The Application of the Context-Aware Access Control Model

Chao Zhang, Zhengping Jin

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China

zhangchaozc215@163.com, zhpjin@bupt.edu.cn

Keywords: access control, context-aware, RFID, monitoring system.

Abstract. Traditional access control model in building safety regulation is not flexible enough in some scenarios, especially in emergency events, which may lead to the alarm events not promptly treated. In order to solve this problem, we design a context-aware access control model which uses RFID technology to identify the user's identity information and the environmental contexts, then we apply it to the intelligent building monitoring system. The application of the new model can bring more flexibility and security.

Introduction

With the speed of urbanization, there is more and more modern buildings, however, modern building security monitoring management can't keep up with the times. Problems may include, but are not limited to, difficult to discover and eliminate all kinds of potential safety hazard in time, the lack of a scientific and effective emergency treatment, the lack of a flexible access control mechanism.

Among these potential security problems, access control security is particularly important. In general, the traditional access control model can play the role of the management of user permissions, but in some scenarios it lacks of flexibility, so that building security may be faced with a certain potential security problem. Traditional access control model doesn't quite suitable because of the context-aware nature of the intelligent building regulation system. In RBAC model, access control depends on specific attributes of the user and the object. In the environment sensitive scenario, attributes of the user and object are important, but so are other environmental contexts, such as location and time, these factors will determine when and where certain access is allowed. For example, in general, archivists should be able to access the archives while in appropriate location (archives) and within a certain period of time (office hours). In addition, there are other important contexts which has to be taken into account for deciding access. For instance, in an emergency situation that equipment alarms, if the equipment maintenance personnel isn't there and couldn't deal with alarm in time, we need to apply access and permissions for the other equipment maintenance personnel who is not responsible for the equipment but is nearest to it according to his location information. However, the traditional access control model can not solve the problems in these scenarios.

Realizing the fact that the access control management is playing the important role in the building safety and that traditional access control can't solve the new problems in the new environment, we propose and implement a context-aware access control system for security monitoring management in this paper, the system can detect the user's environmental context information and change user access permission according to different situations. We apply the system in the specific scenario of intelligent building security monitoring platform to achieve the purpose of ensuring the safety of the platform as much as possible.

The rest of this article is organized as follows: Section II introduces the related work carried out in writing the paper. In Section III, we design and implement the specific process of the new access control system in the building regulation platform. Section IV describes the design of RFID electronic tag and the data acquisition process, as well as the specific access control strategy.

Relevant research

Traditional access control models.

Discretionary Access Control (DAC) [1] permits the granting of access control privileges to be left to the discretion of the individual users. A DAC mechanism allows users to grant access to any of the objects under their control. So users are considered to be the owners of the objects under their control. DAC has certain flexibility and it is often applied to access control lists (ACLs) mechanism. However, the way that users are freedom to grant their access authority is very dangerous, because if an attacker controls the user's account, the attacker will have all of the user's access authority.

Mandatory access control (MAC) [2], the basic idea is that access system assigns a security label for each user and the access object, according to the security level as high or low, system allows or rejects access request. MAC can prevent the illegal disclosure of information effectively, but the use of security labels causes coarser system authorization granularity and more inflexible authorization management, so MAC is commonly used in systems that requires relatively strict security level, but isn't fit in a fine-grained and flexible environment.

Role-based access control (RBAC) [3] is called the standard model in the field of access control. The access control decisions are based on a specific role that each user has in the organization. In order to define roles, comprehensive analysis of how an organization works should be made first. Permissions are assigned to roles rather than to a single user.

Context-aware access control model.

Although RBAC model can satisfy access control requirements of most systems, it is not suitable for context-aware application systems where environmental context information supplies crucial access control parameters for access control decisions. As a result, many researches are trying to establish a connection of RBAC and environmental factors. A paper [4] proposes a role-based trust context sensitive access control model, the model tries to achieve the goal of access security by measuring and validating the user's behavior and other platform environmental context information. Another paper [5] proposes a new access control decision framework based on context awareness(CAAC), expanded the RBAC model with dynamic properties defined in the ontology, implements the access control model "user - role" and "role - permissions" dynamic association.

Radio frequency identification devices (RFID) .

RFID [6] is a kind of two-way communication by radio of automatic identification technology. In general, RFID system consists of three parts: the electronic label (Tag), read and write devices (Reader) and RFID application system.

According to the different methods of power supply, the RFID electronic tag can be divided into active tag and passive tag. The Passive tag doesn't send out information waves itself. Information waves are sent by read and write devices, after the antenna in tags receives the magnetic field produced by the waves, it sends out the information stored in the chip to the read and write devices to process. The Active tag has a power inside besides a chip and antenna, so it can send out the information to the read and write devices actively.

The design and implementation of access control system

The access control system is based on the context-aware access model and uses RFID to detect the user environmental context information. The system can change user's access rights flexibly according to the detected environment to achieve the goal of safety management.

Design goal and scenario analysis.

Our design goal is that the access control system applied in the building monitoring platform system can allow or deny users access to the protected information according to different environmental conditions.

Environmental conditions may include where the user is and when the user tries to access the system, etc. Using RFID, the information can be detected by reading the tag in the smart card which each user takes. The importance of the environmental conditions are showed in the following

scenarios: In scenario 1, archivists are only allowed to access to the files at a certain time period (office hours) and a specific location (archives), in other place or time, the access request will be rejected. But in dealing with emergency, general access control strategy may be covered by new environmental context strategy. In scenario 2, when a equipment has a fault alarm, the corresponding equipment maintenance personnel isn't on the ground and can't handle it in a timely manner, so another equipment maintenance personnel who is closest to the equipment should be granted access to the equipment immediately, after permission, he should rush to the scene to deal with the accident in order to avoid major accidents.

System overview.

This system mainly combine RBAC access control model and environmental context constraints to realize the control of user access control permissions. The system uses RFID to identify whether the user's access is legal based on the environmental context information. In an emergency, we can mobilize corresponding personnel to deal with emergencies according to the location information which is detected from tags in smart cards. Each user in the system is equipped with a smart card, each card contains an active RFID electronic tag and each tag contains an unique user identity information. The system overview is shown below in Fig. 1:

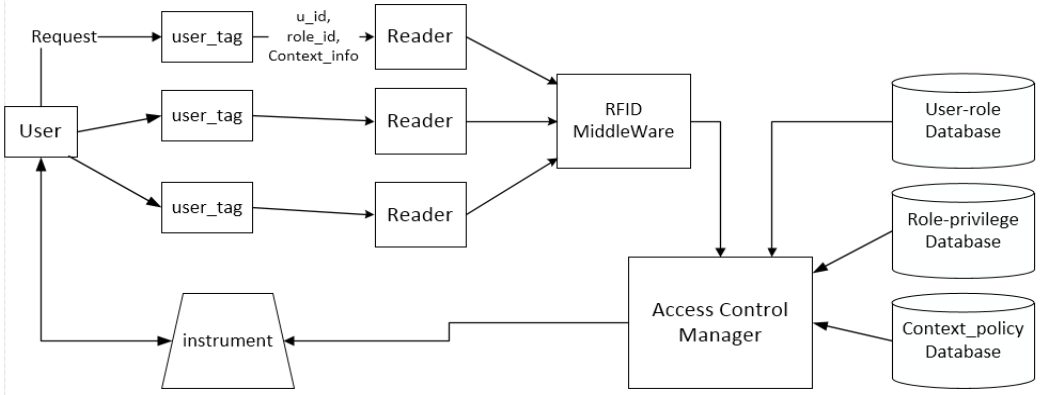

Fig. 1 System overview

As shown in Fig. 1, any access request starts with sending out data signals to read and write devices by the user's smart card. User's role information and user's ID information are contained in the sending signals, but the signals don't include the context and environmental context information. The environmental context information needs to be obtained through certain means. When read and write devices got these information, they send the information to the RFID Middle Ware in where data decoding is managed. The RFID Middle Ware will transmit the decoded data in the key and value format into the Access Control Manager. The Access Control Manager will first determine the role of the user from the user-role repository. Then it will determine whether his access request is legal according to the role-permission repository. If the request is legal, check the context constraints using the context-policy repository. If the requester is found to satisfy the context constraints under the role he assumes, his access request will be granted, and he will be able to exercise his access privileges congruent to the access policy.

RFID data acquisition and access control policy description

RFID data collection and analysis.

Data stored in RFID tags includes identification information, user's role information, additional information, etc. The information is stored as binary. For example, We use 16 bit string "1000, 1000, 1000, 0001," said the ID information in the label, uniquely identifies a user. Because roles in the system include system administrator, site monitoring manager, archivist, equipment maintenance personnel and patrol security officer, we can assign 3 bit string (at most can identify eight kinds of roles) to represent the role information. After RFID Middle Ware decodes and filters the original data in tags, we get a particular combination of encoding rules flag bit sequence, then we can get all kinds of user information respectively by splitting the sequence.

Our system use an active way of searching: It uses the read and write devices to search for the electronic tags within the scope of cover actively. As shown in Fig. 2, the circular area is the read range of a device. When a user with an electronic tag enters this area, the device can read his personal information from his tag, followed by personnel location information is recorded in the system. When more precise positioning accuracy is needed, we can make multiple devices work together to detect the user's location, that said, different device can divided one big area into several sub areas, each device in turn read the electronic tag, we can identify which sub area the target is in by the strength of the signals each device detects. This detection method is shown in Fig. 3.

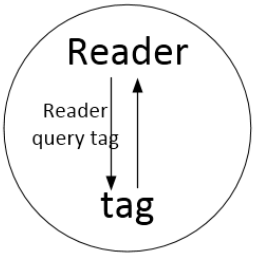

Fig. 2 Search actively

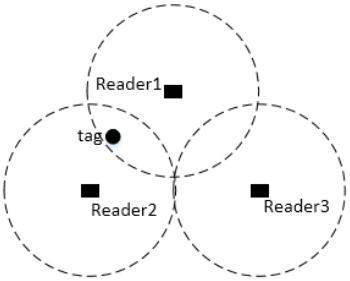

Fig. 3 Integrated search

The RFID Middle Ware.

The System adopt the RFID middleware structure to solve the problem of the communication between the data collected and the data transferred to application. The middleware is divided into two layers: the data layer and logical layer. The function of the data layer is to access to the read and write devices to communicate and interact data with them. Logic layer is the core of middleware, which carries out the analysis of data and equipment management, decoding data obtained from the data layer and providing necessary data for subsequent access rule checks. The data stream obtained from the read and write devices is like "aaaaaa... aaaa" + "bbb" + "cc" + "dd" + "ee". The data stream is a series of bits, "aaaa aaaaaa...", the first 16 binary represents the only identity a user has; "bbb", then 3 binary represents the role information. "ccdd", 4 binary represents the signal information. The first two binary represents signal strength, the left represents signal quality; "ee", 2 binary represents trigger event, one is for button press, the other one is for remove sensor.

Environmental context constraints strategy description.

When a user initiates an access request after identity authentication and role of certification, the relevant environmental factors should also be checked by environmental context constraint strategy, if it conforms to the environmental context constraints, then the user's request is allowed, otherwise the access is prohibited. Some scenes and description strategies are shown in the examples below:

Ex1: The staff who has the role of "equipment management personnel" can check and maintenance management of equipment, and the inspection or repair access request can only be allowed at a certain time period (office hours) and a specific location (Equipment room). Specific access strategy is as follows:

user.role = equipmentManager &
object.id = equipment_#6 & object.userId = user.id &
user.dutyTime Between (beginTime, endTime) &
user.location is equipment_room
Grant{examine, repair}

Ex2: In an emergency situation that equipment alarms, if the corresponding equipment management personnel is not present and can't deal with the emergency, the system will make the personnel who has the same role handle the problems. He must be the nearest person to the equipment according to the location information the read and write devices detect, and the system will issue a command to make him rush there to solve the problems. At the same time, the platform manager will immediately modify the access strategy for the the failing equipment so that the personnel who is coming can get access to the equipment to deal with the problem. The access

strategy is as follows:

```
If(state = emergency)
   user.role = equipmentManager &
   object.id = equipment_#6
   Grant{examine, repair}
```

So this way for emergency processing will ease restrictions which context constraints strategy asks for, making the users who couldn't access to the equipment before have access permissions now.

Summary and prospect

In this paper we propose and realize an access control system based on context-aware access control model combined with RBAC model in order to solve the problems that the traditional access model isn't flexible and secure enough for monitoring management. We place a priority on system design and introduction of how the context-aware access control system works, then we discuss about the environmental context constraint tactics and how to get the environmental context information with the help of RFID.

The main contributions of this paper: 1. We use context-aware access control model to the specific safe production scene, making the access control mechanism more safe and reliable, access control description can change according to the changes of the environment, making the access control mechanism more flexible. 2. We combine the RFID technology with access control model, using RFID to get the identity of the user information and environmental context around the user as RFID is convenient and easy to deploy.

When the emergencies happen, it may expand access privilege for emergency disposal operations, in order to prevent rights abuse, we need a security review mechanism. So subsequent work includes establishing a reasonable and efficient review mechanism to ensure the system more secure.

Acknowledgements

This work is supported by NSFC (Grant Nos. 61300181, 61502044), the Fundamental Research Funds for the Central Universities (Grant No. 2015RC23).

References

[1]. Jordan C S. A Guide to Understanding Discretionary Access Control in Trusted Systems[J]. A Guide to Understanding Discretionary Access Control in Trusted Systems, 1987.

[2]. Latham D C. Department of Defense Trusted Computer System Evaluation Criteria[J]. Department of Defense, 1985, 951(5):págs. 69-72.

[3]. Sandhu R S, Coyne E J, Feinstein H L, et al. Role-Based Access Control Models[J]. Computer, 1996, 29(2):38 - 47.

[4]. Xu F, Xie J, Huang H, et al. Context-Aware Role-Based Access Control Model for Web Services.[J]. Lecture Notes in Computer Science, 2004, 3252:430-436.

[5]. Kayes A S M, Han J, Colman A. A Semantic Policy Framework for Context-Aware Access Control Applications[C]// 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2013:753-762.

[6]. Bai Y, Teng J F, Zhang L Y, et al. Hash Lock-based Strengthen Synchronization RFID Authentication Protocol[J]. Computer Engineering, 2009, 35(21):138-139.