General Framework for Secure IoT Systems

National center of Incident readiness and Strategy for Cybersecurity (NISC)
Government of Japan
August 26, 2016

1. General Framework Objective

Internet of Things (IoT) systems consist of connected things and networks and thus should be regarded as an integrated system of IT with physical components. It is important to ensure physical safety in addition to existing information security measures. It is essential that IoT systems are designed, developed and operated under the principle of "Security by Design," while looking ahead to the future where many individual systems are interconnected with new vulnerabilities possibly introduced. To rationally accomplish this, a two-step approach is appropriate: instituting general requirements on design, development, and operation of all IoT systems, in addition, sector-specific requirements for development and operation based on characteristics of respective sectors.

Based on this concept, this framework aims to clarify the fundamental and essential security requirements for secure IoT systems.

It is expected that this framework will contribute to promoting the industry's active involvement in the development of secure IoT systems and will create an environment in which IoT systems users can utilize the systems with a condition that security and safety is assured, by promoting the interoperability of IoT systems and the implementation of security requirements.

2. Perspectives of the General Framework

An IoT system is a system that produces added value by connecting things or physical objects through the Internet. Safety needs to be considered because physical systems are involved. However, while generating added value by connecting an IoT system to another one, there is concern for a vulnerability in one IoT system which affect other IoT systems. Therefore, keeping this possibility in mind, we should recognize IoT systems as aggregated IoT systems, which should be called a "System of Systems (SoS)". In addition, it is important to ensure safety as well as existing information security for the services provided by such IoT system.

In other words, this framework is established on the assumption of the assurance of four requirements, namely, safety, confidentiality, integrity, and availability.

3. Basic Principles

Physical components in IoT systems are subject to existing legal requirements and practices for ensuring security and/or performance. Communication networks used by IoT system vary in their operational or management organizations, communication mode, network configurations, connections and quality. Therefore, it is necessary to choose an optimal network system that meets requirements for the services provided by such system. However, at this moment, because both the device-side personnel and the network-side personnel do not necessarily know much about the industrial environment or characteristics of one another, connecting objects may not provide sufficient safety and/or quality performance and may cause violation of law as well.

Based these concerns, issues on the network-side could potentially impact security requirements for the device-side and so it is necessary to consider ensuring safety including future network operation.

To create new value-added benefits from integrating networks and devices through mutual understanding and trust among stakeholders, it is necessary to develop an environment that creates more secure IoT systems through the close partnership between public and private sectors. In particular, it is essential to acknowledge that IoT systems have different characteristics from existing information systems, and take measures on the device-side and network-side to ensure security for the whole system that consists of both objects and networks.

Taking these needs into consideration, “Security by Design” should be a fundamental principle in designing, deploying and operating IoT systems. A framework is needed to confirm and verify the fundamental principle prior to deployment. To ensure IoT system security, requirements should be defined and achieved during basic policy development, risk assessment, system design, system development, and system operations and maintenance. The following items should be clarified.

a) Definitions (including the applicability and the scope) of wide-ranging IoT systems should be determined and clarified. Such systems should be categorized based on

system characteristics reflecting their inherent risks and steps taken to properly address those risks.

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

c) Requirements should be determined to ensure secure system operation and service resilience in case of disruptions of functions, including mission assurance rules.

d) Safety assurance standards, including statutory and customary requirements, should be determined for connected things and networks.

e) Confidentiality, integrity, availability, and safety should be ensured in the case of mechanical failure or a cyber-attack, and swift service restoration in case of a system trouble should be planned.

f) Responsibility demarcation boundaries and way of data management issues including the discussions of information ownership regarding IoT systems should be clarified.

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

4. Policy Measures

4.1 Clarification of Requirements

The following requirements should be clarified on connected things and networks to IoT systems;

a) Statutory and regulatory requirements;

b) Essential requirements not stated in a) and,

c) Additional requirements recognized as necessary by industry and others.

4.2 IoT system Modeling

The structure of IoT systems is multilayered. Proper modeling should be conducted through analysis on layer by layer basis, such as device, network, platform including certification, and service. Security requirements should be assessed with reference to such model.

4.3 Response based on Informed Risk

When everything is connected with networks, there are inseparable benefits and risks which should be considered objectively. Thus, security measures and implementation methodologies should be identified in advance, considering the likelihood of unforeseen risk occurring. Considering the possibility that potential risks and the degree of risk acceptance may differ for each use case and that they may change over time, security measures and implementation methodologies should be adopted flexibly in terms of mission assurance.

From this perspective, risk assessment should be conducted regularly and as appropriate. It is required to establish a mechanism to determine and isolate a systemic risk, i.e., a risk in specific IoT system spreads to other IoT systems.

4.4 Proper Application of Performance Requirements and Specification Requirements

The environment surrounding IT is changing rapidly. Therefore, the requirements should be composed of two elements; one is performance-based requirements that are universal and essential. The other element relates to specification requirements that provide effective means and particular methods available at the time.

Specification requirements should be constructed through identification of targeted IoT systems and creation so that they can choose the most appropriate means in a flexible way.

4.5 Step-by-Step and Continuous Approach

Considering continuous changes of IoT systems' function due to the ever-evolving environment, e.g., technological innovation, fundamental requirements should first be identified and then these requirements should be continually advanced on a step-by-step basis.

4.6 Collaboration and Role Sharing

Role sharing among stakeholders of IoT systems such as industry, government and academia should be clarified. Additionally, a mechanism for ensuring security by information sharing, coordination and cooperation among all stakeholders should be determined. All stakeholders should know their responsibility demarcation.

4.7 Consideration of Other Operational Rules

Regarding items relating to IoT systems operations, such as IoT systems coordination, data utilization, and protection of personal information, social rules that span beyond

each sector should be determined. In addition, regarding certification for devices and so on, the roles of certification entities, including multiple-entity coordination, and operational rules should be clarified.

5. Notes

This framework is based on what is currently envisioned for IoT systems and will be updated periodically in response to factors such as advancements in IoT systems functions associated with technological innovations. Such an update will reflect on opinions and discussions of domestic and foreign stakeholders. Future tasks regarding this framework include collaboration with existing domestic and foreign guidelines, standards, and publishing organizations.

# # #