Toward Security and Privacy Policy Enforcement System for IoT Applications

TIANXIANG ZOU[†1] KENJI HISAZUMI[†2]
AKIRA FUKUDA[†3]

Abstract: As the Internet of Things (IoT) is widely used today, IoT security is becoming important. The mechanism to enforce security and privacy policy upon IoT applications which are downloaded from the Internet and run on IoT devices equipped on our private environment is a crucial role in the IoT era. For example, in smart buildings, sensors will transmit the data detected in the user's room to the cloud server in real time. The part of the data that relates to user privacy needs to be handled to prevent the data from being compromised to user's security when others see it. Such kind of scenario might vary according to user requirements. In the paper toward to propose security and privacy policy enforcement system for IoT applications, it clarifies variations of security/privacy requirements which should be enforced to the applications. As the first phase of our proposed system, we clarify scenarios which cause of security and privacy problem for the applications and describes these variations using a feature diagram.

Keywords: Internet of Things, Security and Privacy Policy, Feature Diagram

1. Introduction

Nowadays, the use of Internet of Things (IoT) is becoming more and more popular. In the IoT, for example, smart building application, thousands of devices are connected together over the internet to enable real-time data exchange[1]. If these data are maliciously used or tampered with because of unsafe storage, they may pose a threat to the safety of users. Thus, security and privacy assurance is also an important step in the development of IoT systems today[2].

We believe that it is important to elicit scenarios that can lead to security and privacy problems for different users and environments, and to arrive at a complete solution to the problem, and to prepare for a proposal security and privacy policy enforcement system for IoT applications.

In this paper, we specify variability of security and privacy requirement which should be enforced to the applications by analyzing scenarios. And we propose different security and privacy policies for the variations of requirements and describe these variations and policies by using a feature diagram.

And finally, we will prepare for the realization of the security and privacy policy described in the feature diagram through Domain Specific Language(DSL) design. This is the goal of our entire research.

The rest of paper is organized as follows: Section 2 describes scenarios that lead to security and privacy problems. In Section 3, according to the scenarios above, we propose some methods to the security and privacy issues. Section 4 concludes this paper and mentions future works.

2. Motivational Example

As the first phase of our proposed system, we present and list scenarios which cause security and privacy problem for IoT applications. Depending on the user and environment, as well as on security and privacy requirements, we can roughly divide the scenarios into two categories.

One is focusing on individual user's data privacy. Data privacy, is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them[3]. For example, real-time data, such as room temperature, electricity consumption, healthcare data, etc., if the information is seen by others, others can speculate the user's habit and lifestyle easily based on these data. It may cause troubles for the user's life or pose a threat to the user's safety.

The other is focusing on data security. Data security means protecting digital data, such as those in database, from destructive forces and from unwanted actions of unauthorized users[4]. For example, system configuration and security data, such as configuration file of devices and fingerprint identification data. Once these data are maliciously used or tampered with by others, serious security problems such as device breakdown and access control failure may occur.

At present, a lot of IoT middleware and devices include both scenarios[5]. The consequences of above scenarios can easily be caused if the data is stored in an insecure way or stored in a single way without distinction. Nowadays, IoT applications often involve payment, housing, navigation, shopping and healthcare[6]. Therefore, depending on the requirements of different users and environments in IoT applications, the system mechanism which can adopt different security and privacy policies is necessary.

3. Proposed Method

In this section, we discuss the security and privacy policies according to the scenarios described above and summarize them as a feature diagram to specify commonality and variability of all variation of requirements to the policies.

The feature diagram is a grammar relatively free tree structure diagram, and it can describe a proposed system to end users

†1 Kyushu University. tenshou.su@f.ait.kyushu-u.ac.jp
†2 Kyushu University. nel@slrc.kyushu-u.ac.jp
†3 Kyushu University. fukuda@f.ait.kyushu-u.ac.jp

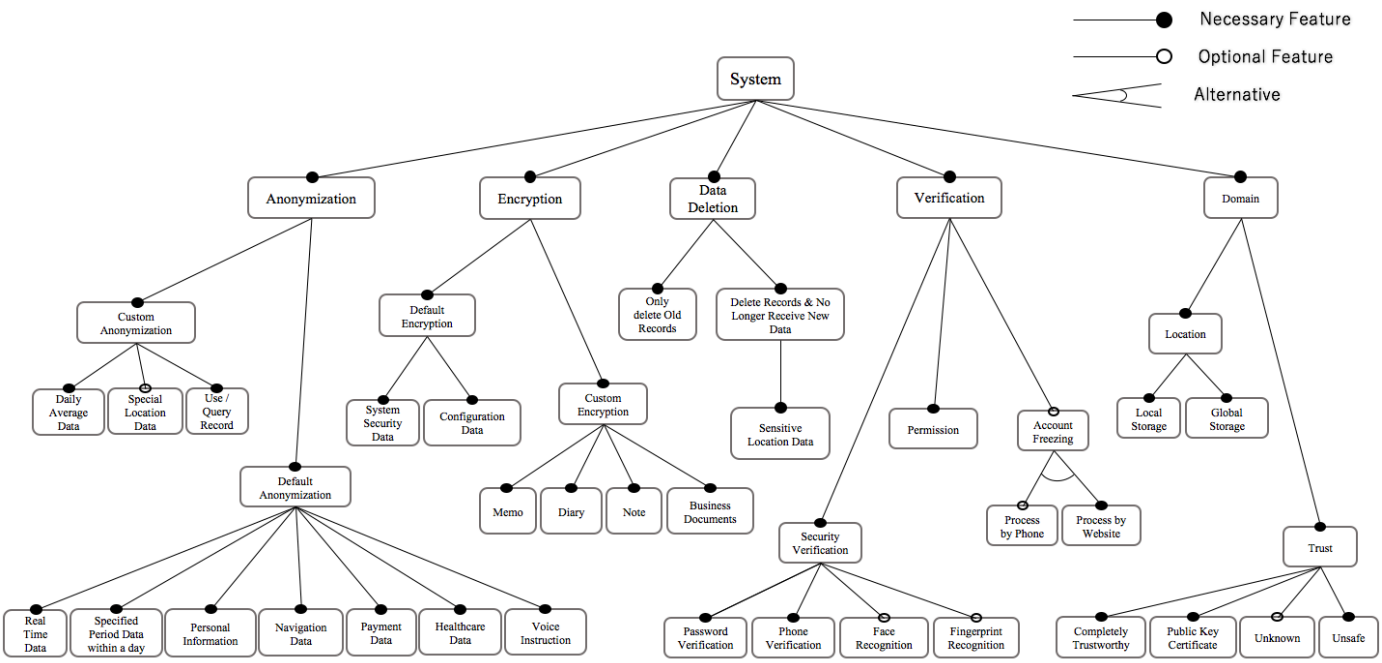

Fig. 1: Feature Diagram of Proposed System

regarding possible feature[7]. According to the feature diagram, we can implement the proposed features by using DSL design.

We can divide the security and privacy policy of enforcement system into two categories: Anonymization and Encryption. At the same time, we base on the status of data storage and Internet, adding three features: Data Deletion, Verification and Domain.

3.1 Anonymization

For data privacy, we propose there is a default way to anonymize privacy information that may threaten user safety.

The user's personal information that has been stored, such as name, address and phone number, etc., needs to be anonymized and is only visible to the user's account.

At the same time, the data that can easily speculate the user's lifestyle and pose a threat to the user's security also needs to be anonymized. These data include real-time data and the data for the specific period within a day.

Real-time data, such as temperature data in the room, data of proximity sensor in the floor, etc., through these data, others can easily speculate the user's presence and absence during this period. Once such data is obtained by criminals, it is likely to pose a threat to the safety of users.

Furthermore, data for a special period within a day should be anonymized except for the users themselves. If the system allows others to view the data of special period that is recorded in the server, then it is easy to use these data to speculate the status of the users. For example, if the room electricity consumption data from 9 am to 6 pm can be viewed by others, it is easy to speculate whether the user leaves home to work or not and whether the room is empty based on these data. Once this happens, it is also likely to pose a threat to the user's security.

Moreover, other important data also need to be anonymized, such as money-related payment data, navigation information related to the user's location, and health data related to user health. The leakage of these data will let other know the user's bank information, preference, and health status, and may expose users to the risk of being stolen and being extorted.

In addition, it should be noted that the operating instruction and voice instruction for the local devices also need to be anonymized. Without being anonymous, others can speculate the status and privacy information of users based on these instructions, and may easily get user's mail, SNS, password, and so on. This will be a threat to the user's security and privacy.

Of course, users also have the right to customize the default rule of anonymization and decide whether to anonymize other specified data, such as daily and monthly average data of room electricity consumption, in normal circumstances, the data were viewed by others, it will not pose a threat to the user. However, if the user travels for a long time, the data may also serve as a basis for speculating whether the room is empty and will be a threat to the user. Similarly, the special location data or query records may also pose a security threat to some users. Thus, whether these data need to be anonymized depends on the user's requirement.

Our proposed features are described in the Anonymization branch on the left side of Figure 1.

3.2 Encryption

As for encryption, we propose a default way to encrypt system security documents, configuration files. Once these data are leaked or maliciously altered by others, the system may be damaged, the devices may be breakdown, and the user may suffer heavy losses. Therefore, these data need to be handled carefully.

Besides, users can also specify files and data that need to be encrypted, such as notes, memos, business documents, or other data. Whether these data need to be encrypted depends on the use's requirement. If the user encrypts an anonymized file or data, the file will be de-anonymized and stored encrypted.

These features are described in Encryption branch in Figure 1.

3.3 Data Deletion

For some stored data, if users do not want to save them on the cloud servers or local devices, they can delete these data.

There are two options for data deletion, one is to delete old records only, and the other is to not receive new such data except to delete old records. For example, users do not want the server to store the data about sensitive locations that they do not want others to know, such as hospital and entertainment place, and they can delete these data immediately.

In the Data Deletion branch in Figure 1, we describe these features.

3.4 Verification

For the security of system and user account, we propose three features for system verification: security verification, permission setting, and account freezing.

For the complex computer and network environment, users need to pass more than two kinds of security verifications in order to login accounts, and users can only do the operations that accord with the current permission. Once the system detects that the account is compromised, or the user finds that the data may be leaked, the account freezing mechanism may be activated and the account can be recovered through mobile phone or website.

As shown in Figure 1, we specify the features in the Verification branch.

3.5 Domain

Finally, about the domain, we can divide the data storage locations into local storage and global storage.

And for the trust, if the servers are set up by users themselves or by acquaintances in secure way, then the storage location can be completely trusted as whitelist. Moreover, the server which has public key certificate, such as Google and Apples, is also able to give full trust. In addition, there are lots of servers with unknown level of security or blacklisted. These servers need to be fully paid attention. And the enforcement system has ability to reject sending data that the user wants to protect to these unsafe servers.

We describe the features of Location and Trust in the Domain branch on the right side of Figure 1.

4. Concluding and Future Works

In this paper, we present scenarios that lead to security and privacy problems in IoT applications for different users and environments and point out the importance of taking different measures depending on situations. For these scenarios, we propose different security and privacy policies and summarize the variations of requirements and the policies by using a feature diagram.

As a task for the future, we plan to describe the security and privacy enforcement policies on the feature diagram by defining domain-specific language (DSL) based on different requirements, and observe whether these requirements are effectively fulfilled.

Reference

[1] Pankesh Patel, and Damien Cassou, “Enabling high-level application development for the Internet of Things”, in The Journal of System and Software 103, 2015, pp. 62-84.

[2] Brice Morin, Nicolas Harrand, and Franck Fleurey, “Model-Based Software Engineering to Tame the IoT Jungle”, https://www.infoq.com/articles/thingml-modeling-iot-jungle, accessed 2017/7/5.

[3] Philip E. Agre, and Marc Rotenberg, Technology and privacy: the new landscape, Jul. 1998.

[4] Summers, G, Data and databases. In: Koehne, H. Developing Databases with Access: Nelson Australia Pty Limited. P4-5, 2004.

[5] Anne H. Ngu, Mario Gutierrez, Vangelis Metsis, Surya Nepal, and Quan Z. Sheng, Member, IEEE, “IoT Middleware: A survey on Issues and Enabling Technologies”, in IEEE Internet of Things Journal, vol. 4, no. 1, Feb. 2017.

[6] Charlie Cabot, “An Introduction to Differential Privacy”, https://www.infoq.com/articles/differential-privacy-intro, accessed 2017/7/22.

[7] Kyo C. Kang, Sholom G. Cohen, James A. Hess, William E. Novak, and A. Spencer Peterson, Feature-Oriented Domain Analysis (FODA) Feasibility Study, Nov. 1990.