Cybersecurity Labelling Scheme

BY CYBER SECURITY AGENCY OF SINGAPORE

Cybersecurity Labelling Scheme (CLS)

CLS Level 4 Supplementary Minimum Test Specifications for Contact Tracing Devices

December 2020
Version 1.0

FOREWORD

The Cybersecurity Labelling Scheme (CLS) is part of Cyber Security Agency's (CSA) efforts to better secure Singapore's cyberspace and to raise cyber hygiene levels.

Under the CLS, the cybersecurity label would provide an indication of the level of security in the network-connected smart devices. It aims to improve security awareness by making such provisions more transparent to consumers and empowers consumers to make informed purchasing decisions for products with better security based on the cybersecurity label.

The CLS seeks to incentivise developer/manufacturers to develop and provide products with enhanced cybersecurity provisions. The labels also serve to differentiate smart devices with better cybersecurity safeguards in the market, from their competitors.

At the same time, CSA intends to engage other like-minded partners for mutual recognition of the CLS with the objective of eliminating duplicated assessments across national boundaries.

The CLS is an initiative under the Safer Cyberspace Masterplan, to create a safer cyberspace and protect the public and enterprises against cyber threats, as Singapore moves towards a Digital Economy and Smart Nation.

The CLS is owned and managed by the Cybersecurity Certification Centre (CCC), under the ambit of the Cyber Security Agency of Singapore (CSA).

AMENDMENT RECORD

Version	Date	Author	Changes
1.0	December 2020	Cyber Security Agency of Singapore	Release

CONTENTS

1 INTRODUCTION

1.0.1 This document supplements the minimum test cases applicable for Contact Tracing Devices for Assessment Tier #4 – Penetration Testing under the Cybersecurity Labelling Scheme (CLS). It outlines the additional set of minimum test cases to be performed by the testing laboratory (TL).

1.0.2 The intended audience for this document are developers intending to get their device labelled and testing laboratories who are responsible for testing the devices, under the CLS scheme.

1.0.3 The following roles are commonly referred in this document:

1. **Developer** of the **Device Under Test (DUT)**
2. **Testing Laboratory (TL)** that performs the CLS Tier 4 – Penetration Testing
3. **Cybersecurity Certification Centre (CCC)** that oversees the CLS assessments and regime

2 MINIMUM TEST SPECIFICATION

2.1 METHOD OF USE

2.1.1 The Testing Laboratory shall first reference the main Minimum Test Specification document [1] to identify the appropriate test cases relevant to the Device Under Test (DUT).

2.1.2 Following which, the Testing Laboratory shall reference this supplementary document for the additional test cases applicable to contact tracing devices to assert that the Device Under Test (DUT) is reasonably resistant to common attacks in order to complete Assessment Tier #4 of the CLS. Details of Tier 4 can be found in CLS Publication #2 – Scheme Specifications [2].

2.1.3 The minimum test specification does not explicitly specify nor restrict the methods, tools, or tests that the testing laboratory may use to meet the test objective. It is up to the testing laboratory to decide on the tools and expertise to validate that the DUT conforms to the requirements. Some tools are suggested for reference.

2.1.4 This supplementary minimum test specification covers the following attack vectors:

1. Bluetooth/BLE
2. Firmware Analysis
3. Basic Hardware Analysis
4. [To be discussed with CCC] Electromagnetic side channel analysis & fault injection (power glitching).

2.2 BLUETOOTH / BLE

2.2.1 Bluetooth protocol is commonly used for exchanges between contact tracing devices.

No.	Test Objective	Remarks
1	To ensure that the data advertised by the device are adequately protected (e.g. by encryption)	This test involves collecting the Bluetooth data packets when the device is in the advertisement mode and attempt to determine whether any sensitive information could be disclosed (e.g. Personal Identifiable Information). Tools: Any Bluetooth sniffer.
2	To ensure that the device does not suffer from being spammed by spoofed packets that limits the effectiveness of contact tracing.	This test involves simple replay attack using the data packets captured in the earlier tests to determine whether another device is accepting it and storing into the flash memory. Specially crafted packets based on understanding of the data packet should also be tested. This test may be performed in conjunction with the hardware test (e.g. monitoring flash activity). Tools: Ubertooth/nRF, gatttool
3	To ensure firmware and data download could be performed only by authenticated and authorised entity.	This test involves bypassing the authentication and attempting to (1) overwrite the firmware and (2) download any data stored in both the internal and external flash memory. The Testing Laboratory shall also determine whether the SoC used is vulnerable to SweynTooth vulnerability Tools: btcrack

2.3 FIRMWARE

2.3.1 The testing laboratory shall attempt to retrieve and analyse the firmware of the device. The testing laboratory may retrieve the firmware via available hardware debugging ports on the device, or by downloading the firmware from the manufacturer's webpage, or through other means such as removing the flash memory and downloading the firmware using flash reading tools etc.

2.3.2 In addition, the developer shall provide the firmware to the testing laboratory and this provision should be documented. The TL shall also verify that the provided firmware is of the same version as what is stated in the application, by means of verifying the hash (SHA-256) or checksum value.

No.	Test Objectives	Remarks
1	To ensure that the device shall not allow an attacker to retrieve sensitive credentials and contents from its firmware.	This test involves the examination of the contents of the firmware for particular sensitive files, configuration files, password files. The firmware can be retrieved either via physical attacks (hardware debug ports, extracting firmware from the NAND/NOR) etc. Tools: IDA Pro, Ghidra, Binwalk.

2.4 BASIC HARDWARE TEST

2.4.1 The testing laboratory shall investigate the hardware security of the device.

No.	Test Objectives	Remarks
1	To ensure that the device does not contain undeclared components that could raise privacy concerns.	This test involves PCB examination to identify key components, such as the chip supporting Bluetooth, GPS and LTE. From public sources, if the developer claims there is no GPS functionality to track user's location but the device is found to have incorporated a GPS chip, this may potentially suggest a false declaration by the developer. In this instance, the Test Lab is required to report this as a finding. Other examples

		could be the inclusion of an LTE chip and in conjunction with other tests which shows that the device is sending user's data periodically to backend server.
2	To ensure unnecessary interfaces are disabled and available interfaces do not disclose sensitive information.	This test involves connecting to the device over available interfaces such as UART, SWD, JTAG etc to: 1) Attach a debugger; 2) Observe whether any debug messages are communicated from the device; 3) Whether it is possible to dump the firmware and memory content; and 4) Whether it is possible to execute arbitrary commands or disrupt the boot up sequence; Tools: Microscope, debugger, soldering iron, connectors.
3	To ensure data stored in external flash are protected.	This test involves connecting to the external flash to attempt to dump out the content. Examples of possible methods include: 1) Connecting over SPI to the flash directly (to the pins itself or test points if available); 2) Desoldering the flash to be read. If data could be read out, the Test Lab shall also determine whether the data are protected. Tools: Bus pirate, Dataman, soldering iron.

2.5 ELECTROMAGNETIC (EM) SIDE CHANNEL ANALYSIS (SCA) & FAULT INJECTION (FI)

2.5.1 While EM SCA and FI may be perceived as higher order attacks, it may be required to be in scope depending on how the specific contact tracing device is being designed and whether any Personal Identifiable Information (PII) is being stored within.

2.5.2 The Test Laboratory is required to discuss the applicability of the test with CCC.

No.	Test Objectives	Remarks
1	It is expected that most general purpose MCUs would not have countermeasures against side channel analysis. Nevertheless, it is important to determine the extent of leakages.	This test is performed with the evaluation board provided by the MCU manufacturer. It involves determining the lowest number of traces required in order to recover the cryptographic key. This would be examined in conjunction with the design to ensure that key rotation is done. Tools: Evaluation board and setup for EM SCA.
2	It is also expected that most general purpose MCUs would not have countermeasures against fault injection. The objective is to determine the impact when FI is successful.	This test is performed with the evaluation board provided by the MCU manufacturer. The Test Laboratory may select the appropriate method, e.g. whether by voltage glitching or EMFI, upon discussion with CCC. The impact is to examine whether a successful FI would enable the firmware and/or sensitive information to be retrieved. Tools: Evaluation board and setup for FI.

3 REFERENCES

[1] Cyber Security Agency of Singapore, “CLS Publication - Minimum Test Specifications and Methodology for Tier 4,” Version 1.0, October 2020.

[2] Cyber Security Agency of Singapore, “CLS Publication #2 - Scheme Specifications,” Version 1.0, October 2020.

[3] Cyber Security Agency of Singapore, “CLS Publication #1 - Overview,” Version 1.0, October 2020.

4 ACRONYMS

The following acronyms are used in CLS Publication 1, 2 and this document:

CC	Common Criteria for Information Technology Security Evaluation
CCC	Cybersecurity Certification Centre
CCTL	Common Criteria Testing Laboratories
CLS	Cybersecurity Labelling Scheme
CSA	Cyber Security Agency of Singapore
DUT	Device Under Test
HPL	Historical Product List
IMDA	Info-communications Media Development Authority
IoT	Internet of Things
LPL	Labelled Product List
SCCS	Singapore Common Criteria Scheme
TL	Testing Laboratory