Telecommunications Regulatory Affairs Advisory Committee

Proposed Code of Practice on Operation and Management of Internet of Things Devices for Public Telecommunications Services

PURPOSE

This paper seeks Members' views on the proposal of issuing a code of practice ("CoP") to set out recommended practices on operation and management of Internet of Things ("IoT") devices for public telecommunications services.

BACKGROUND

2. At present, mobile network operators licensed under the Unified Carrier Licence ("UCL") and service providers licensed under the Wireless Internet of Things ("WIoT") Licence (hereinafter collectively referred as "IoT service providers") provide wireless connections for their customers to connect IoT devices to the public telecommunications networks. These IoT devices may employ different wireless technologies, such as Narrowband-IoT operating in the frequency spectrum assigned for the provision of public mobile services, or Low-Power Wide Area Network (LPWAN) such as Sigfox[1] or LoRa[2] operating in the 920 – 925 MHz band on a shared and uncoordinated basis.

3. Pursuant to General Condition 5.1 of the UCL and the WIoT Licence, IoT service providers are required to provide a good, efficient and continuous service in a manner satisfactory to the Communications Authority ("CA"). Under Special Conditions 1.2 of the UCL and the WIoT Licence, the

[1] Sigfox is a wireless technology developed by the French company Sigfox for long range communications at low bit rate. For details, please refer to http://www.sigfox.com.

[2] LoRa is a wireless technology based on Long Range Wide Area Networks ("LoRaWAN") protocol developed by the LoRa Alliance for long range communications at low bit rate. For details, please refer to https://lora-alliance.org.

CA may issue code of practice or guidelines for the purpose of providing practical guidance to the licensees in respect of the provision of satisfactory service and the protection and promotion of the interests of consumers of telecommunications goods and services.

OPERATION AND MANAGEMENT OF IOT DEVICES

4. IoT devices are typically used for automated machine-to-machine type applications such as lighting control, energy meter management, facilities managements, parking space monitoring, etc. Most of these applications will collect information from IoT devices such as temperature, movement, battery status and other environment data for monitoring, surveillance and control purposes.

5. With the development of new wireless technologies such as the fifth generation ("5G") mobile technologies and new smart city applications, it is expected that there will be a massive number of new IoT devices connecting to public telecommunications networks in the coming years, some of which may also support sophisticated and even mission critical applications such as autonomous vehicles. The proliferation of IoT devices deployed for a wide range of applications and the collection/processing of a vast amount of data using IoT devices will bring challenges for proper data protection and security. There is thus a need to ensure proper operation and management of these devices connecting to public telecommunications networks to safeguard the interests of both businesses and consumers in the IoT era.

THE PROPOSAL

6. Having regard to the characteristics and applications of IoT devices as well as overseas developments on best practices for operation and management of IoT devices (see **Annex**), it is proposed that a voluntary CoP be issued on the operation and management of IoT devices connecting to public telecommunications networks of IoT service providers.

7. The proposed CoP seeks to ensure the provision of satisfactory service by IoT service providers, strengthen consumer protection and enhance user confidence in using IoT devices connecting to public telecommunications networks. IoT service providers licensed under the Telecommunications Ordinance are advised to observe the best practices as set out in the proposed CoP in the provision of services and in providing relevant IoT devices to their customers. For non-telecommunications licensees such as device manufacturers, vendors, application developers etc. which may supply and deploy IoT devices in the telecommunications and other business sectors (e.g. personal, leisure, household, transport, medical, financial sectors, etc,), the proposed CoP can serve as a reference for these sectors in formulating requirements and practices regarding the operation and management of IoT devices/services.

NEXT STEP

8. Taking into account Members' views and comments, OFCA will circulate a draft CoP for further comments by IoT service providers before finalising it for the approval of the CA.

Office of the Communications Authority
March 2019

Annex

Some Best Practices Advocated for the Operation and Management of IoT Devices

United Kingdom ("UK")

The Department for Digital, Culture, Media and Sport of the Government of the UK issued a "Code of Practice for Consumer IoT Security" (the "UK Code")[3] in October 2018 to provide relevant parties with practical guidance to ensure that IoT devices are secure.

2. The UK Code has set out a number of guidelines for implementation by device manufacturer, IoT service providers, mobile application developers and retailers, including –

- no default passwords;
- implement a vulnerability disclosure policy;
- keep software updated;
- securely store credentials and security-sensitive data;
- communicate securely;
- minimise exposed attack surfaces;
- ensure software integrity;
- ensure that personal data is protected;
- make systems resilient to outages;
- monitor system telemetry data;
- make it easy for consumers to delete personal data;
- make installation and maintenance of devices easy; and
- validate input data.

[3] The UK Code is available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf.

GSM Association

3. The GSM Association issued in February 2016 and updated in October 2017 the "GSMA IoT Security Guidelines" ("GSMA Guidelines"), which provide recommendations for the secure design, development and deployment of IoT solutions and addressing cybersecurity and data privacy issues associated with IoT services by referring to currently available solutions, standards and best practices[4].

4. The intended audiences of the GSMA Guidelines include IoT service providers, IoT device manufacturers, IoT developers (who develop IoT services for IoT service providers), and network operators (who provide the network infrastructure for IoT service providers). The GSMA Guidelines comprise four guideline documents, namely –

(a) IoT Security Guidelines Overview Document ("Overview Document");
(b) IoT Security Guidelines for IoT Service Ecosystem ("Service Document");
(c) IoT Security Guidelines for IoT Endpoint Ecosystem ("Device Document"); and
(d) IoT Security Guidelines for Network Operators ("Network Document").

5. The Overview Document proposes a high level IoT service model and establishes a common understanding of IoT security issues by describing the general principles of security challenges including –

(a) availability: ensuring stable connectivity between IoT devices and IoT networks and servers;
(b) identity: authenticating IoT devices, services and the end-user operating the IoT devices;
(c) privacy: reducing the privacy issues associated with the use of IoT devices by end-users; and
(d) security: ensuring that system integrity can be verified, tracked,

[4] The GSM Association is an industrial organisation. Its members include local and overseas mobile network operators and other industry players. The GSMA Guidelines are available at https://www.gsma.com/iot/gsma-iot-security-guidelines-and-assessment-english.

and monitored.

6. The Service Document describes the components that make up the IoT infrastructure for provision of IoT services as well as some examples of IoT security threats from an IoT infrastructure perspective –

(a) networking infrastructure attacks;
(b) cloud or container infrastructure attacks;
(c) application service attacks; and
(d) other issues on privacy, malicious objects, authentication and authorisation, etc.

The Service Document also outlines some IoT security goals from IoT device or infrastructure perspective, and makes recommendations on measures which can be implemented by IoT service providers to achieve the identified IoT security goals.

7. The Device Document sets out various types of security attack that may affect the components of IoT devices such as –

(a) network communications attacks;
(b) network port attacks;
(c) console access attacks;
(d) local bus communications attacks; and
(e) chip set attacks.

The recommendations set out in the Device Document mainly cover the design of hardware components, physical chipsets, possessing unit embedded into IoT device, etc.

8. The Network Document makes recommendations on connection between IoT servers and IoT networks. It also sets out the security mechanisms that can be provided by IoT networks –

(a) identification and authentication of IoT servers, gateway and devices;
(b) access control to these network components; and

(c) data protection and privacy of the information carried by the network for the provision of IoT service.

*****