CCDS Comments on "Draft IoT Device Labeling Criteria"

The Connected Consumer Device Security Council (CCDS), an industry-academia collaborative organization in Japan, has developed and issued guidelines and requirements for IoT security. The CCDS has also implemented a certification program since 2019. We believe that this is the first industry-led certification scheme for IoT devices in the world. We would like to introduce this initiative and hope that NIST will use it as a reference for its own studies.

1. Overview of the CCDS

- The CCDS has more than 200 member organizations, mainly from private companies and academic research institutions in Japan.
- The CCDS is engaged in a wide range of businesses, including technical research, standardization, promotion, education, human resource development, security verification, and certification of products and services.

CCDS web site: https://www.ccds.or.jp/english/index.html

2. Overview of CCDS IoT Devices Security Requirements

(1) Background

- In order to improve the safety of society as a whole, it is important to raise the security level of IoT devices that are widely used in society, including consumer devices. These IoT devices can also be the subject of government procurement.
- The CCDS has been discussing the minimum requirements for IoT devices since 2017 and issued the first draft on November 26, 2018.

(2) Security requirement selection policy

- In order to effectively improve the security level of various IoT devices, CCDS certification requirements have been selected to cover a wide range of vulnerabilities with as few requirements as possible.

(3) Specific approach to selecting security requirements

- Used two approaches in the selection of the requirements: statistical and expertise.
- Statistical : Extracted the top 20 most significant CWEs from the viewpoint of severity and number of vulnerabilities, based on the statistical survey of past vulnerabilities.

- Expertise: Commissioned experts to picked out legacy and typical vulnerability issues in addition to the above.
- Considered countermeasures for IoT-specific hardware components (Bluetooth, USB, Wi-Fi, etc.).
- Gathered comments broadly from CCDS member companies through an internal public comment process to ensure that they would make advantage of the requirements in actual business.
- Updates the requirements every year based on global trends in security measures.

(4) Features of security requirements
- 12 minimal requirements for the security of IoT devices connected to the network.
- Focus on measures against botnets and damage to public networks.
- A layered structure consisting of Level 1 (★), which is the baseline requirements for IoT devices, and Level 2 and 3 (★★ and ★★★), which are higher-level requirements for each product field.

3. Overview of CCDS Certification Program
- In order to accelerate the spread of security measures for IoT devices, a certification program was sequentially implemented from 2019 based on the requirements for each security level.
- The purpose of the CCDS certification program is to make companies' security efforts visible so that even buyers without security expertise can make appropriate product purchasing decisions.
- The certification program is designed to reduce the cost of certification and the burden of product inspection so that even small and medium-sized enterprises can easily bring certified products to market.
- Certified products are covered by cyber insurance to compensate for the cost of responding to incidents.
- Established a human resource development system including training programs on security requirements for product inspectors.

4. Status of CCDS activities - related to certification of IoT devices/services

November 26, 2018 - Published the "Security Requirements Guidelines for IoT Devices (2018 Edition)."

October 30, 2019 - Published "Security Requirements Guidelines for IoT Devices (2019 Edition)."

- Launched the certification program for IoT devices (Level 1).
- Announced the certification of four products as initial certification targets.

October 29, 2020 - Published security guidelines and requirements for the smart home as an IoT service.

November 24, 2020 – Published "Security Requirements Guidelines for IoT Devices (2021 Edition)."
- Launched the certification program (Level 2 and 3) for IoT services.

June 21, 2021 - Published the revised version of the "Security Requirements Guidelines for IoT Devices (2021 Edition)."

August 2, 2021 - Announced the acquisition of Level 2 certification for IoT services (smart home).

5. CCDS website

- CCDS website (English version)
  https://www.ccds.or.jp/english/index.html

- Published guidelines (English version)
  https://www.ccds.or.jp/english/deliverables.html

- IoT Devices Security Requirements Guidelines 2021 (English version)
  https://www.ccds.or.jp/english/contents/CCDS_IoT_Devices_Security_Requirements_Guidelines_2021_ver2.0_eng.pdf