Security Measures in IoT/5G Era

December 11th, 2019

TAKEUCHI Yoshiaki
Director-General for Cybersecurity
Ministry of Internal Affairs and Communications (MIC)
JAPAN
Utilization of IoT

- Healthcare
- Smart Factory
- Energy Management
- Autonomous Drive
Increase in IoT Devices

Graph Title

Telecommunications
Consumer
Computer
Industrial
Medical
Automobile
Ammunition, Aerospace

IHS Technology (predictive value)
Cyberattacks Observed by NICTER

The National Institute of Information and Communications Technology (NICT) is observing cyber attacks globally by monitoring 300,000+ unused IP addresses (NICTER).
Attacks on IoT Devices (Observed by NICTER)

IoT Devices: Router, Web Camera, Sensor, etc.

Number of cyberattacks observed by NICTER in one year

- 2013: 128.8
- 2014: 256.6
- 2015: 545.1
- 2016: 1,281
- 2017: 1,504
- 2018: 2,121

3.9 times increase

About half of attacks are targeted at IoT devices!
On October 21, 2016, Dyn’s DNS server in the United States experienced two large-scale DDoS attacks. A number of companies that use Dyn’s DNS services were also affected due to a communications failure. The attacks originated from a large number of IoT devices infected with malware called “Mirai.”

- A large volume of communication targeting Dyn’s system was generated from over 100,000 IoT devices infected with malware.
- It reportedly reached 1.2 Tbps.
- Many leading Internet services and news sites using Dyn’s DNS service were affected.

Many infected devices with simple and weak ID and PW

ID: root
password: 1234

Status of System Failure

Amazon
NETFLIX
Airbnb
Twitter
Dyn
The New York Times
The Wall Street Journal
<table>
<thead>
<tr>
<th></th>
<th>Why are IoT Devices Targeted?</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>The extent and degree of impact by attacks is severe.</td>
</tr>
<tr>
<td>(2)</td>
<td>The <strong>life cycle</strong> of IoT devices is <strong>long-term</strong>.</td>
</tr>
<tr>
<td>(3)</td>
<td>IoT devices are <strong>not well-monitored</strong>.</td>
</tr>
<tr>
<td>(4)</td>
<td>Interoperability of IoT devices and network is not sufficient.</td>
</tr>
<tr>
<td>(5)</td>
<td>The functions and performance of IoT devices are limited.</td>
</tr>
<tr>
<td>(6)</td>
<td>IoT devices can be connected in a way that the developers never expected.</td>
</tr>
</tbody>
</table>
**Effective Measures**

Identify vulnerable IoT devices, such as ones with default ID/password settings, and alert the users of these devices to change their settings.

**Challenges**

It is prohibited to access IoT devices on the Internet without permission of users.

**Government Action**

Amended the law in May 2018 to legally implement the above measure, and started the “NOTICE” project, in February 2019.
Starting on February 20, 2019, the Ministry of Internal Affairs and Communications (MIC) and NICT, in cooperation with Internet Service Providers (ISPs), have been carrying out the “NOTICE”* project to survey vulnerable IoT devices, and to alert users to any problems found. This project is implemented in compliance with the amendment of the NICT Act.

<Overview of the “NOTICE” Project>

(1) NICT surveys IoT devices on the Internet and identifies vulnerable devices, which are those with weak ID/password settings.

(2) NICT provides information about the identified vulnerable devices to ISPs.

(3) The ISPs identify the users of the devices and alert users.

*National Operation Towards IoT Clean Environment
Along with NOTICE, MIC and the NICT, in cooperation with ISPs, are carrying out the project from mid-June 2019 to identify devices infected with malware by using NICTER, and to notify the ISPs so that they can alert users of the infected devices.

<Overview of the project>

(1) **NICT** identifies the devices generating the malware-infected traffic by using the NICTER.

(2) **NICT provides information** about malware infected devices to ISPs.

(3) The ISPs identify the users of the devices and alert them.
Among 200 million IP addresses in Japan, approximately 100 million IP addresses managed by 34 ISPs that are participating in the projects have been investigated.

<table>
<thead>
<tr>
<th>(1) Results of NOTICE</th>
<th>(2) Results of project to alert users of malware-infected IoT devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of IP addresses in which <strong>ID and password could be entered</strong></td>
<td>Approx. 98,000</td>
</tr>
<tr>
<td>Out of the above, the number of those which were <strong>successfully logged-in to with weak password settings</strong> and were subject to user alert</td>
<td><strong>Total 505</strong></td>
</tr>
<tr>
<td>Number of IP addresses which seem to be <strong>infected with malware</strong> and were subject to user alert</td>
<td>80-559 per day</td>
</tr>
</tbody>
</table>

34 Internet Service Providers are participating in the projects. In addition to these measures, a proactive measures are required. (⇒next page)
Proactive measures for IoT security [C]

Amendment of Technical Conditions of Terminal Equipment for IoT Security

- **Terminal equipment** that is directly connected to telecommunication networks through internet protocols are required to have:
  1) **access control** via a remote control function,
  2) features to **encourage users to change default IDs/passwords**
  3) **firmware update features** for future security fixes, or any equivalent/better security measures to the above.

- The requirement does not apply to personal computers or smartphones that are generally protected by other security measures such as anti-virus software.

- MIC has published guidelines regarding the security requirements for the Technical Conditions, which describe the scope of device types, details of the requirements, etc.

**Schedule**

- The amended Technical Conditions will be enforced effective from April 1, 2020. After this, approval will only be given to terminal equipment that conform to the Technical Conditions.
**Certification Program by CCDS**

**Connected Consumer Device Security council (CCDS)** has started non-mandatory certification program for IoT devices in October 2019.

CCDS is a general incorporated association formed by related businesses / organizations which aims to improve the security of consumer devices including IoT devices. (200 members as of November, 2019)

**Level 1:**
- Common and baseline requirements for IoT devices
- Started in October 2019

**Level 2:**
- Specific requirements introduced by industry groups
- Will be started in April 2020

**Level 3:**
- Specific requirements for the protection of users’ lives and property
- Will be started in April 2020
International Cooperation is Required

- Since botnets are formed globally and cyber attacks are conducted across borders, security measures should be undertaken in all countries.
- To realize a safe and secure cyberspace, it is important that all countries share best practices with each other, and implement IoT security measures.
- In Japan, we are implementing three security measures for IoT devices [A],[B] and [C]. In addition, CCDS initiatives are also expected to be effective measures.

[Proposal]
- We would be happy to cooperate with other countries, for example by sharing Japanese IoT security measures and providing relevant information about malware-infected devices observed by our system (NICTER).
- We would also appreciate it if you could share information about IoT security measures taking place in your country.
CSIRT function requires

- Function of CSIRT: information aggregation & providing information
- Cooperate not only inside but also outside
- Expect technical support, know-how, security education and awareness raising
- ISAC (Information Sharing and Analysis Center) has been established for each industry for the purpose of collecting, analyzing, and sharing the incident information on cyberattacks.
- Telecom-ISAC (currently ICT-ISAC) Japan was established in 2002, as the first ISAC in Japan.
- Financial ISAC, Electricity ISAC, J-AUTO-ISAC, and Software ISAC have been established so far. Medical ISAC and Transportation ISAC etc. are under preparation.

42 members

Japan-US ISAC Collaboration Symposium
Let’s work together to overcome IoT vulnerability!