Singapore Standards Council

TR 67 : 2018
(ICS 35.030; 35.240.80)

TECHNICAL REFERENCE

Connected medical device security

Published by

Enterprise Singapore

TR 67 : 2018
(ICS 35.030; 35.204.80)

TECHNICAL REFERENCE

Connected medical device security

ISBN 978-981-48-3519-0

This Technical Reference was approved by the Information Technology Standards Committee on behalf of the Singapore Standards Council on 28 September 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*
Deputy Chairman	:	Mr Chak Kong Soon	*Singapore Computer Society*
Secretary	:	Mr Tao Yao Sing	*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*
		Mr Hong Tse Min	*Infocomm Media Development Authority*
		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	*Agency for Science, Technology and Research*
		Mr Wong Wai Meng	*SGTech*

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

		Name	Capacity
Chairman	:	Dr Julian Sham	*Accenture Pte Ltd*
Secretary	:	Mr Andy Tan	*National University Health System*
Members	:	Mr Victor Chai	*Integrated Health Information Services*
		Dr Adam Chee	*Binary HealthCare*
		Mr Chiew Sze Fang	*Cisco*
		Mr Yanto Fu	*Integrated Health Information Services*
		Dr Goh Min Liong	*Changi General Hospital*
		Mr John Heng	*3M Singapore*
		Mr Huang Hung Choong	*Intel Technology Asia Pte Ltd*
		Mr Kalyan Madala	*IBM*
		Dr Lee Chi-Ying	*3M Singapore*

Members	:	Dr Lim Soh Min	*Cadi Scientific Pte Ltd*
		Ms Lin Anle	*Health Sciences Authority*
		Mr Michael Low	*Cadi Scientific Pte Ltd*
		Ms Caroline Ng	*Adept Health Pte Ltd*
		Mr Ong Leong Seng	*Integrated Health Information Services*
		Mr Poh Chee Khun	*Health Sciences Authority*
		Mr John Ramesh	*TÜV Rheinland Singapore Pte Ltd*
		Ms Jocelyn Delos Reyes	*TÜV Rheinland Singapore Pte Ltd*
		Mr Vincent Seah	*Integrated Health Information Services*
		Mr Sethuraman Rama	*Health Sciences Authority*
		Mr Sim Bak Chor	*Infocomm Media Development Authority*
		Ms Liz Tan	*TÜV Rheinland Singapore Pte Ltd*
		Mr Tan Yuh Cherng	*ST Electronics*
		Mr Albert Wang	*Intel Technology Asia Pte Ltd*
		Mr Steven Wong	*Singapore Institute of Technology*

The Working Group on Connected Medical Device 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	:	Mr Vincent Seah
Secretary	:	Mr Victor Chai
Members	:	Ms Judy Cheng
		Mr Cheong Yu Chye
		Mr Kenneth Er
		Mr John Ramesh
		Ms Jocelyn Delos Reyes
		Mr Andy Tan
		Mr Alan Tang
		Mr Zhuang Guangyi

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

Health Sciences Authority
Integrated Health Information Systems
IoT Labs
MiRXES Pte Ltd
National University Health System
ST Engineering
TÜV Rheinland Singapore Pte Ltd

(blank page)

Contents

Annexes

Tables

Figures

Foreword

This Technical Reference (TR) was prepared by the Working Group on Connected Medical Device Security appointed by the Technical Committee on Health Informatics under the direction of the IT Standards Committee.

Due to the increasing frequency and severity of malware and cybersecurity attacks, a medical device can no longer be just considered a simple device to collect health data, perform clinical administration tasks or provide medical advice to the clinician. It has the capability to manipulate, alter, store and transmit data and advice to the clinician on the health status of the patient. With that the standards of preventing these attacks should be increased, this TR would be able to help organisations in adopting the standards effectively.

In view of the risks, this TR is developed to give the provisions on the pre-implementation and post-implementation of connected medical devices. The TR highlights the controls that management and institutions should take into consideration when evaluating a connected medical device. The TR should be used for the following purposes:

- Education for the management on the risks and recommended security controls that are required when implementing connected health devices;
- Evaluation process on the potential procurement of connected health devices;
- Consideration of the risk treatment of operating connected health devices within the network.

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. Due to the fast-changing security landscape and advances in medical device technologies and capabilities, the TR may be revised earlier than the typical three-year period if deemed necessary.

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

- IEC/TR 80001-1 Application of Risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities
- IEC/TR 80001-2-1 Application of risk management for IT-networks incorporating medical devices – Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples
- IEC/TR 80001-2-2 Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
- ISO 31000:2009 Risk Management – Principles and Guidelines
- ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements
- ISO 14971: 2012 Medical devices – Application of risk management to medical devices
- ISO 13485: 2012 Medical Devices – Quality management systems – Requirements for regulatory purposes
- MDS2 2013 Manufacturer Disclosure Statement for Medical Device Security
- HSA (Health Sciences Authority) GN-13 and GN-14 Guidance on Risk Classification
- IMDRF/SaMD WG/N12Final:2014 “Software as a Medical Device”: Possible Framework for Risk Categorization and Corresponding Considerations
- FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
- FDA Postmarket Management of Cybersecurity in Medical Devices

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

Acknowledgement is also made to the following organisations for the reproduction of their materials in this TR:

- International Electrotechnical Commission (IEC) for permission to reproduce information from IEC/TR 80001-2-2:2012 into Annex A of this TR. All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced, nor is IEC in any way responsible for the other content or accuracy therein.

- National Electrical Manufacturers Association (NEMA) for permission to reproduce its Standards Manufacturer Disclosure Statement for Medical Device Security (MDS2) Form HN 1-2013.

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.*

Technical Reference for connected medical device security

0 Introduction

0.1 Motivation

Medical devices are key requirements of hospitals and clinics as they provide support to doctors and nurses in terms of diagnosis, monitoring, treatment, investigation and more. Medical devices traditionally are standalone devices used to perform specific medical procedures or actions. However, with the progress of technology, medical devices now have evolved to be network connected. As such, they are exposed to more risks as compared to traditional medical devices.

Although medical devices are now more technologically advanced, many of them have significant security risks due to various reasons, such as interoperability issues, lack of patch support, malware protection updates and others. These security risks not only expose them to potential attacks, but also expose the internal enterprise network to external attackers. In addition, medical devices pose risks to patient safety and confidentiality.

This TR aims to help healthcare institutions and professionals better understand the security risks found in connected medical devices and to provide a framework for them to mitigate these risks in an enterprise network.

0.2 Current state of medical device security

Hospital outreach and community healthcare support services

Medical devices have evolved along with the progress of technology in the last decade. Medical devices are now more connected and more interlinked compared to those of the past. They can now be used to collect health data such as patient vital signs and electro-cardio waveforms, and can provide medical advice to clinicians. They also have the capability to store, transmit and advise clinicians on the health status of the patient. In most hospitals, they are usually standalone devices with no capability to be integrated with the hospital’s electronic medical record database. However, at present, hospitals or community healthcare centres may not have the capability to ensure their devices are properly secured, even though they may have some risk management framework in place. The inability to secure network medical devices may pose a risk to the hospital network.

Personal devices and the Internet of Things (IoT)

The use of personal devices and the Internet of Things (IoT) are common in today’s healthcare to allow objects to be sensed and/or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit. Devices now run on applications that improve ease of use. Wireless communication security, regardless of technology, can be broadly categorised as intrinsic mechanism and extrinsic mechanism. Intrinsic mechanism refers to the wireless network’s inherent security capabilities, whereas extrinsic mechanism refers to device-specific security mechanisms designed by the device’s developer.

Most wireless network technologies come with their own security capabilities or intrinsic mechanism. The following list summarises some of the common wireless technologies and their security capabilities:

a) Wi-Fi
   - Wired Equivalent Privacy (WEP)
   - Wi-Fi Protected Access (WPA)

b) Bluetooth Smart or previously known as Bluetooth Low Energy
   - Just Works
   - Passkey Entry
   - Out-of-band

c) Zigbee
   - Network key
   - Link key

d) LORA
   - Network session key
   - Application session key
   - Application key

It is important to understand each applied technology's security capability and ensure at least one form of them is implemented. For a technology without an intrinsic mechanism, it is prudent to ensure at least one form of extrinsic mechanism is implemented.

Each extrinsic mechanism can be uniquely designed for each device. Typically, the extrinsic mechanism should be independent of the wireless technology intrinsic mechanism, so even if the network intrinsic capability is compromised, there is still an additional layer of security provided by the extrinsic mechanism. In other words, the extrinsic mechanism can work with the wireless network intrinsic capability to enhance the device's communication security.

Some common extrinsic security capability/mechanisms include:

a) Additional encryption
   - Apart from the encryption provided by the network intrinsic capabilities, some developers can add additional encryption to enhance the device's communication security.

b) Challenge response
   - A standard question and answer scheme whereby the initiating party will have to answer a random or fixed question by the accepting party, or vice versa.

1 Scope

1.1 Objectives

This TR intends to provide a framework for healthcare institutions and professionals to mitigate the security risks of connected medical devices in the following scenarios:

- Procurement of new connected medical devices: this TR give provisions on what to include in procurement requirement documents (such as RFPs) to ensure that a relevant baseline set of security requirements is included.
- Day-to-day operations of existing connected medical devices: this TR provides broad recommendations on the security process and controls to consider for the operation of existing connected medical devices.

The framework will discuss the process, contractual and security controls that should be considered when implementing a connected medical device into an enterprise network or when de-commissioning a device from the network.

1.2 Target devices

This TR focuses primarily on connected medical devices, communication channels and the interfaces with device integration solutions.