Information Flow Control Based on the CapBAC (Capability-Based Access Control) Model in the IoT

Shigenari Nakamura, Hosei University, Tokyo, Japan
Tomoya Enokido, Rissho University, Tokyo, Japan
Makoto Takizawa, Hosei University, Tokyo, Japan

ABSTRACT

In the Internet of Things (IoT), not only computers like servers but also devices with sensor and actuator devices are interconnected. It is critical to make the IoT secure, especially devices. In the capability-based access control (CapBAC) model proposed to make IoT devices secure, an owner of each device issues a capability token, i.e. a set of access rights, to a subject. Only a subject holding the capability token is allowed to manipulate the device. However, a subject may get data in a device d1 via another device d2 although the subject holds no capability token to get data from the device d1. Here, the data in the device d1 illegally flow to the subject. In this article, the authors propose the operation interruption (OI) protocol where illegal get operations are interrupted. In the evaluation, the ratio of the number of get operations interrupted to the total number of get operations is kept constant even if the numbers of subjects and access rights granted to each subject increase in the OI protocol.

KEYWORDS


INTRODUCTION

In order to make information systems secure in presence of malicious accesses, various types of access control models (Denning, 1982) and cryptography (Ogiela, 2015; Ogiela & Ogiela, 2016) are proposed. Cryptography is used to prevent every information, i.e. objects, from being forged, stolen, or disclosed by a subject like user and application which are granted no permission, i.e. no access right. In the access control models, only an authorized subject is allowed to manipulate an object in an authorized operation. However, even if a subject is not allowed to get data in an object o, the subject can get the data by accessing another object o (Denning, 1982). Here, illegal information flow occurs from the object o via the object o to the subject. Illegal information flow among subjects and objects has to be prevented in the access control models. The LBAC (Lattice-Based Access Control) model (Sandhu, 1993) is proposed to prevent illegal
information flow among subjects and objects. Here, each entity is assigned a security class. Illegal information flow is defined based on the relations among classes and every operation implying the illegal information flow is prohibited. In our previous studies, various types of protocols to prevent illegal information flow are proposed. In papers (Nakamura et al., 2015a; Nakamura et al., 2015b, Nakamura et al., 2016), types of protocols to prevent illegal information flow occurring in distributed database systems are proposed based on the RBAC (Role-Based Access Control) model (Sandhu et al., 1996). In papers (Nakamura et al., 2019a; Nakamura et al., 2019c), protocols to prevent illegal information flow occurring in P2PPSO (Peer-to-Peer Publish/Subscribe with Object concept) systems (Nakamura et al., 2019c) are proposed based on the TBAC (Topic-Based Access Control) model (Nakamura et al., 2018).

The IoT (Internet of Things) (Hanes et al., 2018; Oma et al., 2018; Soo et al., 2017) is composed of various types and millions of nodes including not only computers but also devices like sensors and actuators. Here, it is difficult to adopt traditional access control models such as the RBAC (Sandhu et al., 1996) and ABAC (Attribute-Based Access Control) (Yuan & Tong, 2005) models for the IoT due to the scalability of the IoT. Since the access list is also scalable, it is difficult to access and manipulate the access lists. Hence, the CapBAC (Capability-Based Access Control) model is proposed (Gusmeroli et al., 2013). Here, an owner of each device issues a capability token to a subject $sb$ like user and application. The capability token is defined to be a set of access rights. An access right is a pair $\langle d, op \rangle$ of a device $d$ and an operation $op$ on the device $d$. The subject $sb$ is allowed to manipulate the device $d$ in an operation $op$ only if the capability token including an access right $\langle d, op \rangle$ is issued to the subject $sb$.

Suppose a subject $sb_j$ is issued a capability token including a pair of access rights $\langle d_j, get \rangle$ and $\langle d_j, put \rangle$ on a pair of devices $d_j$ and $d_j$, by an owner of the devices. Suppose the device $d_j$ is a sensor and the device $d_j$ is equipped with a pair of a sensor and an actuator. A sensor just gives sensor data to a subject. On the other hand, an actuator supports an action to store data to the device. A subject $sb_j$ is issued a capability token including an access right $\langle d_j, get \rangle$ by an owner of the device $d_j$, but not issued an access right $\langle d_j, get \rangle$. First, the subject $sb_j$ gets the sensor data $dt$ obtained by the device $d_j$ and then puts the data $dt$ to the device $d_j$. Next, the subject $sb_j$ gets the data $dt$ from the device $d_j$ by using the capability token including $\langle d_j, get \rangle$. Here, the subject $sb_j$ can obtain the data $dt$ of the device $d_j$ via the device $d_j$, although the subject $sb_j$ is not issued a capability token including the access right $\langle d_j, get \rangle$. Here, the device $d_j$ is a source device of information flow to the subject $sb_j$. This is illegal information flow from the device $d_j$ to the subject $sb_j$. In this paper, the authors define information flow relations among subjects and devices based on the CapBAC model. Then, the authors propose an OI (Operation Interruption) protocol to prevent illegal information flow in the IoT based on the information flow relations. In the OI protocol, it is checked whether or not the illegal information flow to occur by performing an operation on a device $d$ based on the information flow relations among subjects and devices. If the illegal information flow occurs, the operation is interrupted at the device $d$. Hence, every illegal information flow in the IoT is prevented from occurring.

In this paper, the authors evaluate the OI protocol in terms of the number of illegal get operations interrupted. In the evaluation, the authors show the ratio of the number of illegal get operations to the total number of get operations is kept constant even if the numbers of subjects and access rights granted to each subject increase in the OI protocol.

In next section, the authors overview the related studies. Then, the authors define types of information flow relations on subjects and devices based on the CapBAC model. After that, the authors discuss the OI protocol to prevent illegal information flow in the IoT based on the information flow relations. Finally, the authors evaluate the OI protocol in terms of the number of illegal operations interrupted.
Quality of Experience Models for Multimedia Streaming
[www.igi-global.com/article/quality-experience-models-multimedia-streaming/47328?camid=4v1a](www.igi-global.com/article/quality-experience-models-multimedia-streaming/47328?camid=4v1a)

A Generic Context Interpreter for Pervasive Context-Aware Systems
[www.igi-global.com/article/generic-context-interpreter-pervasive-context/53857?camid=4v1a](www.igi-global.com/article/generic-context-interpreter-pervasive-context/53857?camid=4v1a)