive data with a single click.

- **Remote Wipe**: In some cases, you need to react quickly even if the device is not physically with you. For such situations, our devices support remote wipe through the MDM ensuring that all data on the device will not end up in the wrong hands.

- **Sync Wipe**: If adversaries get a hold of your phone there is a high chance that they will disable the phone's connectivity in order to extract data without the risk of getting a remote wipe command. To address this risk, we developed a sync wipe flow that triggers when the device fails to sync with the backend for a pre-set amount of time.

ENCRYPTED BOOTLOADER

The bootloader of a device is its most basic, low-level software. Its purpose is to check and verify the software running on your device before it boots to ensure its integrity.

If the bootloader is unlocked, various custom ROMs and software not approved the organization could easily be pushed to the phone. Additionally, as mobile devices are PIN or password-protected, unlocking the bootloader opens dangerous attack vectors that can be exploited to bypass the password-authentication process if an attacker gains physical access.

Our OS features not only a locked but an encrypted bootloader, preventing any non-authorized third-party software from being installed on the device. This protects against attacks attempting to install a malicious OS that would gain control over the device, as the encrypted bootloader will refuse to load it.

SPYWARE PREVENTION

A common way of adversaries to infiltrate devices is by installing spyware software without the consent or knowledge of the user. Adversaries are able to install malicious software through exploiting native vulnerabilities of smartphones. This software allows them to execute collection attacks to identify and gather information such as sensitive files, user keystrokes, screen activity, browsing history, and more.

For example the Pegasus spyware was installed on consumer smartphones through exploitation of third party or system app vulnerabilities. The spyware allowed the adversary to access devices through zero-click exploitation, where user didn't even have to click a phishing link.

Secure OS allows users and organizations to forbid the installation of any software outside the app store managed by the MDM, ensuring that no untrusted apps are installed.

ANTI DATA MINING

Data mining on Android devices, particularly within Google's ecosystem, involves extensive collection of user data points, including location, search history, app usage, and more. This pervasive data collection raises privacy concerns and exposes users to potential vulnerabilities, especially due to pre-installed bloatware that can introduce security risks.

Secure OS is a completely de-Googled Android Operating System. It relies on in-house developed or open-source technology to deliver necessary mobile microservices such as location, push notifications, time, app updates, and others. Users can easily disabled those services, unlike consumer smartphones.

SOFTWARE INTEGRITY CHECKS

While having the necessary spyware mitigation mechanisms in place is vital for protecting digital data, having a way to detect if those mechanisms fail is equally important.

Secure OS comes with a software integrity feature that compares the local device policies and installed software (apps and OS) to the policies saved on the server. Any discrepancies are reported, and the user is alerted. With this feature, users and organizations can easily identify if their device has been compromised.

TRIPLE PASSWORD PROTECTION

To prevent physical tampering with our encrypted mobile communication devices, we have implemented triple password protection: The storage holding all sensitive information, the OS allowing the phone's basic functions, and the system communication apps storing your correspondence are separately protected by different passphrases. The passwords securing sensitive data, such as the information in your storage, are highly complex, ensuring that even supercomputers cannot penetrate them.

SECURITY-HARDENED LIBRARIES

Libraries are sets of prewritten code that applications use to perform their functionalities. As part of the standard application security testing application stores tests all applications submitted to them and provide developers with instructions on fixing vulnerabilities. However, this model does not consider that in the mobile ecosystem, applications are not isolated from one another. Their libraries and logic coexist with those of other apps. App store's implied security model overlooks the possibility of different behaviors of various libraries within the same mobile stack, leading to three major threats:

- **Malicious Modifications**: Applications' libraries can be modified to be malicious through repacking, which reverse-engineers and rebuilds the library to introduce harmful behavior.

- **Masquerading Libraries**: Adversaries can create libraries that masquerade as existing ones, overtaking their functionalities. For example, they use the same namespace as the legitimate library, as seen with the notorious DavidKungFu malware that uses names like com.google.ssearch and com.google.update to pretend to be legitimate.

- **Aggressive Behavior**: Even legitimate third-party libraries can have aggressive behavior, such as collecting the device owner's email address. The major problem is that most library-centric security threats cannot be adequately addressed by malware-detection software, anti-viruses, and anti-repackaging techniques.

To ensure the security of our device, we have tested all libraries used by our system applications, both in isolation and within the mobile ecosystem. We have also taken rigorous measures to harden library security and introduce a further defense layer through additional device encryption.

NO LOCATION TRACKING

A known technique for tracking device location is through utilization of Silent SMS or Silent call attacks. Those techniques are very effective since al smartphone devices have enabled those services, with the capability to execute SMS and calls without notifying the user.

Even if users have disabled their location through their settings or policy, they are still vulnerable to the attack, since the disabling of location services only prevents the API calls to fetch location from executing,. Instead the Silent SMS and Silent Call attacks help adversaries triangulate the device location by seeing which towers they are pinging on incoming SMS/Call.

Secure OS allows users to disable phone and SMS services on a OS framework level. By disabling those services, they have a guarantee that no SMS or calls will go through, even if initiated by the most sophisticated software.

ENCRYPTED BACKUP

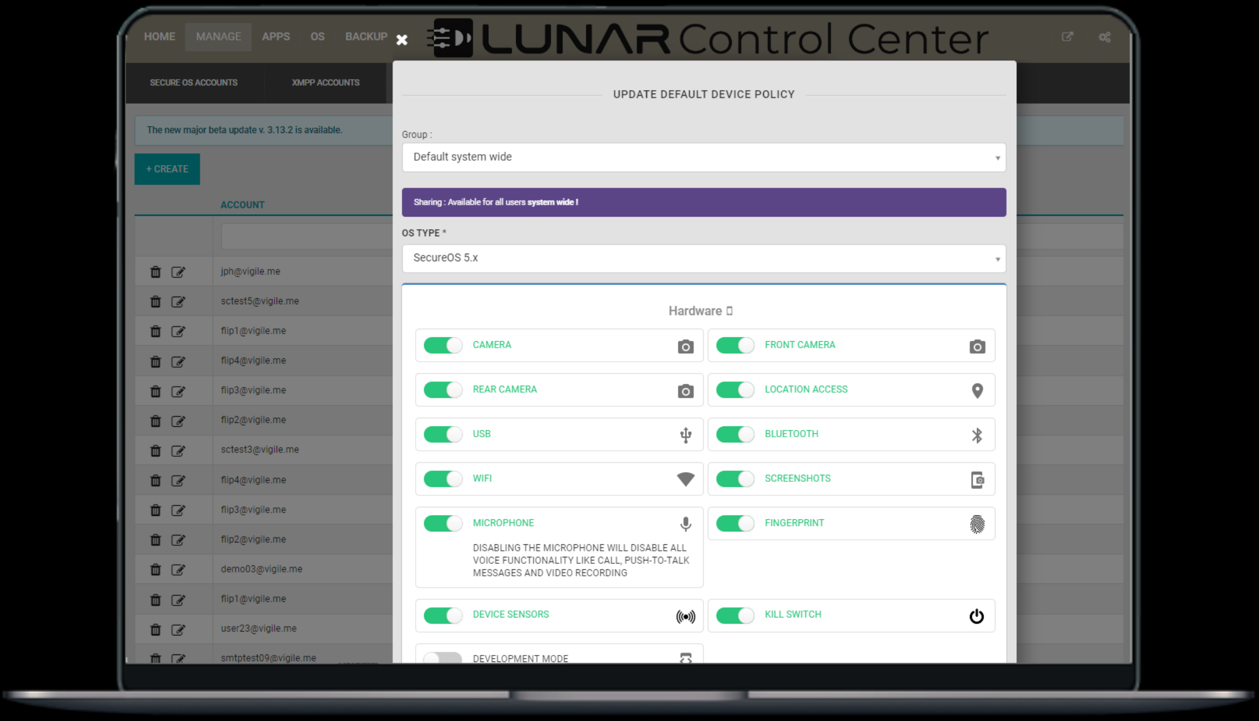
People face challenges when managing their on-device data due to the lack of control over data when it's backed up to the cloud. Current solutions either cannot perform a full device backup (third-party cloud apps) or back up everything without giving users full control or transparency over the process (system backup software of consumer-grade smartphones). Many people are opting out of their data backups due to the risks or complexity of it, risking to lose their most valuable digital assets in case of phone malfunction or theft.

Secure OS supports full device backup and restore functionality through its backup manager feature. The device backup is stored on the self-hosted MDM server, fully encrypted with user-generated keys, ensuring that it cannot be decrypted in transit or at rest. Users can easily delete the backup to guarantee confidentiality.

DEVICE MANAGEMENT

Secure OS is integrated with Lunar Control Center – a Mobile Device Management platform that offers the ability to granularly control the devices administrator level. The granular control helps organizations protect their sensitive information by managing security policies, access to applications, as well as a variety of management actions.

Organizations can host our MDM software on their server, enabling complete control over the security infrastructure and data sovereignty.



The new major beta update v. 3.13.2 is available.

jph@vigile.me
sctest5@vigile.me
flip1@vigile.me
flip4@vigile.me
flip3@vigile.me
flip2@vigile.me
sctest3@vigile.me
flip4@vigile.me
flip3@vigile.me
flip2@vigile.me
demo03@vigile.me
flip1@vigile.me
user23@vigile.me
smtptest09@vigile.me

UPDATE DEFAULT DEVICE POLICY

Group : Default system wide

Sharing : Available for all users **system wide !**

OS TYPE * SecureOS 5.x

Hardware

● CAMERA	● FRONT CAMERA
● REAR CAMERA	● LOCATION ACCESS
● USB	● BLUETOOTH
● WIFI	● SCREENSHOTS
● MICROPHONE DISABLING THE MICROPHONE WILL DISABLE ALL VOICE FUNCTIONALITY LIKE CALL, PUSH-TO-TALK MESSAGES AND VIDEO RECORDING	● FINGERPRINT
● DEVICE SENSORS	● KILL SWITCH
○ DEVELOPMENT MODE	

SECURE DEVICE MANAGEMENT

ROBUST CONTROL

No cybersecurity solution can fully serve an organization’s purposes or be personalized to users' needs without the ability to control devices granularly. To enable remote management of device functionalities and settings, we’ve integrated Secure OS with the security-first Lunar Control Center.

Administrators can push policies to users' devices that control:

- User settings such as minimum password length and password expiration time.
- Device sensors, disabling vulnerable ones such as the camera, microphone, USB, or Bluetooth.
- Functionalities accessible to the user, such as the ability to perform calls or send and receive SMS.
- Built-in Secure Firewall rules, including blacklisted IPs and ports.
- OS builds and app versions on users' devices.

APPLICATION CATALOGUE

Devices often get compromised due to running unauthorized, malicious applications. This is caused by a combination of users' lack of cybersecurity awareness and inadequate security vetting measures by app stores.

Lunar Control Center allows administrators to manage user access to applications by creating a corporate app store. Depending on the policies, applications can be enforced on users or made available for download via the mobile app store. With the application catalog capability, organizations can ensure that users only access the applications they need, reducing the risk of compromise.

TRULY SELF-HOSTED

MDMs on the market are typically offered as fully cloud-based solutions, or at best, allow organizations to self-host part of the stack while using third-party APIs (such as Android Enterprise) to manage devices. This approach raises confidentiality concerns for organizations since sensitive device management actions pass through third-party infrastructure, lacking clarity on how that data is managed and protected.

To address these concerns, our MDM platform is fully self-hosted by organizations. It does not use any third-party APIs not hosted by the organization to manage or collect logs remotely. This ensures that all sensitive device management actions remain within the organization's infrastructure, providing greater control and security over the data.

EASY TO OPERATE AND SUPPORT

Installing and supporting a self-hosted solution usually comes with the burden of having to train system administrators extensively on the specific platform.

Lunar Control Center supports features for easy installation and maintenance of the solution, integrated with a variety of software for infrastructure monitoring.

The self-hosted system is installed, configured, and updated through a CLI, allowing admins to perform changes in minutes following simple guides.

Administrators can interact with a user-friendly Console that allows them to:

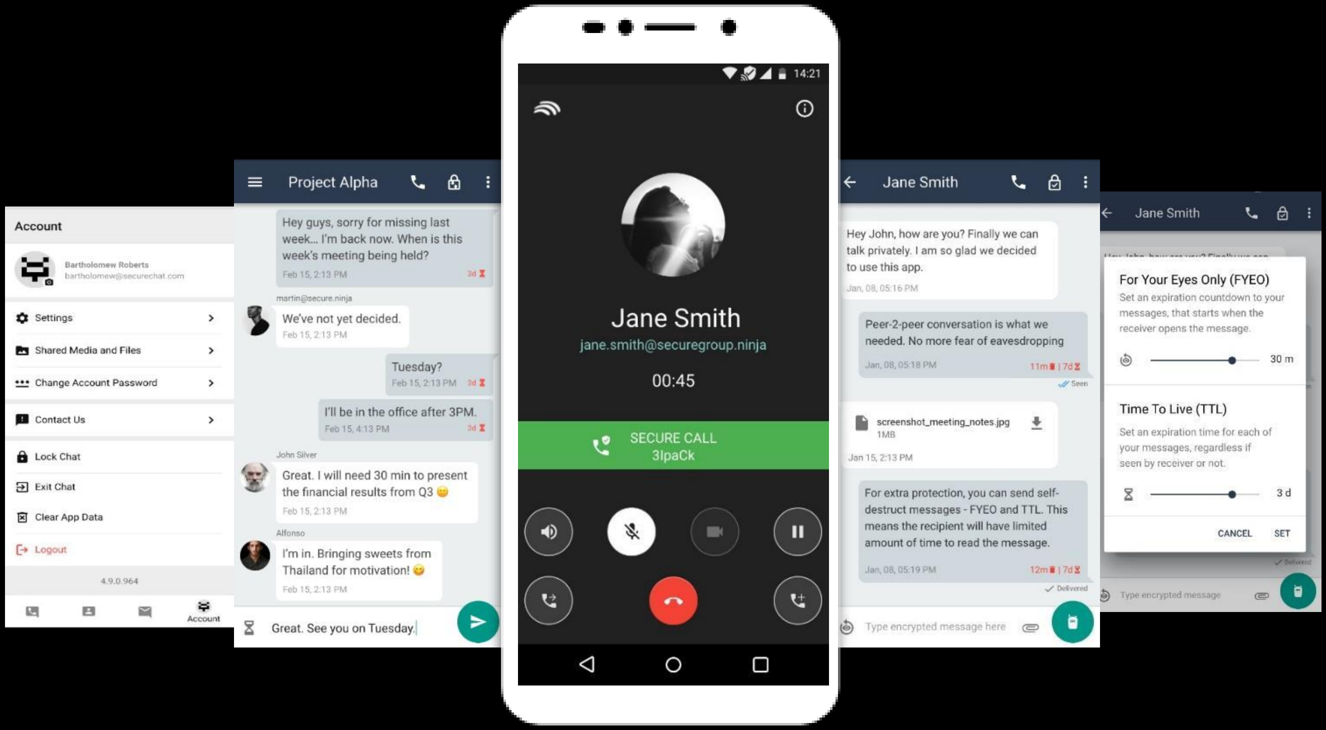
- Manage policies
- Perform user actions
- Access device logs
- Update software
- Manage the corporate app catalogue

SECURE COMMUNICATIONS SUITE

Mobile communication applications transfer data from one peer to another through the provider's server. If not encrypted, this information can be intercepted and read by third parties that gain access to the network, your network service provider, and your application developer. Additionally, almost all mobile apps have built-in analytics that track users' every move and collect it in an integrated data system.

Even encrypted mobile applications are not as safe as their developers claim. They are only as secure as the mobile stack. If malicious software finds its way onto your device, it can mine data and access the application’s database, compromising all sensitive information.

To guarantee the privacy of communication and the safety of user data, we have integrated a Secure Communication Suite, which encrypts traffic end-to-end and stores data at rest in encrypted databases. The applications applications employ database encryption, ensuring that malicious software cannot access the application’s stored information without brute-forcing a complex password. The architecture of the Secure Communication Suite guarantees the thorough security of each possible attack vector.



Account

Bartholomew Roberts
bartholomew@securechat.com

Project Alpha

Hey guys, sorry for missing last week... I'm back now. When is this week's meeting being held?
Feb 15, 2:13 PM 3d

martin@secure.ninja
We’ve not yet decided.
Feb 15, 2:13 PM

Tuesday?
Feb 15, 2:13 PM 3d

I'll be in the office after 3PM.
Feb 15, 4:13 PM 3d

John Silver
Great. I will need 30 min to present the financial results from Q3 😊
Feb 15, 2:13 PM

Alfonso
I'm in. Bringing sweets from Thailand for motivation! 😊
Feb 15, 2:13 PM

Great. See you on Tuesday.

Jane Smith
jane.smith@securegroup.ninja
00:45

SECURE CALL
3lpaCk

Jane Smith

Hey John, how are you? Finally we can talk privately. I am so glad we decided to use this app.
Jan, 08, 05:16 PM

Peer-2-peer conversation is what we needed. No more fear of eavesdropping
Jan, 08, 05:18 PM 11m | 7d
Seen

screenshot_meeting_notes.jpg
1MB
Jan 15, 2:13 PM

For extra protection, you can send self-destruct messages - FYEO and TTL. This means the recipient will have limited amount of time to read the message.
Jan, 08, 05:19 PM 12m | 7d
Delivered

Jane Smith

For Your Eyes Only (FYEO)
Set an expiration countdown to your messages, that starts when the receiver opens the message.
30 m

Time To Live (TTL)
Set an expiration time for each of your messages, regardless if seen by receiver or not.
3 d

360-DEGREE PROTECTION

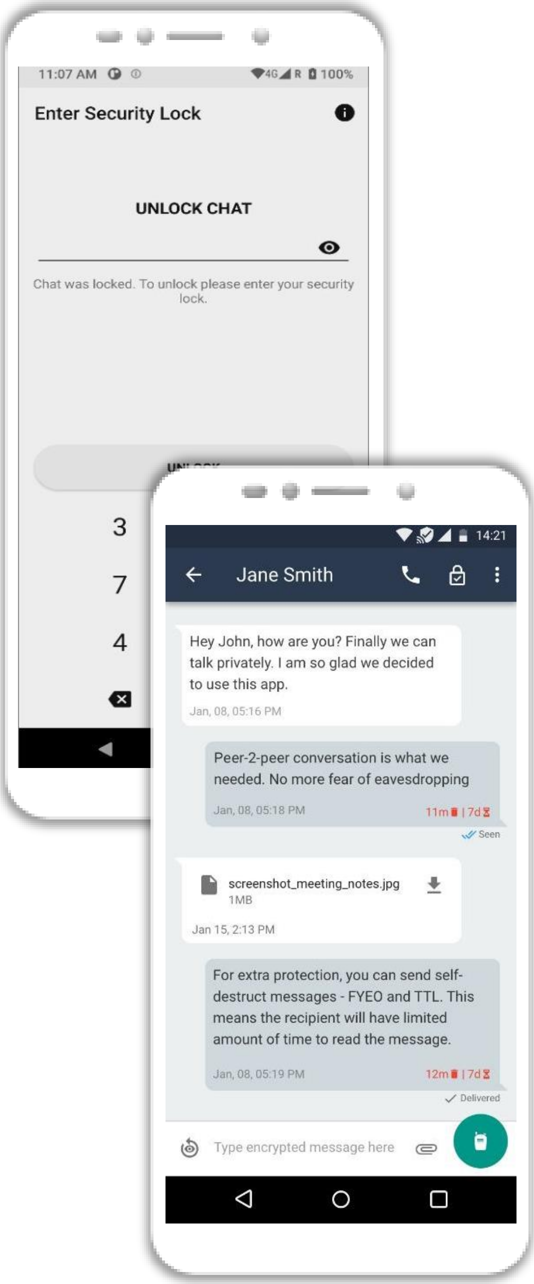
Secure Chat is an end-to-end encrypted messenger app. It allows users to send peer-to-peer messages, join group chats, and make unlimited voice and video calls. The application's architecture ensures that no sensitive data passes through our servers, which act only as facilitators of the communication..

ZERO SERVER TRACE

Most messengers that are advertised to encrypt data communication actually use a centralized encryption that stores communication on the server and uses a key to decrypt it. This opens up several risks for the data of the end-user:

- Adversaries can obtain access to the server storing the data and the encryption keys and decrypt the communications.
- The organization hosting the communication server can see the communication between their users and decrypt it.

To counter all possible vulnerabilities, Secure Chat uses a communication architecture that stores sensitive information only on your device and the one you're communicating with, within an encrypted database, not reachable by third parties. This technique ensures that data transfer leaves no traces across the network or on any servers.



Chat was locked. To unlock please enter your security lock.

Hey John, how are you? Finally we can talk privately. I am so glad we decided to use this app.
Jan, 08, 05:16 PM

Peer-2-peer conversation is what we needed. No more fear of eavesdropping
Jan, 08, 05:18 PM 11m | 7d
Seen

screenshot_meeting_notes.jpg
1MB
Jan 15, 2:13 PM

For extra protection, you can send self-destruct messages - FYEO and TTL. This means the recipient will have limited amount of time to read the message.
Jan, 08, 05:19 PM 12m | 7d
Delivered

ENCRYPTED DATA AT REST

Data stored on a device is usually more vulnerable than data in transit. Messaging app developers often overlook the risks and do not encrypt data when stored, relying only on the security of the OS the app is installed on. This means that if an adversary gains access to an unlocked device, they can see all of the user's saved communications.

Secure Chat encrypts its data at rest using full database encryption via the 256-bit SQLCipher encryption. This guarantees that adversaries will not be able to access the stored app data of the user, even if they manage to get hold of an unlocked device.

PEER-TO-PEER MESSAGING

Secure Chat uses OMEMO encryption for peer-to-peer chats. The server is only involved to validate that both correspondents are online.

When the sender sends a message, the server checks whether the recipient is online. If they are not, the message is not submitted and remains on the sender's phone until both peers are online. All communication-related information is encrypted with a 256-bit AES cipher and stored only on the user devices within a password-protected encrypted database, unbreachable even for supercomputers.

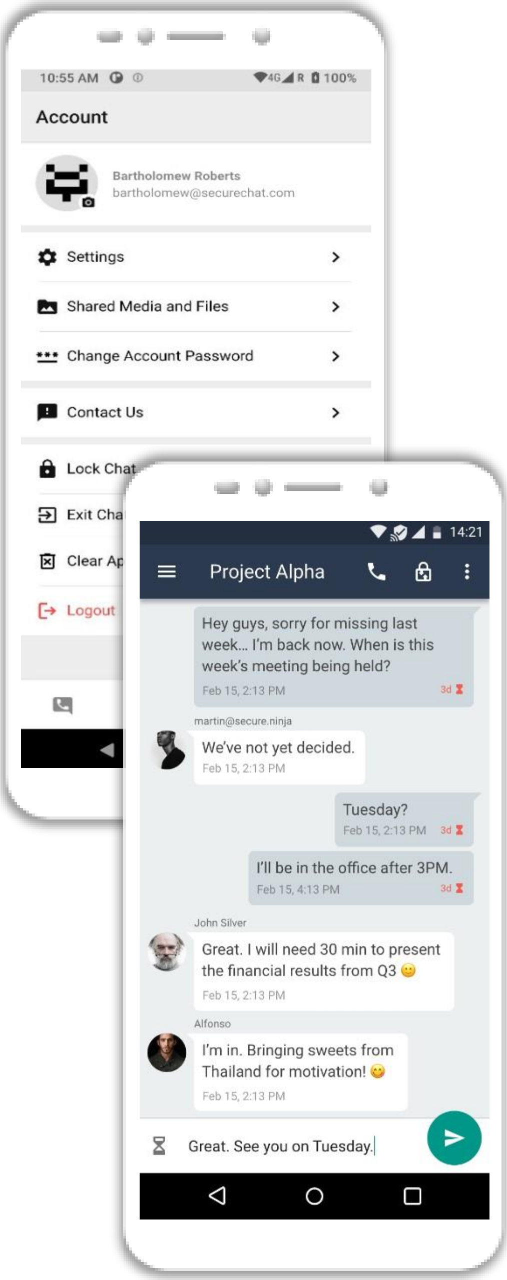
GROUP MESSAGING

Enabling full confidentiality in a group messaging is a harder task on engineering level. Secure Chat OMEMO to encrypt data sent within a group chat with a 256-bit AES cipher. This encrypted data is then pushed to the organization's server, where it remains in encrypted format. This data can only be accessed through the peer's private key, stored solely on their device.

The information is delivered to each participant when they are online directly through the server. After the sensitive data has been delivered to all participants, it is deleted from the server, leaving no trace and making it completely inaccessible to third parties. As an additional security measure, the data is stored on the server for maximum 7 days. If a peer does not come online during this period, they will not be able to receive the messages, as they will be deleted from the server.

DEVICE BOUND ACCOUNT

A common way to compromise someone's communications is to impersonate them by logging in their account on another device. To protect users from such threats, their Secure Chat accounts are bound to the device they are using and cannot be accessed from any other mobile phone.



Hey guys, sorry for missing last week... I'm back now. When is this week's meeting being held?
Feb 15, 2:13 PM 3d

martin@secure.ninja
We've not yet decided.
Feb 15, 2:13 PM

Tuesday?
Feb 15, 2:13 PM 3d

I'll be in the office after 3PM.
Feb 15, 4:13 PM 3d

John Silver
Great. I will need 30 min to present the financial results from Q3 😊
Feb 15, 2:13 PM

Alfonso
I'm in. Bringing sweets from Thailand for motivation! 😋
Feb 15, 2:13 PM

Great. See you on Tuesday.

CONFIDENTIAL CALLS

Standard PSTN telephony is only as secure as your mobile provider allows. Unauthorized access to the provider's infrastructure can lead to intercepted and eavesdropped calls.

VoIP (voice-over-internet protocol) surpasses PSTN in portability and accessibility but can be exploited through MiTM (man-in-the-middle) and DoS (denial-of-service) attacks if not secured.

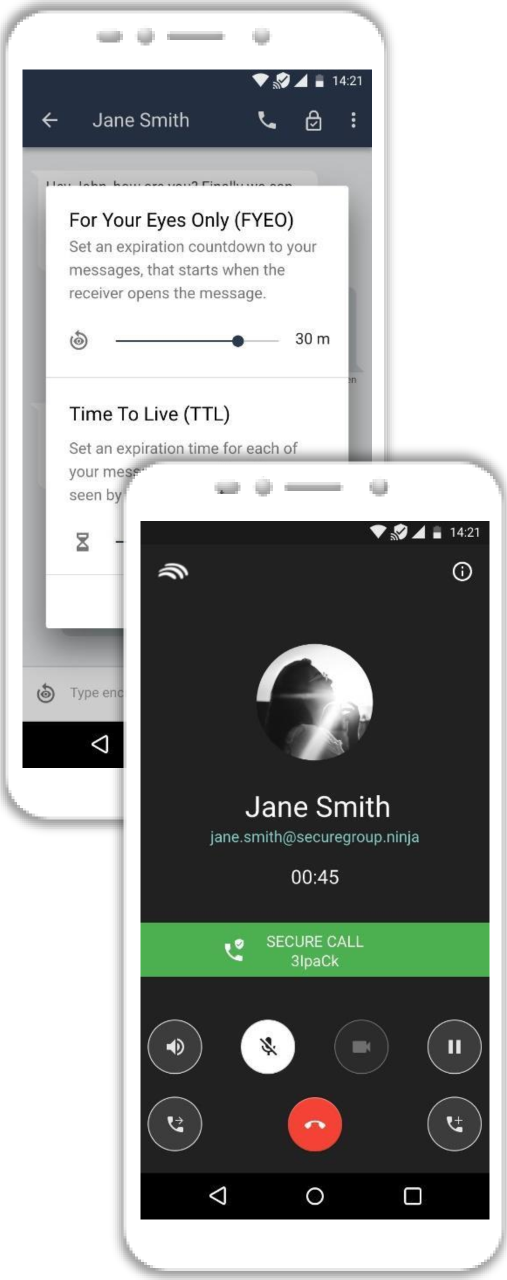
Secure Chat delivers end-to-end encrypted Voice Calls through ZRTP protocol. The phones of the communicating peers act both as receiver and transmitter of information, automatically recognizing that the other side is ZRTP-compliant, and using our servers only to establish the connection. All traffic is encrypted, making it impossible to intercept, even by the network provider, without knowing the shared secret.

SELF-DESTRUCTING MESSAGES

To ensure users' confidentiality, Secure Chat provides an option to send self-destructing messages, with 2 available patterns:

- Time-to-Live (TTL): The sent messages will be viewable only for a preset time, after which they will be deleted, regardless of whether the recipient has seen them or not.
- For-Your-Eyes-Only (FYEO): The countdown starts after the message is seen by the recipient and will be deleted after the preset time runs out, ensuring the peer you're communicating with has seen your message.

These conversations cannot be forwarded, saved, or screenshotted, ensuring they never leave the chat you shared them in.



For Your Eyes Only (FYEO)

Set an expiration countdown to your messages, that starts when the receiver opens the message.

30 m

Time To Live (TTL)

Set an expiration time for each of your mes
seen by

Jane Smith

jane.smith@securegroup.ninja

00:45

SECURE CALL
3lpaCk

PUSH-TO-TALK

For user convenience, the app offers the ability to send encrypted voice messages within the P2P and group chat.

FILE SHARING

Secure Chat supports rich file formats and allows you to send them in an encrypted form.

CHOOSE TO SECURE YOUR DATA

In the digital world, data is the most valuable resource for scaling businesses or achieving your goals as an organization. Consequently, this sensitive information is a prime target for attacks aiming to steal and leverage it. With rapid innovation, access to data collection technologies is becoming much easier, and mobile devices, due to their architecture, are often the weakest link.

To ensure users' data is thoroughly secured and communications are completely confidential, Secure Group offers and end-to-end mobile security solutions with multiple defense layers countering any threat.

As the value of data evolves, the digital threat of stealing this data rises rapidly. The only countermeasure is to make cybersecurity accessible to more people and businesses. This is why we’ve taken rigorous measures to ensure our solutions can be customized to perfectly fit the business needs of each organization. With the state-of-the-art mobile security offered by Secure Group, data protection and conversation confidentiality are now a choice.

Protect your business data today, because tomorrow might already be too late!

USEFUL RESOURCES

COMPANY INFORMATION

- Company website: www.octalassecure.com
- About the company: www.octalas.com/about/company

PRODUCT INFORMATION

- Secure OS documentation: www.os.octalassecure.com
- Lunar Control Center documentation: www.docs.lunarcontrol.center
- Encryption: www.octalassecure.com/technology/encryption

RESEARCH REFERENCES

- Mobile vulnerabilities: www.attack.mitre.org/matrices/mobile
- Guidelines for managing security of mobile devices: