General Framework for Secured IoT Systems (Draft)

National center of Incident readiness and Strategy for Cybersecurity (NISC)
Government of Japan
June 10, 2016

1. The Object of the General Framework

It is essential that Internet of Things (IoT) systems are designed, developed and operated under the principle of "Security by Design", looking ahead to the future where each individual system is mutually connected. To realize this in a rational manner, a two-pronged approach is appropriate: namely, general requirements associated with design, development and operation for all IoT systems will be established on which the sector-specific requirements will be added.

This framework based on the concept mentioned above, aims to clarify the fundamental and essential security requirements for secured IoT systems.

It is expected that this framework will promote the interoperability of IoT systems and the implementation of security requirements. Moreover, based on this framework, it is expected that the industry's active involvement in development of secured IoT systems to create an environment in which IoT systems users can utilize the systems with feeling of security and safety.

2. Perspectives of the General Framework

In this framework, an IoT system is recognized as a system that produces added value by connecting things or physical objects through the Internet. However, while the added value is being generated, a spillover effect, in which a risk in one-IoT system could spread to other IoT systems, could occur. Therefore, keeping this possibility in mind, IoT systems in this framework are recognized as an integrated entity of IoT systems, which is called "System of Systems (SoS)".

IoT systems consist of multi-layered components. Thus, it is appropriate to divide an IoT system into four layers: 1) device layer, 2) network layer, 3) platform layer (including authentication) and 4) service layer. It is desirable that by using this common layered framework for analysis and evaluation, relevant stakeholders have a common understanding when discussing issues on specific security requirements for a specific domain.

Functions of each layer is summarized as follows:

a) Device layer refers to devices such as sensors and acutuators, including chips, firmware and embedded software, which make up these devices.

b) Network layer refers to wired or wireless communication networks including private networks and commercial networks offered by telecom service providers.

c) Platform layer contains a mechanism to aggregate data which is collected through the device layer and the network layer, and produce valuable information for providing services by cross-referencing such aggregated data.

d) Service layer represents services that are realized via the functions of the other three lower-level layers.

Hereinafter, “device side” represents functions at the device layer and “network side” represents functions realized both at the network layer and the platform layer.

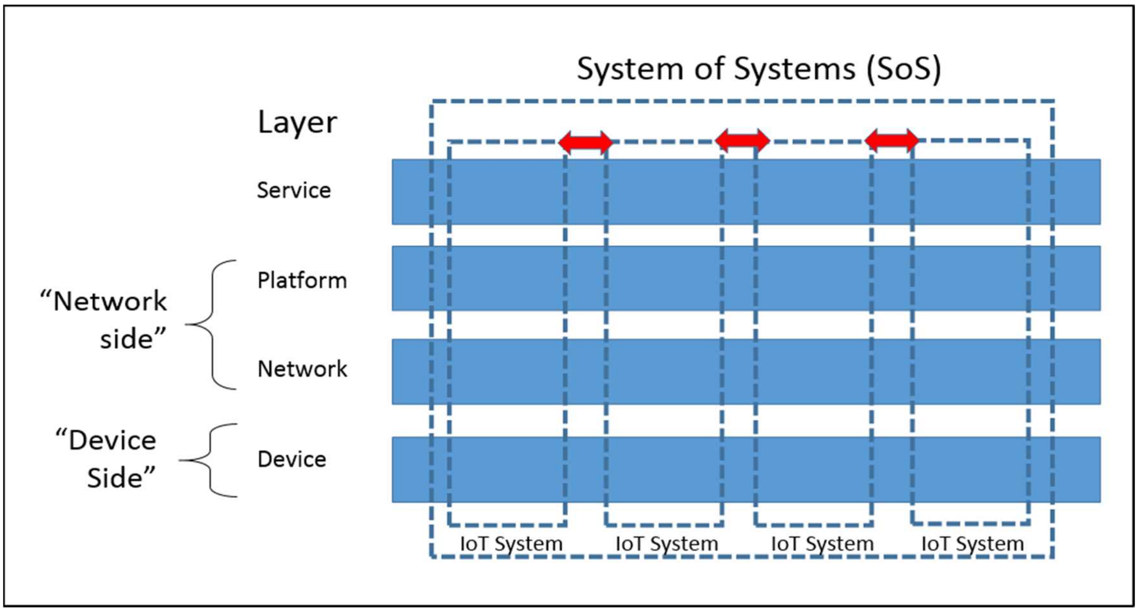

Figure1: IoT System Layers

3. Basic Principles

Physical objects to be connected are subject to existing legal requirements and practices for ensuring security and/or performance. Communication networks vary in their operational or management system, communication tools, network configuration, scope of connection and quality. Therefore, it is necessary to choose an optimized network system that meets the requirements in order to provide the services. However, because both the device side and the network side do not necessarily know well about the industrial environment or characteristics of the other side, connection of objects may not provide sufficient safety and quality performance and could create legal challenges as well.

In particular, the network side environment could change security requirements of the device side. Therefore, it is necessary to consider measures for ensuring security including future network operations in advance. In addition, these concerns should not deter or become an obstacle to assertive efforts from industrial sector.

With collaboration between the device side and the network side, and under mutual understanding and trust among both sides, added value can be generated by integrating networks and devices. This leads to the necessity for developing an environment that creates more secure IoT systems through the close partnership between public and private sectors. In particular, acknowledging that IoT systems have different characteristics from existing information systems, it is essential to ensure security as the whole system in the collaboration between device side and network side, taking measures in ensuring security for the whole system that consists of things and networks.

Taking the above mentioned needs into consideration, “Security by Design” shall be a fundamental principle in designing and deploying IoT systems, and a framework is needed in order to confirm and verify whether security on IoT systems is ensured prior to their operation. For the requirement to ensure IoT system security, conditions required on each phase such as basic policy development, risk assessment, system design, system development, and system maintenance shall be defined. The following items shall be determined.

a) Definitions (including the applicability and the scope) of IoT systems shall be determined and clarified. Also, those systems shall be categorized based on system’s characteristics reflecting their inherent risks.

b) Essential requirements for ensuring users' safety shall be determined, as well as confidentiality, integrity and availability of information on IoT systems including functions of devices.

c) Essential requirements shall be determined to ensure secured system operation and service resilience in case of system failure, including rules of mission assurance.

d) In addition to these items in the above, safety assurance standards, including statutory and customary requirements, shall be determined for connected things and networks.

e) Each item from a) to d) above shall be ensured in case of mechanical failure or cyber-attacks.

f) Responsibility boundary and information ownership of IoT systems shall be clarified.

Items from a) to f) should be applied to the requirements for other cases such as interconnection of IoT systems.

4. Policy Measures

4.1 Determination of Requirements

The following requirements shall be determined on connected things and networks;

a) statutory and regulatory requirements;

b) essential requirements not stated in a) and,

c) other additional requirements recognized as necessary by entities such as industries.

4.2 Risk Informed Approach

In connecting everything with networks, merits and risks brought by the connection are indivisible and these merits and risks shall be objectively considered. Thus, security measures and implementation means to be adopted shall be identified in advance. Considering the possibility that potential risks may be revealed at a later stage and that the degree of risk acceptance may differ for each use case and that it may change over time, security measures and implementation means shall be adopted flexibly in terms of mission assurance.

From this perspective, risk assessment should be used appropriately. It is required to establish a mechanism which systemic risk, a risk in one IoT system spreads to another IoT system, can be isolated.

4.3 Proper application of performance requirements and specific requirements

The environment surrounding IT is changing drastically. Therefore, the requirements shall be composed of two requirements; one is performance based requirements that are universal and essential, and the other is specific requirements that provide effective means and particular method available at the time.

Specific requirements shall be specified through the mechanism to identify IoT systems and to take the most appropriate means in a flexible way.

4.4 Step-by-step and continuous approach

Considering that functions of IoT systems will continuously change due to the change in environment such as technological innovation, fundamental requirements shall be identified initially and then these requirements shall be continuously developed on a step-by-step basis.

4.5 Collaboration and determination of the role-sharing

Role sharing among stakeholders among industry, government and academia on IoT systems shall be determined. In addition, measures for ensuring security, represented by information sharing through coordination and cooperation among each stakeholder and demarcation of responsibility between each stakeholder shall be identified.

4.6 Consideration of other operational rules

Coordination of IoT systems and mechanism for protecting personally identifiable information shall be determined and detail social rules that span beyond each sector. In addition, mechanism shall be established to clarifying the roles of certification entities including coordination of multiple entities and operational rules.

5. Notes

This framework is described based on IoT systems envisioned at the current stage and will be updated in response to factors such as advancement in functions of IoT systems associated with technological innovations. The update of the framework will consider the opinions and discussions of multi-stakeholders.

# # #