Cybersecurity Labelling Scheme

BY CYBER SECURITY AGENCY OF SINGAPORE

Cybersecurity Labelling Scheme (CLS)

Minimum Test Specifications and Methodology for Tier 4

October 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 using the information 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	October 2020	Cyber Security Agency of Singapore	Release

CONTENTS

1 INTRODUCTION

1.0.1 This document provides the test specifications and methodology for Assessment Tier #4 – Penetration Testing under the Cybersecurity Labelling Scheme (CLS). It outlines the set of minimum test cases to be performed by the testing laboratory (TL).

1.0.2 The intended audience for this document is the developers who are interested in getting their device labelled under the CLS 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 projects

2 MINIMUM TEST SPECIFICATION

2.1 METHOD OF USE

2.1.1 The minimum test specification specifies test objectives that shall be met through the tests devised by the Testing Laboratory (TL) to assert that the Device Under Test (DUT) is reasonably resistant to basic attacks in order to complete Assessment Tier #4 of the CLS. Details of Tier 4 can be found in CLS Publication #2 – Scheme Specifications [1].

2.1.2 The minimum test specification is applicable to all categories of devices permissible for labelling under the CLS, as indicated in CLS Publication #1 – Overview [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's tools and expertise to validate that the DUT is indeed conformant to the requirements. However, some tools are suggested for reference.

2.1.4 The minimum test specification spans over the following attack vectors:

1. Ports and Services
2. Firmware
3. Firmware Updates
4. Communications
5. Configuration Portal
6. Mobile Application
7. Authentication
8. Other Attacks
9. Additional device-specific attack vectors

2.1.5 Alongside testing, the TL is also required to verify that the developer's declaration of conformance to the ETSI EN 303 645 is indeed being implemented and sound. If the TL identifies discrepancies between the developer's declaration and device implementation, the TL shall attempt to seek clarifications with the developer and provide such information to the CCC.

2.2 PORTS AND SERVICES

2.2.1 Ports are essential to deliver network services. However, vulnerable implementations may be subjected to exploitation, and the opening of more than the required basic ports further amplifies this risk. With the use of a network port scanner or equivalent tools, the testing laboratory shall identify the list of open ports and services available on the device.

2.2.2 The testing laboratory shall make use of the developer's checklist (particularly the developer's supporting evidence for provision 5.6-1 where the developer provides a list of all enabled network and logical interfaces) as reference information for the following tests in this section.

2.2.3 All open ports and services be further investigated. Unnecessary ports and services shall be reported to CCC. Unnecessary ports and services are defined as those not necessary for the basic functioning of the device. In the example of a wireless router, the primary function is to provide access to the internet and the private network.

2.2.4 It is expected that the device may require certain ports and services to be open for operational purposes. This can be allowed if there is reasonable justification for doing so. However, if the testing laboratory is able to exploit the device through the open ports and services, then the device is deemed to have failed.

2.2.5 If there are any disparities between the testing laboratory's findings and the developer's checklist, or if necessary, the testing laboratory is to seek clarifications with the developer on all detected open ports or services to confirm their functions and purposes.

No.	Test Objective	Remarks
1	To ensure that the device does not have unnecessary or potentially vulnerable open ports and services over its network interfaces.	This test involves multiple discovery scans conducted over each of the available network interfaces (e.g. WLAN, LAN, WAN, etc.). A device can provide different ports and services over different network interfaces. In particular, the following ports and services must not be available over the WAN interface: 1. Telnet over port 23 2. Secure Shell (SSH) over port 22 3. Remote management (e.g. CPE WAN Management Protocol over port 7547) Tools: NMAP, Zenmap, Nessus,

		Hydra, Nexpose NMAP Command: nmap -sU -sT -p0-65535 <IP address> If the testing laboratory has access to the device's command line, the netstat network utility can also be used for this test's purpose. Should the availability of the Telnet and SSH services be configurable via the device's configuration portal, further attempts to investigate these services shall be made. The lab is to enable these services and to connect to these services. If these services request for user credentials, the lab shall attempt to brute-force the login credentials using Hydra or other similar tools (e.g. John the Ripper). It may be possible to discover the required credentials using tools such as the 'creds' module in RouterSploit, related public discussion boards and forums for networking devices or routers, or through related-information attained through Open Source Intelligence (OSINT).
2	To ensure that the device does not suffer from known exploits that can be conducted using typical vulnerability scanning and exploitation tools.	This test involves using various popular vulnerability-scanning tools such as (e.g. RouterSploit, Metasploit, Routerpwn, Immunity Canvas - D2 Exploitation Pack PwnRouter etc.) to scan the device.

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 dumping the firmware root access via Telnet/SSH, or removing the flash memory and downloading the firmware using flash reading tools.

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 (including the manufacturer's website) shall not allow an attacker to retrieve sensitive credentials and contents from its firmware (i.e. secure storage).	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), or via logical attacks (gaining root access via Telnet/SSH/command injection attacks on the device's configuration portal). Examples of sensitive of sensitive materials not limited to the following: - Universal manufacturer wide default accounts and password materials - cryptographic key materials - Login credentials - Login credentials to back-end servers. For root credentials obtained, the testing laboratory shall determine whether this credential is valid only for a specific unit or valid across all units of the same device model. Tools: Binwalk, Binary Ninja

2	To ensure that the device does not have hidden accounts that are undocumented to the end-user.	Hidden or undocumented account could include user, device management, and service accounts. For such accounts, the permissions or privileges shall be reported in the test report and provided to CCC. Password cracking may be performed as appropriate.
3	To ensure that software services should run with least privileges unless necessary.	This can be done by checking the permissions of running processes after initialization.

2.4 FIRMWARE UPDATES

2.4.1 The testing laboratory shall investigate the security of the firmware update process of the device.

2.4.2 Firmware updates are typically provided either as a full binary firmware package or as a smaller binary package containing only updated portions of the code.

2.4.3 Firmware updates are typically performed over the following methods:

- Manual update
- Automated update

No.	Test Objectives	Remarks
1	**Secure Firmware Transmission**: To ensure that the device retrieves a firmware update securely.	This test involves checking that the device retrieves a firmware update via HTTPS, and that HTTPS is securely configured.
2	**Firmware Downgrade**: To ensure that the device does not allow an attacker to downgrade the firmware.	This test involves intentionally uploading a lower version of the firmware to check if the device rejects a lower version firmware. The manufacturer is to provide a lower version firmware to facilitate testing.
3	**Unsigned Firmware**: To ensure that the device does not install an unsigned firmware.	This test involves intentionally uploading an unsigned firmware to check if the device rejects an unsigned firmware. The manufacturer is to provide an unsigned firmware package for testing.
4	**Tampered and Illegitimate Firmware Update**: To ensure that the device does not accept a tampered firmware update package from an untrusted source.	This test is applicable if the device offers an avenue for the user to upload a firmware update package manually to the device. The firmware is typically downloaded from the manufacturer's portal. The test involves uploading an illegitimate and tampered firmware update package and checking if the device rejects the update. While the developer may offer advanced/expert users the ability to load custom firmware, this function should not be the

		default configuration and users should be explicitly notified that the loading of customised firmware is not recommended and users who wish to proceed would need to accept the associated security risks. Example scenarios: 1. Incorrect signatures (e.g. one bit of the signature is changed) 2. Valid signature tested with misconfigured DUT (system date set to a value outside of the validity of the public key) 3. The device only checks that the signature field is filled but does not verify the signature.
5	**Unencrypted Firmware:** To ensure that the firmware binary file is encrypted if it is available for download on the manufacturer's web portal.	The testing laboratory shall confirm if the firmware update file is indeed encrypted and not compressed. Should encryption be used, the testing laboratory shall examine whether the encryption key is retrievable.

2.5 COMMUNICATIONS

2.5.1 The testing laboratory shall investigate if the device is susceptible to the following attacks.

No.	Test Objectives	Remarks
1	Default communication settings should be secured. For example, routers should employ WPA2-PSK-AES-CGM on its wireless interface.	E.g for routers, use of WEP or WPA is not allowed. Disallowing the use of WEP or WPA prevents simple brute force attack against the WEP or WPA password.
2	To ensure that the device communicates in a secure manner with associated cloud services over the internet, configuration portal, and the companion mobile application.	If the device does not secure communications over the internet, on its configuration portal, or the companion mobile application, then it may be possible for an attack to conduct a man-in-the-middle attack and sniff critical user credentials. The testing laboratory shall test that the device is protected against MiTM attacks, version downgrades and negotiations to use weak cipher schemes. Tools: wireshark, tcpdump, testssl.sh, SSLstrip
3	To ensure that the communication protocol implementation not vulnerable to common attacks. Examples for TLS: Heartbleed, POODLE, etc. Examples for Bluetooth: SweynTooth, etc	For Bluetooth protocol, the testing laboratory shall test for replay attacks and other attacks that could lead to revealing users' device information and potentially personal data. For Zigbee, the test laboratory shall test whether the ZigBee implementation is vulnerable such that it is possible for an attacker to join the local network by exploiting known vulnerabilities (e.g. CVE-

		2020-6007). Tools: testssl.sh, hci tool, Gatttool, Zbwireshark, KillerBee, Zbreplay, zbassocflood, etc
4	To ensure that the device does not collect and send device's network statistic or telemetry data back to the manufacturer by default.	For most devices, this function is configurable via the configuration portal. However, even if disabled, the testing laboratory shall attempt to monitor outgoing traffic coming from the device to ensure that the router is indeed conformant and not sending such data. If data is still being sent, the testing laboratory shall record the destination IP address(s) and where possible the type of data being sent. If the device supports sending of network statistic or telemetry data back to the manufacturer, the data shall be protected prior to sending. Tool: Wireshark

2.6 CONFIGURATION PORTAL

2.6.1 The testing laboratory shall investigate the following regarding the device's configuration portal. Majority of the configuration portals are typically accessed by means of webpage or via a mobile application. For web configuration portals, standard tests such as directory traversal, cross-site scripting, cross site request forgery, etc. would apply. This is especially so, if the web configuration portal is made available remotely (i.e. over Internet). The testing laboratory should consider other suitable web application penetration testing during the freeform testing phase.

2.6.2 For mobile applications, Chapter 2.7 - Mobile Application relating to companion mobile apps would apply.

No.	Test Objectives	Remarks
1	To ensure that the device does not have hidden URLs (configuration pages, firmware update pages, URLs that can be used to enable telnet or other services, etc.).	The testing laboratory is to conduct a brute-force attack the configuration portal to determine if such unknown/hidden URLs exists. Tools: OWASP ZAP, Dirbuster, Dotdotpwn
2	To ensure that the device does not allow unauthenticated users to configure the device or to access the configuration portal.	The device shall allow only authenticated users to access the configuration portal and to make changes (settings, firmware update, etc.). The device should authenticate the administrator and such authentication should not be bypassable. E.g. brute force.
3	Where databases are involved, to ensure it is not vulnerable to SQL injection attacks.	The device shall validate or sanitize inputs or implement other mitigation measures such as prepared statements to prevent SQL injection attacks.
4	To ensure that the device's configuration portal is not susceptible to command injection attacks.	The device shall implement minimum session time outs and cross-site-request-forgery (CSRF) tokens for its configuration portal. Tool: Commix
5	To ensure that the device is protected against session hijacking attacks.	The device shall implement minimum session time outs and cross-site-request-forgery (CSRF) tokens for its configuration portal.

6	To ensure that the device is protected against cross-site scripting attacks.	-

2.7 MOBILE APPLICATION

2.7.1 The testing laboratory shall investigate the following through:

No.	Test Objectives	Remarks
1	To ensure that the app does not communicate in an unsecure manner.	Using Wireshark or other similar tools, the network traffic from the companion application shall be inspected for the use of HTTPS. The testing laboratory shall examine the TLS version and permitted cipher suites used. Tool: Wireshark, testssl.sh
2	To check that the app employs SSL pinning.	Internal Note: There are two ways to bypass SSL. 1. Adding a custom Certificate Authority to the User Certificate Store (e.g. using BurpSuite proxy). This is easy. 2. Instrumentation attack (Frida Hook). This typically required a rooted or jailbroken phone. By ensuring that the app at least utilises SSL pinning, this prevents the first method of using custom Certificate Authority certificates is prevented. This makes it slightly more difficult for an attacker to perform a man-in-the-middle attack on the SSL connection. An attacker can conduct a SSL-bypass attack on the app to conduct research on communications between the app-server-device. By monitoring the requests between the mobile app client and backend, an attacker can easily map available server-side APIs and gain insight into the communication protocol, and also replay and manipulate requests to test for server-side vulnerabilities.
3	To ensure that the app does not store sensitive	For Android applications, the application should preferably store

	credentials in an unsecure manner.	credentials using the Android KeyStore system as the bare minimum. For iOS, the application should preferably make use of the Apple Keychain services API.
4	To ensure that the mobile app is only communicating to legit URLS	Internal note: The objective of the check is quickly check that the device/app is not communicating with suspicious servers/services. This would require developers to submit a list of servers/services that the device makes use of, and then the laboratory is to verify that indeed the device/app is not connected to any other URLs outside of the list.
5	To ensure that the app does not contain hard-coded sensitive materials (private keys, router passwords, etc.)	-
6	To check that the logs do not contain sensitive information.	-

2.8 AUTHENTICATION

2.8.1 The following are applicable to all passwords available on the device not limited to the following:

- Wi-Fi passwords, configuration portal passwords, PINs, etc.

2.8.2 The TL shall also make use of the developer's checklist (particularly the developer's supporting evidence for provision 5.1 – No universal default passwords) to ensure that the device has indeed implemented all security mechanisms and policies as claimed in the checklist.

No.	Test Objectives	Remarks
1	To ensure that the device is not susceptible to a brute-force attack on its login function.	The testing laboratory is to examine the device's login functions for the possibility of a brute-force attack. This test is applicable on all login functions of the device (configuration portal, companion mobile application, etc.). The TL shall verify that the device has indeed implemented all authentication rate limiting mechanisms as described in their developer checklist, and that they are adequate and suitable to make brute-force attacks impracticable.
2	If the device comes with a pre-installed password, ensure that the device's pre-installed password is unique per device.	The pre-installed passwords of several units shall be compared to ensure that each of them is unique and sufficiently randomized. The passwords should not appear to be easily guessable.
3	If the device comes with a pre-installed password, check that the password does not appear in breach corpuses[1].	-
4	Ensure that the device does not default to a common password upon factory reset.	The tester shall perform a factory reset on two units. If the passwords of the two devices are of the same value, then the device shall be deemed as failed.

[1] Reference list of Common passwords are available at:

https://github.com/danielmiessler/SecLists/tree/master/Passwords,

2.9 OTHER ATTACKS

2.9.1 Listed below are other attack vectors that are to be considered by the TL.

No.	Test	Remarks
1	Physical attacks	Physical attack could be considered for applicable product categories, especially if it is non-damaging. Invasive/damaging physical attacks could be considered (e.g. accessing debug interfaces or even physical memory extraction) if it allows the retrieval of a universal secret.
2	Side channel analysis and fault injection	Simple side channel analysis and fault injection could be considered if allows the retrieval of a universal secret.
3	To ensure that the device does not have hardware ports such as JTAG or UART.	This test involves opening the device to examine for the presence of JTAG or UART ports on the PCB and to see if the JTAG/UART ports can be used to retrieve critical credentials or attain super user access. I.e. An attacker may be able to retrieve critical credentials (e.g. root administrator or super user access) via means of JTAG/UART access, or by manipulating the bootloader to boot the device in Single User mode. This vulnerability is severely critical if the recovered credentials are applicable to other devices of the same model or even other models/products of the same brand.
4	To ensure that the device does not have unnecessary exposed physical interfaces.	This test seeks to ensure that the device do not have unnecessary exposed physical interfaces that would present an additional attack interface. For example, if the USB port is

		only used for powering up the device, then the data pins of the USB port shall be disconnected.
5	To ensure that the device limits the number of allowed USB device classes to be connected on its USB interfaces.	This test seeks to ensure that the device limits the USB classes to the required minimum (for operation) in an effort to restrict the attack surface. Tools: USB emulator (e.g. FaceDancer)

2.10 ADDITIONAL TEST OBJECTIVES FOR WIRELESS ROUTERS

2.10.1 For wireless routers, the testing laboratory shall verify the following:

No.	Test	Remarks
1	To ensure that the wireless router is not susceptible to a brute force attack on the PIN entry implementation of the Wi-Fi Protected Setup (WPS) service.	WPS shall be disabled by default. However, if the wireless router allows the end-user to enable the WPS functionality, the testing laboratory shall investigate if the WPS - PIN entry implementation is susceptible to a practical brute force attack “Bully”. In addition, a scan shall be conducted to ensure that the WPS service is indeed unavailable even when it is configured to be disabled in the configuration portal. If WPS is instead disabled, the WPS status value should be “No”. Other values such as ‘Configured’, ‘Not Configured’ or ‘Locked’ indicates that WPS is enabled. Tool: WifiInfoView by NirSoft An exception for the use of WPS-PIN may be given if WPS is disabled in the initialized state and that a new PIN is generated after the registration of a new device using WPS-PIN.
2	To ensure that the wireless router disables the following services by default.	The following services must be disabled for routers: 1. Wi-Fi Protected Setup (WPS) 2. Home Network Administration Protocol (HNAP) 3. Remote Administration 4. Universal Plug and Play (UPNP) 5. NAT Port Mapping Protocol (NAT-PMP) Tool: NMAP and Nessus
3	To ensure that the wireless router employs a strong	Access to Residential Gateway’s administrative login page and

	password policy.	device's configuration settings shall only accept unique passwords that meet the following requirements: a. The minimum length of a password shall be 10, and shall meet at least 3 out of the following 4 complexity rules: i. Minimally 1 uppercase character (A-Z) ii. Minimally 1 lowercase character (a-z) iii. Minimally 1 digit (0-9) iv. Minimally 1 special character (punctuation and/or space) b. The password shall not have consecutive identical characters. c. Values used in the login ID and password shall not be the same.
4	To ensure that the Guest WLAN does not allow access to the configuration portal of the device, or to other devices in the main private-WLAN.	Devices on the Guest-WLAN should not be able to communicate with devices on the Private-WLAN or LAN. In addition, the devices shall not have access to the configuration portal, or other open ports and services that can be used to configure the wireless router. The guest and private WLANs must be logically separated. This can be verified by the following: 1. IP network of the guest WLAN should be on a different subnetwork compared to private-WLAN or LAN. 2. NMAP port scans and network sniffing from both directions.

2.11 ADDITIONAL TEST OBJECTIVES FOR SMART HOME HUBS

2.11.1 For Smart Home Hubs, the testing laboratory shall verify the following:

No.	Test	Remarks
1	To ensure that the pairing process of the device is secure.	-
2	To ensure that the device do not have privacy issues (e.g. interfaces such as camera, microphone, and etc. do not suffer from vulnerabilities that would leak to a compromise of the user's privacy).	-

3 REFERENCES

[1] C. S. A. o. Singapore, “CLS Publication #2 - Scheme Specifications,” Version 1.0, October 2020.

[2] C. S. A. o. 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