Basic Security Baseline for Mobile Applications

V1.4

Industrial Development Bureau, Ministry of Economic Affairs

2020

History of Basic Security Baseline for Mobile Applications Revision

Date	Basic Security Baseline for Mobile Applications Revision
April 2015	V1.0
October 2016	V1.1
May 2018	V1.2
Sept 2020	V1.4

Table of Contents

1. Introduction

The mobile device has made people’s life convenient and has become indispensable. Various mobile applications (Apps) have emerged as the times require, but some programmers lack security awareness about developing the applications. Thus, the relevant security issues are not considered, which may result in the risk of leakage of user data or financial loss. Industrial Development Bureau, Ministry of Economic Affairs actively studied and planed the "Security Regulations for Mobile Application" based on the 26th Council Meeting of National Information & Communication Security Taskforce on June 24, 2014.

In this way, Industrial Development Bureau, Ministry of Economic Affairs authorized Institute for Information Industry to set up a task force formed by domestic experts in the field of security, to consider the international relevant security standards and guidelines, and to carry out the compilation of this regulation. At each stage of revision, through expert forums and public seminars, we sought advice from the industry, government, and research institutes, and listened to opinions broadly. According to those, we have revised and completed this regulation for the industry to adopt voluntarily while developing applications by themselves. This regulation has been revised to V1.2 in May 2018.

This regulation is non-mandatory. The main purpose is to improve the basic security protection capability of our country's mobile applications. From the initial stage of design, the basic concept of capital security is introduced, and the key elements of the regulation are used to remind App developers to strengthen basic security awareness and gradually improve APP security protection.

This regulation includes six security benchmarks, namely, "Mobile Application Release Security", "Protection of Sensitive Data", "Transaction Resource Security Controls", "Identity Authentication and Authorization, and Connection Management Security of Mobile Application Users", "Security of Mobile

Application Code", and "Server-side Security Testing". Application developers can refer to the regulation, improve the security quality of the mobile application, enhance trust and willingness of users to use the applications, and create a win-win situation for developers and users.

2. Applicability

This regulation addresses basic information security requirements for mobile applications on the mobile device side and includes information security requirements on the server-side.

This regulation applies to non-specific[1] mobile applications and common features[2] of mobile applications. Applications for specific areas and the information security regulations required for their domain should be set by the respective business authorities.

This regulation is a basic information security guideline for operators of mobile applications, and it is a voluntary guideline that can be followed by industry.

[1] Specific : Refers to a specific area, regulated by specific authorities and laws, such as finance, medical, taxation, etc.

[2] Common features：Refers to the common functions and similar basic functions required for the operation of mobile applications, such as data storage and transmission protection mechanisms or user identity authentication mechanism, etc.

3. Terms and Definitions

3.1. Mobile Application

A designed application for smartphones, tablet PCs, and other mobile devices.

3.2. Application Store

A platform or website in the built-in device for mobile device users to browse, download, and purchase.

3.3. Personal Data

According to the "Personal Information Protection Act", all individual's data could be recognized directly or indirectly, included, but not limited to the name of a natural person, date of birth, national identity card number, passport number, characteristics, fingerprints, marriage, family, education, occupation, medical history, medical care, gene, sex life, health checks, criminal record, contact information, financial status, social activities, International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), and other information that directly or indirectly identify the individual.

3.4. Sensitive Data

Information that is created, stored, or transmitted by the mobile device and its associated storage media due to the user's actions or the operation of the mobile application, which may cause the leakage of the information and further cause damage to the user. Except for the definition of personal data defined in 3.3., the user’s information includes, but not limits to passwords, keys, video, photos, calls, audio files, instant messaging messages, call history, texting, memos, contacts, notes, geographic locations, calendars, device identifiers, and other relevant information about personal privacy.

3.5. Password

A set of characters that allow the user to use the system or to identify the users, including the password of the local stored encrypted data, account and

password of users, account, and password of remote web service.

3.6. Transaction Resource

The additional features, content, or subscriptions that are available directly or indirectly by purchasing in the mobile app. Transaction Resource is defined as a monetary event, whether it is a virtual or physical currency (including points or serial numbers) and other valuable items. For example, if a ticket is purchased in the ticketing system, a set of QR codes can be used as a voucher for the ticket. If the e-book is purchased in the online bookstore App, the content of the e-book can be read. To subscribe or purchase the transaction service item in the App, it provides new features, removes the use restriction function, or remove the advertising function after the transaction. Or the payment network app provides the payment function; the bank type app provides the transfer or the app provides the function of purchasing the entity or virtual goods.

3.7. Session Identification, Session ID

The identification code is assigned to the connection when the connection is established and is used as the unique identification code during the connection. When the connection ends, the identification code can be released and reassigned to the new connection.

3.8. Server Certificate

The signature verification data, providing mobile application authentication server identity and data transmission encryption.

3.9. Certificate Authority

The authority or legal person that issues the certificate.

3.10. Malicious Code

The infringement of user rights without the user's consent, including but not limited to any code with malicious features or behavior.

3.11. Vulnerability

The flaws in the security of mobile applications, threatening the confidentiality, integrity, and availability of a system or mobile application data.

3.12. Library

Involving or packaging a complex or hardware-related program into a function or an object and compiling it into binary code to provide the code to the programmer.

3.13. Code Injection

The malicious instructions entered by the user due to a fault in the mobile application design, including but not limited to Command Injection and SQL Injection.

3.14. Mobile Operating System

The operating systems that operate on mobile devices.

3.15. Mobile Resource

The functions or services provided by mobile devices, including but not limited to cameras, photos, microphones, wireless networks, sensors, and geographic locations.

3.16. In-App Update

Update the mobile application content and features through a customized method without updating the major version released in the mobile application store.

3.17. Common Vulnerabilities and Exposures

Referred to as "CVE". The vulnerability management program sponsored by the US Department of Homeland Security, the only common number recognized globally for each vulnerability project.

3.18. Secure Encryption Function

An encryption function that conforms to FIPS 140-2 Annex A.

3.19. Known Vulnerabilities

A vulnerability with a CVE number.

3.20. Authentication

The guarantee of the identity claimed by the individual.

3.21. Advanced Encryption Standard

The National Institute of Standards and Technology (NIST) in 2001 released in the AES (Advanced Encryption Standard) encryption algorithm, file number FIPS PUB 197 standard, and officially implemented in 2002. AES can support 128-bit Data Block and support 128, 192, and 256-bit Key Size for improved security. AES encryption and decryption contains more than ten Round Numbers. Each round contains four main basic units.

3.22. Triple Data Encryption Standard

A product cipher method uses a Triple Data Encryption Standard to process 64-bit data blocks.

3.23. Elliptic Curve Cryptography

An algorithm establishes public-key cryptography, which is an additive group or mathematical structure generated by an elliptic curve. The use of elliptic curves in cryptography was proposed by Neal Koblitz and Victor Miller in 1985, respectively.

3.24. Certificate Pinning

The server voucher pre-stored in the application is used to confirm whether it matches the server voucher when connecting.

3.25. Hash

The data fingerprint calculated by an algorithm in a series of data, often used to identify whether files and materials have been tampered with to ensure that the files and materials are indeed provided by the original.

3.26. Obfuscation

Conversion of the mobile application source code to an unreadable form without affecting function execution.

3.27. Using Sensitive Data

The application uses the data for itself or provides it to third parties.

3.28. Log File

System logs, application logs, security logs, debug logs, or custom log files for debugging purposes only.

3.29. Device Identifier

Refers to the unique identification information of hardware or software, including International Mobile Equipment Identity (IMEI), Mobile Equipment Identifier (MEID), International Mobile Subscriber Identity (IMSI), Integrated Circuit Card Identifier (ICCID), Media Access Control Address (MAC address), Android Identifier (Android ID), Android System Advertising ID (Android Advertising ID, AID), iOS IFAID (Identifier for Advertisers Identifier, IFAID), and Windows Phone Device ID.

3.30. Cache Files or Temporary Files

The files that are generated by the mobile application and are not related to the functionality of the application. They are usually deleted at the end of the application. The existence of this file does not affect the functionality and performance of the mobile application when it is executed again, such as temporary archiving or cache. Besides, if deleting a file causes the automatic login function to be invalid, the file should belong to the profile instead of the cache file or temporary file.

3.31. Configuration File

The file that the mobile application stores the relevant settings of the mobile application, which will affect the performance of the function when the mobile application is executed again.

3.32. Encode

The action of converting data into code or characters, and the code or character can be translated or resolved into the original data.

3.33. Decode

The action of translating the encoded code or character into the original data.

3.34. Payload

The valid information or instructions in the contents of a package, a message, or a part of code.

3.35. Collecting Sensitive Data

The mobile application obtains Sensitive Data built into the mobile device or input by the user.

3.36. Storing Sensitive Data

Storing the Sensitive Data as a file to the mobile device or a subsidiary storage media.

3.37. Common Vulnerability Scoring System

Referred to as "CVSS". It uses the characteristics and the impact of IT vulnerabilities to score. It is developed by the National Infrastructure Advisory Council (NIAC), now transferred to the Forum of Incident Response and Security Teams (FIRST). Currently, it is the third edition.

3.38. Secure Random Number Generator

A random number generation function that conforms to or references the ANSI

X9.17 standard.

3.39. Secure Domain

The applicability includes developers and customer-owned domains, or commonly well-known public domains. Commonly well-known public domains include applications that support the OAuth 2.0 protocol, such as Facebook, Google, or Twitter.

4. Technical Requirements

4.1. Mobile Application Information Security Technology Requirements

This section is intended for different mobile applications for the technical requirements of security, including the five-oriented: "Mobile Application Release Security", "Protection of Sensitive Data", "Transaction Resource Security Controls", "Identity Authentication and Authorization, and Connection Management Security of Mobile Application Users" and "Security of Mobile Application Code".

4.1.1. Mobile Application Release Security

This mainly applies to Information Security requirements for the released mobile application, including the release, updates, and the problem in return.

4.1.1.1. Mobile Application Release

Mobile applications shall be released in reliable App Stores.

Mobile applications, when released, shall be noted the Sensitive Data accessed by applications, the mobile device resources, and the declaration of the permission and purposes.

4.1.1.2. Mobile Application Update

Mobile applications shall be released the updates to reliable App Stores.

Mobile applications shall provide an update mechanism and notify active announcements when security updates.

4.1.1.3. Mobile Application Security Issues in Return

Mobile application developers should provide a channel of return on security issues.

Mobile application developers should respond and improve the problem within a reasonable period.

4.1.2. Protection of Sensitive Data

This applies mainly for Sensitive Data and personal data related to technical requirements of information security, including collection, use, storage, transmission, sharing, and deletion of Sensitive Data.

4.1.2.1. Sensitive Data Collection

Before the mobile applications collect Sensitive Data, they should get users' consent and provide the users the right to refuse them.

4.1.2.2. Sensitive Data Usage

Before the mobile applications use Sensitive Data, they must obtain the users' consent and provide the users the right to refuse them.

If mobile applications use password authentication, they should actively remind the users to set more complex passwords.

Mobile applications should remind users to regularly change their passwords.

4.1.2.3. Sensitive Data Storage

System credentials storage facilities are used to appropriately to store sensitive data, such as PII, user credentials, or cryptographic keys.

The keyboard cache is disabled on text inputs that process sensitive data.

No sensitive data is exposed via the IPC mechanism.

No sensitive data, such as passwords or pins, is exposed through the user interface.

Before the mobile applications store Sensitive Data, they should get users' consent and provide the users the right to refuse them.

Sensitive Data stored in mobile applications should be used only for the intended use statement.

Sensitive Data stored in mobile applications should avoid redundant

Sensitive Data stored in log files or archives.

Sensitive Data should adopt appropriate and effective length of the key and encryption algorithm, and it should be encrypted before saving.

Sensitive Data should be stored in a protected area by the operating system to prevent unauthorized access from other mobile applications.

Sensitive Data should be avoided in the code of mobile applications.

Mobile applications should take the initiative to alert the user when capturing the screen, and should remove sensitive data from views when moved to the background.

The app enforces a minimum device-access-security policy, such as requiring the user to set a device passcode.

4.1.2.4. Sensitive Data Transmission

Mobile applications transmitting Sensitive Data through the Internet should be encrypted by using an appropriate and effective key length of the encryption algorithm.

4.1.2.5. Sensitive Data Sharing

Different mobile applications within mobile devices should get users' consent and provide the users the right to refuse them before sharing sensitive data.

When mobile applications share Sensitive Data, they should prevent unauthorized access from other mobile applications.

4.1.2.6. Sensitive Data Deletion

The function of deletion should be provided if mobile applications store users' Sensitive Data.

4.1.3. Transaction Resource Security Controls

This is mainly applied for the related information security testing standard on

transaction resource controls, including the use and controls of transaction resources.

4.1.3.1. Use of Transaction Resources

Mobile applications should proactively notify users before using transaction resources and provide the user the right to refuse it.

4.1.3.2. Transaction Resources Control Management

Mobile applications should identify users before using transaction resources.

Mobile applications should record the transaction resources and time after using transaction resources.

4.1.4. Identity Authentication and Authorization, and Connection Management Security of Mobile Application Users

This is mainly applied for mobile applications related to information security technical requirements of identity authentication and authorization, and connection management, including identity authentication and authorization, and connection management mechanisms.

4.1.4.1. User Identity Authentication and Authorization

Mobile Applications should have appropriate identity authentication mechanisms to confirm users' identities and authorize users depending on users' identities.

4.1.4.2. Connection Management Mechanism

Mobile Applications should avoid session identification code with regularity.

Mobile Applications should confirm the validity of the server's certificate.

A certificate of mobile applications connecting to the server shall be issued by the trusted certificate authority.

Mobile Applications should avoid connecting and transmitting data with the

server with no valid certificate.

4.1.5. Security of Mobile Application Code

This mainly applied for the Information Security requirements for developing mobile applications, including protection against malicious code and preventing information security vulnerabilities, mobile application integrity, library reference security, and user input validation.

4.1.5.1. Protection against Malicious Code and Prevention for Information Security Vulnerabilities

Mobile Applications should avoid products containing malicious code.

Mobile Applications should avoid information security vulnerabilities.

4.1.5.2. Mobile Application Integrity

Mobile Applications should use appropriate and effective verification mechanisms to ensure integrity.

4.1.5.3. Reference Library Security

When updating the reference library of mobile applications, they should prepare for an updated version. As for updating requirements, please refer to Mobile Application Release Security.

4.1.5.4. User Input Validation

Mobile applications should check the security and provide relevant injection attack protection mechanism when user input strings during the input stages.

4.1.5.5. Protection Against Dynamic Analysis and Tampering

The application detects, and responds to, the presence of a rooted, jailbroken, or improperly secured device either by alerting the user or terminating the app.

The app detects, and responds to, tampering with executable files and critical

data within its own sandbox.

The app detects, and responds to, the presence of widely used reverse engineering tools and frameworks on the device.

The app detects, and responds to, tampering the code and data in its own memory space.

The app implements multiple mechanisms in each defense category. Note that resiliency scales with the amount, diversity of the originality of the mechanisms used.

All executable files and libraries belonging to the app are either encrypted on the file level and/or important code and data segments inside the executables are encrypted or packed. Trivial static analysis does not reveal important code or data.

If the goal of obfuscation is to protect sensitive computations, an obfuscation scheme is used that is both appropriate for the particular task and robust against manual and automated de-obfuscation methods, considering currently published research. The effectiveness of the obfuscation scheme must be verified through manual testing. Note that hardware-based isolation features are preferred over obfuscation whenever possible.

4.2. Server-side Information Security Technology Requirements

This regulation is intended to put forward the basic information security requirements for mobile applications. If mobile applications involve the need for information security on the server-side, it is suggested that the industry should self-declare or decide its server-side protection and information security management measures, or issue the third-party certificate to prove the information security and management of their server-side service.

4.2.1. Server-side Security Management

Server-side security is suggested to aim at the applications and services to do the threat model analysis of the application and service to identify security risks to the service, to implement the necessary follow-up and effective control measures.

4.2.2. Server-side Security Testing

The nature of the server-side mobile application platform is websites and web service server. Without proper secure design and development, there will be vulnerabilities like traditional web applications. Therefore, in the server-side security testing, the developer may use appropriate penetration test mode for testing.

4.2.2.1. WebView Security Testing

Mobile applications should use WebView to exchange web resources with a remote server.

When the mobile application rendering to WebView, the connection should be in Secure Domain.

5. Mobile Application Category

Different categories for mobile applications have different security requirements. This chapter distinguishes different types of applications with different requirements of information security, which have been divided into three categories, namely:

Level 1: no requiring the identity authentication of the mobile applications.

Level 2: requiring the identity authentication of the mobile applications.

Level 3: containing the mobile application transactions.

For each category for mobile applications, the definition should be consistent with the minimum set of technical requirements for information security matters; i.e., mobile applications should comply with the information security technology requirements under its category. The special cases that are not mentioned above will be explained separately in “Testing Standards”.

6. Reference Materials

Open Web Application Security Project (OWASP)

[1] Mobile Application Security Checklist 0.9.3

https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide, 2017

Cloud Security Alliance (CSA)

[2] Mobile Application Security Testing Initiative, https://www.csaapac.org/mast.html, 2016

United States

[3] Vetting the Security of Mobile Applications App, NIST Special Publication 800-163, http://dx.doi.org/10.6028/NIST.SP.800-163, 2015

[4] Cryptographic Algorithm Validation Program (CAVP), http://csrc.nist.gov/groups/STM/cavp/, NIST

[5] Cryptographic Module Validation Program (CMVP), http://csrc.nist.gov/groups/STM/cmvp/, NIST

[6] Government Mobile and Wireless Security Baseline, Federal CIO Council, https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf, 2013

Europe

[7] Smartphone Secure Development Guidelines, https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016, ENISA, 2017

China

[8] Wisdom mobile terminal security capabilities technical requirements, YD / T 2407-2013, 2013

[9] The mobile terminal security capability wisdom shift test method, YD / T 2408-2013, 2013

Japan

[10] Security Guideline for using Smartphones and Tablets - Advantages for workstyle innovation - [Version 1], https://www.jssec.org/dl/guidelines2012Enew_v1.0.pdf, JSSEC, 2011

International Standards

[11] ISO / IEC 27001: 2013 (Information security management)

[12] ISO / IEC 20000: 2011 (Information technology - Service management)

[13] ISO / IEC 19790: 2012 (Information technology - Security techniques - Security requirements for cryptographic modules)

[14] ISO / IEC 15408: 2009 (Information technology - Security techniques - Evaluation criteria for IT security)

[15] ISO / IEC 14598: 2001 (Information technology - Software product evaluation)

[16] ISO / IEC TR 9126-4: 2004 (Software engineering - Product quality)

Domestic Laws

[17] Personal Data Protection Act (December 30, 2015, Republic of China)

[18] Personal Data Protection Act Enforcement Rules (March 2, 2016, Republic of China)

Appendix I. Technical Requirements Table with Other Countries

TECHNICAL REQUIREMENTS	OWASP CORRESPONDING ITEM	US NIST [NOTE 1]	EUROPE ENISA [NOTE 2]	CHINA YD / T 2407-2013 [NOTE 3]
4.1.1.1. Mobile Application Release	N / A	Executive Summary	9. Secure Software Distribution	5.5.2 Requirements of Security Authentication Mechanism for Applications
4.1.1.2. Mobile Application Update	N / A	Executive Summary	9. Secure Software Distribution	5.5.4 Security Requirements of Pre-applications
4.1.1.3. Mobile Application Security Issues in Return	N / A	Executive Summary	9. Secure Software Distribution	5.5.4 Security Requirements of Pre-applications
4.1.2.1. Sensitive Data Collection	N / A	4. Mobile Application Evaluation - Privacy and Personally Identifiable Information	1. Identify and Protect Sensitive Data	5.5.4 Security Requirements of Pre-applications
4.1.2.2. Secure Sensitive Data Usage	V2.1: Verify that system credential storage facilities are used appropriately to store sensitive data, such as user credentials	4. Mobile Application Evaluation - Privacy and Personally Identifiable Information	1. Identify and Protect Sensitive Data	5.5.4 Security Requirements of Pre-applications 5.6.2 Authorized Access to User Data Files

TECHNICAL REQUIREMENTS	OWASP CORRESPONDING ITEM	US NIST [NOTE 1]	EUROPE ENISA [NOTE 2]	CHINA YD / T 2407-2013 [NOTE 3]
	or cryptographic keys			
4.1.2.3. Sensitive Data Storage	V2.1: Verify that system credential storage facilities are used appropriately to store sensitive data, such as user credentials or cryptographic keys	4. Mobile Application Evaluation - Protect Sensitive Data	1. Identify and Protect Sensitive Data on the Mobile Device	5.6.3 Storage of Users' Encrypted Data
4.1.2.4. Sensitive Data Transmission	V2.6: Verify that no sensitive data is exposed via IPC mechanisms	4. Mobile Application Evaluation - Protect Sensitive Data	4. Ensure Sensitive Data Protection in Transit	5.5.4 Security Requirements of Pre-applications 5.6.2 Authorized Access to User Data Files
4.1.2.5. Sensitive Data Sharing	V2.3: Verify that no sensitive data is shared with third parties unless it is a necessary part of the architecture	4. Mobile Application Evaluation - Preserve Privacy	1. Identify and Protect Sensitive Data on the Mobile Device	5.6.2 Authorized Access to User Data Files
4.1.2.6. Sensitive Data Deletion	V2.1: Verify that system credential storage facilities are	N / A	1. Identify and Protect Sensitive Data on the Mobile device	5.6.4 Complete Deletion of Users' Data

TECHNICAL REQUIREMENTS	OWASP CORRESPONDING ITEM	US NIST [NOTE 1]	EUROPE ENISA [NOTE 2]	CHINA YD / T 2407-2013 [NOTE 3]
	used appropriately to store sensitive data, such as user credentials or cryptographic keys			
4.1.3.1. Transaction Resources	V4.9: Verify that step-up authentication is required to enable actions that deal with sensitive data or transactions	N / A	8. Protect Paid resources	5.5.4 Security Requirements of Pre-applications
4.1.3.2. Transaction Resource Control Management	V4.9: Verify that step-up authentication is required to enable actions that deal with sensitive data or transactions	N / A	8. Protect Paid resources	5.5.4 Security Requirements of Pre-applications
4.1.4.1. User identity Authentication and Authorization	V4.1: Verify that if the app provides users with access to a remote service, an acceptable form of authentication such as	4. Mobile Application Evaluation - Privacy and Personally Identifiable Information	3. Handle Authentication and Authorization Factors Securely on the Device Correctly	5.6.2 Authorized Access to User Data Files

TECHNICAL REQUIREMENTS	OWASP CORRESPONDING ITEM	US NIST [NOTE 1]	EUROPE ENISA [NOTE 2]	CHINA YD / T 2407-2013 [NOTE 3]
	username/password authentication is performed at the remote endpoint			
4.1.4.2. Connection Management Mechanism	V5.4: Verify that the app either uses its certificate store, or pins the endpoint certificate or public key, and subsequently does not establish connections with endpoints that offer a different certificate or key, even if signed by a trusted CA	4. Mobile Application Evaluation - Network Events	2. User Authentication, Authorization and Session Management	5.5.4 Security Requirements of Pre-applications
4.1.5.1. Protection Against Malicious Code and Prevent Information Security Vulnerabilities	V1.7: Verify that a threat model for the mobile applications and the associated remote services, which identifies potential	4. Mobile Application Evaluation: Malicious Functionality Malware Detection Communication with Known Disreputable	6. Secure Data Integration with Third-Party Code 10. Handle Runtime Code Interpretation	5.5.4 Security Requirements of Pre-applications

TECHNICAL REQUIREMENTS	OWASP CORRESPONDING ITEM	US NIST [NOTE 1]	EUROPE ENISA [NOTE 2]	CHINA YD / T 2407-2013 [NOTE 3]
	threats and countermeasures, has been produced	Sites Libraries Loaded		
4.1.5.2. Mobile Application Integrity	V7.2: Verify that the app has been built in release mode, with settings appropriate for a release build (eg. non-debuggable)	4. Mobile Application Evaluation - Classes Loaded	N / A	5.5.4 Security Requirements of Pre-applications
4.1.5.3. Reference Library Security	V1.2: Verify all third party components used by the mobile app, such as libraries and frameworks, are identified and checked for known vulnerabilities	4. Mobile Application Evaluation: Native Methods Libraries Loaded	6. Secure Data Integration with Third-Party Code	5.5.4 Security Requirements of Pre-applications
4.1.5.4. User Input Validation	V6.2: Verify that all inputs from external sources and the user are validated and if necessary sanitized	4. Mobile Application Evaluation - Input Validation	10. Handle Runtime Code Interpretation	5.5.4 Security Requirements of Pre-applications

TECHNICAL REQUIREMENTS	OWASP CORRESPONDING ITEM	US NIST [NOTE 1]	EUROPE ENISA [NOTE 2]	CHINA YD / T 2407-2013 [NOTE 3]
	This includes data received via the UI, IPC mechanisms such as intents, custom URLs, and network sources.			
4.2.2.1. WebView Security Testing	N / A	N / A	N / A	N / A

[NOTE 1] Vetting the Security of Mobile Applications App, NIST Special Publication 800-163, http://dx.doi.org/10.6028/NIST.SP.800-163, 2015

[NOTE 2] Smartphone Secure Development Guidelines, https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016, ENISA, 2017

[NOTE 3] Wisdom Mobile Terminal Security Capabilities Technical Requirements, YD / T 2407-2013, 2013

Appendix II, Technical Requirements Reference Checklist

LINE ITEM	NO.	SKILLS REQUIREMENT
4.1.1.1. Mobile Application Release	1	Mobile applications shall be released in reliable App Stores.
	2	Mobile applications, when released, shall be noted the Sensitive Data accessed by applications, the mobile device resources, and the declaration of the usage rights.
4.1.1.2. Mobile Application Update	3	Mobile applications shall be released the updates to reliable App Stores.
	4	Mobile applications shall provide an update mechanism and notify active announcements when security updates.
4.1.1.3. Mobile Application Security Issues in Return	5	Mobile application developers should provide a channel of return on security issues.
	6	Mobile application developers should respond and improve the problem within a reasonable period.
4.1.2.1. Sensitive Data Collection	7	Before the mobile applications collect Sensitive Data, they should get users' consent and provide the users the right to refuse them.
4.1.2.2. Sensitive Data Usage	8	Mobile applications, such as password authentication, should actively remind the users to set more complex passwords.
	9	Mobile applications such as the use of sword authentication should take the initiative to remind the user to set more complex passwords.
	10	Mobile applications should remind users to regularly change their passwords.
4.1.2.3. Sensitive Data Storage	11	Before the mobile applications store Sensitive Data, they should get users' consent and provide the users the right to refuse them.
	12	Sensitive Data stored in mobile applications should be used only for the

LINE ITEM	NO.	SKILLS REQUIREMENT
		intended use statement.
	13	Sensitive Data stored in mobile applications should avoid redundant Sensitive Data stored in log files or archives.
	14	Sensitive Data should adopt appropriate and effective length of the key and encryption algorithm, and it should be encrypted before saving.
	15	Sensitive Data should be stored in a protected area by the operating system to prevent unauthorized access from other mobile applications.
	16	Sensitive Data should be avoided in the code of mobile applications.
	17	Mobile applications should take the initiative to alert the user when capturing the screen.
4.1.2.4. Sensitive Data Transmission	18	Mobile applications transmitting Sensitive Data through the Internet should use the appropriate and effective key length of the encryption algorithm for secure encryption.
4.1.2.5. Sensitive Data Sharing	19	Different mobile applications within mobile devices should get users' consent and provide the users the right to refuse them before sharing sensitive data.
	20	When mobile applications share Sensitive Data, they should prevent unauthorized access from other mobile applications.
4.1.2.6. Sensitive Data Deletion	21	The function of deletion should be provided if mobile applications store users' Sensitive Data.
4.1.3.1. Transaction Resources	22	Mobile applications should proactively notify users before using transaction resources and provides the user the right to refuse it.
4.1.3.2. Transaction Resources Control Management	23	Mobile applications should identify users before using transaction resources.

LINE ITEM	NO.	SKILLS REQUIREMENT
	24	Mobile applications should record the transaction resources and time after using transaction resources.
4.1.4.1. The User Identity Authentication and Authorization	25	Mobile Applications should have appropriate identity authentication mechanisms to confirm users' identities and authorize users depending on users' identities.
4.1.4.2. Connection Management Mechanism	26	Mobile Applications should avoid communicating identification code with regularity.
	27	Mobile Applications should confirm the validity of the server's certificate.
	28	A certificate of mobile applications connecting to the server shall be issued by the trusted certificate authority.
	29	Mobile Applications should avoid connecting and transmitting data with the server with no valid certificate.
4.1.5.1. Protection Against Malicious Code and Prevent Information Security Vulnerabilities	30	Mobile Applications should avoid products containing malicious code.
	31	Mobile Applications should avoid information security vulnerabilities.
4.1.5.2. Mobile Application Integrity	32	Mobile Applications should use appropriate and effective verification mechanisms to ensure integrity.
4.1.5.3. Security Reference Library	33	When updating the reference library of mobile applications, they should prepare for an updated version. As for updating requirements, please refer to Mobile Application Release Security.
4.1.5.4. User Input Validation	34	Mobile applications should check the security and provide relevant injection attack protection mechanism when users input strings in the input stages.

LINE ITEM	NO.	SKILLS REQUIREMENT
4.2.2.1. WebView Security Testing	35	Mobile applications should use WebView to exchange web resources with a remote server.
	36	When the mobile application rendering to WebView, the connection should be in Secure Domain.