MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

C129 Certification Report

SECIRON – Android Mobile Application Hardening Sandbox Module version: 7.0 (AMAHSM)

File name: ISCB-5-RPT-C129-CR-v1a
Version: v1a
Date of document: 7 February 2024
Document classification : PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
200601006881 (726630-U)
www.cybersecurity.my
Level 7, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia
T +603 8800 7999 F +603 8008 7000 H 1 300 88 2999

SECURING OUR CYBERSPACE

SIBER MALAYSIA MADANI

C129 Certification Report

SECIRON – Android Mobile Application Hardening Sandbox Module version: 7.0 (AMAHSM)

7 February 2024

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C129 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C129-CR-v1a
ISSUE:	v1a
DATE:	7 February 2024
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

The copyright of this document, which may contain proprietary information, is the property of CyberSecurity Malaysia.

The document shall be held in safe custody.

©CYBERSECURITY MALAYSIA, 2024

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 201601006881 (726630-U)

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems, and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 28th December 2023, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	22 January 2024	All	Initial draft
v1	29 January 2024	All	Final version
v1a	7 February 2024	Page 4, 7, 8 – 11	• Include threats under Section 1.3 • Remove table in Section 1.7 a) for consistency • Remove Section 1.8.1 – 1.8.4 and make reference in the Security Target

Executive Summary

The Target of Evaluation (TOE) is SECIRON – Android Mobile Application Hardening Sandbox Module (AMAHSM) version: 7.0 The TOE can be categorised a mobile application hardening tools that allow users to protect their android mobile application (APK file).

The scope of the evaluation is defined by the Security Target (Ref [6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations, and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by Cybertronics Lab, and the evaluation was completed on 15 January 2024.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at http://www.commoncriteriaportal.org

It is the responsibility of the user to ensure that SECIRON – ANDROID MOBILE APPLICATION HARDENING SANDBOX MODULE (AMAHSM) meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

IronWALL is a cutting-edge security solution that helps manage, prevent and protect mobile applications from security risks. IronWALL is designed to safeguard against a wide range of threats, including mobile application tampering, reverse engineering, debugging, jailbreaks, application cloning, malware, repackaging and other attacks on untrusted environment.

Furthermore, IronWALL also effectively mitigates potential risks by reducing attack surface exposure. Android Mobile Application Hardening Sandbox Module is a product designed by SECIRON and developed as part of IronWALL. This product integrates protection technologies for various security flaws into the application client without changing the application code, providing customers with a full lifecycle management covering application development, packaging, distribution, and operation. The integrated security guarantee service effectively prevents malicious attacks against mobile applications such as de-compilation, repackaging, memory injection, dynamic debugging, data theft, transaction hijacking, and application phishing, and comprehensively protects application software security.

The hardening core technology includes:

- Code Anti-Reverse
- Application Tamper Protection
- Memory Anti-Debug Protection
- Data Leakage Protection
- Operating Environmental Protection

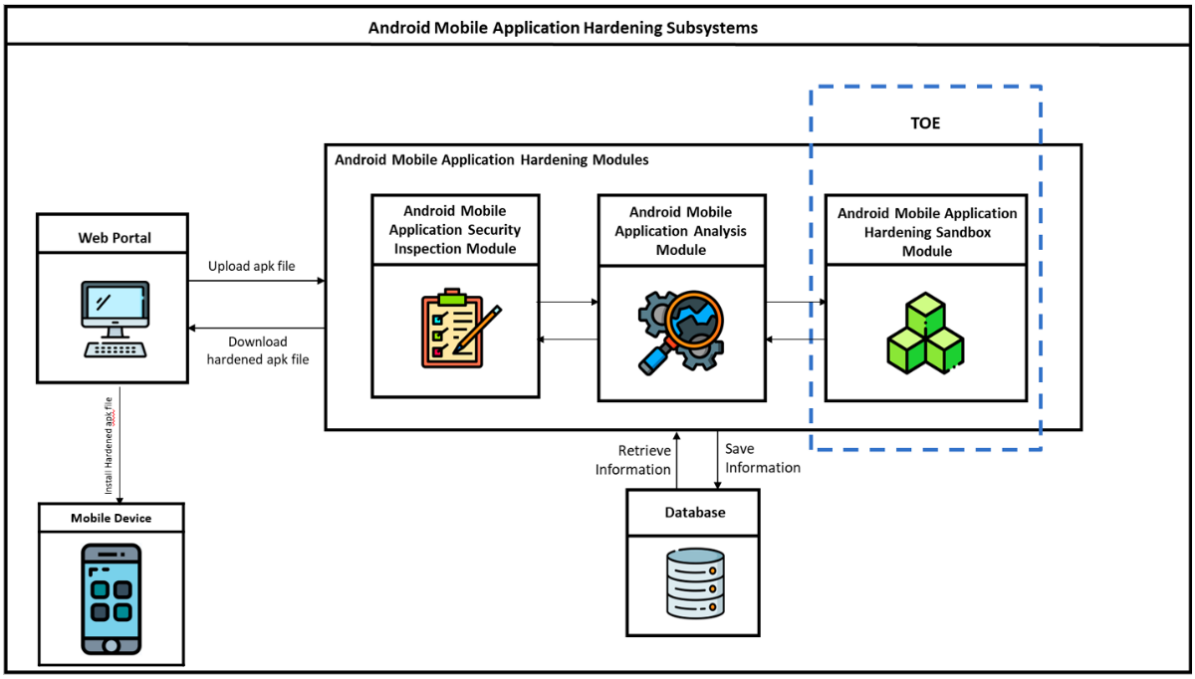

Figure 1: IronWALL High Level Diagram

Mobile application package will be uploaded by the User through Web Portal which allow User to create and define mobile application hardening rules that understand by the TOE. Once mobile application package is hardened, mobile application package will be installed in mobile device for testing to ensure the hardening in place.

The Android Mobile Application Hardening Sandbox Module (AMAHSM) is a product hosted on the cloud and packaged as SaaS service that provides mobile application security hardening. Users can upload their APK files to be hardened, select the desired hardening policy, and download the hardened APK file with hash verification.

The major security features of the TOE included in the evaluation is:

- Cryptographic Support
- Protection of the TSF
- Security Audit

1.2 TOE Identification

The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C129
TOE Name	SECIRON – ANDROID MOBILE APPLICATION HARDENING SANDBOX MODULE (AMAHSM)
TOE Version	7.0
Security Target Title	SECIRON – Android mobile Application Hardening Sandbox Module (AMAHSM) version:7.0 – Security Target
Security Target Version	1.0
Security Target Date	28 December 2023
Assurance Level	Evaluation Assurance Level 2
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL2
Sponsor	SecIron (Malaysia) Sdn. Bhd. (201801025495 (1287515-T)) Unit 704, Uptown One, No. 1, Jalan SS21/58, Damansara Uptown, 47400 Petaling Jaya, Selangor E-mail: business@seciron.com Tel: +601133503181 Website: https://www.seciron.com
Developer	SecIron (Malaysia) Sdn. Bhd. (201801025495 (1287515-T)) Unit 704, Uptown One, No. 1, Jalan SS21/58, Damansara Uptown, 47400 Petaling Jaya, Selangor E-mail: business@seciron.com

	Tel: +601133503181 Website: https://www.seciron.com
Evaluation Facility	Cybertronics Lab C-5-15, Centum @ Oasis Corporate Park No 2, Jalan PJU 1A/2, Ara Damansara 47301 Selangor, Malaysia Tel: +603-7627 4060 Fax: +603-7627-4070 Website: https://www.acrossverticals.com

1.3 Threats and Organisational Security Policy

Threats that are addressed by the TOE are described in section 3.2 of the Security Target (Ref [6]). There are no organisational security policies defined regarding the use of TOE.

1.4 TOE Architecture

The TOE includes both physical and logical boundaries which are described in Section 1.5 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

The TOE consists of the following security functions identified in the Security Target (Ref [6]).

Table 2: TOE Logical Boundaries

Cryptography Support	The TOE generates cryptographic key (decryption keys) that are to be stored within the encrypted SO Library files. The TOE performs several cryptographic operations including code encryptions, SO Library Files encryption, hash generation and RSA signature generation. These cryptographic operations are performed in accordance to strong encryption algorithm with adequate key length.
Protection of TSF	During the hardening process, the data from Classes.DEX, AndroidManifest.XML, and SO Library Files in the APK file are extracted separately to be hardened and modified accordingly. A hash is generated to ensure the integrity of the file throughout the process. The hardening process will

	verify integrity of files to ensure there were no unauthorized tampering during runtime. Should the verification failed, the execution process will be terminated.
Security Audit	The TOE generates logs from the web portal operations. The logs shall include events from the web portal such as user login, hardening submission and hardening policy addition or modification. These logs are stored in the server and not on the user's local device to prevent unauthorized modifications.

1.4.2 Physical Boundaries

There is no physical scope of the TOE as the TOE is hosted on the cloud as a SaaS application.

1.5 Clarification of Scope

The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand their own IT environment and requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

1.6.1 Operational Environment Assumptions

Assumptions for the TOE environment as described in the Security Target (Ref [6]):

Table 3: Assumptions for the TOE environment

Assumption	Statements
A.USER	The users are trusted; the users shall not maliciously compromise the security functionality of the TOE. The users are well-trained; the user shall comply to the operating procedures stipulated in the user guidance.
A.DATAFLOW	The data flow to the TOE must be between the subsystems and TOE as defined in the use case.

1.7 Evaluated Configuration

Figure 1 shows the testing environment to test the TOE. Android Mobile Application Hardening Modules consists of three (3) components which are the Android Mobile Application Security Inspection Module, Android Mobile Application Analysis Module and the TOE, Android Mobile Application Hardening Sandbox Module.

The web application communicates directly with the Android Mobile Application Hardening Modules when using the hardening functions. User needs to have an account on the web application to be able to upload mobile application through the web portal for hardening.

Once the mobile application package had been uploaded it will first flow through Android Mobile Application Security Inspection Module. Mobile Application Package Scanner will perform a scan to ensure uploaded mobile application package meets security requirements and free from malware or malicious codes.

Next, the mobile application package will be sent to Android Mobile Application Analysis Module. Mobile Application package will perform analysis before hardening process to identify for mobile application package related information such as UI/UX and Framework Information.

Lastly, the mobile application package will be sent to Mobile Application hardening module which harden mobile application package based on configured policy defined by SecIron and Customer. User activity and Hardening Activity will be logged by the system and stored it in database for troubleshooting and security audit purpose. Created hardening Policy will be stored in the database as well.

Once the mobile application package is successfully hardened, user needs to download the hardened application from the web portal and install it onto a mobile device.

Components required to be setup before testing:

a) Web Portal

Web portal allow user to setup mobile application hardening policy and upload mobile application package for hardening purpose.

Compatible Browser: -

Compatible with IE8 browser and later.

Compatible with Google Chrome browser.

Compatible with Firefox browser.

Compatible with Safari browser.

Compatible with Edge browser.

b) Android Mobile Application Security Inspection Module

Mobile Application Package Scanner to ensure uploaded mobile application package meets security requirements and free from malware or malicious codes.

c) Android Mobile Application Analysis Module

Mobile Application package analysis before hardening process to identify for mobile application package related information such as UI/UX and Framework Information.

d) Android Mobile Application Hardening Sandbox Module (TOE)

Mobile Application hardening module which hardened mobile application package based on configured policy defined by SecIron and Customer.

e) Database

Storage for Application Files, System Configuration, Management Information and Security Policies. User activity and Hardening Activity will be logged by the system and stored it in database for troubleshooting and security audit purpose. Created hardening Policy will be stored in the database as well.

f) Mobile Device

Mobile device to perform testing on hardened mobile application package to ensure hardening policy is in place.

Equipment	Components	Android Version
Mobile Device #1	Google Pixel 5	11
Mobile Device #2	Asus ROG Phone 2	13

1.8 Delivery Procedures

The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

The evaluators also examined the aspects of the delivery process and determined that the delivery procedures are used.

1.8.1 Product Documentation

List of documentation and description provided by the developer that the user can use as guidance for installation:

- SECIRON – Android Mobile Application Hardening Sandbox Module (AMAHSM) version: 7.0 Guidance Document v1.0
- IronWALL_v7_2_0_UserGuide_v1_0_5
- SecIron IronWALL v7.2 deployment guide_v1.1.2

2 Evaluation

The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the ISCB Product Certification Schemes Policy (Product_SP) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators confirmed that the TOE provided for evaluation is labelled with its reference and the TOE references used are consistent.

The evaluators examined that the method of identifying configuration items and determined that it describes how configuration items are uniquely identified

The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the SECIRON – ANDROID MOBILE APPLICATION HARDENING SANDBOX MODULE (AMAHSM) version: 7.0 Configuration Management version 1.0.

2.1.2 Development

Architecture

The evaluators examined the security architecture description (contained in Section 4) and determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

The security architecture description describes the security domains maintained by the TSF.

The initialisation process described in the security architecture description preserves security.

The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

Functional Specification

The evaluators examined the functional specification and determined that:

- The TSF is fully represented;
- It states the purpose of each TSF Interface (TSFI); and
- The method of use for each TSFI is given.

The evaluators also examined the presentation of the TSFI and determined that:

- It completely identifies all parameters associated with every TSFI; and
- It completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI.

The evaluators also confirmed that the developer supplied tracing links of the SFRs to the corresponding TSFIs.

TOE Design Specification

The evaluators examined the TOE design (contained in [17]) and determined that the structure of the entire TOE is described in terms of subsystems.

The evaluators also determined that all subsystems of the TSF are identified.

The evaluators determined that interactions between the subsystems of the TSF were described.

The evaluators examined the TOE and determined that each SFR supporting or SFR-non-interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is not SFR-enforcing.

The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

The evaluators examined the TOE design and determined that it provides a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

The evaluators determined that all SFRs were covered by the TOE design and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.3 Guidance documents

The evaluators examined the operational user guidance determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

The evaluators examined the operational user guidance in conjunction with other evaluation evidence and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

The evaluators confirmed that the TOE guidance fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

Testing at EAL 2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by Cybertronics Lab. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

2.1.4.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator). The results of the evaluators' tests are consistent with the developers' test results defined in their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

At EAL 2, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Table 4: Independent Functional Test

TEST ID	DESCRIPTIONS	RESULTS
Test Case AVCC009-FT001	To ensure mobile application's source code data are encrypted after hardening.	Passed. Result as expected.
Test Case AVCC009-FT002	To ensure mobile application's resources are encrypted after hardening.	Passed. Result as expected.
Test Case AVCC009-FT003	To ensure direct access to TOE docker is not allowed.	Passed. Result as expected.
Test Case AVCC009-FT004	To ensure that the integrity verification information file is generated under the assets/meta-data directory.	Passed. Result as expected.
Test Case AVCC009-FT005	To ensure mobile application's source code tamper resistance after hardening process.	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
Test Case AVCC009-FT006	To ensure mobile application's library file (.SO) is tamper resistance after hardening process.	Passed. Result as expected.
Test Case AVCC009-FT007	To ensure that the audit records are generated based on auditable events.	Passed. Result as expected.

All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration testing

The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other requirement for exploitation

The evaluators' search for vulnerabilities also considered public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables. The following public domain sources were searched:

a) https://cwe.mitre.org

b) https://capec.mitre.org

c) https://nvd.nist.gov

d) https://uwnthesis.wordpress.com

e) https://owasp.org

f) https://www.cvedetails.com

The penetration tests focused on:

a) Improper Credential Usage;

b) Insufficient Binary Protection;

c) Security Misconfiguration;

d) Insecure Data Storage;

e) Insufficient Cryptography; and

f) Root/Jailbreak Detection Bypass

The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in Section 1 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all tests conducted were PASSED as expected.

3 Result of the Evaluation

After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of SECIRON – Android Mobile Application Hardening Sandbox Module version: 7.0 (AMAHSM) performed by Cybertronics Lab.

Cybertronics Lab found that SECIRON – Android Mobile Application Hardening Sandbox Module version: 7.0 (AMAHSM) upholds the claims made in the Security Target (Ref [6]) and supporting documentations and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2.

Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

EAL 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and complete interface specifications, guidance documentation and a description of the design of the TOE to understand the security behaviours.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

3.2 Recommendation

The Malaysian Certification Body (MyCB) is strongly recommending that:

a) A strict adherence to guidance documentations and procedures provided by the developer are highly recommended.

b) The TOE users should be aware and implement available security or critical updates related to the TOE security features and its supporting hardware, software, firmware, or relevant guidance documents.

c) Users are advice to seek assistance or guidance directly from the developer of the TOE if specific requirements shall be configured or implemented by the TOE to meet certain policies, procedures, and security enforcement within the users' organization. This is important to reduce operational error, misconfiguration, malfunctions, or insecure operations of the TOE that may compromise the confidentiality, integrity and availability of the assets that is protected by the TOE.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] MyCC Scheme Requirement (MYCC_REQ), v1a, CyberSecurity Malaysia, January 2023.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v3, January 2023.

[6] SECIRON – Android Mobile Application Hardening Sandbox Module (AMAHSM) version: 7.0 Security Target, Version 1.0, 28 December 2023.

[7] SECIRON – Android Mobile Application Hardening Sandbox Module (AMAHSM) version: 7.0, Evaluation Technical Report, Version 1.0, 15 January 2024.

[8] SECIRON – Android Mobile Application Hardening Sandbox Module (AMAHSM) version: 7.0 TOE Design Documentation, Version 1.0, 28 December 2023.

A.2 Terminology

A.2.1 Acronyms

Table 5: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme

Acronym	Expanded Term
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 6: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.

Term	Definition and Source
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---