FINTELLIGENT

BharatDroid + Vault

Semi-Immutable Probed Privacy and System Test Results

Nothing Phone (1) / Spacewar / Android API 37 prototype

Fresh evidence window: 19 September 2026 | Asia/Calcutta

TESTED OUTCOME: STRONG BOUNDED CONTROLS, ONE RADIO GAP REMAINS

No unexpected public egress, no direct DNS/NTP/DoT, no Google packages or named APK paths, and all 152 sensor registration attempts were denied. Two locked windows each recorded a five-record modem link-local/QMAP burst. This is not public Internet payload, but it prevents a claim of complete radio silence.

PROTOTYPE TEST RESULTS - NOT A CERTIFICATION OR UNIVERSAL ZERO-TELEMETRY CLAIM

Prepared from fresh live-device captures, logs, package state, partition readback and reproducible probe applications. Raw summary evidence is embedded as PDF attachments.

Executive summary

681 s	1,143	0	152/152
fresh measured window	packets captured	unexpected public packets	sensor registrations denied

What is proven

Within three fresh bounded windows, ordinary probe apps could not obtain hardware identifiers, location, camera, microphone samples, sensor delivery, direct hardware attestation or qseecom access. Public traffic was limited to the configured WireGuard endpoint. The installed system partitions match the sealed image and are mounted read-only without overlayfs.

What is not proven

The phone is not production-immutable: the real bootloader is still unlocked, root ADB can be re-enabled, displayed green/locked properties are not authoritative, slot A is unverified, recovery is donor-derived and trusts a test OTA certificate, and factory-reset survival is untested. Universal zero leakage and RF silence are not claimed.

Area	Result	Evidence / interpretation
System partitions	PASS	system, system_ext and product hashes match the signed candidate; mounted read-only; no overlay mount.
Google payload absence	PASS	Zero Google namespace packages, zero targeted Google payloads and zero Google-named APK paths in the tested scope.
Bounded public egress	PASS	Only 194.180.34.13:51820/UDP, the configured WireGuard endpoint; no direct DNS, NTP or DoT.
App telemetry access	PASS	Identifiers masked or denied; sensor, camera, microphone and location access rejected for normal probes.
Locked public payload	PASS	No public payload packets during settled locked intervals.
Locked radio silence	PARTIAL	Five modem link-local/QMAP capture records appeared in two locked windows.
Production immutable	NOT YET	Unlocked bootloader, root-capable engineering path, donor recovery and untested reset survival.

What semi-immutable means on this phone

The current device has crossed from a purely mutable overlay prototype to signed, read-only operating-system partitions. It has not crossed the final hardware trust boundary.

Area	Result	Evidence / interpretation
Read-only base	**Implemented**	Vault/BharatDroid content is baked into system, system_ext and product. A normal runtime cannot edit those mounts.
AVB content chain	**Implemented**	RSA-4096 signatures and dm-verity cover the tested candidate; the live vbmeta digest matches the candidate.
Vault policy/data	**Mutable by design**	Runtime policy databases, PIN, installed apps, Wi-Fi credentials and upstream profile remain under /data.
Hardware root of trust	**Not enforced**	The bootloader is physically unlocked; reported green/locked properties are currently not proof of enforcement.
Reset survival	**Unverified**	A reset should retain baked partitions but erases /data. First-boot restoration has not been destructively tested.
Recovery/update trust	**Incomplete**	Recovery remains donor-derived and /system/etc/security/otacerts.zip contains testkey.x509.pem.

Installed-state anchors

```
Device: Spacewar / serial 528c2acb / slot B
Candidate vbmeta digest: 67b59442b8ca6f1b636910c61476c9dd47030b6b6d89138317844af0a1d234c1
System SHA-256: 2eda76e243a528e53b3f0767312e2b9b7cac13cc87ad21c828459137cbe15b69
System_ext SHA-256: 23d4b2e62038abd10c5590449ad4a32ca8b3a5ee0ae3d887c080dc9dfb4514a3
Product SHA-256: 74a9ad2ac0df2b7edd09cbfc17caaa3351517bde8050fd23fd3a9b493b15dbe5
```

Fresh test design and evidence window

This report uses only measurements collected from the current phone after the final Google-removal image was installed. Earlier reports are not reused as measurement evidence.

Area	Result	Evidence / interpretation
Window A	**226 seconds**	Two normal apps: awake, foreground A, foreground B, lock transition, 35-second settled lock, PIN unlock, post-unlock probe.
Window B	**132 seconds**	Connected Wi-Fi, one normal probe, 34-second settled lock, authenticated wake and Wi-Fi reconnection.
Window C	**323 seconds**	Awake baseline, four-minute settled lock observation (258 seconds measured), authenticated wake.

Measurement instruments

- Packet capture on all Linux interfaces using LINUX_SLL2 with full packet length and kernel-drop accounting.
- Two independently installed normal probe APKs with different UIDs, package scopes and key aliases.
- PackageManager, mount table, dm-verity/AVB image metadata, WebView provider, Vault bootstrap and policy database checks.
- Framework API calls for identifiers, location, sensors, camera, microphone, Wi-Fi scan, DNS and key operations.
- Kernel and Android logs collected by a temporary root observer. Probe APKs were removed after each test; ADB is returned to non-root after evidence collection.

Interpretation boundary

A packet capture can prove what was observed during the measured windows. It cannot prove universal zero leakage for every future app, baseband state, carrier network or RF condition. Link-local modem control is analyzed separately from public Internet payload.

Network boundary held for public payload

0	0	1	0
unexpected public packets	direct DNS/NTP/DoT	public destination	capture kernel drops

Area	Result	Evidence / interpretation
Main probe	550	All public TCP/UDP destinations resolved to 194.180.34.13:51820/UDP (WireGuard).
Wi-Fi cycle	371	Same single WireGuard endpoint; Wi-Fi returned after authenticated unlock.
Long lock	222	Same single WireGuard endpoint while awake; no public payload in settled lock.

Destination policy result

- app-measurement.com resolved to 0.0.0.0 or failed resolution in probe results.
- No port 53, 123 or 853 packet left a physical interface in any measured window.
- No second public IP address or direct application destination was observed.
- The VPN still exposes the chosen upstream server to the access network; anonymity depends on the owner-selected upstream.

```
tcpdump: data link type LINUX_SLL2
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
550 packets captured
550 packets received by filter
0 packets dropped by kernel

Public endpoint: 194.180.34.13:51820/UDP
Unexpected public packets: 0
Direct DNS/NTP/DoT: 0
```

Lock boundary blocked payload, not every modem control frame

Area	Result	Evidence / interpretation
Main lock	5 records	IPv6 router-solicitation and QMAP-control records on rmnet interfaces; no public destination or app payload.
Wi-Fi lock	0 records	No settled-lock physical packet during the 34-second Wi-Fi lifecycle window.
Long lock	5 records	The same modem link-local/QMAP pattern repeated during 258 seconds of settled lock.

Why this happened

The records are below ordinary app traffic. Three are IPv6 ICMP router solicitations from a link-local modem address to ff02::2, and two are QMAP control records. Vault stopped public data egress, but the Qualcomm modem/rmnet stack still performed a small link-maintenance exchange. A single logical event can appear on multiple capture layers, so five capture records do not necessarily mean five over-the-air transmissions.

Security consequence

- No content, DNS name, public server or application payload was exposed by these records.
- They still demonstrate that software lock is not identical to hardware RF silence.
- For a battlefield radio-silent posture, the modem must be explicitly powered down or the device must enter a validated airplane/radio-off state; an RF-lab test remains required.

```
Observed destination: ff02::2 (IPv6 all-routers link-local multicast)
Interfaces: r_rmnet_data0 and rmnet_ipa0
Transport: ICMPv6 type 133 plus QMAP control
Public Internet payload during settled lock: 0
```

Ordinary apps received no tested sensor or hardware telemetry

152	0	0	0
sensor registrations attempted	sensor registrations accepted	camera opens	microphone recordings

Area	Result	Evidence / interpretation
Motion and sensor classes	DENIED	38 enumerated classes per probe run; no registration accepted and no samples delivered.
Location	DENIED	SecurityException; no coarse or fine location permission.
Camera	DENIED	SecurityException before camera open.
Microphone	DENIED	AudioRecord remained uninitialized; no audio read.
IMEI	REDACTED	Probe result empty.
Wi-Fi identifiers	MASKED	Unknown SSID; null or 02:00:00:00:00:00 BSSID/MAC.
Android ID	SCOPED	Probe A and Probe B received different values.
Active Wi-Fi scan	DENIED	startScan=false and result count zero for the ordinary probe.

Observed scoped Android IDs

```
Probe A: daeafda9f2c56d18
Probe B: e71f6bb155dc3b1e
Result: different per-app values; no real hardware identifier observed.
```

Vault mediated tested key operations

Area	Result	Evidence / interpretation
Default Keystore2 binder	ABSENT	android.system.keystore2.IKeystoreService/default was not found by either normal probe.
Vault broker binder	PRESENT	android.system.keystore2.IKeystoreService/vault was found.
AES round trip	PASS	Round trip succeeded; key encoding was null (non-exportable); security level reported as 1.
Cross-UID decrypt	REJECTED	Probe B could not decrypt Probe A ciphertext; AEADBadTagException.
Challenge attestation	REJECTED	Normal probes could not generate a challenged hardware-attested key pair.
qseecom	DENIED	Direct /dev/qseecom open failed with EACCES.
ion/hwbinder handles	PARTIAL	Nodes could be opened but the probe recorded no readable data. Further SELinux hardening remains desirable.

What this proves

The tested normal apps used Vault-facing key behavior, received non-exportable keys, were isolated from each other's ciphertext and could not directly request hardware attestation. This is strong evidence for the tested paths, not proof that every framework/native caller is universally intercepted.

Google-owned application payloads were absent

0	0	0	2/2
Google namespace packages	targeted Google payloads	Google-named APK paths	AOSP WebView relros

Area	Result	Evidence / interpretation
GMS / GSF / Play	ABSENT	No active, uninstalled or static-library package match in the tested package scope.
Chrome / Trichrome	ABSENT	No package or physical APK path match.
WebView	HEALTHY	com.android.webview 145.0.7632.218; two relros started and two completed.
Emergency component	PRESERVED	Open-source AOSP com.android.emergency retained under EmergencyInfoAosp without INTERNET permission.
References and SDK strings	OUT OF SCOPE	Android namespaces, open-source libraries, third-party SDK references and denylist strings are not proprietary Google APKs.

```
Package query matches: 0
Google/GMS/GSF/Play/Chrome/Trichrome APK path matches: 0
Read-only/no-overlay verification: PASS
Partition readback matches signed candidate: PASS
```

Verified content is ready for further hardening, not relocking today

Area	Result	Evidence / interpretation
Candidate AVB	PASS	RSA-4096, flags 0, consistent key, dm-verity enabled, live vbmeta digest matches.
Real bootloader	UNLOCKED	Fastboot preflight previously reported unlocked=yes. Current green/locked properties are not authoritative.
Slot B	VERIFIED	Installed, booted and read back against candidate hashes.
Slot A	UNVERIFIED	Not prepared as a known-good signed fallback.
Recovery	DONOR-DERIVED	Current boot/vendor_boot baseline and recovery behavior remain donor-derived.
OTA certificate	TEST KEY	otacerts.zip contains testkey.x509.pem, not the Vault release OTA certificate.
ADB	NON-ROOT AFTER TEST	A temporary root observer was used for evidence. The build can still reactivate root ADB and is not production hardened.
Factory reset	UNTESTED	Baked partitions should remain, but Vault first-boot restoration has not been destructively proven.

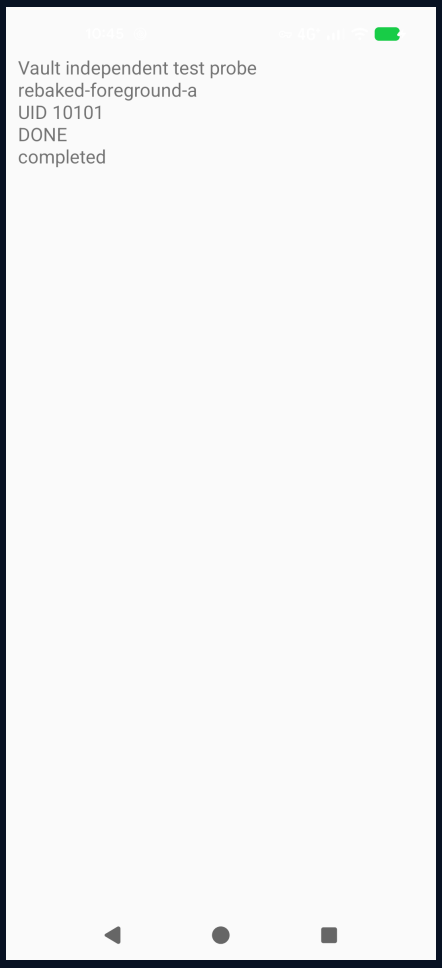
Recommended gate order

- Build Vault-controlled recovery and replace OTA trust with the Vault release certificate.
- Remove root-ADB capability and boot-state spoofing; reconcile build identity.
- Install and verify the same signed chain on both slots.
- Enroll the custom AVB public key while unlocked and verify acceptance.
- Run an explicitly authorized reset-survival rehearsal.
- Only then consider destructive bootloader relocking.

Live-device evidence

Screenshots were captured by the test harness from the connected phone. They are presentation evidence only; the JSON and packet-capture summaries carry the measured assertions.

BharatDroid/Vault home after the fresh probe run



Independent normal probe completed on-device

UI observation outside the privacy verdict

The screenshots still show three-button Android navigation. That is a product/UI completion item and does not change the measured network, sensor, key or package results in this report.

Priority findings and next decisions

Area	Result	Evidence / interpretation
P0	**Recovery and OTA trust**	Create Vault recovery, install Vault OTA certificate, prove signed sideload and remove testkey dependency.
P0	**Root and truthful boot state**	Permanently remove root ADB capability and boot-state spoofing before any relock attempt.
P1	**Locked modem control**	Define whether software lock must power down cellular. If yes, gate modem power/state and validate in an RF lab.
P1	**A/B readiness**	Prepare and independently boot-test slot A as a signed fallback.
P1	**Reset survival**	After backup and explicit approval, prove Vault setup, policy and app restoration after /data wipe.
P2	**Hardware nodes**	Tighten ion/hwbinder exposure where compatibility permits; prove no downstream regression.
P2	**UI completion**	Replace remaining three-button navigation and donor recovery assets for the intended product experience.

Current decision

Keep the phone unlocked for engineering. The semi-immutable base is suitable for continued controlled testing, but not for a military deployment, final relock or universal zero-telemetry claim.

Reproducibility and evidence index

The attached JSON files preserve the exact computed summaries and probe results used in this document. PCAP files remain local because they are binary captures; their SHA-256 values and sizes are in evidence-manifest.json.

Reproduction sequence

- Verify exact Spacewar identity, serial, slot and boot completion.
- Compare live system, system_ext and product block hashes with image-sha256.json.
- Confirm read-only mounts and absence of overlayfs.
- Install normal probes A and B, capture all interfaces, execute awake/lock/wake phases, then uninstall probes.
- Parse LINUX_SLL2 records by interface, direction, destination, protocol, port and phase.
- Count sensor registration attempts and accepted results; inspect key, identifier and hardware-node outcomes.
- Run the independent Wi-Fi lifecycle and four-minute locked observation.

Attached evidence

integrity-result.json - SHA-256 dbdb1e98e2747f8667412155cd8c5609ed9751ee217d1d625e9c08ef5430f1b6 - 784 bytes
main-smoke-analysis.json - SHA-256 0f0fa8138ba752a9b4232d4c339f989100ecbe64a68bd8d4e9d44e5bff0a3e55 - 2,110 bytes
main-smoke-tests.json - SHA-256 301a96621e43281fe95b8f9c4f77b92767c3d3972461b6615296e585dc6f6454 - 32,305 bytes
wifi-smoke-analysis.json - SHA-256 f5d732387ac52ff908a71e2b38e167c560033f633653766387fffaaf1287832e - 759 bytes
lock240-smoke-analysis.json - SHA-256 ec8561bc758d4ee426f7a699f0aafa158fd1ddf516031eab5f1a6a12b1cbe13a - 2,109 bytes
runtime-result.json - SHA-256 e247981bbaf02d1c4aae1ab14d2fdb52b4ba55cdb98a9ca5f1318dac5697c76b - 2,708 bytes
live-state.json - SHA-256 9e740b5a15b42080a96274ee73c47975702e1e7cd49e8b1c85ade8a394fa7381 - 2,052 bytes
evidence-manifest.json - SHA-256 bc44cf7092802b74fc5cbe4cd9076aa8e027a125261be13af1b86d2be7188a90 - 1,959 bytes

Important limitations

- No RF laboratory measurement was performed.
- Baseband firmware behavior is not fully controlled by Android framework policy.
- No factory reset or bootloader relock was performed.
- No claim is made about applications, networks or operating periods outside the tested scope.
- The temporary root observer expands test visibility; it is also a release blocker until permanently removed.

Prepared by Fintelligent from live-device test evidence. This report is a prototype engineering assessment, not a certification, accreditation, penetration-test attestation or deployment authorization.