RKS Global

September 2025 • rks.global

Surveillance Testing in MAX on Android

I. Study of MAX behavior on a user's phone with permissions enabled

Hypothesis

On Android, the MAX messenger uses granted permissions autonomously.

Tasks

1. Check which permissions the app requests;
2. Check how the app uses those permissions and whether it does anything on its own.

Methodology

1. Monitoring the app via adb logcat
2. Monitoring app traffic via PiRouge
3. Monitoring app activity via Android's built-in tools (Permission Controller), which shows which apps used permissions
4. adb bugreport error log

Study conditions

1. Google Pixel 7a, stock firmware, BP2A.250605.031.A2

2. All phone traffic is routed through PiRouge Wi-Fi, version 2.0.5
3. MAX messenger installed from the Play Store, version 25.9.2
4. MAX was granted all permissions it requested (Camera, Location, Microphone, Notifications, Photos & Videos, Contacts)
5. Phone connected to a laptop for adb monitoring, Android Debug Bridge version 1.0.41, Version 34.0.4-debian

The app was tested with a Russian IP address, geolocation, and phone number, as well as with an IP address and geolocation outside Russia.

Research process

1. Over a 48-hour period, the phone with the app installed was monitored.
2. The app was in various states:
    a. Minimized with the phone locked
    b. Minimized with the phone unlocked (home screen)
    c. In the foreground
    d. In the foreground with a nearby speech source active
3. After obtaining the files, adb logs and the .pcap file were analyzed using Python.

Study results

In none of the observed test configurations was improper access detected to the Camera, Location, Microphone, Notifications, Photos & Videos, or Contacts. Technically, the app is capable of collecting and transmitting these data, but we did not observe this occurring. It may occur selectively or depending on location.

Anomalies:

In the configuration where the app was open, it was observed sending packets (about ~2.48 kB) to the server 217.20.152.209 and, at the same time, occasionally executing a UI re-rendering task. No references to user data were seen in the UI rendering commands, but the traffic was not decrypted due to the specifics of the test setup (no traffic decryption mechanism was configured because of the urgency of the study).

Potential further research

1. Decrypt the traffic to examine the contents of these and other packets.
2. Capture anomalies (change geolocation, switch the phone number to CIS countries, etc.).
3. Investigate hosts and domains (api.oneme.ru, i.oneme.ru, tracker-api.vk-analytics.ru, pimg.mycdn.me, st.max.ru, sdk-api.apptracer.ru).

Media

1. Sync activity with the app interface open

Time	Category	Application	Domain	Source IP	Destination IP	Country	I/O	community_id_b64
2025-09-04 22:34:42.006	Web	TLS		10.8.0.151	217.20.152.209	RU	2.83 kB	MTpqQUdZUXBzVWRk...
2025-09-04 22:30:20.978	Web	TLS		10.8.0.151	217.20.152.209	RU	2.48 kB	MTpqQUdZUXBzVWRk...
2025-09-04 22:25:59.948	Web	TLS		10.8.0.151	217.20.152.209	RU	2.66 kB	MTpqQUdZUXBzVWRk...
2025-09-04 22:21:38.859	Web	TLS		10.8.0.151	217.20.152.209	RU	2.48 kB	MTpqQUdZUXBzVWRk...
2025-09-04 22:17:17.895	Web	TLS		10.8.0.151	217.20.152.209	RU	2.92 kB	MTpqQUdZUXBzVWRk...
2025-09-04 22:12:56.806	Web	TLS		10.8.0.151	217.20.152.209	RU	2.48 kB	MTpqQUdZUXBzVWRk...
2025-09-04 22:08:35.837	Web	TLS		10.8.0.151	217.20.152.209	RU	2.66 kB	MTpqQUdZUXBzVWRk...
2025-09-04 22:04:14.815	Web	TLS		10.8.0.151	217.20.152.209	RU	2.48 kB	MTpqQUdZUXBzVWRk...
2025-09-04 21:59:53.713	Web	TLS		10.8.0.151	217.20.152.209	RU	2.48 kB	MTpqQUdZUXBzVWRk...
2025-09-04 21:55:32.753	Web	TLS		10.8.0.151	217.20.152.209	RU	2.92 kB	MTpqQUdZUXBzVWRk...
2025-09-04 21:51:11.722	Web	TLS		10.8.0.151	217.20.152.209	RU	2.48 kB	MTpqQUdZUXBzVWRk...
2025-09-04 21:46:50.709	Web	TLS		10.8.0.151	217.20.152.209	RU	2.92 kB	MTpqQUdZUXBzVWRk...
2025-09-04 21:42:29.674	Web	TLS		10.8.0.151	217.20.152.209	RU	3.35 kB	MTpqQUdZUXBzVWRk...
2025-09-04 21:38:08.650	Web	TLS		10.8.0.151	217.20.152.209	RU	2.48 kB	MTpqQUdZUXBzVWRk...
2025-09-04 21:33:47.597	Web	TLS		10.8.0.151	217.20.152.209	RU	2.92 kB	MTpqQUdZUXBzVWRk...
2025-09-04 21:29:26.590	Web	TLS		10.8.0.151	217.20.152.209	RU	2.48 kB	MTpqQUdZUXBzVWRk...
2025-09-04 21:25:05.543	Web	TLS		10.8.0.151	217.20.152.209	RU	2.98 kB	MTpqQUdZUXBzVWRk...
2025-09-04 21:20:44.536	Web	TLS		10.8.0.151	217.20.152.209	RU	3.28 kB	MTpqQUdZUXBzVWRk...
2025-09-04 21:16:23.507	Web	TLS		10.8.0.151	217.20.152.209	RU	3.35 kB	MTpqQUdZUXBzVWRk...
2025-09-04 21:12:02.487	Web	TLS		10.8.0.151	217.20.152.209	RU	2.92 kB	MTpqQUdZUXBzVWRk...

2. Other network activity

2025-09-03 18:14:56.428	Web	TLS	api.oneme.ru	10.8.0.151	217.20.155.18	RU	7.30 kB	MTpUR0k1ZlhUdWhJR...
2025-09-03 18:14:56.428	Web	TLS	api.oneme.ru	10.8.0.151	217.20.155.18	RU	7.30 kB	MTpFODZrZUpxM25Pbj...
2025-09-03 18:14:56.428	Web	TLS	tracker-api.vk-analytics.ru	10.8.0.151	95.163.41.56	RU	9.53 kB	MToybW41T2FKRitCY...
2025-09-03 18:14:56.427	Web	TLS	api.oneme.ru	10.8.0.151	217.20.155.18	RU	6.31 kB	MTpYd2MzT0xMbDNT...
2025-09-03 18:14:56.427	Web	TLS	api.oneme.ru	10.8.0.151	217.20.155.18	RU	7.03 kB	MTpLd2hweGlPbFBod...
2025-09-03 18:13:16.928	Web	TLS	i.oneme.ru	10.8.0.151	185.16.148.79	RU	48.2 kB	MTpMRDBPdGhERGtW...
2025-09-03 18:13:15.307	Web	TLS	iu.oneme.ru	10.8.0.151	185.16.148.115	RU	77.0 kB	MTpRenZ4cXI2cjMvND...
2025-09-03 18:13:14.854	Web	TLS	iu.oneme.ru	10.8.0.151	185.16.148.115	RU	8.62 kB	MTpacHhvejVGb1pwZD...
2025-09-03 18:13:07.286	Web	TLS	api.oneme.ru	10.8.0.151	217.20.155.18	RU	19.9 kB	MTpRZkUydzh0YVFCO...
2025-09-03 18:13:06.395	Web	TLS	api.oneme.ru	10.8.0.151	217.20.155.18	RU	7.15 kB	MTpqL05DYk5vVnloMC...
2025-09-03 18:13:06.331	Web	TLS	tracker-api.vk-analytics.ru	10.8.0.151	95.163.41.56	RU	4.54 kB	MTplNy8raTVaaTF2MX...
2025-09-03 18:10:28.478	Web	TLS	i.oneme.ru	10.8.0.151	185.16.148.79	RU	34.0 kB	MTprUm91emswd25FZ...
2025-09-03 18:10:26.608	Web	TLS	iu.oneme.ru	10.8.0.151	185.16.148.115	RU	72.7 kB	MTpLazE5aDZNbVZJO...
2025-09-03 18:10:26.149	Web	TLS	iu.oneme.ru	10.8.0.151	185.16.148.115	RU	8.62 kB	MToyaUlkTEpNSGVQbl...
2025-09-03 18:10:20.724	Web	TLS	tracker-api.vk-analytics.ru	10.8.0.151	95.163.41.56	RU	3.49 kB	MTpOS2NGTk50dlpRb2...
2025-09-03 18:10:20.137	Web	TLS	api.oneme.ru	10.8.0.151	185.16.148.119	RU	20.2 kB	MTovNEszODF0SVk1c...
2025-09-03 18:10:19.642	Web	TLS	api.oneme.ru	10.8.0.151	185.16.148.119	RU	7.49 kB	MTpyOGVyZWNBQ1M...
2025-09-03 18:10:19.642	Web	TLS	api.oneme.ru	10.8.0.151	185.16.148.119	RU	8.41 kB	MTplR3Q1WDFITXNNT...
2025-09-03 18:10:16.601	Web	TLS	tracker-api.vk-analytics.ru	10.8.0.151	95.163.41.56	RU	3.42 kB	MToxZFphSllHMVhpNT...
2025-09-03 17:58:33.807	Web	TLS	api.oneme.ru	10.8.0.151	185.16.148.119	RU	17.9 kB	MTp2NloxL0VjekFla2V...
2025-09-03 17:58:32.969	Web	TLS	tracker-api.vk-analytics.ru	10.8.0.151	95.163.41.56	RU	4.35 kB	MTp5ZU94cS9mTVNo...

Time	Category	Application	Domain	Source IP	Destination IP	Country	I/O	community_id_b64
2025-09-19 17:30:41.981	Web	TLS	sdk-api.apptracer.ru	10.8.0.151	217.20.156.179	RU	20.4 kB	MTovMTBISVIaODRMaDZ…
2025-09-19 17:30:39.659	Web	TLS	sdk-api.apptracer.ru	10.8.0.151	217.20.156.179	RU	20.1 kB	MTpzZmpycG5xQWRaMV…
2025-09-19 17:30:38.953	Network	DNS	sdk-api.apptracer.ru	10.8.0.151	10.8.0.1		203 B	MTo3UC9kSjlxaW91azFX…
2025-09-19 17:24:54.121	Web	DNS.Google	edgedl.me.gvt1.com	10.8.0.151	10.8.0.1		224 B	MToyL3h0UlJ3OGkzRURZ…
2025-09-19 17:24:54.121	Web	DNS.Google	edgedl.me.gvt1.com	10.8.0.151	10.8.0.1		183 B	MTpHa0g1aU5mcUtZZG9…
2025-09-19 15:06:06.373	Web	TLS	pimg.mycdn.me	10.8.0.151	5.101.40.2	NL	38.8 kB	MTo1Q2prN0pXRnJoOGI5…
2025-09-19 15:06:05.766	Network	DNS	pimg.mycdn.me	10.8.0.151	10.8.0.1		221 B	MToyL1QrSmVUUEY3UFd…
2025-09-19 15:06:05.579	Web	TLS	i.oneme.ru	10.8.0.151	185.16.148.79	RU	9.89 kB	MTo2VjZMelM0SkxQckVq…
2025-09-19 15:01:32.447	Web	TLS	i.oneme.ru	10.8.0.151	185.16.148.79	RU	7.33 kB	MToyNXBCL2tER09MMm…
2025-09-19 15:01:32.182	Web	TLS	i.oneme.ru	10.8.0.151	185.16.148.79	RU	196 kB	MTpvcjhGTHRlRGdGOGV…
2025-09-19 14:55:15.427	Web	TLS	i.oneme.ru	10.8.0.151	185.16.148.79	RU	32.0 kB	MTpZTWVNbDBwYUNwN…
2025-09-19 14:55:09.453	Web	TLS	i.oneme.ru	10.8.0.151	185.16.148.79	RU	6.14 kB	MTp4UTVyenlHZ08rOGNu…
2025-09-19 14:55:09.453	Web	TLS	i.oneme.ru	10.8.0.151	185.16.148.79	RU	6.14 kB	MTppb3Y0R2NsRi95ZXp5…
2025-09-19 14:55:09.224	Web	TLS	tracker-api.vk-analytics.ru	10.8.0.151	95.163.41.56	RU	1.90 kB	MTptbEVHQ0lSdWg1V0h…
2025-09-19 14:55:09.224	Network	DNS	i.oneme.ru	10.8.0.151	10.8.0.1		183 B	MTpsM3Rjc2F0MzFMWD…
2025-09-19 14:55:08.533	Web	TLS	api.oneme.ru	10.8.0.151	217.20.152.209	RU	24.2 kB	MTpaSEFyYXBPRzNNMEI…
2025-09-19 14:55:08.088	Web	TLS	tracker-api.vk-analytics.ru	10.8.0.151	95.163.41.56	RU	4.38 kB	MTpVNEtzTG9GOElvNzhQ…
2025-09-19 14:55:07.624	Web	TLS	api.oneme.ru	10.8.0.151	217.20.152.209	RU	7.27 kB	MToxcEN3WDRZSk1VTllo…
2025-09-19 14:55:07.624	Web	TLS	api.oneme.ru	10.8.0.151	217.20.152.209	RU	6.18 kB	MTpIYW15TnVsQUFoaTYr…
2025-09-19 14:55:07.456	Network	DNS	api.oneme.ru	10.8.0.151	10.8.0.1		203 B	MTo3dXpDZ2ZyNHlmZ3g…
2025-09-19 14:55:07.456	Network	DNS	api.oneme.ru	10.8.0.151	10.8.0.1		203 B	MTpXRHdhRWx1REJ3Ym…
2025-09-19 14:55:07.456	Network	DNS	tracker-api.vk-analytics.ru	10.8.0.151	10.8.0.1		201 B	MTptd0h3RGdmOWp3Q2l…

3. App inactivity

```
09-04 00:32:11.810 31175 31183 I ru.oneme.app: Background concurrent mark compact GC freed 57MB AllocSpace bytes, 0(0B) LOS objects, 75% free, 19MB/77MB, paused 653us,1.576ms total 101
.714ms
09-04 00:32:46.330 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 00:42:46.335 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 00:52:46.340 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 01:02:46.345 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 01:12:46.350 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 01:22:46.355 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 01:32:46.361 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 01:42:46.367 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 01:52:46.374 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 02:02:46.380 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 02:12:46.385 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 02:22:46.390 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 02:32:46.395 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 02:42:46.401 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 02:52:46.406 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 03:02:46.412 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 03:12:46.418 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 03:22:46.424 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 03:32:46.428 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 03:42:46.431 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 03:51:16.152 31175 31183 I ru.oneme.app: Background concurrent mark compact GC freed 57MB AllocSpace bytes, 0(0B) LOS objects, 75% free, 19MB/77MB, paused 924us,1.783ms total 104
.658ms
09-04 03:52:46.435 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 04:02:46.439 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 04:12:46.445 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 04:22:46.451 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 04:32:46.457 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 04:42:46.462 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 04:52:46.467 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 05:02:46.470 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 05:12:46.474 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 05:13:26.428 31175 31183 I ru.oneme.app: Background concurrent mark compact GC freed 57MB AllocSpace bytes, 0(0B) LOS objects, 75% free, 19MB/77MB, paused 865us,1.930ms total 125
.208ms
09-04 05:22:46.479 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
09-04 05:32:46.484 31175  3207 I PhenotypeProcessReaper: Memory state is: 100
```

4. Some UI rendering events

```
09-04 18:35:58.273 31175 31175 D VRI[MainActivity]: visibilityChanged oldVisibility=true newVisibility=false
09-04 18:35:58.318 31175 31175 I AutofillManager: onInvisibleForAutofill(): expiringResponse
09-04 18:36:16.694  1416  1947 D ActivityManager: freezing 31175 ru.oneme.app
09-04 18:39:47.742  1416  5664 D ActivityManager: quick sync unfreeze 31175 for 1
09-04 18:39:47.745  1416  1679 D ActivityManager: sync unfroze 31175 ru.oneme.app for 1
09-04 18:39:47.757 31175 31175 D ViewRootImpl: Skipping stats log for color mode
09-04 18:39:47.777 31175 31175 W Bundle  : Key is.last.message.completely.visible.on.detach expected String but value was a java.lang.Boolean.  The default value <null> was returned.
09-04 18:39:47.780 31175 31175 W Bundle  : Attempt to cast generated internal exception:
09-04 18:39:47.780 31175 31175 W Bundle  : java.lang.ClassCastException: java.lang.Boolean cannot be cast to java.lang.String
09-04 18:39:47.780 31175 31175 W Bundle  :      at android.os.BaseBundle.getString(BaseBundle.java:1448)
09-04 18:39:47.780 31175 31175 W Bundle  :      at tr.a(Unknown Source:513)
09-04 18:39:47.780 31175 31175 W Bundle  :      at one.me.messages.list.ui.MessagesListWidget.onAttach(Unknown Source:254)
09-04 18:39:47.780 31175 31175 W Bundle  :      at wv3.attach(Unknown Source:80)
09-04 18:39:47.780 31175 31175 W Bundle  :      at vqf.b(Unknown Source:33)
09-04 18:39:47.780 31175 31175 W Bundle  :      at wv3.activityStarted(Unknown Source:7)
09-04 18:39:47.780 31175 31175 W Bundle  :      at doc.s(Unknown Source:26)
09-04 18:39:47.780 31175 31175 W Bundle  :      at doc.s(Unknown Source:51)
09-04 18:39:47.780 31175 31175 W Bundle  :      at doc.s(Unknown Source:51)
09-04 18:39:47.780 31175 31175 W Bundle  :      at qgg.O(Unknown Source:35)
09-04 18:39:47.780 31175 31175 W Bundle  :      at com.bluelinelabs.conductor.internal.AndroidXLifecycleHandlerImpl.onActivityStarted(Unknown Source:0)
09-04 18:39:47.780 31175 31175 W Bundle  :      at android.app.Application.dispatchActivityStarted(Application.java:401)
09-04 18:39:47.780 31175 31175 W Bundle  :      at android.app.Activity.dispatchActivityStarted(Activity.java:1615)
09-04 18:39:47.780 31175 31175 W Bundle  :      at android.app.Activity.onStart(Activity.java:2154)
09-04 18:39:47.780 31175 31175 W Bundle  :      at androidx.fragment.app.b.onStart(Unknown Source:9)
09-04 18:39:47.780 31175 31175 W Bundle  :      at bm.onStart(Unknown Source:0)
09-04 18:39:47.780 31175 31175 W Bundle  :      at p5.onStart(Unknown Source:0)
09-04 18:39:47.780 31175 31175 W Bundle  :      at one.me.android.MainActivity.onStart(Unknown Source:0)
09-04 18:39:47.780 31175 31175 W Bundle  :      at android.app.Instrumentation.callActivityOnStart(Instrumentation.java:1696)
09-04 18:39:47.780 31175 31175 W Bundle  :      at android.app.Activity.performStart(Activity.java:9198)
09-04 18:39:47.780 31175 31175 W Bundle  :      at android.app.ActivityThread.handleStartActivity(ActivityThread.java:4305)
09-04 18:39:47.780 31175 31175 W Bundle  :      at android.app.servertransaction.TransactionExecutor.performLifecycleSequence(TransactionExecutor.java:214)
09-04 18:39:47.780 31175 31175 W Bundle  :      at android.app.servertransaction.TransactionExecutor.cycleToPath(TransactionExecutor.java:194)
09-04 18:39:47.780 31175 31175 W Bundle  :      at android.app.servertransaction.TransactionExecutor.cycleToPath(TransactionExecutor.java:176)
09-04 18:39:47.780 31175 31175 W Bundle  :      at android.app.servertransaction.TransactionExecutor.executeNonLifecycleItem(TransactionExecutor.java:129)
09-04 18:39:47.780 31175 31175 W Bundle  :      at android.app.servertransaction.TransactionExecutor.executeTransactionItems(TransactionExecutor.java:103)
09-04 18:39:47.780 31175 31175 W Bundle  :      at android.app.servertransaction.TransactionExecutor.execute(TransactionExecutor.java:80)
09-04 18:39:47.780 31175 31175 W Bundle  :      at android.app.ActivityThread$H.handleMessage(ActivityThread.java:2823)
```

II. Study of MAX behavior on a user’s phone with permissions revoked

Hypothesis

If MAX’s permissions are revoked on Android, it will try to regain them.

Tasks

Check whether the app will request permissions again, in which cases, and how persistently.

Research process

1. All permissions were revoked via Android settings.
2. When opening the MAX app, it does not request permissions.
3. When navigating to the Contacts tab, it requests access.
4. In the Calls tab, you can see the “Turn on microphone” button. If you tap it, the app requests access; if you don’t, it does not ask.
5. In the Chats tab, you can see the “Connect contacts” button. If you tap it, the app requests access; if you don’t, it does not ask.

6. In a Chat, you can see the “Attach file” (paperclip) button. If you tap it, the app requests access; if you don’t, it does not ask.
7. In a chat, there is a button resembling the Instagram icon (for recording video messages/stories). If you tap it, the app requests access; if you don’t, it does not ask.
8. In a chat, there is a microphone button (for recording voice messages). If you tap it, the app requests access; if you don’t, it does not ask.

Study results

If you do not activate a function that requires a permission, those permissions are not requested.