ioXt 2020 Mobile Application Profile

Version 1.0

Document C-20-11-18
Date 12/10/20
Document Status: Release

1. Notice of Use and Disclosure

Copyright © ioXt Alliance, Inc. (2018 – 2020). All Rights Reserved. This information within this document is the property of the ioXt Alliance and its use and disclosure are restricted.

Elements of ioXt Alliance documentation, specifications, and test plans may be subject to third party property rights, including without limitation copyrights and patents. The ioXt Alliance is not responsible and shall not be held responsible in any manner for identifying or failing to identify any or all such third-party intellectual property rights.

This document and information contained herein are provided on a “AS IS” basis.

THE IOXT ALLIANCE DISCLAIMS ALL WARRANTIES EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OF THIRD-PARTIES, OR ANY IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR USE, TITLE, NON INFRINGEMENT, OR GUARANTEE OF PRODUCT SECURITY. IN NO EVENT WILL THE IOXT ALLIANCE BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OF DATA, INTERRUPTION OF BUSINESS, OR FOR ANY OTHER DIRECT, INDIRECT, SPECIAL OR EXEMPLARY, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, IN CONTRACT OR IN TORT, IN CONNECTION WITH THIS DOCUMENT OR THE INFORMATION CONTAINED HEREIN.

The above notice must be included in all copies of this document.

2. Document Version Information

Version	Date	Author	Description
0.9	11/23/2020	Eugene Liderman	1. Initial draft of Mobile Application profile. 2. VPN extension
1.0	12/10/2020	Brad Ree	1. Document cleaned for release.

1. Participants

Amit Agrawal, Amazon (Vice-Chair)	Tomislav Nad, SGS
Jorge Coronel, Google	Parthiv Parikh, SGS
Brooke Davis, Google (Vice-Chair)	Suresh Pattar, iClimb Systems
Shubha Gopalakrishna, Bureau Veritas	Mariela Pavlova, Infineon Technologies
Dominick Gregory, Buzr	Bridgette Roberts, ioXt Alliance
Gabriel Groen, ioXt Alliance	Brad Ree, ioXt Alliance
Jameson Hyde, NCC Group	Joel Scambray, NCC Group
Dave Kleidermacher, Google	Pawel Smietanka, Silvair, Inc.
Rutwij Kulkarni, Acumen Security	Jordi Ventayol, Applus Laboratories
Eugene Liderman, Google (Chair)	Jorge Wallace, Dekra
Lloyd Linder, Mobilitie	Rob Wood, NCC Group
David Weinstein, NowSecure	

2. Introduction

2.1. Purpose

The ioXt Mobile Application profile provides a base security level for all cloud connected applications running on mobile devices. The profile also provides a set of extensions which may be applied based on the features contained in the application. For example, an IoT controller application would only need to certify under the Mobile Application profile (without extensions). However, an application with VPN and password manager functions must comply against the Mobile Application profile, plus the VPN and password manager extensions.

The profile may only be applied to applications which run on mobile devices, and are distributed through an authentic source.

2.2. Acronyms and Abbreviations

Acronym	Definition
OTA	Over the Air
OWASP	Open Web Application Security Project
MASVS	Mobile Application Security Verification Standard (published under OWASP)
PII	Personal Identifiable Information
IPC	Interprocess Communication
VPN	Virtual Private Network

2.3. Definitions

Term	Definition
OS KeyStore	An OS provided Keystore system lets you store cryptographic keys in a container to make it more difficult to extract from the device. Once keys are in the keystore, they can be used for cryptographic operations with the key material remaining non-exportable. Moreover, it offers facilities to restrict when and how keys can be used, such as requiring user authentication for key use or restricting keys to be used only in certain cryptographic modes.
Authentic source	An authentic source may be a curated application repository, such as the Google Play Store, Amazon Appstore, Apple AppStore, or any other repository that has published policies and guidelines. Alternatively downloading the applications directly from the developers website can also be considered an authentic source.

	The authentic source shall provide a means for securely downloading the application, provide automatic updates, and host links to a developer's privacy and update policies.
Guessing attacks	A password guessing or brute force attack is an attack in which the attacker repeatedly attempts to guess the user's credentials based on a list of known passwords, dictionary, or other such methods.
Known security vulnerabilities	Known security vulnerabilities are any verified vulnerability in which a researcher has submitted to the developer, vulnerabilities received from the developer of SDKs or other libraries included in the application, or vulnerabilities published in the NIST NVD for any previous versions of the developer's application.
Remote attack	Remote attacks are defined as any attack in which the attacker is not located on the local network of the device. Typically, these attacks are launched from the Internet towards the user or the server. Man in the Middle attacks are NOT remote attacks.
Proximity attack	Proximity attacks are any attack in which the attacker is within radio range of the device, or is located on the same local network as the user. The attacker may not be physically located on the local network, but may have remote control of another device on the local network.
Sensitive Data	See OWASP definition

2.4. References

OWASP Mobile Security Testing Guide

3. Profile Scope

3.1. Application Requirements

- The application shall run on Smartphones or tablets.
- The application shall come from an authentic source.
- The application communicates to/through cloud services or directly to an IoT device.

3.2. Applications which are in Scope

- The application is used to configure or manage IoT devices.
- The application may utilize sensitive on-device permissions or sensors.

- The application may store or transmit sensitive data.
- The application may relay or tunnel data through a cloud server to another 3rd party.

4. Requirements

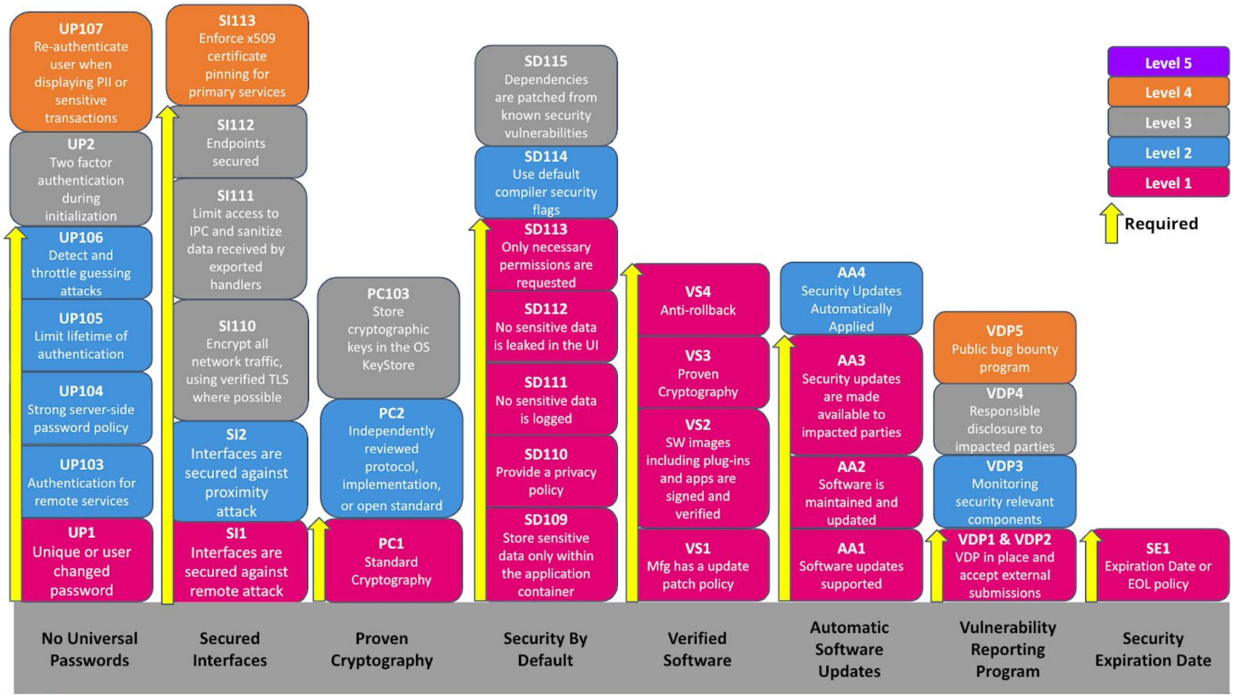
4.1. Test Case Library Version

The profile requirement document only describes the test cases needed for certification by test case ID. The actual text of the test cases are located in the ioXt Test Case Library. As the test case library is a shared document used by all profiles, there may be newer versions of the library than was approved when this profile was created.

The Mobile Application profile version 1.0 shall only use ioXt Test Case Library version 4.0.

The Mobile Application profile test cases provide a reference back to the OWASP MASVS, though many of the OWASP test cases have been updated to reflect security controls provided by the authentic source repositories, or updates to the security services provided by the mobile OS. However, the associated OWASP MASVS are listed in the additional information section of applicable ioXt test cases.

4.2. Profile Summary


UP107
Re-authenticate user when displaying PII or sensitive transactions
UP2
Two factor authentication during initialization
UP106
Detect and throttle guessing attacks
UP105
Limit lifetime of authentication
UP104
Strong server-side password policy
UP103
Authentication for remote services
UP1
Unique or user changed password
SI113
Enforce x509 certificate pinning for primary services
SI112
Endpoints secured
SI111
Limit access to IPC and sanitize data received by exported handlers
SI110
Encrypt all network traffic, using verified TLS where possible
SI2
Interfaces are secured against proximity attack
SI1
Interfaces are secured against remote attack
PC103
Store cryptographic keys in the OS KeyStore
PC2
Independently reviewed protocol, implementation, or open standard
PC1
Standard Cryptography
SD115
Dependencies are patched from known security vulnerabilities
SD114
Use default compiler security flags
SD113
Only necessary permissions are requested
SD112
No sensitive data is leaked in the UI
SD111
No sensitive data is logged
SD110
Provide a privacy policy
SD109
Store sensitive data only within the application container
VS4
Anti-rollback
VS3
Proven Cryptography
VS2
SW images including plug-ins and apps are signed and verified
VS1
Mfg has a update patch policy
AA4
Security Updates Automatically Applied
AA3
Security updates are made available to impacted parties
AA2
Software is maintained and updated
AA1
Software updates supported
VDP5
Public bug bounty program
VDP4
Responsible disclosure to impacted parties
VDP3
Monitoring security relevant components
VDP1 & VDP2
VDP in place and accept external submissions
SE1
Expiration Date or EOL policy
Level 5
Level 4
Level 3
Level 2
Level 1
Required
No Universal Passwords
Secured Interfaces
Proven Cryptography
Security By Default
Verified Software
Automatic Software Updates
Vulnerability Reporting Program
Security Expiration Date

4.3. Proven Cryptography

4.3.1. Requirements

ID	Test Case
PC1	Standard cryptography
PC2	Independently reviewed protocol, implementation, or open standard
PC103	Store cryptographic private keys in the OS KeyStore.

4.3.2. Security Levels

Security Level	Test Cases	Required For Certification
1	PC1	Yes
2	PC2	
3	PC103	

4.4. No Universal Password

4.4.1. Requirements

ID	Test Case
UP1	User credentials shall not be common or predictable, or the credentials must be required to change at initial use.
UP103	Require authentication for remote services containing user data.
UP104	Enforce a strong server-side password policy.
UP105	Limit lifetime of authentication materials.
UP106	Detect and throttle guessing attacks.
UP2.1	Availability of two factor authentication for products which have a user facing interface during initialization
UP2.2	Availability of two factor authentication for products which have a user facing interface during management
UP107	App shall re-authenticate the user when displaying sensitive PII data or conducting sensitive transactions.

4.4.2. Security Levels

Security Level	Test Cases	Required for Certification
1	UP1	Yes
2	UP103 UP104 UP105 UP106	Yes
3	UP2.1 UP2.2	
4	UP107	

4.5. Verified Software

4.5.1. Requirements

ID	Test Case
VS1	Manufacturer has an update patch policy
VS2	Software images including plug-ins and apps are signed and verified
VS3	Proven Cryptography
VS4	Anti-Rollback

4.5.2. Security Levels

Security Level	Test Cases	Required for Certification
1	VS1 VS2 VS3 VS4	Yes

4.6. Security by Default

4.6.1. Requirements

ID	Test Case
SD109	Store sensitive data only within the application container or system credential storage facilities.
SD110	Provide a privacy policy.
SD111	No sensitive data is logged.
SD112	No sensitive data is leaked in the UI.
SD113	Only necessary permissions are requested.
SD114	Use default compiler security flags.
SD115	Dependencies are patched from known security vulnerabilities.

4.6.2. Security Levels

Security Level	Test Cases	Required for Certification
1	SD109 SD110 SD111 SD112 SD113	Yes
2	SD114	
3	SD115	

4.7. Secured Interfaces

4.7.1. Requirements

ID	Test Case
SI1.1	Remote Attack: All certifiable protocols used on the interfaces contained in the device shall be Certified
SI1.2	Remote Attack: Unused Services are disabled
SI1.3	Remote Attack: Authentication
SI1.4	Remote Attack: Secured Communications
SI2.1	Proximity Attack: Unused Services are disabled
SI2.2	Proximity Attack: Authentication
SI2.3	Proximity Attack: Secured Communications
SI110	Encrypt all network traffic, using verified TLS where possible.
SI111	Limit access to IPC and sanitize data received by exported handlers.
SI112	Endpoints do not expose unnecessary open services and are secured against any medium+ vulnerabilities.
SI113	Enforce x509 certificate pinning for primary services.

4.7.2. Security Levels

Security Level	Test Cases	Required for Certification

1	SI1.1 SI1.2 SI1.3 SI1.4	Yes
2	SI2.1 SI2.2 SI2.3	Yes
3	SI110 SI111 SI112	Yes
4	SI113	

4.8. Automatically Applied Updates

4.8.1. Requirements

ID	Test Case
AA1	Software updates supported
AA2	Software is Maintained and Updated
AA3	Software updates are made available to impacted parties
AA4	Security Updates applied automatically, when product usage allows

4.8.2. Security Levels

Security Level	Test Cases	Required for Certification
1	AA1 AA2 AA3	Yes
2	AA4	

4.9. Vulnerability Reporting Program

4.9.1. Requirements

ID	Test Case
VDP1	VDP in place
VDP2	Accept external submissions
VDP3	Monitoring security relevant components.
VDP4	Responsible disclosure of defects to impacted parties that must take action.
VDP5	Public Researcher Rewards program

4.9.2. Security Levels

Security Level	Test Cases	Required for Certification
1	VDP1 VDP2	Yes
2	VDP3	
3	VDP4	
4	VDP5	

4.10. Security Expiration Date

4.10.1. Requirements

ID	Test Case
SE1.1	End of life notification policy is published
SE1.2	Expiration Date is published

4.10.2. Security Levels

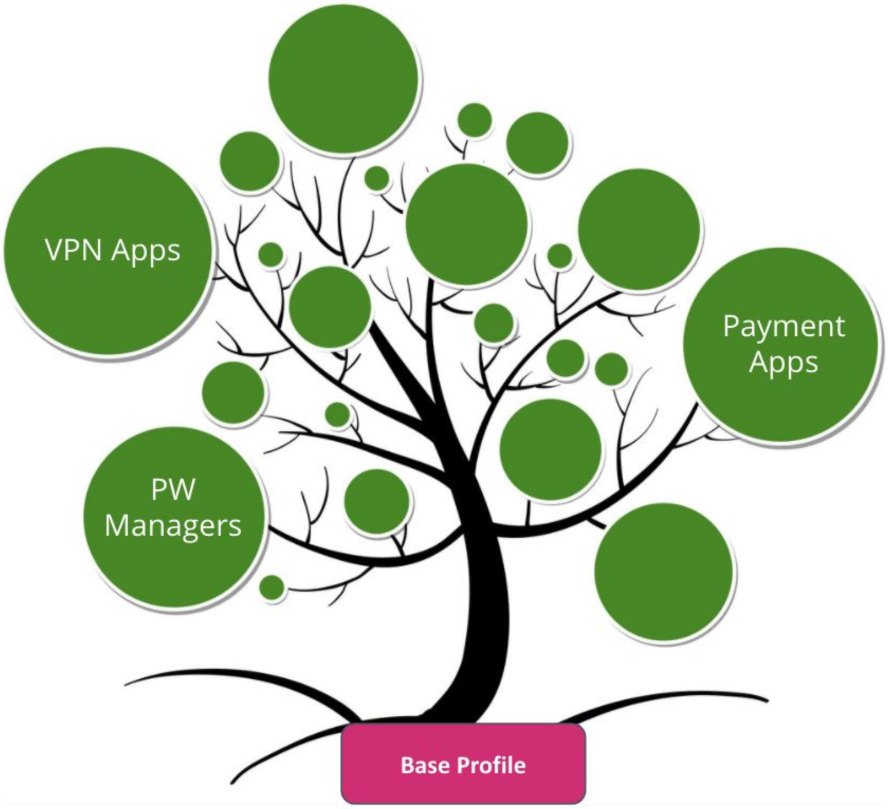
Security Level	Test Cases	Required for Certification
1	SE1.1 or	Yes

	SE1.2	

5. Extensions

5.1. Overview

The wide diversity of mobile application security threats may not be fully defined with a single security profile. However, the same base security requirements are needed for all types of connected applications. Thus, extensions may be applied on top of the mobile application profile requirements. These extensions shall build upon the mobile application profile, but will not replace any requirements of the profile. However, each extension may be applied separately to a device. For example, a VPN application which contains a password manager would need to meet the Mobile Application profile requirements, plus BOTH the VPN extension and Password Manager extension (if one is created).



5.2. VPN

5.2.1. Scope

5.2.1.1. Application Requirements

- The application provides an encrypted tunnel through a cloud relay to protect your internet communications.

5.2.1.2. Applications which are in Scope

- Consumer oriented Virtual Private Network apps/services that:
  - Provide online privacy and/or
  - Anonymize online activity and/or
  - Provide an additional layer of transport encryption between the smartphone and the VPN termination point (cloud relay)

5.3. Requirements

The following requirements shall be applied on top of the mobile application profile requirements listed in section 6. These requirements build on top of the highest level for each pledge item.

ID	Test Case
PC104-VPN	Review that acceptable protocols are supported and that the app defaults to a secure protocol in UI.
SI114-VPN	Verify if network traffic is leaked outside of the VPN tunnel.
SI115-VPN	Verify application supports Always-On, automatic reconnect to VPN, and killswitch functionality.
SI116-VPN	Verify if the VPN server attempts to intercept TLS connections or injects scripts into HTTP requests.