CONSULTATION PAPER ISSUED BY

THE INFOCOMM MEDIA DEVELOPMENT AUTHORITY

ON

IOT CYBER SECURITY GUIDE

25th January 2019

CONTENTS

1. INTRODUCTION

Internet of Things (IoT)

1.1 The Internet of Things ("**IoT**") paradigm is one where devices are connected to one another, and are able to either convey information about the surroundings or themselves, or be controlled by others to perform some actions. The uses of IoT have been gradually integrated into our daily life, increasing our dependence on them. They include health monitoring, tracking public transport (buses, taxis, etc), and controlling our home appliances remotely. In addition, there is also a growing trend of public sector and industry uses of IoT sensors and actuators. For example, street lighting can now act as IoT devices that use radar to detect unusual situations on the road and convey information back to the traffic controller, or they could be autonomous in decision making. The Smart Street Lighting market is estimated to reach US$39.0 billion by 2022[1].

1.2 While the connections of these large number of devices could help enhance our lives, it also means that the disruptions to their designed operations, either intentionally or unintentionally, will likely bring great inconvenience and possibly monetary losses to users and providers of IoT technology. In smart manufacturing, disruptions to the IoT devices used in the production line would mean that products may not be delivered on time, or that they could be made inferior because quality checks become defective.

1.3 If not managed properly, these IoT devices could also be exploited to launch attacks on other networks, resulting in Distributed Denial of Services ("**DDoS**"). While traditional mitigation techniques have been sufficient to cushion the effects as the network capacity is much bigger than the size of the Botnet (network of infected IoT devices), they will not be sustainable for long with the ever increasing Botnet size.

1.4 Besides the need to secure IoT devices from attacks and being used for malicious activities, data stored in the devices will also need to be protected against unauthorised access as large amount of personal data could be collected and stored in the devices. For example, wearables can monitor and store information of user's living habits such as steps taken, heart rate, sleep patterns, etc.

1.5 In building a more digitally connected Singapore, it is important to secure our infrastructure and the IoT devices and networks deployed. While many users and/or vendors are aware of the need to implement security for their IoT devices

[1] https://www.marketwatch.com/press-release/smart-street-lighting-market-to-reach-3980-billion-by-2022-2018-06-13

and networks, they do not know where and how to start. There is currently also no regulatory guidance for the implementation of security for private or personal use of IoT devices in Singapore; users can easily buy IoT devices without any built-in security features. IMDA has thus developed an IoT Cyber Security Guide (hereafter refer to as the "**Guide**"), providing recommendations and guidance to IoT users and vendors in securing their IoT devices and networks.

IoT Cyber Security Guide

1.6 The Guide aims to promote best practices in implementing security for IoT devices and networks, and to cultivate awareness that security should not be an afterthought but needs to be built-in during the design stage. In this initial version of the Guide, key principles of IoT security are explained, and recommendations to essential ways of tightening security are also provided. With the rapid evolution of technologies and threats, the Guide will need to be updated accordingly in response to the changes.

1.7 Although there are several similar documents on IoT security published by organisations in overseas jurisdictions, there is still merit in developing one for Singapore's adoption. First, local enterprises and government agencies will be able to take reference from a common guide, adopting the same lingo, terminology, and approaches in addressing security threats. This will also facilitate better integration of IoT networks deployed in Singapore, if required. Second, threats that are more relevant to the local context will be identified, allowing vendors and users to better focus their resources in implementing more relevant security solutions. Third, this guide seeks to cover broader areas, providing not only recommendations for both the deployment and operating phases of IoT systems but also, threat modelling and vendor disclosure checklists, which are currently not available in many similar documents.

1.8 IMDA would like to seek views and comments from members of the public and the industry on the proposed IoT Cyber Security Guide which is enclosed with this Consultation Document.

1.9 This consultation will be open for a period of six weeks, and will close by 12 noon on 8th Mar 2019.

2. BASELINE RECOMMENDATIONS

2.1 It is important that a basic level of security is built into each IoT device. The Baseline Recommendations section thus lists a set of proposed essential steps that could be taken by various parties at the deployment and operating phases to ensure a core level of security in IoT devices and networks. As the list is not meant to be exhaustive, adherence to these recommendations does not give IoT devices and networks total immunity from security threats. However, adopting the recommendations will offer a base level of protection, which would be adequate to address most of the common and straightforward cyberattacks.

Question 1: *IMDA would like to seek views and comments on the usefulness of the security measures given in the Baseline Recommendation sections of the Guide, and whether they are adequate and relevant. What other security measures do you think should be included in the Baseline Recommendations?*

3. THREAT MODELLING CHECKLIST

3.1 Threat modelling is a systematic approach to identify and understand potential vulnerabilities and threats in a system, prioritise them, and thereafter identify suitable risk-mitigation techniques to address them. Threat modelling allows limited resources to be applied efficiently in addressing the security threats and it is thus widely adopted by many organisations.

3.2 There is no 'right' approach for threat modelling as each has its own way of evaluating threats and organising data. Nonetheless, threat modelling is generally carried out based on the steps below:

i) Determine the attack surface of the device/software/network/services
ii) Assign risk level to the various threats identified
iii) Consider different ways to mitigate threats identified

In some threat modelling approaches, tests are conducted to ensure that the proposed mitigating solutions are rigorous.

3.3 The approach to threat modelling in the Guide has been structured in the form of a checklist, which offers an organised way for system developers to examine if they have been following essential steps. It is thus necessary to ensure that all the important tasks have been listed and that each task set out in the checklist is adequate.

Question 2: *IMDA would like to seek views and comments on the usefulness, as well as the clarity and adequacy of the threat modelling checklist proposed in the Guide. What additional items do you think should be included in the checklist?*

4. VENDOR DISCLOSURE CHECKLIST

4.1 Uses of IoT have spanned across almost all sectors today and many of these IoT users are traditionally not well versed with cybersecurity matters. Hence, it is assessed to be beneficial to provide these users a checklist, allowing them to use it as a guide for the procurement of IoT systems, i.e., to scope the vendor disclosure checklist as part of the tender submission requirement. This will help ensure vendors/tenderers include basic security measures implemented in their products and/or services and allow users to compare the security measures proposed and/or implemented by vendors/tenderers in their submissions. Vendors can also voluntarily choose to adopt the checklist and self-disclose the security measures taken, providing confidence to their potential customers on the products/systems.

***Question 3**: IMDA would like to seek views and comments on the usefulness and adequacy of the proposed vendor disclosure checklist in the Guide and the items listed within. For example, which checklist items are most, least or not applicable to you. What other items do you think should be included in the checklist?*

5. INFORMATIVE ANNEXES

5.1 Annex A introduces the security concepts used in the Guide for a holistic approach to identify and mitigate the threats and vulnerabilities of IoT systems.

5.2 Annex B provides a case study on Home Control System (HCS) that demonstrates the application of the recommendations in the Guide.

***Question 4**: IMDA would like to seek views and comments on the usefulness of providing Annex A, which explains the foundational concepts on threat modelling and how to secure an IoT system.*

***Question 5**: IMDA would like to seek views and comments on the usefulness of Annex B and seek suggestions on what other case studies could be included.*

6. OVERALL IOT CYBER SECURITY GUIDE CONTENT

***Question 6**: IMDA would like to seek views and comments on the usefulness and the clarity of the Guide, and whether the coverage of the Guide is sufficient. What other areas do you think the Guide should also cover, which would further help the industry to better secure IoT systems.*

***Question 7:** IMDA would like to seek views and comments on whether it would be useful and practical to introduce a certification scheme for IoT devices to be deployed in Singapore. If so, should the certification be voluntary or mandatory?*

7. INVITATION TO COMMENT

7.1 IMDA would like to seek views and comments from members of the public and the industry on the issues outlined in the above sections.

7.2 Parties that submit comments on the issues identified in this Consultation Document should organise their submissions as follows:

i. Cover page (including their personal/company particulars and contact information);
ii. Table of contents;
iii. Summary of major points (structured to follow the individual Parts of the Consultation Document);
iv. Statement of interest;
v. Comments (in response to the Questions set out in the Consultation Document and any other comments); and
vi. Conclusion.

Supporting material may be placed in an Annex.

7.3 Where feasible, parties should identify the specific sections of the Consultation Document on which they are commenting and provide reasons for their proposals.

7.4 All submissions must reach IMDA by 12 noon on 8th March 2019. Softcopy of submissions in both Microsoft Word and Adobe PDF format should be provided. Parties submitting comments should include their personal/company particulars as well as the correspondence address, contact number and email addresses on the cover page of their submission. All comments should be addressed to:

Ms Aileen Chia
Deputy Chief Executive / Director-General (Telecoms & Post)
Infocomm Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Please submit your softcopy via email to: Consultation@imda.gov.sg

7.5 IMDA reserves the right to make public any written submissions and to disclose the identity of the source. Commenting parties may request confidential treatment of any part of the submission that the commenting party believes to be proprietary, confidential or commercially sensitive, with supporting

justification for IMDA's consideration. In such cases, the submission must be provided in a non-confidential form suitable for publication, with any confidential information redacted as necessary and placed instead in a separate annex.

7.6 If IMDA grants confidential treatment, it will consider, but will not publicly disclose the information. If IMDA rejects the request for confidential treatment, it will return the information to the party that submitted it and will not consider the information as part of its review. As far as possible, parties should limit any request for confidential information submitted. IMDA will not accept any submission that requests confidential treatment for the entire, or a substantial part of, the submission.