INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG17-LS102

STUDY GROUP 17

Original: English

Question(s): 6/17

Ref.: SG17-TD1188

Source: ITU-T Study Group 17

Title: LS on latest activities on IoT security in ITU-T SG17

Purpose: Information

LIAISON STATEMENT

For action to: -

For comment to:

For information to: oneM2M, ITU-T JCA-IoT and SC&C

Approval: ITU-T Study Group 17 meeting (Geneva, 20-29 March 2018)

Deadline: -

Contact: Jonghyun Baek
Rapporteur of ITU-T Q6/17
Republic of Korea
Tel: +82 2 405 6540
Fax: + 82 2 405 5219
E-mail: jhbaek@kisa.or.kr

Contact: Bo YU
China Unicom
P.R.China
Tel: +86 18601106282
Fax: +86 68799696
Email: yubo49@chinaunicom.cn

ITU-T Study Group 17 thanks oneM2M and ITU-T JCA-IoT and SC&C for your continuous collaboration with Q6/17. It is our pleasure to share the current updates of our work on IoT security (as of March 2018) with you as follows:

A) Draft Recommendation X.1361 (X.iotsec-2), Security framework for Internet of things (determined)

Recommendation ITU-T X.iotsec-2 describes the security framework for Internet of things. The Recommendation analyses security threats and challenges the Internet of things environment, and describes security capabilities that could mitigate these threats and address security challenges. A framework methodology is provided for determining which of these security capabilities will require specification for mitigating security threats and addressing security challenges for Internet of things

B) Draft Recommendation X.iotsec-3, Technical framework of PII (Personally Identifiable Information) handling system in IoT environment

IoT devices can collect many kinds of data, and some kinds of data include PII (Personally Identifiable Information). Because the PII data is useful for several kinds of services, they can be shared with multiple service providers. It is better for users to handle own data including PII in IoT environment based on their intention. Because the situation of data usage in IoT environment with multiple service providers will be complicated, the user's intention on data usage should be

reflected flexibly. For example, if the IoT platform has the following functions, the user can recognize that the collected data including PII can be controlled properly. The users can set up PII control preference. This preference includes the list of permitted data for shared by each service provider. The collected data is controlled access based on the PII control preference. Unauthorized data cannot be shared with other service providers. The users can check the history log of data sharing among the service providers. The users can understand the timing of data usage. This Recommendation will provide the technical framework of PII handling system for IoT environment to fulfil these functions.

C) Draft Recommendation X.secup-iot, Secure Software Update Procedure for IoT devices

This Recommendation aims to provide a basic model for secure update of IoT software/firmware and a common secure update procedure for IoT software/firmware implemented in IoT devices and systems.

D) Draft Recommendation X.nb-iot, Security Requirements and Framework for Narrow Band Internet of Things

This Recommendation analyses the potential deployment scheme and typical application scenarios of NB IoT, specifies the security threats and requirements specific to the NB IoT deployments and thus establishes the security framework for the operator to safeguard this new technology applications.

E) Draft Recommendation X.ibc-iot, Security framework for use of identity-based cryptography in support of IoT services over Telecom networks

The traditional certificate-based solution involves heavyweight key management operations including certificate issuing, querying, and revocation. Such systems face great difficulty to keep up with the pace of device increment of IoT at the same time maintaining decent performance.

Identity-based cryptography (IBC) technology is another type of public-key technology which uses an entity's identity as a public key. As one of the essential features of IoT, everything has a unique identifier. Using such identifiers as public keys, no certificates are required. Consequently, IBC security solution utilizes simpler key management, enables distributed authorities controlling their own devices and scales well to both the high number of endpoints and the diversity of the devices.

This Recommendation provides security framework for use of IBC public key technology in support of IoT services over Telecom networks including mechanisms of identity management, key management architecture, key management operations and authentication.

F) Draft Recommendation X. ssp-iot, Security Requirements and Framework for IoT Service Platform (New Work Item)

This Recommendation intended to assess the security threats and challenges to IoT service platforms, and to describe security measures that could mitigate the security threats and challenges.

_____