TR 91 : 2021
(ICS 35.030)

TECHNICAL REFERENCE

Cybersecurity labelling for consumer IoT

Singapore Standards Council

TR 91 : 2021
(ICS 35.030)

TECHNICAL REFERENCE

Cybersecurity labelling for consumer IoT

Published by Enterprise Singapore

ISBN 978-981-5024-09-8

The content of this Technical Reference was approved on 28 July 2021 by the Information Technology Standards Committee (ITSC) under the purview of the Singapore Standards Council.

First published, 2021

ITSC consists of the following members:

		Name	Representation
Chairman	:	Mr Chak Kong Soon	*Individual Capacity*
Deputy Chairman	:	Mr Harish Pillay	*Individual Capacity*
Advisor	:	Mr Yap Chee Yuen	*Individual Capacity*
Secretary	:	Mr Ong Chih Hsing	*Infocomm Media Development Authority*
Members	:	Assoc Prof Benjamin Gan	*Singapore Management University*
		Assoc Prof Huang Zhiyong	*National University of Singapore*
		Prof Li Xiaoli	*Institute for Infocomm Research*
		Mr Sam Liew	*Singapore Computer Society*
		Ms Lim Bee Kwan	*Government Technology Agency*
		Mr Lim Soon Chia	*Cyber Security Agency of Singapore*
		Mr Kelvin Ng	*Nanyang Polytechnic*
		Mr Ong Hian Leong	*Individual Capacity*
		Mr Andy Phang	*Infocomm Media Development Authority*
		Mr Andy Sim	*SGTech*

ITSC set up the Technical Committee on Internet of Things (IoT) to oversee the preparation of this standard. The Technical Committee consists of the following members:

		Name	Representation
Chairman	:	Mr Lim Chee Kean	*Individual Capacity*
Secretary	:	Mr Steven Tan	*Infocomm Media Development Authority*
Members	:	Mr Jacky Bek	*Individual Capacity*
		Mr Vito Chin	*Microsoft*
		Mr Hui Wing Hong	*Singapore Polytechnic*
		Mr Jayanth Nagarajan	*Internet Society (Singapore Chapter)*
		Mr Colin Koh	*Singapore Industrial Automation Association*
		Mr Ken Koh	*Singapore Chinese Chamber of Commerce & Industry*
		Mr Benjamin Lee	*Home Team Science & Technology Agency*
		Mr Lee Siew Kit	*Changi Airport Group*
		Assoc Prof Ng Teck Khim	*National University of Singapore*
		Mr Gerry Ong	*GPS Lands (Singapore) Pte Ltd*
		Mr Quek Yang Boon	*Government Technology Agency*
		Mr Senthil Nathan	*Capgemini Pte Ltd*
		Mr Sim Bak Chor	*Infocomm Media Development Authority*

Members	:	Dr Tan Guan Hong	*Individual Capacity*
		Mr Jonathan Tan	*SGTech*
		Mr Vinod Bijlani	*Hewlett Packard Enterprise International Pte Ltd*

The Technical Committee set up the Working Group on Cybersecurity Labelling for Consumer IoT to prepare this standard. The Working Group consists of the following experts who contributed in their *individual capacity*:

		Name
Co-Convenors	:	Mr Lim Soon Chia
		Dr Woo Kang Wei
Members	:	Dr Chiew Tuan Kiang
		Mr Goh Eng Koon
		Prof Keoh Sye Loong
		Mr Daryl Koh
		Dr Melvyn Kuan
		Mr Vincent Ong
		Dr Debora Poon
		Mr Sanjay Kumar Das
		Prof Sudipta Chattopadhyay
		Dr Tan Guan Hong
		Mr Tan Jingwei Emil
		Mr Vinod Bijlani

The organisations in which the experts of the Working Group are involved are:

AN Security Pte Ltd
Aztech Technologies Pte Ltd
Cyber Security Agency of Singapore
Hewlett Packard Enterprise International Pte Ltd
Government Technology Agency
Oracle Corporation Singapore Pte Ltd
QuantumCIEL Pte Ltd
Rekindle Pte Ltd
Singapore University of Technology and Design
ST Engineering Land Systems Ltd
UL International Singapore Pte Ltd
University of Glasgow

(blank page)

Contents

Foreword

This Technical Reference was prepared by the Working Group (WG) on Cybersecurity Labelling for Consumer IoT set up by the Technical Committee on Internet of Things (IoT) under the purview of ITSC.

This TR makes reference to the schemes and its related publications developed by the Cybersecurity Certification Centre (CCC) as well as international standards and guidelines. It is intended to raise the cybersecurity hygiene of consumer IoT devices, and create a safer and more secure cyberspace through the use of labels. The TR explains the fundamental concepts that drive the labelling scheme and its implementation to help stakeholders participate in the process of improving cybersecurity standards for consumer IoT devices. It also puts the activities relating to cybersecurity labelling in Singapore in the context of existing international standards.

This TR is a provisional standard made available for application over a period of three years. The aim is to use the experience gained to update the TR so that it can be adopted as a Singapore Standard. Users of the TR are invited to provide feedback on its technical content, clarity and ease of use. Feedback can be submitted using the form provided in the TR. At the end of the three years, the TR will be reviewed, taking into account any feedback or other considerations, to further its development into a Singapore Standard if found suitable.

In preparing this TR, reference was made to the following publications:

1. CLS Publication No. 1 – Cybersecurity Labelling Scheme (CLS) – Overview of the Scheme
2. CLS Publication No. 2 – Cybersecurity Labelling Scheme (CLS) – Scheme Specifications
3. CLS Supplementary Publication – Cybersecurity Labelling Scheme (CLS) – Minimum Test Specifications and Methodology for Tier 4
4. ETSI EN 303 645 – Cyber Security for Consumer Internet of Things: Baseline Requirements
5. IMDA Guidelines – Internet of Things (IoT) Cyber Security Guide
6. The Internet of Things (IoT) Security Landscape Study
7. NISTIR 8259 – Foundational Cybersecurity Activities for IoT Device Manufacturers
8. NISTIR 8259A – IoT Device Cybersecurity Capability Core Baseline

Acknowledgement is made for the use of information from the above publications.

This TR is expected to be used by manufacturers, developers, testing bodies and suppliers of consumer IoT devices.

Attention is drawn to the possibility that some of the elements of this TR may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as "Mature Standards". Mature Standards will not be subject to further review, unless there are requests to review such standards.*

2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore and the Singapore Standards Council shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.*

3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

Cybersecurity labelling for consumer IoT

0 Introduction

Globally, we are witnessing an explosive increase in the number of IoT (Internet of Things) devices. Consumer smart devices are usually developed within a short time-to-market cycle. The relative low price-points and low margins for consumer items also mean that these devices are often not designed or manufactured with adequate provisions for cybersecurity. Fundamental security weaknesses such as universal default passwords can be commonly found in such products. As these connected devices proliferate, the lack of adequate provisions for cybersecurity in such devices creates extensive attack surfaces increasing cybersecurity risks.

While formal evaluation and certification schemes such as Common Criteria (CC) provide high level security assurance for IoT devices, they are often not feasible for consumer IoT products as the evaluation costs and certification duration can be prohibitive for most device developers. A scheme tailored to provide guidance for developers and users on essential security traits for such devices can encourage the incorporation of good cybersecurity design in the product development cycle.

The cybersecurity label provides an easy-to-use method for consumers to recognise the level of security in such products. Consumers are thereby empowered to make informed purchasing decisions. Cybersecurity labelling enhances consumer awareness and incentivises developers to make products with better security features for the market, leading towards a safer and more secure cyberspace.

1 Scope

This standard introduces a multi-levelled and cost-effective cybersecurity labelling for consumer IoT. It aims to raise the cybersecurity hygiene of the IoT ecosystem by improving the transparency of cybersecurity provisions. Cybersecurity labelling for consumer IoT provides a basic level of security assurance through the elimination of common vulnerabilities using a simple, tiered, and progressive assessment model for IoT devices that avoids resource-intensive security evaluations.

Cybersecurity labelling for consumer IoT provides a basic level of security hygiene which is typically expected for consumer IoT, i.e. to be able to deter casual adversaries utilising common attack vectors such as default factory credentials or the exploitation of vulnerable protocols. Cybersecurity labelling for consumer IoT does not offer formal security assurance. Given sufficient time, determined adversaries who possess advanced skillsets and tools can be capable of compromising such IoT devices, regardless of whether it is labelled. Users seeking higher security assurance—e.g. enterprise, manufacturing, industrial applications and healthcare—are strongly recommended to consider devices certified under formal evaluation and certification schemes[1].

2 Normative references

The following referenced documents are indispensable for the application of this standard. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories

[1] Details relating to these higher assurance schemes are available on the Cyber Security Agency of Singapore (CSA)'s website: https://www.go.gov.sg/common-criteria.