

Casing The Vault: Security Analysis Of Vault Applications

Margie Ruffin, Israel Toldeo-Lopez, Kirill Levchenko, Gang Wang

21st Workshop on Privacy in the Electronic Society (WPES '22)



<https://mruffin.github.io>



UNIVERSITY OF
ILLINOIS
URBANA - CHAMPAIGN

Mobile devices are practically an extension of ourselves...

Mobile devices are increasingly used to carry sensitive data.



Mobile devices are practically an extension of ourselves...

Mobile devices are increasingly used to carry sensitive data.

This makes them attractive targets used to monitor people.



Mobile devices are practically an extension of ourselves...

Mobile devices are increasingly used to carry sensitive data.

This makes them attractive targets used to monitor people.

Users may be forced to give up their phones for warrantless inspection.

- Law enforcement demanding access to phone
- Abusive partner snooping through your phone




What would you do?

News > World > Europe

Moscow police 'stopping people to go through their phones' amid anti-war protests

Russia is cracking down on anti-war protesters and western social media as it continues Ukraine invasion

Sravasti Dasgupta • Tuesday 08 March 2022 09:47 •  **Comments**



[1] Sravasti Dasgupta. 2022. Moscow police 'stopping people to go through their phones' amid anti-war protests. (March 2022). Retrieved November 1, 2022 from <https://www.independent.co.uk/news/world/europe/ukraine-moscow-protests-phones-war-b2030786.html>

What would you do?

It's time to admit that 'boyfriend phone hacks' are cyber abuse

Checking your partner's messages or tracking their calls are emotionally harmful behaviours, though TikTok might have you believe otherwise.

BY [BETH ASHLEY](#) | 19.10.21

[f Share](#) [t Tweet](#) [s Snap](#)

News > World > Europe

Moscow police 'stopping people from going through their phones' amid anti-war protests

Russia is cracking down on anti-war protesters and

[Sravasti Dasgupta](#) • Tuesday 08 March 2022 09:47 • [Comments](#)



[1] Sravasti Dasgupta. 2022. Moscow police 'stopping people from going through their phones' amid anti-war protests. (March 2022). Retrieved November 1, 2022 from <https://www.independent.co.uk/news/world/europe/ukraine-moscow-protests-phones-war-b2030786.html>

[2] Beth Ashley. Cheating hacks TikTok is encouraging harmful behaviour. Retrieved November 4, 2022 from <https://i-d.vice.com/en/article/epxg4n/boyfriend-phone-hacks-tiktok-cyber-abuse>

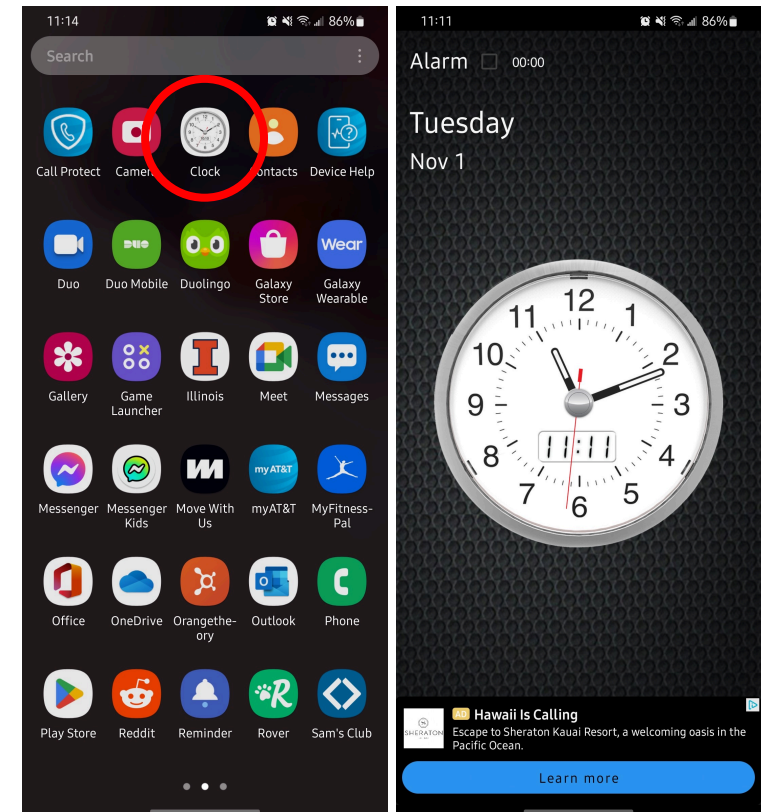
Securing information through **Vault Apps**

These **Vault Apps** can store and hide various user data on the phone:

- Images
- Videos
- Audio
- Documents
- Sometimes even other sensitive apps

Some vault apps can appear **inconspicuously** on a device

- Disguised as a calculator or a clock



Do Vault Apps Work?

Threat Model

- Novice Level Attacker
- Intermediate Level Attacker
- Advanced Level Attacker

Data Collection

Selected a list of 20 Android Vault apps

- 10 commonly studied in prior works
- 10 that are highly popular in the Google Play store

All apps have the same setup

Security Analysis

- Determine the **existence** of vault apps on phone
- **Uncover** and **retrieve** hidden files stored

Threat Model

- Novice Level Attacker
- Intermediate Level Attacker
- Advanced Level Attacker

Data Collection

Selected a list of 20 Android Vault apps

- 10 commonly studied in prior works
- 10 that are highly popular in the Google Play store

All apps have the same setup

Security Analysis

- Determine the **existence** of vault apps on phone
- **Uncover** and **retrieve** hidden files stored

Threat Model

- Novice Level Attacker
- Intermediate Level Attacker
- Advanced Level Attacker

Data Collection

Selected a list of 20 Android Vault apps

- 10 commonly studied in prior works
- 10 that are highly popular in the Google Play store

All apps have the same setup

Security Analysis

- Determine the **existence** of vault apps on phone
- **Uncover** and **retrieve** hidden files stored

Detailed Threat Model

1) Adversaries in our threat model do not have sophisticated technical expertise

2) Only have temporary access to phone

- **Novice Level Attacker**

3) Only after a vault app is discovered are further forensic analysis employed

- **Intermediate Level Attacker**
- **Advanced Level Attacker**

3 Types of Security Analysis

Novice Level Security Analysis

- Attacker with limited time and can only inspect the phone's UI
- Check features of app: app icon, display name, app size, functionality etc.
 - E.g., Police may stop a protestor and ask to look through their phone

3 Types of Security Analysis

Novice Level Security Analysis

- Attacker with limited time and can only inspect the phone's UI
- Check features of app: app icon, display name, app size, functionality etc.
 - E.g., Police may stop a protestor and ask to look through their phone

Intermediate Level Security Analysis

- Somewhat knowledgeable attacker with ability to collect files from phone
- Use off-the-shelf Android tools to examine whether files could be discovered
 - E.g., Abuser may take phone but doesn't have adv. tech knowledge, uses other tools (Cellebrite)

3 Types of Security Analysis

Novice Level Security Analysis

- Attacker with limited time and can only inspect the phone's UI
- Check features of app: app icon, display name, app size, functionality etc.
 - E.g., Police may stop a protestor and ask to look through their phone

Intermediate Level Security Analysis

- Somewhat knowledgeable attacker with ability to collect files from phone
- Use off-the-shelf Android tools to examine whether files could be discovered
 - E.g., Abuser may take phone but doesn't have adv. tech knowledge, uses other tools (Cellebrite)

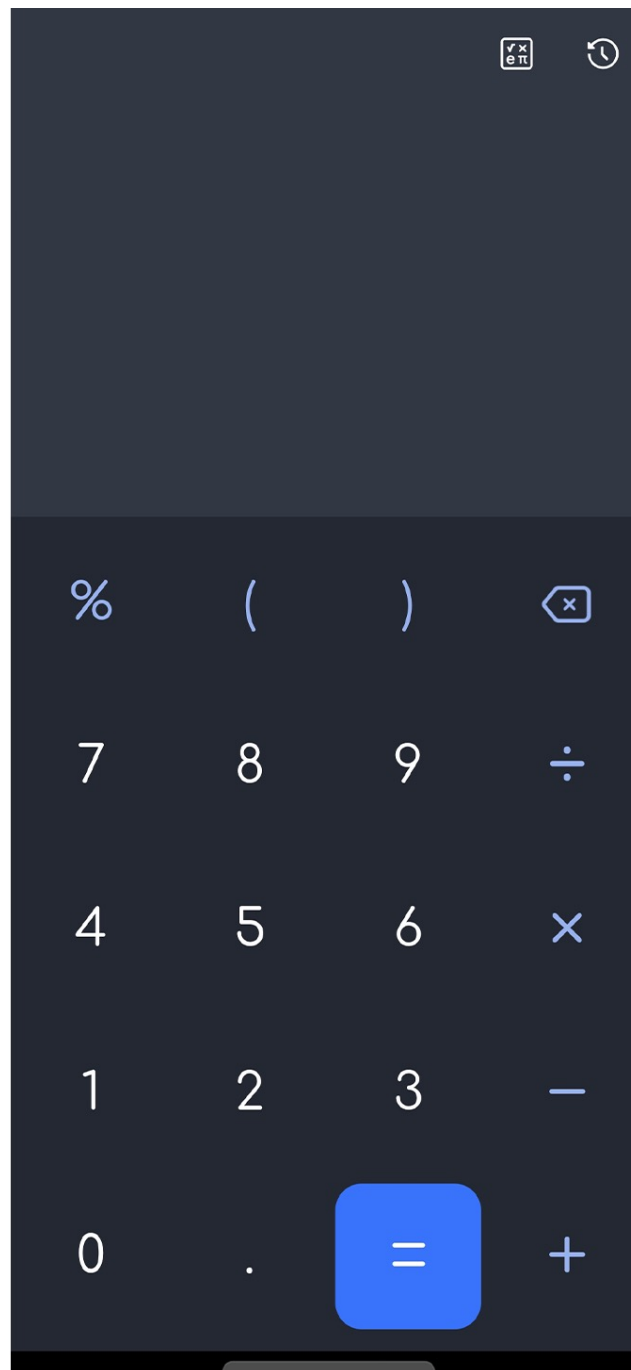
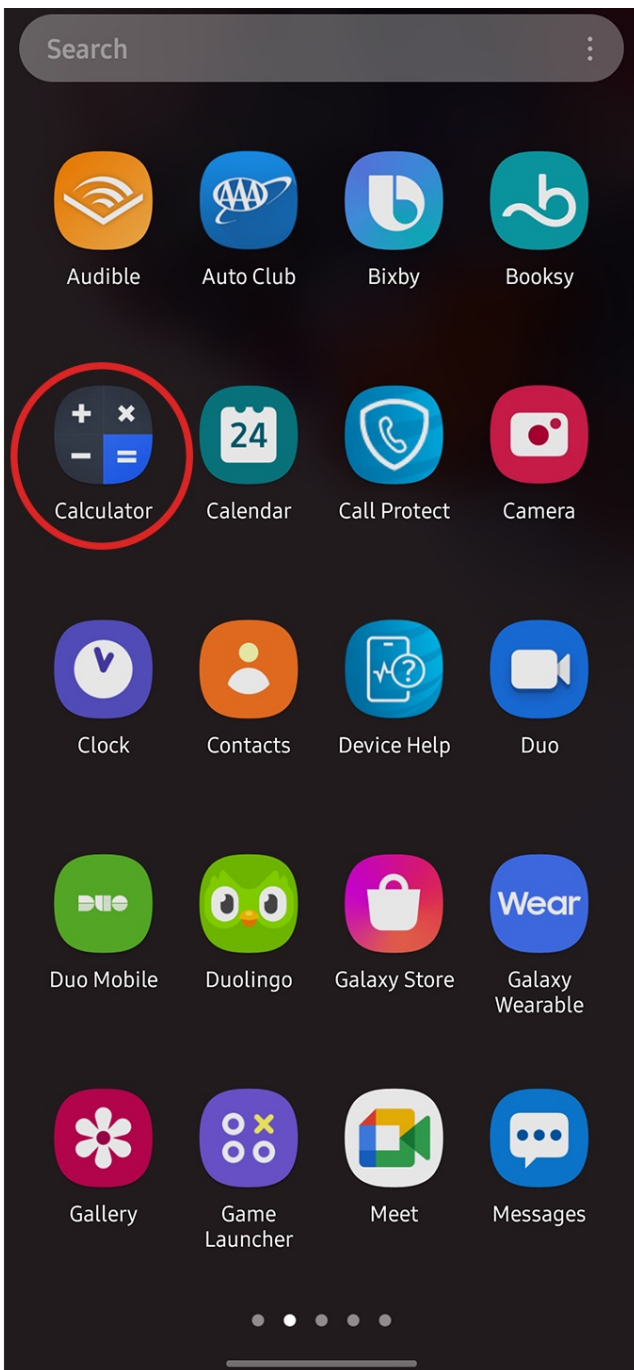
Advanced Level Security Analysis

- Technologically sophisticated attacker with ability to root the phone of interest
- Conduct a thorough analysis of the app's files using decompilation methods
 - E.g., Forensic experts who may have the time and skills to detect and retrieve files from phone

Our Findings

Novice Level

- 10 out of 20 apps have a decoy app as a disguise
- Most common are Clocks and Calculators
- 7 out of 10 disguises are truly functional
- 3 of the 10 apps kept disguise in app library
- Vault app's storage size (MB) can be a giveaway



Name: Calculator

- Disguised
- Functioning Disguise
- Disguise is consistent in app Library
- App Size (MB) Before and After
37.17 → 99.10

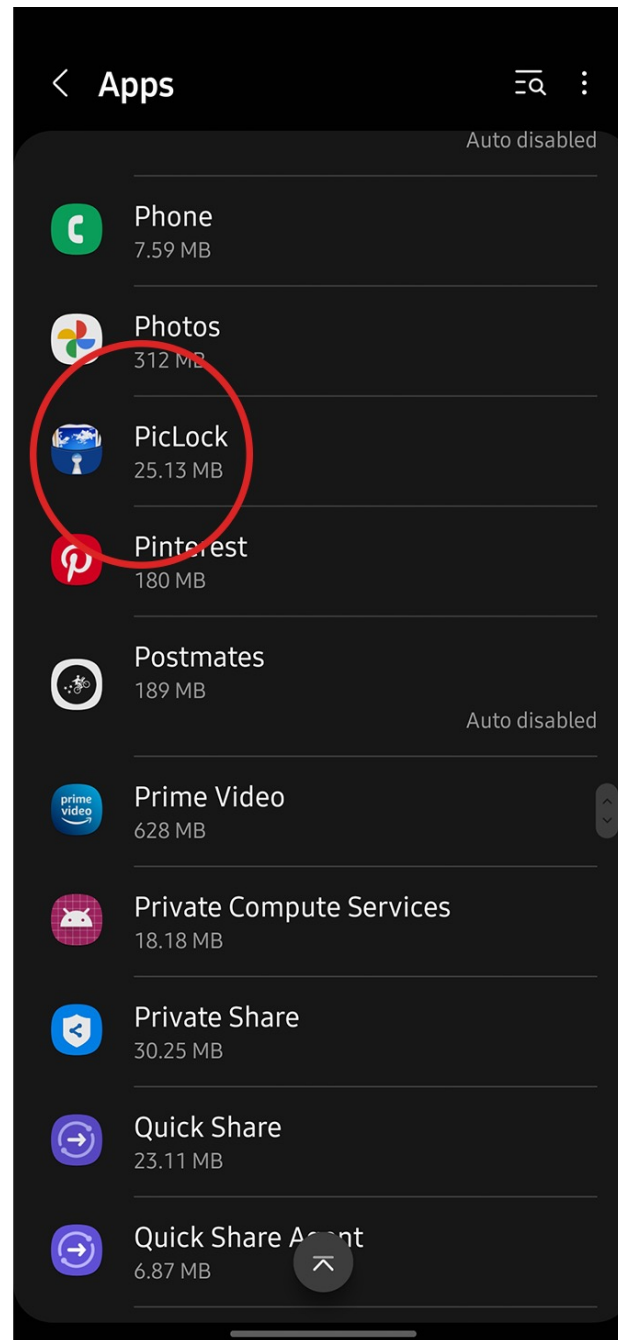
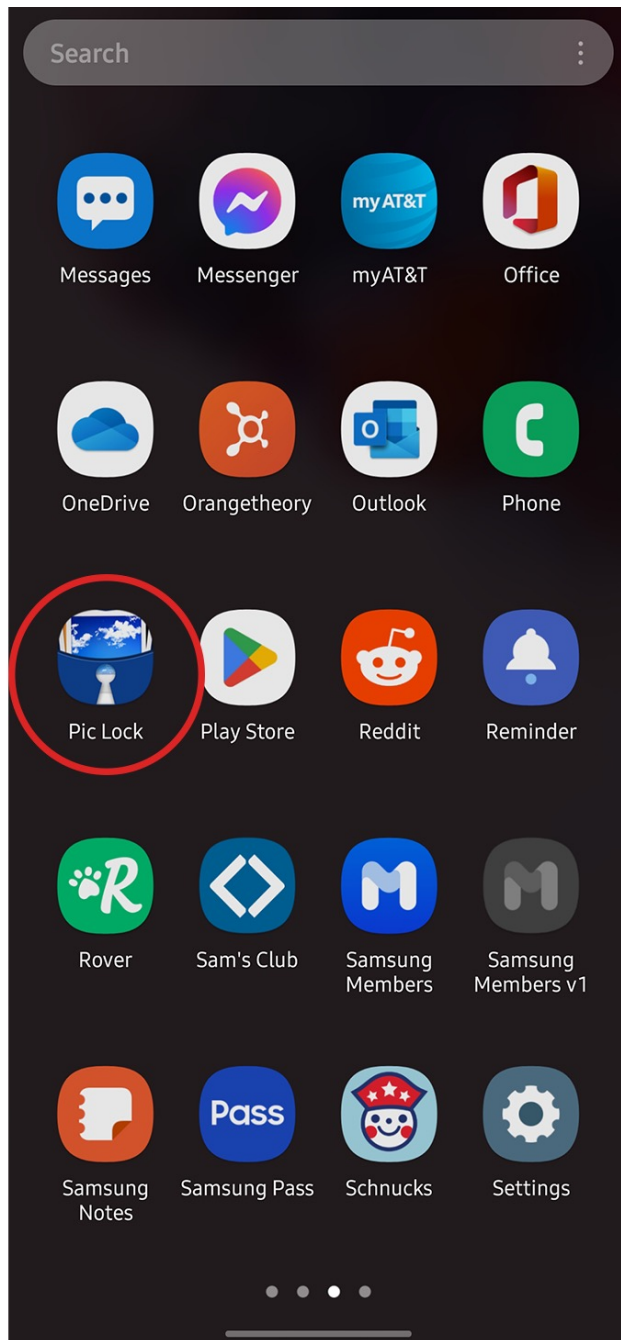
Our Findings

Novice Level

- 10 out of 20 apps have a decoy app as a disguise
- Most common are Clocks and Calculators
- 7 out of 10 disguises are truly functional
- 3 of the 20 apps kept disguise in app library
- Vault app's storage size (MB) can be a giveaway

Intermediate Level

- 10 of the 20 vault apps have the allowBackup flag set to "true"
- For remaining apps, an attempt to pull using adb reveals 5 compromised apps
- They do not employ real encryption of data



Name: PicLock

- No disguise
- Visible in app library

Novice Level Finding

- Has allowBackup:True
- Plaintext information in backup

Intermediate Level Finding

Our Findings

Novice Level

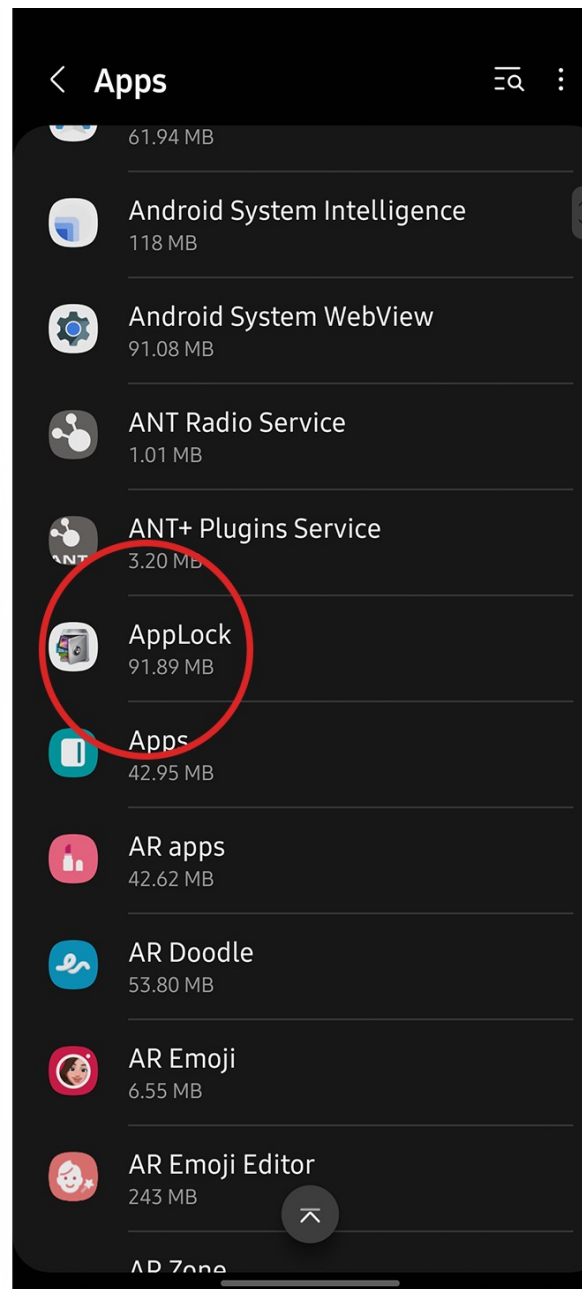
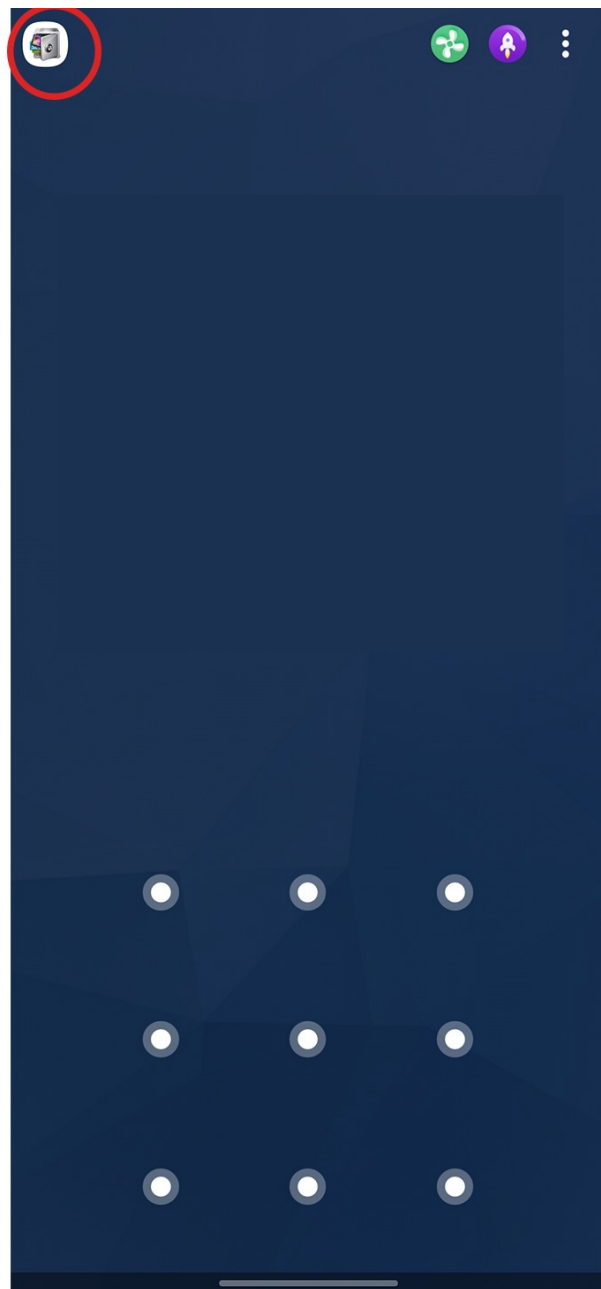
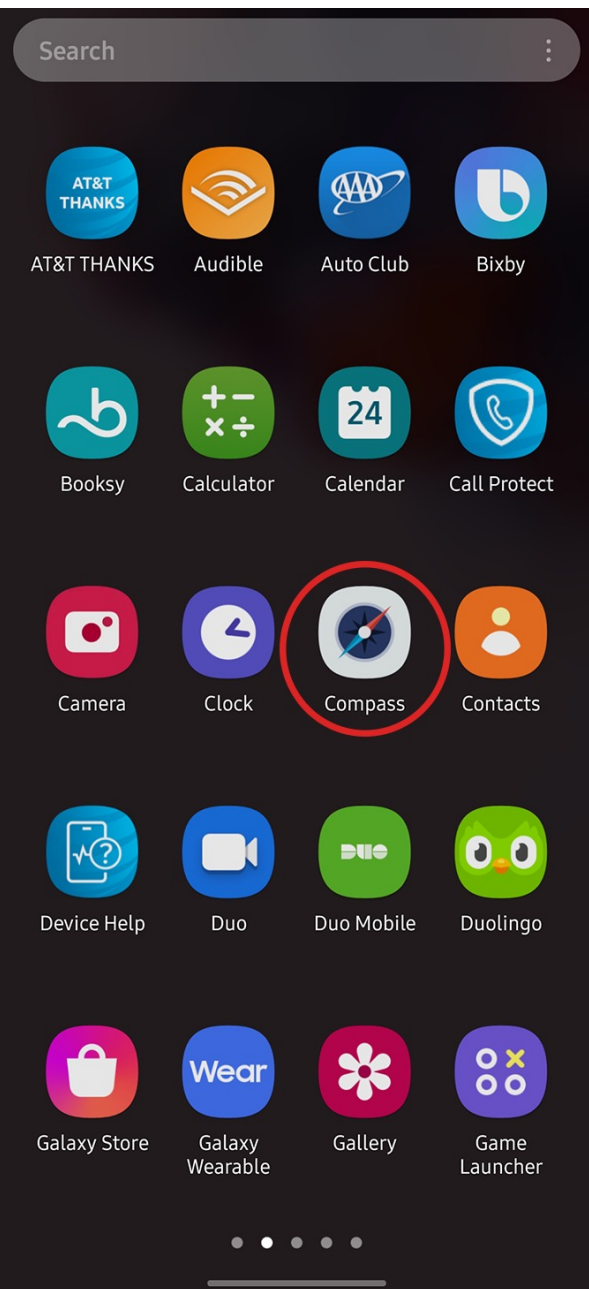
- 10 out of 20 apps have a decoy app as a disguise
- Most common are Clocks and Calculators
- 7 out of 10 disguises are truly functional
- 3 of the 20 apps kept disguise in app library
- Vault app's storage size (MB) can be a giveaway

Intermediate Level

- 10 of the 20 vault apps have the allowBackup flag set to "true"
- For remaining apps, an attempt to pull using adb reveals 5 compromised apps
- They do not employ real encryption of data

Advanced Level

- With root access we could recover files from 2 of the remaining 5
- Only these remaining 5 out of 20 apps have used some encryption schemes to protect the files



Name: AppLock

- Disguised
- Non-functioning disguise
- Visible in app library

Novice Level Finding

- Has allowBackup:False

Intermediate Level Finding

- Does employ encryption

Advanced Level Finding

Recommendations

1. Vault apps should maintain a consistent icon disguise and name disguise everywhere on the phone.
2. Developers should implement functionally disguised apps so that they don't immediately raise suspicion.
3. The entry point to the hidden files within the disguised app should be oblivious to inspectors.
4. Developers should apply encryption schemes to encrypt the stored files.

Recommendations

1. Vault apps should maintain a consistent icon disguise and name disguise everywhere on the phone.
2. Developers should implement functionally disguised apps so that they don't immediately raise suspicion.
3. The entry point to the hidden files within the disguised app should be oblivious to inspectors.
4. Developers should apply encryption schemes to encrypt the stored files.

+ Future Work

- Extend the analysis scope to cover more vault apps (including the less popular ones).
- Automate the vault application analysis procedure to make them easier to evaluate.

+ Future Work

Developer Solutions

Boot and store info on more than one OS

Developer makes a proof of concept multi-boot solution for Android devices

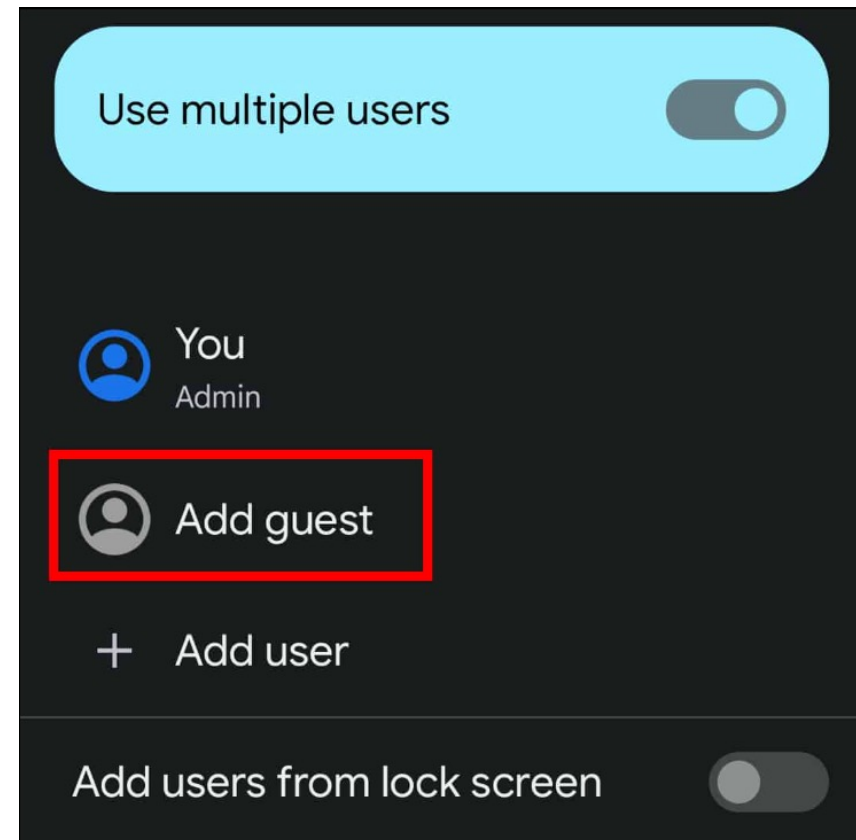
Thanks to XDA Recognized Developer phhusson, we now have a proof of concept multi-boot solution for Android devices. Read on to know more!

BY SKANDA HAZARIKA
PUBLISHED APR 21, 2021



Android Guest Mode

Limit what others have access to on your phone



Summary



- Adversaries with **limited knowledge** and **technical capability** can identify the presence of vault apps via various side channels (e.g., app library, displayed name and icon, app interface).
- Most vault app developers did not implement truly **functional disguises** (e.g., a working calculator) or failed to **maintain the disguise** across different interfaces.

App Package Name	Default Name on Phone Screen	Decoy App	Automatic Disguise?	Functional Disguise?	Configurable Disguise?	Disguise in App Library?	Hide Photos	Hide Videos	Hide Audio	Hide Documents	Lock Apps	Hide Apps	Intruder Alert	Allow Backup?	ADB Pulled?	App Size (MB) Before Vs After
com.domobile.applockwatcher	AppLock	Calculator Compass Spirit Level			✓		✓	✓	✓	✓	✓		✓		✓	45.17 → 95.63
com.netqin.ps	Vault	N/A					✓	✓			✓				✓	42.92 → 57.12
com.kii.safe	Keepsafe	Anti Virus			✓		✓						✓			52.39 → 62.32
com.thinkyeah.galleryvault	Gallery Lock	Calculator		✓	✓		✓	✓								47.19 → 62.58
com.cyou.privacysecurity	LOCX	N/A					☐				✓		✓	✓		13.97 → 26.69
com.app.calculator.vault.hider	Calculator	Calculator	✓	✓	✓	✓	✓	✓				✓		✓		35.17 → 99.10
com.theronrogers.vaultyfree	Vaulty	N/A					✓	✓							✓	13.98 → 21.61
com.morrison.gallerylocklite	Gallery Lock	N/A			☐		✓	✓							✓	31.63 → 41.38
com.xcs.piclock	Pic Lock	N/A			☐		✓	✓					✓	✓		19.79 → 28.68
com.handyapps.videolocker	Video Locker	N/A						✓						✓		34.28 → 43.07
com.apusapps.launcher	APUS	N/A									✓	✓				67.18 → 96.59
com.alpha.applock	AppLock	N/A					✓	✓			✓			✓		17.65 → 49.48
com.flatfish.cal.privacy	Calculator	Calculator	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	72.09 → 237.0
com.ushareit.lockit	Lockit	N/A					✓	✓			✓			✓		27.54 → 36.86
com.ultra.applock	ULTRA APPLOCK	Calculator			✓						✓					30.35 → 39.66
ws.clockthevault	Clock	Clock	✓	✓	✓		✓	✓	✓	✓	✓			✓		24.12 → 72.59
com.sp.protector.free	AppLock	N/A									✓		✓	✓		07.47 → 17.13
com.hld.anzenbokusucal	Calculator	Calculator	✓	✓	✓	✓	✓	✓		✓						36.20 → 39.07
com.app.hider.master.pro	App Hider	Calculator		✓	✓		✓	✓				✓		✓		32.92 → 40.93
com.hideitpro	Audio Manager	Audio Manager Calculator Currency Converter No Icon Joke of the Day	✓	✓	✓		✓	✓	✓					✓		32.99 → 48.19

Table 1: Qualitative Analysis of Vault Applications—We perform a qualitative review of each vault app highlighting its security and privacy features. “✓” means a given feature is supported and it is functional; “☐” means the feature exists but it is nonfunctional during our test.

App Package Name	Plaintext Info?	Encryption?	Hidden Folder?
com.domobile.applockwatcher		✓	✓
com.netqin.ps			✓
com.kii.safe	✓		✓
com.thinkyeah.galleryvault		✓	
com.cyou.privacysecurity			
com.app.calculator.vault.hider		✓	
com.theronrogers.vaultyfree			
com.morrison.gallerylocklite			✓
com.xcs.piclock	✓		✓
com.handyapps.videolocker	✓		✓
com.apusapps.launcher		✓	
com.alpha.applock			✓
com.flatfish.cal.privacy			✓
com.ushareit.lockit		✓	✓
com.ultra.applock	✓		
ws.clockthevault	✓		
com.sp.protector.free	✓		
com.hld.anzenbokusucal			
com.app.hider.master.pro			
com.hideitpro	✓		

Table 2: Additional Qualitative Analysis of Vault Applications—
This table provides additional results from our qualitative review.
“✓” means a given feature is supported and it is functional