The Huawei Report

Security Considerations For Releasing Mobile Banking Apps On The Huawei AppGallery

Author:	Petr Dvořák
Contact:	petr@wultra.com
Date:	02 November 2020
Version:	1.0

Executive Summary

Huawei, a global provider of ICT infrastructure and smart devices, has been in a negative spotlight lately. Many national security agencies have flagged this company as a potential security risk [1], with some countries imposing sanctions to impede Huawei's operations [2]. Banks are considered critical infrastructure in most states. As a result, they need to evaluate their approach to Huawei, especially in the context of smartphones and portable devices their customers use to access digital banking. At the same time, they cannot merely ignore Huawei because it is currently the biggest smartphone vendor with a global smartphone market share of approximately 20%.

The national security agencies are relatively vague in their recommendations. This may be intentional since providing industry-specific advice is complicated. As a result, banks and financial companies are often missing specific guidelines for dealing with Huawei-related questions. They often need to seek help and practical consulting from external cybersecurity experts.

The question they ask the most is the following:

> “ Should we release our mobile banking to the Huawei AppGallery, and if we do, should we also invest in integrating Huawei Mobile Services (HMS)?

It is not easy to answer this question with confidence for various reasons. Besides considering the security of the Huawei ecosystem and potential privacy risks, one must also consider the cost impact of maintaining the mobile app on a third marketplace. On the other hand, it is also impossible to ignore the large user base with Huawei devices. Huawei is currently the largest smartphone vendor worldwide. Based on the claimed sales figures, we assume the Huawei devices are likely to stay.

While we frame our recommendation in the context of the ongoing global conversation concerning Huawei, we would like to point out that many of the suggestions we make are beneficial in general. Banks should consider them even if they do not plan to take any special precautions specific to Huawei devices.

Recommendation Summary

After evaluating factors that we outline later in this document, we recommend the following:

- **Banks should release their applications to the Huawei AppGallery only if they are able to implement additional active in-app protection measures** outlined below.
- When releasing apps to the Huawei AppGallery, **banks must implement at least the following security measures**:
  - Repackaging protection - Ensures application bundle integrity so that the app functionality cannot be modified using "at rest" approaches.
  - Runtime application self-protection (RASP) - Ensures the application cannot be tampered with during runtime by injecting foreign code via the debugger, native code hooks, or via the framework injection.
  - Anti-malware protection - Ensures that the application can actively detect and respond to a malware infection on the device.
  - User data protection hardening - Ensures that user data cannot leak using various channels, such as unencrypted connections (TLS/SSL), accessibility services, custom keyboards, etc.
- **Banks must assess the risks related to possible social and demographic profiling of their customer base** by Huawei and evaluate the commercial trade-off between extending the app user base and sharing data with Huawei.
- **Banks who decide to release an app on AppGallery should carefully consider their investment in implementing HMS**. We suggest releasing mobile banking without HMS despite losing some functionality to minimize the amount of data shared with Huawei, as well as initial costs for the third store overhead.
- **Banks who decide to release an app on AppGallery should implement a quarterly security review procedure** to closely monitor development around Huawei, specifically for signs of fundamental technology (Kirin) or software quality (HMS) degradation and evaluate Common Vulnerabilities and Exposures (CVEs) found in the Huawei mobile ecosystem.
- **Banks who decide to release an app on AppGallery should identify high-value targets in their customer base** and meticulously monitor potential account breaches and other risks associated with their mobile devices.

Specific Risk Factors

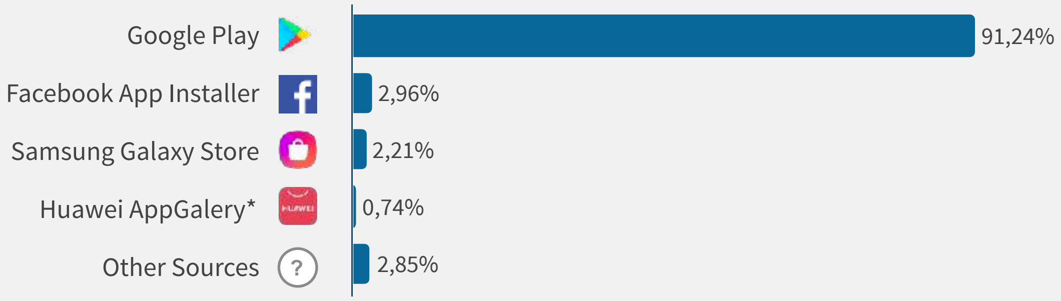
To prepare the recommendations, we took the following areas into account:

1. Crumbling App Ecosystem

Users will always find a way around an issue they face. The fact that many companies will not release their apps on the Huawei AppGallery will force them to look for the app on alternative distribution channels. As a result, most Huawei users will eventually unlock their smartphones for app installation from untrusted sources. Besides installing apps from alternative marketplaces, such as Aptoide, APKMirror, or ApkPure, users will also leave their devices vulnerable to installing potentially malicious apps from links (for example, sent by SMS message), e-mail attachments, or file storage apps.

Installation Sources

While Google Play is the main source of app installations on Android devices, people install apps on their devices from over 250+ alternative sources.



* *Currently, we only collect data from Huawei devices where Google Play is still available. As a result, data from most new devices with only Huawei AppGallery in place are not reflected.*

As a result, it might be much easier for users to have their mobile devices infected. Banks will need to reconsider the risks associated with mobile malware and repackaged mobile banking apps. Since Google Play Protect is not available due to the lack of Google Play Services, banks need to rely on the isolated Huawei security substitute and their own measures to mitigate potential problems.

Specific recommendations

- Implement integrity checking in your mobile banking app to complicate repackaging attempts.
- Implement an active scan for mobile malware and restrict app usage when the device is infected.
- Check the app installer to ensure that the user installed mobile banking from the whitelisted marketplace, not an alternative untrusted channel. Prevent users from running the mobile banking app installed from an untrusted source.

2. Powerful State Actor

The issue that was the most difficult for us to evaluate was the role of the Chinese state in the Huawei company. We must admit that we would appreciate better guidance from the national security agencies on this subject. Despite this, we did our best to cover it with our limited research capacities.

The dark side of smartphones' ubiquity is the hanging threat of an intrusion to personal privacy, for example, by monitoring location updates, the content of messages, or social interactions. The parties who control the mobile ecosystems have almost unlimited power to abuse access to users' data on a large scale. The Chinese government has often been criticized - rightfully or not - for issues in human rights and personal freedom. The theoretical possibility (we must note that speculative, according to our current knowledge) that a government actor could have on-demand access to mobile device data, such as user location, contacts, call information, messages, etc., is problematic [3].

Considering that the Chinese government is an actor with firm control of all China-based companies, banks need to consider the possibility of government-grade spyware attacks, especially in the case of high-value targets (politicians, government personnel, police, military, top management in large companies). These spyware attacks may be much more severe than with regular mobile malware we see in the ecosystem controlled by Google since the entire mobile OS is potentially under the control of a malicious actor, and nothing about runtime security can be guaranteed.

Releasing a mobile banking app on Huawei AppGallery also, to some extent, enables social and demographic profiling of the bank's customer base by Huawei. Huawei AppGallery requires users to create an account before they can install apps. When a user installs a specific mobile app, and whenever an app performs certain actions (for example, registers for a push notification), such an event will be linked to the related customer profile. There is arguably a legitimate interest behind such activity. For example, user profiling may help to recommend the most appropriate content or improve user experience. However, additional data will be shared with a company close to the Chinese government. We understand that Huawei cannot remedy this issue in any way since connecting the AppGallery user profile to HMS data is necessary for the provided service to work. But we recommend a cautious approach when deciding if sharing the data with Huawei makes a good business trade-off for an expanded user base.

The Chinese government also never acted with sufficient vigor whenever companies with Chinese government presence infringed on intellectual property. Historically, we have seen Huawei's attempts to perform industrial espionage [4] without any distancing from the Chinese government's side.

Note that you cannot judge Huawei using western standards when evaluating all the risk factors mentioned earlier. While US or EU tech companies unarguably had security and privacy issues in the past, these became very broadly and publicly discussed, resulting in intense pressure from multiple sources: independent journalists, government and state legislators, and the general public. This pressure ultimately led to improvement and remedies of specific security and privacy concerns. Considering the political establishment in China, we cannot assume a similar type of domestic pressure on Huawei. Security and privacy incidents might be downplayed or even actively covered up.

It is not easy to separate the geopolitical view from the practical recommendations related to the Huawei company. From an idealist point of view, by supporting Huawei in any way, one also indirectly supports the Chinese global ambition with all its negatives. We see why this point of view matters and why the banks hesitate to release their apps to the Huawei AppGallery. However, we also observe that Huawei devices are not going away. People like Huawei devices, often citing “good value for money" as the reason, and they continue to use them despite not having access to Google Play. We need to address the situation and provide recommendations to ensure that they use their mobile banking securely.

This is why we recommend app makers to take additional individual precautions when implementing mobile apps and provide robust built-in security features.

Specific recommendations

- Implement techniques that mitigate the impact of spyware, such as protection against untrusted screen-readers, protection against untrusted keyboards (ideally, use your built-in keyboard instead).
- Encrypt data "at rest" with application-level encryption.
- Prevent runtime tampering by protecting the app process with RASP (foreign code injection by debugger connection, framework injection, or native code hooks).
- Monitor problematic applications on mobile devices for signs of spyware and other malware types.
- Harden the secure communication channel with TLS/SSL certificate pinning and support this measure with RASP to ensure it cannot be globally disarmed in a compromised operating system.
- Identify high-value targets in your user base and monitor potential account breaches, as well as other risks associated with their mobile devices.
- Assess the risks related to possible social and demographic profiling of your customer base by Huawei and evaluate the commercial trade-off between extending the app user base and sharing data with the third party.

3. Questionable Software Engineering

Google is one of the most dominant companies in software engineering. It provides superb software engineering quality across the board and attracts the best global talent. We are not sure that Huawei can be a match for Google in this area. Hence, we anticipate that the software parts not written by Google - specifically, the HMS related software - might have ongoing quality issues [5]. As a result, the software components delivered by Huawei might be more vulnerable to bugs and security issues. Huawei may also be slower in releasing software vulnerability patches.

As a result, banks need to take the lower quality of underlying software into their security considerations and take proactive action to remedy the issue.

Specific recommendations

- Postpone implementing HMS, release your app as-is, with some features disabled.

- Implement a system for monitoring CVE vulnerabilities that are present on mobile platforms with a specific focus on Huawei devices.
- Once a quarter, assess risks associated with CVE vulnerabilities present on mobile devices your customers use.
- Implement runtime application self-protection (RASP) to mitigate issues resulting from weak runtime and software vulnerabilities.
- Follow the DevSecOps principle when building your apps and use tools and services that identify (and ideally fix) potential security issues.

4. Secluded HiSilicon

One of the latent and less visible risks lies in the uncertain future of the Kirin secure element platform produced by HiSilicon, the secure element vendor for Huawei devices. Due to US sanctions, the company has restricted access to software and various tools (mostly made in the US) needed to manufacture the chips. As a result, the Kirin platform chips cannot be produced since September 15, 2020 [6].

The secure element chip is a necessary component of every modern mobile device. It makes local storage for sensitive data safe, it provides secure runtime for sensitive cryptography, and it lies in the core of the biometric authentication chip. Device makers often brand the secure element for the public. Readers might be familiar with Apple's “Secure Enclave” or Android's “StrongBox.”

If the quality of the secure element on Huawei devices deteriorates and no sufficient replacement is found, the banks will need to take extra steps to avoid impacts of impaired runtime and storage security on such devices, for example, by:

- Disallowing biometric authentication.
- Providing alternative software-based secure local storage.

Specific recommendations

- Evaluate the secure element capabilities of newly released Huawei mobile devices in quarterly reviews and assess if the currently released chips are good enough for the use-cases required in mobile banking, such as biometry template storage used for user authentication.

5. Additional Implementation Costs

Deciding whether to implement a banking app for a new platform is never easy. While based on Android, the Huawei ecosystem can easily be considered a new platform. Besides the initial investment into developing support for Huawei, there are also ongoing maintenance and support costs associated with publishing an app on a third marketplace.

Luckily, transitioning to the Huawei ecosystem can be done gradually. You can release the same APK app as you would for Google Play, which dramatically decreases the initial, as well as an ongoing effort. However, this simple path comes with an inevitable sacrifice. Since Google Play Services are not available on new Huawei devices, your mobile app will not be able to:

- Display Google Maps.
- Receive push notifications via Firebase Cloud Messaging.
- Use other Firebase features, such as data storage.
- Support NFC payments using Google Pay.
- Use Google Analytics.
- Protect the app with the SafetyNet API.

Banks should evaluate these limitations in their context and consider if their mobile banking app can provide sufficient value without these services. For example, many banks already use some alternative analytics providers or embed NFC payment functionality inside the mobile banking app via a 3rd party SDK. For those banks, the missing support of the features via Google Play Services will not be a big issue. Otherwise, banks need to implement support for Huawei Mobile Services (HMS) that provide proprietary replacements.

Note that if a customer downloads the mobile banking app from an untrusted source, these services will also be unavailable. Publishing an app to the Huawei AppGallery without HMS has no fewer features than in an app installed from an untrusted source. However, it will provide at least some guarantees of the ecosystem and application source.

Specific recommendations

- Evaluate if your app can provide value to users without Google Play Services.

- Release the first app version with zero or little Huawei specific modifications to minimize the initial implementation costs.
- Evaluate user demand and consider implementing new HMS features based on app usage and user feedback.

References

1. National Cyber and Information Security Agency: Software and hardware of Huawei and ZTE is a security threat
   https://www.govcert.cz/en/info/events/2682-software-and-hardware-of-huawei-and-zte-is-a-security-threat/

2. Bloomberg: Life Is Getting Much Harder for Huawei
   https://www.bloomberg.com/news/newsletters/2020-08-21/life-is-getting-much-harder-for-huawei

3. Huawei says it would never hand data to China’s government. Experts say it wouldn’t have a choice
   https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html

4. US indicts Huawei for stealing T-Mobile robot arm, selling US tech to Iran
   https://arstechnica.com/tech-policy/2019/01/us-indicts-huawei-for-stealing-t-mobile-robot-selling-us-tech-to-iran/

5. Wired: Huawei's Problem Isn't Chinese Backdoors. It's Buggy Software
   https://www.wired.com/story/huawei-threat-isnt-backdoors-its-bugs/

6. The Verge: Huawei says it’s running out of chips for its smartphones because of US sanctions
   https://www.theverge.com/2020/8/9/21360598/huawei-chips-us-sanctions-trump-china-privacy-smartphone