Singapore Standards Council

TR 64 : 2018
(ICS 35.030)

TECHNICAL REFERENCE

Guidelines for IoT security for smart nation

Published by

Enterprise Singapore

TR 64 : 2018
(ICS 35.030)

TECHNICAL REFERENCE

Guidelines for IoT security for smart nation

All rights reserved. Unless otherwise specified, no part of this Technical Reference may be reproduced or utilised in any form or by any means, electronic or mechanical, including photocopying and microfilming, without permission in writing from Enterprise Singapore. Request for permission can be sent to: standards@enterprisesg.gov.sg.

ISBN 978-981-47-8497-9

This Technical Reference was approved by the Information Technology Standards Committee on behalf of the Singapore Standards Council on 7 May 2018.

First published, 2018

The Information Technology Standards Committee, appointed by the Standards Council, consists of the following members:

		Name	Capacity
Chairman	:	Mr Yap Chee Yuen	*Individual Capacity*
1st Deputy Chairman	:	Mr Chak Kong Soon	*Singapore Computer Society*
2nd Deputy Chairman	:	Ms Samantha Fok	*Infocomm Media Development Authority*
Secretary	:	Mr Yip Mann Fai	*Infocomm Media Development Authority*
Members	:		
		Mr Chau Chee Chiang	*Government Technology Agency*
		Mr Cheong Tak Leong	*Enterprise Singapore*
		Assoc Prof Benjamin Gan Kok Siew	*Singapore Management University*
		Assoc Prof Huang Zhiyong	*National University of Singapore*
		Mr Kendrick Lee	*Information Technology Management Association*
		Mr Lim Soon Chia	*Cyber Security Agency*
		Mr Kelvin Ng	*Nanyang Polytechnic*
		Mr Ni De' En	*National Research Foundation*
		Mr Harish Pillay	*Internet Society (Singapore Chapter)*
		Mr Tan Boon Yuen	*Singapore Polytechnic*
		Mr Victor Tan Hein Kiat	*Defence Science and Technology Agency*
		Dr Henry Wong Chuen Yuen	*Agency for Science, Technology and Research*
		Mr Wong Wai Meng	*SGTech*

The Technical Committee on Internet of Things, appointed by the Information Technology Standards Committee and responsible for the preparation of this standard, consists of representatives from the following organisations:

		Name	Capacity
Co-Chairmen	:	Ms Lee Wan Sie	*Infocomm Media Development Authority*
		Mr Lim Chee Kean	*Ascent Solutions Pte Ltd*
Secretary	:	Mr Steven Tan	*Infocomm Media Development Authority*
Members	:	Mr Ani Bhalekar	*SGTech*
		Mr Jacky Bek	*National Environment Agency*
		Mr Sebastien Blandin	*IBM Singapore*
		Mr Vito Chin	*Microsoft Singapore*
		Dr Chuah Jun Wei	*Surbana Jurong*
		Mr Gordon Mark Falconer	*Schneider Electric*
		Mr Goh Eng Koon	*Amazon Web Services*
		Mr Kevin Goh	*Smart Nation and Digital Government Office*

COPYRIGHT

Members	:	Mr Harish Pillay	*Internet Society (Singapore Chapter)*
		Mr Colin Koh	*Singapore Industrial Automation Association*
		Ms Koh Kok Theng	*Housing & Development Board*
		Mr Lee Siew Kit	*NCS Pte Ltd*
		Ms Lim Siew Eng	*Centre of Innovation (Electronics & IoT), Nanyang Polytechnic*
		Mr Gerry Ong	*GPS Lands (Singapore) Pte Ltd*
		Ms Quek Soo Boon	*Singapore Chinese Chamber of Commerce and Industry*
		Mr Quek Yang Boon	*Government Technology Agency*
		Prof Sekhar Narayana Kondepudi	*National University of Singapore*
		Mr David Tan Cheow Beng	*ST Electronics*
		Dr Tan Guan Hong	*Individual Capacity*
		Mr Eddie Teo	*StarHub*
		Mr Teo Shin Jen	*Singapore Polytechnic*
		Mr Zhou Yimin	*Ministry of National Development*

The Working Group on Internet of Things Security, appointed by the Technical Committee to assist in the preparation of this standard, comprises the following experts who contribute in their *individual capacity*:

		Name
Convenor	:	Dr Woo Kang Wei
Secretary	:	Mr Ong Chih Hsing
Members	:	Mr Bryce Boland
		Mr Dheeraj Chandwani
		Dr Goh Kwong Huang
		Dr Kang Meng Chow
		Prof Lam Kwok-Yan
		Mr Lee Ser Yen
		Mr Leng Soon Pak
		Dr Lua Rui Ping
		Mr Eric Seow
		Mr Sim Bak Chor
		Mr Henry Tan
		Dr Wang Weiguo
		Mr Wong Onn Chee
		Dr Yap Chern Nam
		Mr Yun Ta Chun
Resource Members	:	Mr Koh Lian Chong
		Mr Tao Yao Sing

COPYRIGHT

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

Amazon Web Services
C3S Pte Ltd
Cyber Security Agency
FireEye Singapore Pte Ltd
Government Technology Agency
Infineon Technologies Asia Pacific Pte Ltd
Infocomm Media Development Authority
Infotect Security Pte Ltd
KPMG Services Pte Ltd
Land Transport Authority
Nanyang Technological University
QuantumCIEL LLP
Temasek Polytechnic
Thales Solutions Asia Pte Ltd

COPYRIGHT

Contents

Page

Foreword 7

1 Scope 9
2 Normative references 9
3 Definitions, abbreviations and acronyms 9
4 Security needs 14
5 Security concepts 14
6 Recommendations 28

Annexes

A Relationship with other standards 35
B IoT common vulnerabilities 40
C Guidance on the use of this Technical Reference 46

Tables

1 Examples to illustrate usage of security categories 18
2 Examples of IoT threat categories 19
3 Examples of IoT attack surfaces 21
4 IoT security requirement categories 27
5 Common requirements for cryptographic support 28
6 Common requirements for security function protection 28
7 Common requirements for identification and authentication 29
8 Common requirements for network protection 30
9 Common requirements for data protection 31
10 Common requirements for access protection 31
11 Common requirements for security management 32
12 Common requirements for resiliency support 33
13 Common requirements for security audit 33
14 Common requirements for lifecycle protection 34
A.1 IoT common standard interfaces 36
A.2 Securing IoT common standard interfaces 37
A.3 Mapping to IoT security requirement categories 39
B.1 OWASP top 10: vulnerabilities and possible mitigations 40
B.2 Video surveillance products/solutions mitigations 41
B.3 Mobile devices and wearables mitigations 42
B.4 Industrial devices mitigations 44

COPYRIGHT

Page

C.1 Applicability for IoT security principles, functional layers and threat categories ________ 48
C.2 Applicability to IoT lifecycle stages ________ 53
C.3 Applicability to stakeholders ________ 54

Figures

1 IoT threat modelling outline ________ 15
2 IoT security model ________ 16
3 Security properties ________ 17
4 Security impact categories ________ 17
5 IoT threat categories________ 18
6 Aspects of threat assessment ________ 20
7 IoT attack surface categories ________ 21
8 IoT operating environments ________ 23
9 IoT lifecycles________ 24
10 Applying IoT security design principles ________ 26
A.1 IoT standards suite for Smart Nation ________ 35
A.2 Typical IoT solution architecture________ 36
A.3 Relationship with ISO/IEC 27001 and ISO/IEC 15408 ________ 38
C.1 Usage overview ________ 46
C.2 IoT security requirement category relationships ________ 47

Bibliography ________ 59

COPYRIGHT

Foreword

This Technical Reference (TR) was prepared by the Working Group on IoT Security appointed by the Technical Committee on Internet of Things (IoT) under the direction of the Information Technology Standards Committee.

The objectives of this TR is to provide guidelines to safeguard the confidentiality, integrity and availability of large-scale IoT systems.

This TR will help to:

- establish the foundational security concepts and terminology for IoT systems;
- define a holistic approach for identifying and mitigating the threats and vulnerabilities of IoT systems; and
- provide recommendations on common security requirements for IoT systems.

Ultimately, the TR will help to promote the development of and foster mass adoptions of secure IoT systems.

This TR can be used by:

- Users who want to procure secure IoT systems.
- Developers who want to design, develop and deploy secure IoT products and systems. Examples of developers include solution architects, programmers, manufacturers and system integrators.
- Operators who need to roll-out, configure, operate, maintain and de-commission IoT systems securely. Examples of operators include service providers and system operators.

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

1. ISO/IEC 15408-1 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
2. ISO/IEC 15408-2 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components
3. ISO/IEC 15408-3 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components
4. FIPS PUB 199 Standards for security categorization of federal information and information systems
5. FIPS PUB 200 Minimum security requirements for federal information and information systems

Some definitions in Clause 3 of this TR are based on the ISO/IEC publications and are reproduced with the permission of the International Organization for Standardization.

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

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.

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.*

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 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.*

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

Guidelines for IoT security for smart nation

1 Scope

This Technical Reference (TR) introduces the foundational security concepts and terminology for Internet of Things (IoT) systems and demonstrates their applications. A holistic approach for identifying and mitigating the threats and vulnerabilities of IoT systems is also introduced. Guidance is provided on how to conduct threat modelling for IoT.

This TR also identifies four basic IoT security design principles and demonstrates their applications. Guidance is also provided on how to classify IoT security requirements and their usefulness in supporting the identification of security requirements. For each category, security requirements are provided along with examples of how to mitigate common IoT vulnerabilities.

Annex A shows the relationship of this TR with other IoT standards. Annex B list the common vulnerabilities and possible mitigations to these vulnerabilities. Guidance on the use of this TR is given in Annex C.

2 Normative references

There are no normative references for this TR.