MobSPA Technology

Discover mobile application risk & vulnerabilities

Table of Contents

1 Overview

With the rising popularity of smart terminals, there is an explosive growth in terms of the number and types of applications for Android, the largest mobile system platform. As Android is an open system, its users are now more and more concerned with security issues associated with all kinds of applications, such as the reverse engineering and decompilation of installation packages, malicious code injection, pirated applications, interface hijacking, message hijacking, and input monitoring. These not only create copyright infringement issues for the applications, but, more importantly, they may lead to information breaches and even economic losses for the users. Security in mobile phone applications has become a critical issue that impacts the development of the entire application market.

Although they are aware of the security situation in the current applications market, ordinary developers and users may not fully comprehend the security risks and vulnerabilities in apk packages because of the professional terms used in the mobile application security domain. Hence it is difficult to conduct an in-depth evaluation and analysis on security in mobile phone applications. It is even more challenging to resolve the security issues in these applications one by one. The limited number of professional mobile application security engineers and the high costs involved means that the huge demand generated from the need to assess the security features of a large number of applications cannot be met.

Building on the technology and experience Bangcle Security has acquired over the years from studying Android security issues, the company has launched an automated security testing platform for Android applications to manage the security issues in these applications. The main purpose of this platform is to provide an automated and comprehensive means of security testing to help application developers understand the security issues inherent in their own applications and to identify the methods to fix these issues. The platform can also help organizations to detect and evaluate the security level of a large number of applications. Thus, this platform helps to serve a gap in the applications market by monitoring security threats and providing early warnings of potential security issues inherent in these applications.

2 Features

Bangcle Security MobSPA provides developers with a convenient, intelligent and comprehensive evaluation method. The evaluation table is wholly designed for use in application programs in the Android system, and the developers only need to submit the apk documents related to the application they are working on to the platform, and the evaluation platform will automatically start the tests and assess the apk based on key security indicators. For each evaluation item, the evaluation results include the evaluation goals, the dangers that each item may create details and the corresponding solutions. The results will also assign an overall security score for the evaluated application.

Bangcle Security MobSPA can perform a comprehensive evaluation on mainstream security issues that the application may face, and it can accurately pinpoint the source of these security issues and obtain the relevant solutions. At the same time, automated testing is very efficient and convenient as many applications can be quickly and automatically tested in batches, while statistics can be collated for the many applications tested in the same batch. Whether it is to evaluate a single application or multiple applications, the system can provide automated official reporting documents.

The platform supports both private and public cloud deployment, as well as direct access to the public cloud for delivery. It also supports system upgrades in order to respond to unexpected security issues in the Android market. Private cloud deployment can be upgraded using the local file system, while public cloud deployment can be upgraded either locally or online.

The following describes MobSPA key features.

2.1 Automated Assessment Items

Bangcle Security MobSPA provides developers three main categories of evaluation items, namely security testing, risk assessment and vulnerability scanning. Automated evaluation item can be selected from the settings page.

2.1.1 Security Testing

Checks the APK to determine if the internal behavior of the application complies with security regulations. Such internal behavior can lead to information breach, permissions confusion, and injection of sensitive

content, virus or advertisements. There are 7 automated evaluation items, including:

- App information
- Permissions tests
- Behavior tests
- Sensitive word detection
- Virus detection
- Third party SDK detection
- Advertisement SDK detection

2.1.2 Risk Assessment

Assess the risks of external attacks for the current apk implementation. Presently, such risks are the most common type of security risks in the apk application environment, where illegal operations such as repackaging, theft of sensitive data and tampering of user data can happen. There are 22 automated risk test items, including

- Reverse engineering the Java code
- Decipher shared objects (.so) files
- Tampering and repackaging
- Dynamic injection attack
- Screen hijacking
- Key logger
- Insecure transport layer protocol
- Webview security: Passwords stored in plaintext
- Presenting digital certificate in plaintext
- Information disclosure through log debugging
- Exposure of resource files
- Dynamic debugger attack
- Activity component security
- Service component security
- BroadcastReceiver security
- ContentProvider security

- Application signature verification check
- Unrestricted backup/restore file
- Sensitive function call
- Risk of dynamic debugging at java layer
- Loading .dex file from SDcards
- Implicit calls of Intent component

2.1.3 Vulnerability Scanning

Analyze the apk to determine if there is any available technical vulnerabilities when the code is implemented. Hackers can make use of such vulnerabilities to attack the application, perform unauthorized operations, cause the application to fail, steal data, and others. There are 13 automated executable items in this segment

- Webview security: remote code execution
- SQL injection
- ContentProvider data leakage
- Encryption algorithm mode check
- SSL certificate validation
- Unrestricted apk download through app
- World readable and writable files
- In device denial of service attack
- Internal network testing information
- Webview security: bypass certificate validation
- Random number vulnerability check
- Intent scheme URL attack
- Fragment injection attack

2.2 Display Test Results

The evaluation results for Bangcle Security MobSPA can be browsed online, and the official evaluation report can be downloaded in both MSWord and PDF formats.

Based on the user's level of authorization, the platform can provide two kinds of evaluation reports, including a detailed evaluation report for a single application, as well as the statistics from evaluating multiple applications.

2.3 System Upgrade

Bangcle Security MobSPA can be upgraded in two ways, either online remotely or offline using local files. Together with the platform's ability to rapidly expand the evaluation items, the user can upgrade quickly in order to conduct a comprehensive assessment that covers all the security issues in the market.

3 Value Proposition

Bangcle Security MobSPA offers great value to customers who are concerned about mobile security.

3.1 Comprehensive coverage with the ability to pinpoint security issues accurately

It can effectively identify the main security issues in the application, and accurately pinpoint the source of the problem, and this is useful for monitoring and to provide early warnings of the security issues in the application.

3.2 Protect customer's data privacy

Both private cloud and local independent deployment are supported so that information about the user's application and the evaluation results can be completely isolated so as to protect the user's data privacy and security.

3.3 Efficient performance that saves time

Evaluation time is short, and the results of the application security evaluation can be obtained immediately. Hence, it eliminates the waiting time so that the user can quickly detect and repair security issues in the application.

3.4 Cost savings with no manual operation

Automatic single-key operation without the need for participation by professional security personnel, and this significantly reduces manpower costs

and technology learning costs.

3.5 Timely response to security issues in the market

Supports the rapid expansion of evaluation items so that the detection of unexpected security issues can be added in time for the evaluation of the application. Functions can be upgraded remotely or locally. This provides a timely response to mobile application security issues in the market.

3.6 Big data scanning to grasp trending vulnerabilities

The capability can be extended with a hardware server to perform security evaluations for a massive number of applications, and collate the statistics from the batch evaluation results to offer an insight into the distribution and trends in terms of vulnerabilities in applications.

4 Application Scenarios

4.1 Application Scenario - Evaluation Agencies

- ***Customer type***: Evaluation organizations, application security evaluation entities
- ***Customer requirement***: Perform evaluation for a large number of applications.
- ***Why product is a fit***: Evaluation items cover current mainstream security issues;
    - Automated evaluation can quickly and efficiently handle a large number of test requirements;
    - Can be deployed independently to protect data privacy.

4.2 Application Scenario - Regulatory agencies

- ***Customer type***: Information security regulators
- ***Customer requirement***: To analyze and compile statistics on security issues for specific type of applications in the market or for a specific industry.
- ***Why product is a fit***: An automated solution is the best as there is a huge number of industry-type applications to be evaluated;
    - APIs are available where the evaluation system will complete the evaluation of core security issues and return the evaluation results and statistical data to the customer;
    - Can be combined with channel monitoring systems for large data collection and analysis.

4.3 Application Scenario - Large corporations like banks

- ***Customer type***: Large corporations like banks with applications that have many users
- ***Customer requirements***: To evaluate the numerous applications offered by the corporation to improve the security features in these applications.
- ***Why product is a fit***: A fast automated evaluation system that supports continuous testing and iterations;
    - Independent deployment to ensure the security of the application code;
    - Evaluation items can be customized according to requirements.

4.4 Application Scenario - Small and medium enterprises and individual developers

- ***Customer type***: Small and medium enterprises and individual developers
- ***Customer requirements***: To evaluate the applications they develop to improve the security features in these applications; Unable to afford an independent deployment or maintain a security team.
- ***Why product is a fit***: Online testing platform using cloud account is available where the cost is lower;
    - Ability to offer specific period of use for individual accounts and limited number of tests;
    - Evaluation items cover the current mainstream security issues and can pinpoint the issue accurately

5 System Requirements

5.1 Hardware requirements

	Lowest configuration (evaluation task does not support concurrency)	**Recommended configuration (evaluation task supports 3 concurrent sessions)**
CPU	Quad-core, clock speed of 2.8 or higher	Octa-core, clock speed of 3.5 or higher
Memory	8G	16G
Hard disk	200G	500G
Number of Servers	1	3
Bandwidth	4M	12M

5.2 Software requirements

- ubuntu = 12.04_x86_64 server
- python >= 2.7.3
- Java(TM) SE Runtime Environment 1.7
- Rabbitmq >= 2.7.0
- Android SDK = 4.1