9.0

Mobile App Security

Now there are more than 6.7 billion smartphones in use worldwide, with 5% growth year-on-year[70], the need for a strengthened mobile application security posture is more evident than ever. When consumers purchase a new smartphone, many give consideration to security, privacy and data protection[71]. Overall smartphone security can be considered as a combination of the security of the operating system, the device platform and interfaces, the security of installed software, mobile network security services and the user actions in operating the device.

Smartphones typically run both pre-installed and user-loaded applications. Software application security is therefore an important factor in the overall secure operation of the device. Smartphones usually contain up to four types of apps:

- pre-installed system permission apps which cannot be uninstalled by the device user
- pre-installed non-system permission apps which can be uninstalled by the device user
- Device user apps installed from a controlled source (e.g., the App Store or Google Play)
- Device user apps 'sideloaded' directly to the device[72]

Google evaluates apps on the Google Play Store and estimates[73] that less than 1% of all downloads from Google Play are potentially harmful applications (PHAs). One way in which bad actors attempt to circumvent Google Play's security controls is through versioning. Versioning occurs when a developer releases an initial version of an app on the Google Play Store that appears legitimate, but later an update is pushed from an attacker-controlled server, changing the code on the end user device that enables malicious activity. Another example from the same report[74] highlights dynamic code loading (DCL) as an attack method that enables attackers to download and execute code not included in the original application after installation. This technique enables an attacker to evade static analysis and pre-publication checks. One malware variant using this technique is SharkBot, which initiates money transfers from compromised devices.

Meanwhile, the Open Worldwide Application Security Project (OWASP) has published[75] its initial release of the top 10 mobile risks, which include inadequate supply chain security, improper credential usage and insufficient data storage. The OWASP[76] Mobile Application Security Verification Standard[77] (MASVS) is a community-led initiative for mobile app security. It can be used by mobile software architects and developers seeking to develop secure mobile applications, as well as security testers to aid completeness and consistency of test results.

[70] From GSMAi statistics and forecasts
[71] 7 things you need to know before you buy a mobile phone - Which? News
[72] Google Online Security Blog: Enhanced Google Play Protect real-time scanning for app installs (googleblog.com)
[73] https://services.google.com/fh/files/blogs/gcat_threathorizons_full_jul2023.pdf
[74] https://services.google.com/fh/files/blogs/gcat_threathorizons_full_jul2023.pdf
[75] https://owasp.org/www-project-mobile-top-10/
[76] a nonprofit foundation that works to improve the security of software
[77] https://github.com/OWASP/owasp-masvs/releases

Following a consultation in 2023, the UK government will request that the app industry sign-up to a new code of practice that aims to boost security and privacy requirements on all apps and app stores available in the UK. The voluntary code of practice[78] for app developers and operators aims to protect the UK's app market.

Analysis

Robust device security operation is important given the high volume of smartphones and apps in use. The GSMA has established a Mobile Device Security Certification (MDSCert) working party to start assessing this topic. This MDSCert group has:

- analysed existing device certification programmes.
- investigated the market/regulatory needs for varying assurance levels by conducting a gap analysis.
- liaised with ETSI TC Cyber and provided input into a revised version of ETSI's consumer mobile device protection profile specification[79].
- conducted a consumer-focused study that was run across 11 markets with over 22,000 participants.
- documented the essential requirements and methodologies for a smartphone security certification scheme.

Device certification and labelling have significant potential to raise consumer awareness of device security capabilities. As this area matures, consumers can expect to see greater device security transparency and additional information that can inform subsequent purchase decisions and in-life device security operation.

In the UK, the voluntary code of conduct for app store operators and developers sets out seven practical steps to protect users. In combination with the MASVS programme and application repository protection services, such as Apple's built-in App Store controls and Google Play Protect[80], there is potential to create a stronger baseline for mobile application security that complements the previously described device security needs.

As side-loaded apps may not have the additional security assurances available from controlled sources, particular care should be applied to side-loaded installations.

[78] https://www.gov.uk/government/news/new-rules-for-apps-to-boost-consumer-security-and-privacy
[79] https://www.etsi.org/deliver/etsi_ts/103700_103799/10373201/02.01.01_60/ts_10373201v020101p.pdf
[80] https://developers.google.com/android/play-protect