Research on Android Application Security Protection in China

Wenjie Song* and Hao Li
Technology Center, NARI Group Corporation, 211106 NanJing, China

ABSTRACT

With the development of mobile internet, it is necessary to take mobile application security into consideration as a strategic focus of enterprise’s IT construction. This article firstly introduces the establishment of mobile security standard and guidance. Then a lifecycle security protection from five perspectives is presented in detail to help to implement security strategies and solutions, including security assessment, security development, security test, security reinforcement and security monitoring. Finally, new security technique and tendency of mobile application is discussed to provide enterprise IT manager with more ideas.

INTRODUCTION

According to the statistical figure of Statista [1], as of March 2017, there are 2.8 million apps in Google Play. The Apple Store also has gone from 800 apps in July 2008 to 2.2 million in January 2017. The explosive growth in the number of mobile application increases the security attack surface. A mobile security project, Open Web Application Security Project (OWASP) lists a top 10 mobile risks subproject is provided, including following security aspects: improper platform usage, insecure data storage, insecure communication, insecure authentication, insufficient cryptography, insecure authorization, client code quality, code tampering, reverse engineering, extraneous functionality [2].

However, a mobile security report presented by NowSecure mentions 24.7 percent of mobile apps include at least one high-risk security flaw and 35 percent of communications sent by mobile devices are unencrypted [3]. The reason is clear that application builders and information security defenders aren’t always on the same page. A vulnerability and data leakage status report of mobile app security released by FreeBuf in June 2017 shows a very real situation that 69 percent of APP developers think safety is the work of others [4]. Many information security engineers don’t understand software development, most application developers don’t understand security. Builders and defenders have fundamentally different drivers. Builders and their managers are focused on delivering features and meeting time-to-market expectations, rather than on making sure that software is secure.

In this article, we firstly introduce the establishment of mobile security standard and guidance. Then a lifecycle security protection from five perspectives will be presented in detail to help application developers and security engineers work in collaboration to implement security strategies and solutions, including security assessment, security development, security test, security reinforcement and security monitoring. Finally, we will discuss new technology and tendency of mobile application security in future.
STANDARD AND GUIDANCE

In recent years, research on Android security has increased dramatically. Papers from conference, periodicals and network cover a wide area. In [5,7], authors summarized and analyzed the advances in Android security from multidimensional perspective, covering security model, Android architecture, major threats, etc. While these are targeted towards detailed analysis techniques, the establishment of mobile security standard and guidance is less concerned. We searched papers for the overview and analyze of mobile application security standard and the number is a lot less.

Ning summarized the overview of mobile internet security standard [8]. The National Information Assurance Partnership (NIAP), which is developed to help improve information system and network security, has released some protection profiles for mobile security like “Protection Profile of Mobile Device Fundamentals Version 3.1” [9], “Protection Profile for Mobile Device Management Version 3.0” [10], “Protection Profile for Application Software Version 1.2” [11], etc. The National Institute of Standards and Technology (NIST) uses special publication subseries to publish mobile security and guidelines. For example, “Vetting the Security of Mobile Applications” (SP 800-163) [12] is a guide to help organizations vet mobile applications and ensure that they are able to properly assess the security and privacy risks associated with mobile apps. Related guidelines includes SP 800-124 Revision 1 [13], SP 800-46 Revision 2 [14] and so on as well.

![Diagram](image)

Figure 1. Security architecture of mobile smart terminal.

In China, the standard GB/T 32927-2016 is released to put forward the security architecture (see Figure 1) and describe security requirements of mobile smart terminal, referring to early drafted YD/T 1699-2007, YD/T 2407-2013, YD/T 2408-2013, etc. YD/T 1699-2007 includes general security requirements of terminal hardware, terminal software, operating system and mobile application. YD/T 1700-2007 is the other one standard of this series which provides the testing methods for the requirements referred in YD/T 1699-2007, mobile terminal access security, information transmission security and mobile terminal personal information security. YD/T 2407-2013 and YD/T 2408-2013 provides the requirements and testing methods for smart mobile terminal including the object of peripheral interface and user data in addition. YD/T 2407-2013 and YD/T 2408-2013 provides the requirements and testing methods for smart mobile terminal including the object of peripheral interface and user data in addition. YD/T 3039-2016 is the first standard released for smart mobile terminal application which belongs to a series standard including YD/T 2674-2013, YD/T 2407-2013, YD/T 2408-2013, YD/T 1886-2009 and some standards that are being revised like “code signature technical requirements for mobile application”, “testing methods for code signature of mobile application” and “evaluation methods for software security of mobile application”. TABLE I shows the title of these standards.
According to the current establishment of standard and guidance, most standards are referred in mobile terminal level. Standard formulation lags behind current mobile application development which results in a lack of specification in mobile application market. China is gradually taking steps to standardize mobile application development requirements. In July 2016, China Academy of Information and Communications Technology (CAICT) submits an application of the standard of mobile application development security capability assessment method to China Communications Standards Association (CCSA). The project has been included in the first batch of revision plan in 2017. In September 2016, Shanghai Information Security Testing Evaluation and Certification Center officially releases the “software safety general technical specifications for mobile Internet applications”, putting forward the general safety requirements from two aspects of technique and management for mobile applications in design, development and testing.

SECURITY PROTECTION

Security Assessment

Security assessment is an approach for security engineers to understand and mitigate mobile security threats and risks according to the safety requirements. The purpose for assessment is to prevent potential security events and take methods to the risks that have occurred. LIU discusses the framework and method of security test and evaluation for the mobile application software from the aspects of source code, security function, program protection, data protection, standard compliance and vulnerability monitoring [15]. CHANG proposes the mobile application security assessment method, including the client security, server security and business process security [16]. These papers are focusing on detail assessment items. Form different perspectives, we propose a framework through the lifecycle of mobile application.

<table>
<thead>
<tr>
<th>Number</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>YD/T 1699-2007</td>
<td>information security technical specification for mobile terminal</td>
</tr>
<tr>
<td>YD/T 1700-2007</td>
<td>testing methods for mobile terminal information security</td>
</tr>
<tr>
<td>YD/T 1886-2009</td>
<td>security requirements and test specification for system on chip in mobile terminal</td>
</tr>
<tr>
<td>YD/T 2407-2013</td>
<td>technical requirements for security capability of smart mobile terminal</td>
</tr>
<tr>
<td>YD/T 2408-2013</td>
<td>test methods for security capability of smart mobile terminal</td>
</tr>
<tr>
<td>YD/T 2674-2013</td>
<td>design guidance of information security for smart mobile terminals</td>
</tr>
<tr>
<td>GB/T 32927-2016</td>
<td>information security technology—security architecture of mobile smart terminal</td>
</tr>
<tr>
<td>YD/T 3039-2016</td>
<td>security technical requirements for smart mobile terminal applications</td>
</tr>
</tbody>
</table>
Figure 2. Security assessment framework of mobile application.

In Figure 2, the framework is divided into four parts. Development assessment requires safety infrastructure in the matter of environment and coding specification. Application assessment is at the very core of the framework, including program analysis and reinforcement strategies. Compliance assessment is used to avoid the compliance risks of the business because of the misunderstanding of correlative policy and insufficient ability of security technique and the application should comply with national and industry standards which is discussed in the last chapter. Risk disposition is not about security technique but security management, including security knowledge training, monitoring of application market and prepared emergency plan to those emergent conditions. In the following section, we will introduce the definition and common methods and tools used to implement the protection of Android application.

Security Development

In this section, we will discuss how to develop security from the development environment, coding principles, source code management and application client in a developer's perspective.

1. Development environment: to prevent the XcodeGhost event from happening again, unofficial softwares and tools are strictly prohibited. The test environment and production environment requires independence, and production data is not allowed to be copied into the test environment. Authority management is indispensable for user account in the development and test environment.

2. Coding principle: validation of data entry, exception handling and secure coding specification are the key points of coding principle. Android application developers may follow the standard of the google java style guide [17].

3. Source code management: version control of the source code and disaster recovery mechanism need to be established. All test interfaces and code fragments should be deleted before release.

4. Application client: The client security contains the following aspects: data storage, transmission, authentication, authorization and so on. TABLE II shows the detailed security requirements.
TABLE II. SECURITY DEVELOPMENT REQUIREMENTS.

<table>
<thead>
<tr>
<th>Content</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Storage</td>
<td>sensitive local data is encrypted to store and select the appropriate encryption algorithm</td>
</tr>
<tr>
<td>Transmission</td>
<td>SSL/TLS encryption for sensitive information transmission and verifies the validity of SSL certificates</td>
</tr>
<tr>
<td>Authentication and Authorization</td>
<td>security storage protection of key and password, suitable security authentication, security session mechanism and no overauthorization</td>
</tr>
<tr>
<td>Data upload</td>
<td>limited upload function and review of the compliance of uploaded data</td>
</tr>
<tr>
<td>WebView</td>
<td>traditional web security for SQL injection, XSS, CSRF, etc.</td>
</tr>
<tr>
<td>Oxynger KeyShield</td>
<td>prevention of keyboard hijacking and screenshots</td>
</tr>
<tr>
<td>Integrity Checking</td>
<td>check integrity of the application when it is started and updated to prevent it from being tampered with</td>
</tr>
</tbody>
</table>

Security Test

The type of security test used in security domain could be static or dynamic [18]. Static test examines the program structure to reason about its potential behaviors. A decompilation of the application with tools like APK Tool and dex2jar is used to scan and analyse anti-compiled Java files, XML files and other files. Dynamic test executes the program to observe its actual behaviors at runtime. The application will be run independently by using sandbox or virtual machine. In [19], authors suggest sub-dimensions that further classify these two categories from related references, including analysis data structures, sensitivity of analysis, code representation, inspection level and input generation technique. The first three classify static analysis techniques and the next two are applied to dynamic analyses.

The advantage of using automated static tools is to make it possible to large-scale code inspections. But this method mainly depends on the keyword matching, if there is a lack of context analysis or developers just define a function of the same keywords or the code that has loopholes has not been called at all, there will be misreporting in the result. In addition, if the dynamic detection is unable to cover most of the application interface and functions to generate effective business data, there will be a large number of omission. Actually, for program analysis, it is preferred to not miss any potential security threat, even at the cost of generating false warnings.

TABLE III. SECURITY TESTING TECHNOLOGY AND TOOL.

<table>
<thead>
<tr>
<th>Content</th>
<th>Detail</th>
<th>Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuzzy Testing</td>
<td>Often used in binary vulnerability mining. In mobile security domain, it is usually used in mining system component vulnerabilities, vulnerabilities of file resolution class and third-party component vulnerabilities</td>
<td>PeachFuzzer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Afl-fuzz</td>
</tr>
<tr>
<td>Taint Analysis</td>
<td>Often used in the analysis of malicious application and information leak detection. It is also being used for vulnerability detection</td>
<td>TaintDroid</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FlowDroid</td>
</tr>
<tr>
<td>Unpacking</td>
<td>Static analysis of the APP code can not be done without automated unpacking or even run on the simulator for dynamic analysis</td>
<td>ZjDroid</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DexHunter</td>
</tr>
</tbody>
</table>

Since 2015, the development of the online platform provided by security companies such as 360, alibaba, tencent, etc has made security test more convenient. Some open
source online platforms like MobSF and Drozer also reduce the cost of customized requirement. In TABLE III, fuzzy testing, taint analysis, general decription and other academic and industrial techniques have also been applied to security testing.

**Security Reinforcement**

Security reinforcement is used to enhance the anti-cracking ability by recompiling, adding shell protection and changing the sequence of instruction. The intensity and the compatibility should be balanced to avoid the consequence that the application is not available or running slowly. Core functions of the reinforcement consists of the following aspects.

1. Anti-reverse: reverse engineering can be used for creating a piratic application in a low price by analyze the structure of the original application. Shell technique is the basic method to protect application from being reversed by decompilation tool.

2. Anti-tamper: code tampering, resource file tampering and signature tampering are main contents. Once the file of the application is changed by hacker, anti-tamper mechanism will be triggered to stop the running of the application.

3. Anti-debug: techniques and tools are developed to prevent malicious code injection or code falsifications. However, these techniques also can be analyzed by using debuggers. Anti-debug technique is used to prevent reinforcement strategy being cracked at the debug level.

   WU proposed an reinforcement scheme base on DEX files’ dynamic loading to resist reverse attack [20]. But with DEX unpack tools based on Android source code emerging endlessly, cracking DEX codes becomes more easier, developers turn to pay more attention to native layer dynamic link library file. Based on executable and linking format and the research on linker on the Android platform, HAN gives a SO reinforcement scheme based on specific function protection [21]. Actually, to improve the ability of security reinforcement, anti-reverse, anti-tamper and anti-debug technique should be integrated in the comprehensive solution [22, 23].

   Attackers can still obtain the complete decrypted DEX file from memory by dump technology. When the complete DEX file is cracked, hackers will get sensitive information and data of the application. The virtual machine technology called VMProtect is referred to increase the complexity of the software after the packer process, which improves the difficulty of reverse analysis [24].

**Security Monitoring**

Security monitoring includes piracy monitoring, vulnerability monitoring and mobile situational awareness. Piracy monitoring is a real-time monitoring of phishing and pirated applications released on the application market. Vulnerability monitoring aims at getting the information of vulnerabilities from well-known platform like CVE, CNCERT and MetaPloit in time. These kind of passive monitoring provides limited defense against those hackers with clear economic or political purpose. Security event like XcodeGhost has made developers realize organized and premeditated attack need more active ways like information collecting, hacker tracing and behavior analyzing to build an all-around situational awareness mechanism for security monitoring called mobile situational awareness. ZHANG proposed a framework of mobile terminal’s situational awareness on the basis of analyzing the security situation of mobile internet.
She designed and implement a prototype system of mobile security situational awareness based on Android which is an exploration and practice in the field of mobile situational awareness [25].

**CONCLUSIONS**

This paper firstly states the standard and guidance establishment of mobile terminal and application.

![Figure 3. Standard establishment of mobile terminal in China.](image)

Figure 3 shows the development history of mobile terminal standard and guidance in China. With the release of network security law in 2016, mobile application security requirements have been referred as very important content by law. The protection has transitioned from compliance-driven to compulsion-driven. Although the security production is in its initial stage in China, the lifecycle production scheme is gradually becoming the general solution to IT manager for mobile application. We propose a security assessment framework through lifecyle of application development, test, reinforcement and monitoring and discuss the definition and solution of each issue in detail. We listed some well-known tools and research to help IT manager to design and implement security strategies and solutions faster and directly.

In the future, a more robust and intelligent system for mobile application security protection will be built. For example, hybrid approaches combining static and dynamic methods and machine learning like SVM [26] are the most widely used techniques. Also the precision of program analysis needs to be improved by scale up the number and complication of application. Finally, there is no definite security in this world. Endless loopholes and vulnerability will be found and used by hackers. Sharing of security research and information is significant to effectively compete against those hackers.

**REFERENCES**