Monday, 4 October 2021

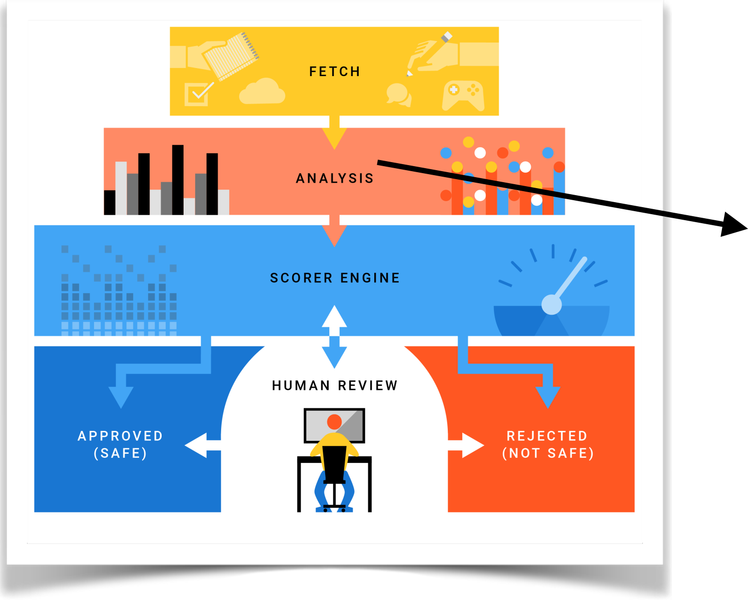
Google Play Protect mechanisms - overview

- On-device security

- Potentially Harmful Applications*(PHAs)* scanning services
  - Daily PHA scan: Every day a scan is performed in all the apps installed, including Google apps. If some PHA is found the user is asked to remove it, or it is automatically removed[1].
  - On-demand PHA scan: Similar to Daily PHA scans, but explicitly launched by the user. The device requests Google servers the latest information and scans all apps.
  - Offline PHA scan: In case of poor or no network connection. The device has an off-line database of well-known PHAs that determines the results of the scan.
  - Unknown app: Apps outside Google Play can optionally be scanned, if the option "*Improve harmful app detection*" is selected in Google Play.
  - Others: Google also gathers and scans apps in third party stores and other sources.

- Cloud-based security

- Before an app becomes available on Google Play, it is analysed using automated mechanisms and human reviews.



Google app review flowchart

Developer Information, compliance with policies.

Machine learning:

- **Static analysis**: The app's code is analyzed and compared against potential bad behavior.
- **Third-party reports**: Feedback from academic reports.
- **Signatures**: Comparison against a database of known malicious app and vulnerabilities.
- **Developer relationships**: Check developer association with PHA and other app relationships.
- **Dynamic Analysis**: Interactive behavior that cannot be seen in the static analysis. Identifies attacks that require network connections, or payload downloads.
- **Heuristic and similarity analysis**: Tries to find trends that show evidence of harmful apps.
- **SafetyNet**: Identifies apps and other threats that can harm devices.

References:

1. Help protect against harmful apps with GGP: https://support.google.com/accounts/answer/2812853?hl=en#zippy=%2Chow-malware-protection-works%2Chow-privacy-alerts-work
2. Google Play Protect: https://developers.google.com/android/play-protect
3. GPP on-device security: https://developers.google.com/android/play-protect/client-protections
4. GPP on-cloud security: https://developers.google.com/android/play-protect/cloud-based-protections
5. PHA categories: https://developers.google.com/android/play-protect/phacategories

Footnotes:

[1] Depending on the PHA classification and its reputation, an app can be automatically blocked. In case it is not automatically blocked, the user is prompted and can choose to block it or not.

Author:

- Pedro Gomes: Github profile, webpage, pegom0896@zoho.eu, PGP fingerprint: 72EDA4D14F94A284C48B4D2BE64A43FDFC17827C