PRIVORO SAFECASE™ PLATFORM: Security and Trust Verification

PRIVORO®

OVERVIEW

The Privoro SafeCase provides mobile protections in isolation from the vulnerabilities of the smartphone ecosystem to safeguard the sensitive information of some of the most highly targed individuals in the world. A common question is: How do individuals, or the people responsible for protecting them, verify the security and trust of the Privoro SafeCase platform and associated protections?

To answer this question, it is helpful to break the system into two categories:

1. **Anti-Surveillance (AS) Protections**
   a. Camera Blocking
   b. Audio Masking
2. **The SafeCase platform**

Approaches to verify AS protections along with information related to the security and trust of the underlying platform follow. However, it is important to note that, unlike typical software-only protections, the AS protections provided by SafeCase are physical – the audio masking signals and camera blocks provided by the SafeCase platform exist in the real world.

Accordingly, these protections may be physically measured and assessed by the user or responsible organization in both simple and sophisticated ways. Independent test equipment may be used to detect if the protections or underlying platform have been compromised, even without detailed knowledge or visibility into the underlying system.

SMARTPHONE CAMERA PROTECTION

PROTECTION VERIFICATION
(protection is operating as specified)

ACTION/STEPS

- Launch any app that has access to the smartphone's cameras.
- View or record the camera's input with the SafeCase hood up (cameras exposed) and hood down (cameras covered).

EXPECTED RESULT

- Camera(s) should not display visual content when the SafeCase cover is down and the cameras are covered.

TRUST VERIFICATION
(protection is not backdoored
or hacked/compromised)

ACTIONS/STEPS

- Same as for Protection Verification.

EXPECTED RESULT

- Same as for for Protection Verification.
- Rationale: Protection is via a physical block and hack or compromise of this protection would be evident in the image displayed or captured by the camera being protected.

SMARTPHONE AUDIO MASKING

PROTECTION VERIFICATION (protection is operating as specified)

LEVEL 1: USER TEST

OVERVIEW:
This test specifies how end users may test that audio masking is operational.

THREAT MODEL:
SafeCase is broken or non-operational (e.g., battery is dead, device is off, device is compromised such that masking LEDs are on when masking is actually off, etc.).

ACTION/STEPS

1. **Launch any app that has access to the smartphone's microphones.**

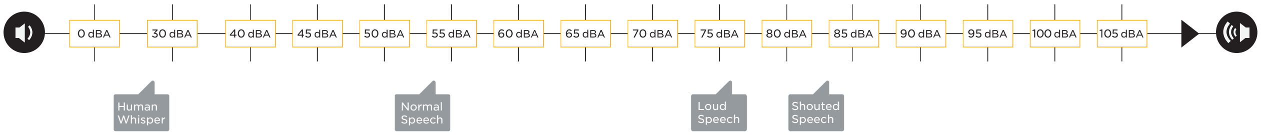
2. **Make a recording while talking, ensuring that the SafeCase audio protections are active (power on, hood down).**
   - Do this for all of the microphones to which the app provides access.
   - Note: The Privoro App provides access to 3 microphones to ease the verification process.

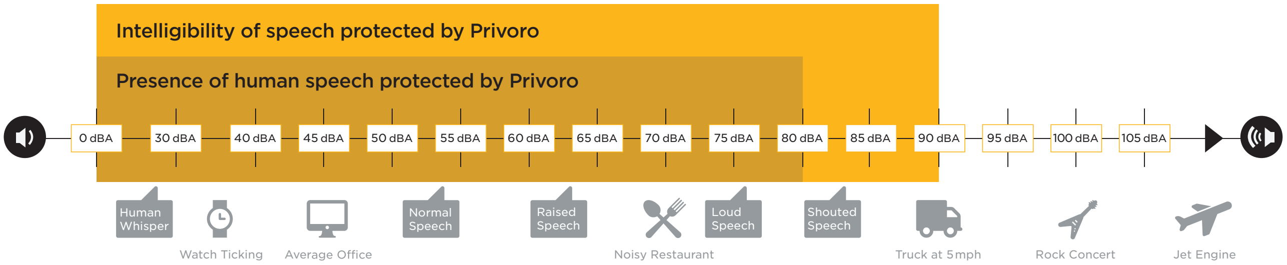
3. **Play the recording.**

EXPECTED RESULT

1. **Speech should not be discernible in the recording.**

2. **Additonal notes:**
   - The SafeCase has protection specifications – protection from detecting the Presence of speech up to 80 dBA and Intelligibility of speech up to 90 dBA, both measured from a distance of 1 meter – and speech/sounds exceeding those specifications may be discernible in the recording.
   - Users without calibrated equipment may vary the volume of their speech to test the level of protection provided (e.g, the volume at which speech becomes detectible and intelligible).





Tested one meter from audio source

VARIANTS/ENHANCEMENTS

1. **Test App: Functionality Check**

   a. Overview: Verify test app functionality by making recordings other than of SafeCase protections to ensure app is operating correctly.

   b. Threat Model: Hacked app gives false positive on SafeCase audio protections.

2. **Test App: Diversity**

   a. Overview: Use a variety of apps to repeat the User Test. A variant would be to download a new app from the app store to perform the test.

   b. Threat model: A known app consistently used for verification is compromised.

3. **"What You know" phrase/ content to test both the Test App and SafeCase Protections.**

   a. Overview: Use known and variable content and timing while making the recording that tests SafeCase's audio (and video) protection.

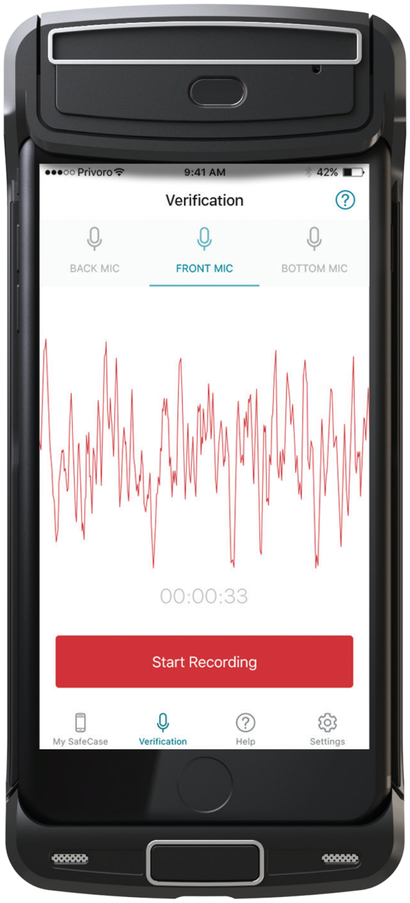
   b. Threat Model: A hacked app consistently spoofs the SafeCase masking signals during testing.

   c. Actions/Steps

   - Make recording with app and SafeCase under test.
   - During recording raise and lower the hood (deactivating and activating audio protections) during and for a random amount of time while speaking. For example, count down from 10 to 1 and lift the hood while speaking the numbers 4 and 3 (vary this with each test).

   d. Expected result: In this example, the speech should be masked except for the numbers 4 and 3.

   e. Rationale: This approach would expose a hacked app that consistently plays a spoofed masking signal.



4. **Change Test Device**

   a. Overview: Use a different phone to test the SafeCase in question while simultaneously using the approach outlined in the User Test Variant 3 "What You Know" Test.

   b. Threat Model: A hacked app that is able to synchronize a spoofed masking signal with detection of the activation/ deactivation of SafeCase protections.

   c. Actions/Steps

   - Use a different phone and its apps, or a newly downloaded app, to verify the audio protections of the SafeCase under test.
   - Follow the actions/ steps outlined in the User Test Variant 3 "What You Know" Test.

   d. Expected result: Same as for User Test Variant 3 "What You Know" Test.

   e. Rationale: Would require an attacker to compromise a second and likely unknown/ random phone and associated apps in order to create a false positive signal.

LEVEL 2: AUDIO FORENSIC TEST: VOICE CONTENT EXTRACTION

OVERVIEW:
Conduct signal analysis similar to what a sophisticated attacker might attempt in order to verify the inability to extract underlying voice content.

THREAT MODEL:
Attacker with sophisticated tools and techniques attempts to extract voice content from recordings by filtering or subtracting the masking signal, enhancing the voice signal or other audio forensic techniques.

ACTIONS/STEPS:

1. Techniques vary.
2. Privoro is willing to engage with appropriate customer or 3rd party laboratory testing teams/facilities:
   - To support analysis of its protections.
   - To discuss internal and third-party analysis of its protective technologies.

NOTES

1. Privoro uses a nation-state threat model (high sophistication, high-budget attacker) when designing its protections.
2. Privoro uses TRNG-based, independent, signal-shaped audio masking for each microphone in the smartphone to prevent the recording of one masking signal being used to attack another.

TRUST VERIFICATION (protection is not backdoored or hacked/compromised)

ACTIONS/STEPS

- Same as for Protection Verification.

EXPECTED RESULT

- Same as for for Protection Verification.
- Rationale: Protection is via physical signals that can be independently verified by the user or protecting organization, revealing if the underlying system is backdoored or hacked/compromised.
- Note: Privoro puts security first and has spent material time and effort to secure its underlying platform. To learn more, please review the Privoro Platform section.

PRIVORO PLATFORM

SECURITY VERIFICATION (platform is hardened and difficult to attack)

OVERVIEW:

- Privoro uses a nation-state threat model when designing/developing its security architecture and many layers of protection are in place.
- Privoro is willing to engage with appropriate customer or 3rd party laboratory testing teams/facilities to further review these protections.
- Privoro is continually monitoring its security and threats and will add additonal protections as/if required to secure its products.

SUPPLY CHAIN & MANUFACTURING

- Products are built in a U.S.-based, ITAR-certified facility.
- Secure supply chain techniques, including counterfeit electronic protection processes, are in place.

INDUSTRIAL DESIGN AND MECHANICAL ENGINEERING

- SafeCase meets FIPS 140-3, Section 5 Physical Security Level X standards

ELECTRONICS

- Single-die, secure processor with side-channel attack protections.
- Secure provisoning process.
- The SafeCase private key is never exposed (it is generated and maintained in the device).
- Post-provisioning lockdown: All JTAG and debug ports disabled.
- FIPS 140-2 LVL 2 compliant
- 3rd party hardware security reviews/testing

FIRMWARE

- Secure bootloader.
- Closed PKI system.
- Technical control requiring 2-person review and approval of all code.
- Cryptographic code-signing is validated at firmware download and update time.
- Firmware update is only available through a cryptographically verified update.

TRUST VERIFICATION (protection is not backdoored or hacked/compromised)

- Privoro conducts technical reviews on all controlled artifacts (e.g., source code for Embedded systems, Cloud software, App software) as part of the process of introducing any new change.
- Strict control is imposed on changes to critical security elements to prevent introduction of malicious functionality.
- Privoro conducts end-to-end stress testing of primary security elements for each release to ensure no loss in integrity.
- Privoro is willing to further review its security architecture with appropriate customers, up to and including details about the hardware, software and cryptographic security mechanisms.

PRIVORO®