Internet Research Task Force
Internet-Draft
Intended status: Informational
Expires: March 12, 2021

H. Baba
The University of Tokyo
Y. Ishida
Japan Network Enabler Corporation
T. Amatsu
Tokyo Electric Power Company, Inc.
K. Kunitake
BroadBand Tower, Inc.
K. Maeda
Individual Contributor

September 8, 2020

Problems in and among industries for the prompt realization of IoT and safety considerations
draft-baba-iot-problems-09

Abstract

This document contains opinions gathered from enterprises engaging in the IoT business as stated in the preceding version hereof, and also examines the possibilities of new social problems in the IoT era. Recognition of the importance of information security has grown in step with the rising use of the Internet. Closer examination reveals that the IoT era may see a new direct physical threat to users. For instance, the situation at a smart house may lead it to judge that the owner has only temporarily stepped out, causing it to unlock the front door, which in turn makes it easier for thieves to enter. These kinds of scenarios may occur without identity fraud, hacking, and other means of compromising information security. Therefore, for the purpose of this document, this issue shall be referred to as "IoT Safety" to distinguish it from Information Security.

We believe that it is necessary to deepen our understanding of these new IoT-related threats through discussion and ensure there are measures to address these threats in the future. At the same time, we must also coordinate these measures with the solutions to the problems described in the previous version of this document.

This Internet-Draft will expire on March 12, 2021.

Table of Contents

1. Introduction

Many activities are progressing in various fields, such as the proposal of standards for creating an IoT world. There are also many reports that analyze and predict the benefits that IoT can bring to the economy and society. These developments remind us of the end of the 20th century, when the effect and impact of the Internet was actively debated.

The authors tried using the following approach to clarify the issues for the prompt realization of IoT. First, the players were conveniently divided into two groups: ICT industry players and Things industry players. Next, we met major players in the ICT industry and Things industry and asked about the challenges they faced and the challenges the other side faced in creating IoT.

The ICT industry players mentioned here include communication carriers, ICT equipment vendors, the Internet service providers, application vendors, and software houses. The Things industry players include home and housing equipment manufacturers, infrastructure providers such as railways companies and power companies, and manufacturers of home appliances such as air conditioners and refrigerators, which are also the ICT users.

This paper is principally a summary of the meetings results, and a presentation of the micro case studies about the challenges for realizing IoT services. It is not an overview of the IoT world or a macro-proposal intended to promote the benefits of IoT.

In addition, the revised version includes an examination of the possibilities of new direct physical threats in the IoT era that have not yet been seen. These threats should affect the safety of our bodies, lives, and "things," which includes property. For this reason, this issue shall be referred to as "IoT Safety" to distinguish it from Information Security for the purpose of this document.

For the past few years, we got new findings through COMMA House, the experimental smart house owned by The University of Tokyo. Therefore, we will add new topics to the next version.

2. Technical Challenges

2.1. Safety, Security and Privacy

2.1.1. Challenges in protecting lives and property from IoT-related threats (IoT Safety)

The introduction of IoT may generate threats to "Safety" through the actual operation of mechanical devices, in addition to the Information Security problems discussed in Section 2.1.2 below. For example, the spread of applications for visualizing electric power consumption allows for mischief in device operation without the use of identity fraud or hacking. In addition, there is the potential for problems to arise in the normal operation of individual devices that are not caused by abnormal current or voltage, another troubling aspect of the introduction of IoT. These issues cannot be resolved

with ordinary information security measures for Network Layer 4 or lower. In another case, a command to an IoT device is proper by itself, but it may conflict with the other commands or its environmental status. Therefore, the authors consider it necessary to have a system for interpreting the details of operations of many appliances and preventing operations according to the necessity in Layer 7 (what the authors tentatively call "Sekisyo".)

These threats are categorized into three types: threat to physical safety; the threat of the failure or destruction of equipment and property; and the threat of impeding the proper performance of equipment. The following section introduces examples of the different threats.

2.1.1.1. Safety of body/life

Information on things such as the use of faucets and housing equipment, the locking of the front doors and windows, and the state of electric power consumption based on the smart meter is used by smart houses to regulate homes. This information is used to determine whether anyone is at home, and the electronic lock of the front door and windows is unlocked and a notice of absence is issued to a thief.

2.1.1.2. Safety of equipment

Air conditioners and other equipment that normally are not expected to be frequently started or stopped each a day can be caused to break down by repeatedly turning them on and off as many as hundreds of times a day.

2.1.1.3. Proper performance of equipment

Water heaters containing a hot well can be caused to operate erratically. This is done by frequently transmitting signals from the mischief application instead of operation panel to tell the water heater that only 10% of the normal amount of hot water is needed, leaving the water heater perpetually low on water.

2.1.2. Information Security

We have confirmed two viewpoints regarding the information security of services using IoT equipment and devices. The first is tangible information security involving the critical infrastructure. The second concerns the information security of individuals and homes.

In regards to information security involving the critical infrastructure, the basic policy in the past was to stay physically

disconnected from an external network, such as the Internet, to ensure information security. However, because of the advance in the systems from proprietary communication protocols to open IP protocols to detect symptoms of problems and to remotely maintain a large number of facilities spread over a wide area, connecting to an external network will become unavoidable to achieve various goals. In addition, it is clear that isolated networks are also subject to the same kind of risks, even though it is not directly connected to the outside. There is no major difference in the information security risks because isolated networks are already the target of international cyber terrorism, with internal crimes and targeted attacks occurring more frequently. Based on these reasons, the ICT security of the social infrastructure requires an extremely high level of information security.

Looking at the information security of micro units, such as individuals and homes, the improved convenience provided by the introduction of IoT will lead to greater risks. For example, there is a product available for connecting the entrance door to the network. In ICT security technology, increasing the key length of the encryption makes it much harder to break. But even if the latest information security technology is used when it is installed, the information security technology will become obsolete and even pose a risk about halfway through the twenty- to thirty-year lifetime of the entrance door. As has been explained in other items, the ICT sense of time is completely different from that of Things.

2.1.3. Privacy in acquiring data

The problem of privacy in handling acquired data is a huge challenge for companies promoting IoT. In addition, the ownership of this data poses yet another challenge.

For example, railway companies have installed many cameras for station security and for marketing beverage vending machines. This creates problems for personal identification and privacy. At the present time, the companies are processing the images in real time and do not store the images to avoid the problems.

Another huge challenge is the ownership of data. Up until now, there has been a divided debate on whether data belonged to the company or to the users. Likewise, the relationship inside a small user group is also extremely diverse and complicated. One specific example is of a company that had obtained permission from the head of the household to use the data when it carried out an HEMS trial. Later on, the spouse of the head of the household disagreed and as a result permission to use the data was withdrawn.

2.2. Challenges posed by data acquisition, data distribution, data management and data quantity

2.2.1. Traffic patterns

The manner in which data is acquired from and distributed to IoT equipment/devices differs immensely from the traffic patterns of the present Internet. The present form of the Internet focuses on distributing information, and its systems focus on effectively delivering contents to the users. On the other hand, routinely or temporarily sending or receiving data through a huge number of various sensors and devices presents a very different kind of Internet traffic. However, questions such as how much traffic will come from what kind of Things, and how will they superimpose each other have not been sufficiently studied. There is no concrete explanation about the backbone design and operation of traffic, and there have been many cases in which the unclear specifications for IoT traffic made the design difficult on the communication company side. There are many challenges related to the set up and management of IoT equipment. We have heard from the construction companies that the configuration of IoT equipment with a large number of sensors involves a lot of hard work.

2.2.2. Acquired mass data

It is necessary to develop a management method to reuse acquired data safely and effectively. Even now, there are occasional instances of the theft and leakage of social data (such as IDs) that can be used to identify individuals. In the IoT era, there will be mass data that can lead to Things, and the Things in turn will lead to individuals. There are IoT industry players who do not invest as much in ICT systems as government agencies and large companies do, and thus a management system to safely and effectively reuse the acquired data needs to be developed. The laws and regulations related to ID management differ vastly by country and region. These issues related to society and individuals are largely affected by differences in common sense, and therefore need to be localized.

2.2.3. Explosive increase and diversity of data

In the future IoT era, there are concerns about the explosive increase in data quantity and the diversity of data sent from sensors and IoT equipment. On the other hand, M2M communication does not require mass data like images, and an extraordinary increase in traffic will be unlikely despite the increase in the number of sensors.

If data is sent from all Things, there will be an infinite number of different kinds of data. In addition, with the present form of Internet traffic, data is received by people, and most of it consists of video or image downloads. The download traffic is several times greater than that of the upload traffic. If there is a tremendous increase in the use of IoT, such as M2M communication, the difference between upload and download traffic will probably not be that much. It might be necessary to fundamentally review the network and in particular the last mile characteristics. The importance of this issue is not yet widely recognized.

2.3. Mapping of the physical world and the virtual world

2.3.1. Physically handling acquired data

The acquired data simply represents certain kinds of digital value, and it is important to uncover the meaning of this data. As described previously, configuration of IoT equipment, such as the large number of installed sensors, requires a lot of hard work. An even greater amount of effort will be needed to determine the meaning of the data and connect it to the physical world.

In energy management experiments, data is mapped manually. This is a time consuming process, and one that is prone to human error. Cases that rely on the use of human hands require the configuration of automated setting systems to reduce labor, costs, and human errors to introduce IoT

2.3.2. Data calibration

Another important thing is calibration. This involves properly linking the data sent from Things to the Things concerned, and correctly indicating the operating conditions.

It may be necessary to have a tool to treat this problem concerning continuation of operation and the one pertaining to introduction of IoT described previously as a package.

2.4. Product lifetime, generation management, and the cost of equipment updates

2.4.1. Product lifetime

The life of most ICT equipment is about 5 years or less, while the life of IoT equipment and devices is at least 10 years. There is a clear gap between these two types of equipment.

In the example of the entrance door connected to the network mentioned earlier, the door is often used for about twenty to thirty years after installed. If is connected to a network, the communication technology and communication service will most likely have undergone numerous generation changes in that twenty- to thirty-year time span. This presents a large gap between the ICT industry and the Things industry.

A solution to this problem that was reached during the meeting with the housing equipment manufacturers is that with the automatic control of multiple shutters in a building, the portion between the controller and the multiple shutters, the so-called mature technology, can be placed under the control of the shutter manufacturers, while the controller connected to the network will deal with the generation changes of the communication service.

2.4.2. Introducing IoT equipment into commodity equipment

It costs a lot to make the many different types of commodity equipment popular around the world usable as IoT equipment and devices. There are two ways to change commodity equipment into IoT equipment. One way is to convert it to IoT compatible equipment. The other way involves adding devices to commodity equipment. There are costs in both cases, and it will take a long time to introduce IoT unless different incentives are offered to help to overcome the burden of cost.

2.5. Too many related standards and the speed of standardization

2.5.1. Too many related standards

There are many standards related to IoT equipment and devices. There are multiple standards, technologies and services for communication technology, such as Bluetooth, Wi-Fi, NFC, and LTE, and it is difficult to choose which to apply.

The Things industry players do not always have the communication technology professionals needed for IoT. In the meeting, we learned that many companies were uncertain and hesitant about fields outside their own area of expertise. On the other hand, technological competition will improve quality as well as the level of completion, and thus will be beneficial for users.

In the future, a consulting business for clarifying ICT technology for the Things industry players may emerge. If there is a system that can interconnect multiple standards, it will accelerate the Things industry to enter IoT

2.5.2. Speed of standardization

The concept of product life in ICT industry is completely different from that of the Things industry, and as a result the concept of standardization also varies greatly. Before standardization occurs in the ICT industry, many different proposals are made, from which the best is selected. The final decision often changes, and products have to be updated in order to follow the changes in standards. But in the Things industry, the standards have to remain unchanged for as long as possible because of the long product lifetimes. Therefore, it takes a long time to determine when a particular standard has become mature. When the Things industry goes to implement a standard from the ICT industry, it feels that the standard is incredibly fluid and seemingly undecided. Furthermore, the standardization process of the two industries is very different, and making it difficult to work on the other side when trying to determine a standard.

2.6. Interoperability, fault isolation, and total quality assurance

2.6.1. Interoperability

The verification of interoperability poses a major challenge because of the configuration used by multi-vendors. In addition to interoperability between equipment, the ability to ensure backward compatibility is also important for bringing about the IoT world.

If these capabilities cannot be provided, it will be very difficult to create an IoT world in which past products can function.

2.6.2. Fault isolation

The method for fault isolation that may occur presents another challenge.

Many PC users have experienced various kinds of problems. When their PC experiences a problem, they have to isolate the faults by themselves, with no one available to lend a helping hand.

In the IoT world, these issues become more difficult and complicated. For example, a smart home is equipped with air conditioners, kitchen supplies, and doors connected to the Internet. A problem that occurs in the smart home poses a much more serious problem to end users than an e-mail failure or problem with a PC.

If users are left to isolate the fault on their own, they may not know which manufacturer they contact for repairs if they are unable to isolate the fault on their own, or the manufacturer may refuse to perform repairs because they fall outside the scope of their

responsibility. As can be seen, the issue is an important challenge that will determine whether the B2C specific IoT world can be established.

2.6.3. Quality assurance

The quality assurance of individual pieces of IoT equipment does not guarantee the total quality of IoT. Since IoT involves connecting multiple Things and communication, it is natural to assume that the total service quality will depend on the quality of the IoT equipment and devices, which can sometimes become bottleneck. However, users are not aware of this.

As was mentioned previously in Section 2.6 issues that are not directly related to the quality of an individual component can be important factors in determining the quality of the service. In this way, the quality of IoT is not decided by each individual Thing, but needs to be considered as a service spread across the network.

2.7. Product design policy

2.7.1. Changes in design policy

The design policy has to be changed from placing emphasis on the high functionality of a single product to stressing the singular function of individual products as well as how they work in coordination with other products. For many years, the Things industry has focused on producing high functionality products with added value. But in the IoT era, the implicit assumption is to confine Things to their basic function and enhance the level of coordination between Things, rather than focusing on the added value. Simplified Things must be able to be controlled with an external application that can also be used by the Things of cross manufacturers.

Given this situation, the Things industry faces the challenge of adopting a completely different policy. During the meeting with the manufacturing industries, we could sense their difficulty in understanding and recognizing the need to change the policy.

2.8. Various technology restrictions within actual usage

2.8.1. Using radio waves

There are many cases that have provided us with insight about issues related to the use of radio waves in IoT (such as the wave traveling range and whether or not it travels further than stated in assumptions available). The suppliers or providers who configure IoT are not always wave communication technology experts. People who are

unfamiliar with radio waves seem to think that waves travel from antenna to antenna in a straight line, and that they can be blocked by obstacles. As a result, they often ask questions about how many meters radio waves can travel or whether radio waves can actually travel. Few people understand the fact that the emitted radio waves are reflected from various locations and are superimposed at the reception point where they are received, or that depending on how waves are reflected a change in the reception signal intensity, called fading, may occur. The lack of engineers who can advise on specialized matters such as these poses a major obstacle.

2.8.2. Batteries

The power capacity and lifetime of batteries represent another set of challenges similar in nature to the issue of radio waves traveling distance. There are questions such as the difference between the real and catalog specifications, as well as factors that affect the battery power capacity. The IoT providers, who are also users of IoT, have to solve these issues, while these are difficult problems even for experts.

2.8.3. Wiring

The incredible amount of wiring and its complexity (power lines and communication lines) pose major challenges. The complexity of wiring- such as the large number of sensors and equipment, the power lines that drive them, and the communication lines that connect them to the network for acquiring information-is to the point that people doing IoT installation work will start wishing for a wire harness. In addition, the installation of cables and electric work are often done by different engineers. This make the issue even more complicated.

2.8.4. Being open

A single company alone cannot make all the commodities for IoT. The IoT world needs to be open, and this can only be achieved with the cooperation of many different industries. Up until now, companies in the Things industry have developed products in a closed loop process, seeking to capture users with their company's own products. For this reason, they lack an open design concept of interoperability. Today, an entirely new design concept is needed to design products that can interconnect with the products of other companies.

3. Non-technical Challenges

3.1. Changing the product paradigm

3.1.1. Ecosystems

While the goal of setting up IoT is to generate new value, it may actually lead to the destruction of the ecosystems in which industries operate. In the IoT era, the traditional vertically integrated way of producing Things in manufacturing industries will consume too much time and cost. This approach also makes it difficult to incorporate the ideas of other cultures. The need for paradigm shift is easy to understand, but difficult to implement. Promoting this shift will pose a management challenge that requires a considerable amount of skill and effort to overcome.

3.1.2. Coordination and significant changes in strategy

It will become necessary to run businesses jointly with new partners, as well as cooperate and work in coordination with other industries and competitors. This issue-even when it is fully understood-will be very difficult to address and put into practice.

We have seen instances in which only a limited amount of information was given when parties exchanged opinions. There have also been instances in which communication was difficult because of differences in terminology and culture.

3.1.3. Competition with existing industries

The issue of competition with existing industries often arises when attempts are made to change or reform a business model change or reform. This issue can also be viewed as the reorganization of industries, rather than competition between existing industries. However, this realignment of industries is difficult to move forward in the absence of supervisors.

3.2. Benefits

3.2.1. Rising costs and monetization

Introducing IoT within products will cause costs to go up, and yet the benefits it provides are unclear. There is no specific killer application available, and the number of users will not rise immediately. Therefore, finding a way to make the business profitable will be very difficult. This issue is especially difficult for businesses and products that rely on cost reductions to deliver low prices that make them competitive.

3.3. Information security and privacy of social systems

3.3.1. Classification of ownership, location, and the usage of data

There are many questions regarding the wide variety of data gathered from IoT equipment, including questions related to ownership, storage location, and the authorization to grant a license to use data. These need to be addressed so that the system and equipment can be accepted by society.

For example, if a company installs a door in a house that gathers data on the opening and closing of the door, questions about the data will arise. Does it belong to the users or the company? Can another company use this data?

3.4. Disclosure of data

3.4.1. Side effects and malicious use potentially caused by the disclosure of data

For example, it has been shown that the electricity smart meter can lead to burglary because it shows when electricity is used and not used, providing an indication of the time when no one is home. This particular example demonstrates the importance of ensuring information security and privacy.

3.5. Preparing social support

3.5.1. Regulations

Systems of laws and regulations are important for ensuring the safety of the conventional products, but they can also be a barrier for innovation.

IoT can be affected by laws and regulations at home and abroad, and can also be influenced by regulations that extend across multiple countries. Regulatory authorities need to monitor IoT carefully and adjust the regulations and laws they oversee in a way that does not negatively impact the global competition environment.

3.5.2. Corporate social responsibility

In addition to pursuing profit, companies that promote IoT also need to improve the benefits offered to users and society

3.5.3. Customization for individual customers

There is an ongoing shift in demand away from general products to customized products for individual customers. This could also be viewed as a shift away from manufacturing businesses to service businesses. IoT will play an important role in this shift.

Instead of manufacturing Things through mass production, it will be easier to customize a product by moving some of the functions to an application. Likewise, the manufacturing business also needs to move forward with the previously mentioned paradigm shift in order to achieve customization

3.5.4. IoT literacy of the users

Because Things are connected to the network, apps will need to be created. Some of these will serve as the interface with which people interact with IoT.

In the IoT era of the future, users will need to possess a certain amount of knowledge about IoT apps

3.5.5. Individual vs. family

The issue of whether the data of Things in the house belongs to the family or the individual will largely affect data analysis and the handling of privacy.

As was mentioned in Section 2.1.2, the spouse could later object to the head of the household granting authorization to use data.

4. Security Considerations

Meetings with the players in various IoT fields provided insight into information security issues. These issues are described in the following sections.

- Section 2.1.2 Physical damper of devices
- Section 2.1.2 Product lifetime and encryption strength

For details, please see the corresponding text.

5. Privacy Considerations

Similarly, issues regarding privacy are described in the following sections.

- Section 2.1.2, Section 3.3.1 Ownership of the data
- Section 3.4.1 Data disclosure and malicious use
- Section 3.5.5 Individual vs. family

For details, please see the corresponding text.

6. IANA Considerations

This document has no actions for IANA.

7. Acknowledgments

We would like to thank the foundation the promotion of industrial science and its RC-88 member companies for their cooperation.

And we also appreciate Ministry of Internal Affairs and Communications.

Authors' Addresses

Hiroyuki Baba
The University of Tokyo
Institute of Industrial Science
4-6-1 Komaba
Meguro-ku, Tokyo 153-8505
Japan

Email: hbaba@iis.u-tokyo.ac.jp

Yoshiki Ishida
Japan Network Enabler Corporation
7F S-GATE Akasaka-Sanno.
1-8-1 Akasaka
Minato-ku, Tokyo 107-0052
Japan

Email: ishida@jpne.co.jp

Takayuki Amatsu
Tokyo Electric Power Company, Inc.
1-1-3 Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-8560
Japan

Email: amatsu.t@tepco.co.jp

Koichi Kunitake
BroadBand Tower, Inc.
Hibiya Parkfront.
2-1-6, Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011
Japan

Email: kokunitake@bbtower.co.jp

Kaoru Maeda
Individual Contributor
Japan

Email: kaorumaeda.ml@gmail.com