Guidelines for the Construction of Basic Security Standard System for Internet of Things

物联网基础安全标准体系建设指南

(2021 version)

September 2021

Table of Contents

Guidelines for the Construction of Basic Security Standard System for Internet of Things

I General requirements

Guided by Xi Jinping's New Era Chinese Characteristics Socialism Thought, thoroughly implement General Secretary Xi Jinping's important thoughts on network powerful-country. Adhering to the overall national security concept, AND targeting on building Internet of Things [IoT] and preventing public network security risks, strive to build the basic security standard system of IoT, strengthen standard overall planning, steadily promote standard development, promote standard implementation, to support and guarantee the secured and orderly development of IoT industry.

(1) Basic principles

Demand traction, strengthen overall planning. Closely follow the development status and trends of IoT industry; focus on building a scientific, reasonable, advanced and applicable, open and integrated basic security standard system; strengthen the overall coordination of standard work; guide the orderly development of standard formulation.

Focus on the key points and give priority to emergency. Focusing on IoT infrastructure and key industry applications, accelerate the development of key and urgently needed standards, such as basic general purpose, key technologies, test methods, so as to meet the security needs of IoT industry, in a timely manner.

Participate extensively and strengthen implementation. Consolidate equipment manufacturers, telecommunications enterprises, security enterprises, internet enterprises, scientific research institutions, universities and other industry-university-research forces; encourage leading enterprises to play a leading role in demonstration, to promote the effective implementation of standards.

(2) Construction goals

By 2022, initially establish a basic security standard system for IoT; develop

more than 10 key industry standards; clarify the security requirements for key basic links, such as IoT terminals, gateways, platforms, to meet the basic security requirements of IoT, thereby promoting the improvement of basic security capabilities of IoT.

By 2025, promote the formation of a relatively complete basic security standard system for IoT; develop more than 30 industry standards; improve the coverage of standards in subdivided industries and fields; improve the security level of cross-industry applications of IoT, to ensure the secured use of consumers.

II Construction details

(1) Framework of standard system

The basic security standards of IoT mainly refer to the security standards of key basic links, such as IoT terminals, gateways, platforms. The basic security standard system of IoT includes five major standard categories, including overall security, terminal security, gateway security, platform security, security administration (see Figure 1).

(2) Key areas

1 Overall security

Overall security is the basic, guiding, universal standard for basic security of IoT, which mainly includes the definition of basic security terms, architecture models, security scenarios, security integration, security grading, security protocols, etc. of IoT (see Figure 2).

Figure 2 -- Overall security

(1) Terms and definitions of basic security of IoT: Standardize the concepts of basic security for IoT; unify the understanding and use of related terms.

(2) Architectural model of the basic security of IoT: Mainly propose the basic security system framework of IoT and the reference models of various parts; clarify and define the functions, relationships, roles, boundaries, responsibilities of the cloud, administration, terminal levels.

(3) Scenarios of basic security of IoT: Mainly provide examples and specifications for security requirements in different types of scenarios.

(4) Integration of basic security of IoT: In the process of planning, integration, implementation of IoT system, guarantee the security and reliability of objects, at all levels of the infrastructure system, by establishing security models and other methods.

(3) Communication chip security: Mainly include communication encryption algorithm, key administration, encryption and decryption capabilities, signature verification, data storage, chip security baseline requirements, etc.

(4) Card security: It is divided into administrative requirements and technical requirements. Among them, the administrative requirements are mainly to regulate the sales, registration, use administration of IoT cards; the technical requirements mainly include card identity authentication, grading and classification, construction of technical means.

(5) Industry terminal security: Mainly refer to the security requirements of IoT terminals with specific functions, which are closely related to various vertical industries, such as the unique security requirements of specific industry terminals, including smart door locks and monitoring equipment.

(6) Test and evaluation of terminal: Mainly include security test of IoT card, test of hardware security, test of operating system security, test of software security, test of access authentication security, test of data security, test of communication protocol security, test of firmware security, etc.

3 Gateway security

Gateway security mainly includes generic security of IoT gateway, security of gateway communication and interface, security of gateway physical environment, security of gateway component, test and evaluation of gateway, etc. (see Figure 4).

(2) Security protection of platform: Standardize the security protection requirements for IoT platform, as well as the security protection requirements for the access control, anti-code reverse, security audit, tampering and injection prevention, etc., of the industry business systems and external application components, which are developed based on IoT platform, mainly including the basic security of platform business, security protection requirements of platform, etc.

(3) Interaction security of platform: Standardize the security requirements for data interaction, encrypted transmission, interactive interface configuration and auditing, between IoT platforms, platforms and upper-level business systems or administration systems, platforms and lower-level access devices, mainly Including the interaction between different IoT platforms, the interaction between the platform and the southbound and northbound directions, etc.

(4) Security monitoring of platform: Standardize the functional construction of the security monitoring and situation summary of IoT platform, mainly including the network security monitoring and early warning platform of IoT, the network security situation awareness platform of IoT, etc.

(5) Test and evaluation of platform: Standardize the test and evaluation methods of the generic security of IoT platform, security protection of platform, internal and inter-platform interaction security, security administration of platform, etc., mainly including the evaluation of the capabilities of IoT platform, test of security protection, test of interactive security, evaluation of security administration, etc.

5 Security administration

Security administration standards are used to guide the industry to implement general security administration requirements, including data security administration, security information collaboration, administration and maintenance security, security authentication (see Figure 6).

the goals and tasks, which are specified in the Standards System, strengthen the coordination of work among all parties including industry, academia, research, application; focus on the integration of the basic security standards of IoT with the actual development of the industry; promote the development of standards, in a systematic manner.

The second is to implement dynamic updates. Track the development trend of new technologies and applications of IoT; actively adapt to the continuous improvement of the level of security development of IoT; strengthen the dynamic update and improvement of the standard system, to effectively meet the needs of industrial security development.

The third is to deepen the application of standards. Encourage industry associations, standardization technical organizations, etc. to carry out publicity and training of key standards, for producers, users, third-party testing and authentication agencies, to guide enterprises to meet standards, thereby promoting the implementation of standards.

The fourth is to carry out exchanges and cooperation. Support Chinese and foreign enterprises, associations, standardization agencies, etc., to carry out international exchanges and cooperation, on basic security standards for IoT; actively participate in the formulation of international standards for IoT security; contribute Chinese technical solutions, to improve the security level of global IoT.