Access Control Mechanism supporting Scalability, Interoperability and Flexibility of Multi-Domain Smart Grid System*

Jihyun Kim[1], Yanghyun Kwon[1], Yunjin Lee[1],
Jungtaek Seo[2], and Howon Kim[1,**]

[1] IS Laboratory, Computer Engeneering Department,
Pusan National University, Busan, Korea
{jihyunkim,yanghyeon_k,astroium,howonkim}@pusan.ac.kr
[2] National Security Research Institute, Deajeon, Korea
{seojt}@ensec.re.kr

Abstract. With increasing interests in efficient energy management follows a rapid development of smart grid. With the help of information technology in smart grid, many smart grid subjects such as a user, a service provider, or even a service component, can access to another smart grid system components freely and frequently. Such highly occurring access controls between smart grid components may raise the possibilities of security breaches such as an unauthorized access to a resource or a system breakdown. To address these security issues, we need to develop proper access control mechanisms for smart grid system. Therefore, we propose access control mechanisms optimized for smart grid. We first defined security requirements of smart grid and analyzed existing access control models whether existing access control models can be applied for smart grid applications. Next we proposed an improved access control framework which satisfies the security requirements we have defined. Finally, based on our proposed access control mechanisms, we have defined access control policies for each smart grid domains.

Keywords: Smart Grid, Access Control Machanism

1 Introduction

With a massive increase in oil prices and drained energy resources bring interests of developing the alternative energy and efficient management of electric power. Such a situation calls for the developments of the smart grid technology. One of the features of the smart grid is the two-way communication across the grid between the customers and electric energy providers[1].

* This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No.2010-0026621).
** Corresponding Author

This two-way-communication feature which puts the grid system and IT together issues security problems belonged to the only public network. For example, analyzing the pattern of electric power consumption can reveal the privacy of users and manipulate the usage data. Additionally, attacks disabling functions on smart grid connected to the public Internet should be considered[2].

For these reasons, the analysis of security requirements to keep operations in stable and the policies implementing these requirements also should be followed in smart grid. This leads the access control model into development for efficient and consistent policy management. However, the existing access control models are suitable for a single system and lack of abilities to complicated features for smart grid. It consists of a number of systems in it.

In this paper, we analyze the features and security requirements of smart grid system and existing access control models for developing optimized access control mechanism for smart grid. We set the range of the system with the upper layer of the smart grid except the transmission/distribution part in this study. We first analyze security requirements and features of smart grid and the existing access control models in Section 2. In section 3, we propose several concepts for developing ideal access control mechanism for smart grid. In section 4, we apply our policies into smart grid domains. In the last section, we make a conclusion.

2 Related Work

2.1 Security Requirements and Features of Smart Grid

Table 1. NIST Smart Grid Security Requirements

Requirement	**Description**
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Identification & Authentication	Smart grid information system uniquely identifies and authenticates users and devices.
Authorization	Smart grid information system enforces assigned authorizations for controlling the flow of information within smart grid information system and between interconnected smart grid information systems in accordance with applicable policy.
Session Management	Once a session is granted, its revocation should be guaranteed.
Boundary Protection	Defines the boundary of smart grid information system and monitoring and controlling communications at the external boundary of the system and at key internal boundaries within the system.

To develop access control mechanism, we have to consider security requirements in smart grid. National Institute of Standards and Technology(NIST) announced *Guidelines for Smart Grid Cyber Security* and we select the security requirements for smart grid from it. Table 1 shows smart grid security requirements. But regarding only security requirements is insufficient to develop optimized access control mechanism for smart grid. We have to reflect features of smart grid. Smart grid has features of system of systems(SoS) in which a large number of users, devices, and systems are participate[3]. Therefore, access control mechanism for smart grid should be suitable for management of many participants. In addition, access control mechanism should provide interoperability among participants and scalability for new participants. And flexibility to handle variety condition in the real world also be considered. We need to develop access control mechanism covers all those security requirements and features up.

2.2 Existing Access Control Models

Role Based Access Control(RBAC) is an access control model which gives easy handling for management of many users. Role in RBAC is a collection of permissions[4]. User is assigned to a role which has permissions for execution of certain operations. Access control system manages roles rather than each user for permission assignment. This feature makes management of access privileges easier. However, real world involves multiple, complex factors and number of roles needed to cover these factors will grow exponentially.

On the other hand, case of Attribute Based Access Control(ABAC), those factors can be added with ease. Attribute is a factor that describes identity or feature of a subject. In ABAC, access is granted on the basis of attributes of the user[5]. To grant access, the user has to prove his/her attributes are satisfying claims specified on access control policy of the system.

Recent studies suggest Role Attribute Based Access Control(RABAC) as a suitable access control model for distributed system. RABAC follows the advantages of RBAC and ABAC[6]. Thus it can manage many kinds of users in detail.

3 Our Proposal

In this section we propose improvements on requirements for smart grid access control mechanism analyzed in section 2. To satisfy scalability and interoperability, we suggest Domain of Domains(DoD) concept and communication format. Also, we apply RABAC to smart grid in order to manage many kinds of users and devices. Lastly, we suggest combination view to meet flexibility.

3.1 DoD

Domain is a set of elements which has same functions or structural features. DoD combines the same sort of domains from more than two actors[3]. The extracted domains can form a domain which can be used another purposed actor. As a result, domains compose smart grid. In this paper we organized 5 different kinds of domains(Table 2).

Table 2. Domains of Smart Grid

Domain	Description
User	The set of users. It can be assigned to the role containing normal user, administrator, staff and so on. It can request the service domain to get service.
Database	The set of the information. It verifies the request from the sender and provides the service to it.
Service	The set of the service element. The service element consists of operations. It receives the request of service and processing it. It calculates or manipulates data for request. It also request data or service which they cannot handle itself to the other service.
Management	The set of elements which generate the command monitoring and controlling the system.
Device	The set of elements which send data to the management domain periodically. The device would be operated followed by the command from management domain.

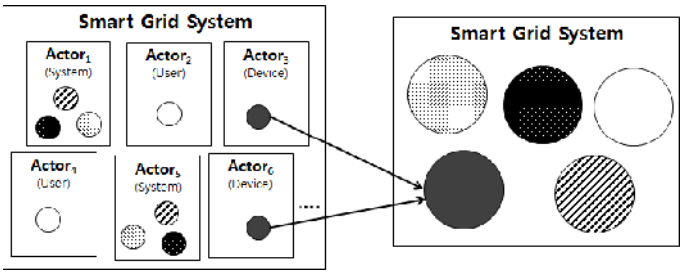

Fig. 1. Actor Concept and Domain Concept of Smart Grid System

Fig.1 shows how to construct smart grid with actors and domains. Domains in *Actor3* and *Actor6* make a same sort of domain by DoD concept. This feature makes smart grid has scalability.

[3] Actors include devices, systems, or programs that make decisions and exchange information necessary for performing applications[3].

However we need to consider interoperability for communication between domains, because smart grid is composed of the heterogeneous networks. Thus we suggest communication format. Our communication format is modelled on Extensible Authentication Protocol(EAP)[7]. It will be encapsulated in communication frame of the heterogeneous networks. Fig.2 shows Data Format and Authentication Format. To support different of kinds of authentication protocol,

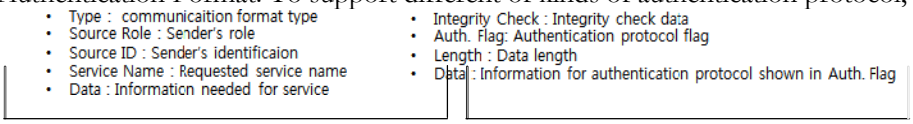

Fig. 2. Data & Authentication Format

authentication format has Auth. Flag and Data. And we define Interface which executes identification and authentication process. We assume that all domain has interface.

3.2 RABAC Applied in Smart Grid

Smart grid contains a number of users, devices, and systems so we must consider all those components. In addition, we need to consider about various factors which complicate implementation in real world.

We apply RABAC to smart grid to cover both numerous components and factors up. Fig.3 shows how to assign roles to an actor and its domains hierarchically. An actor is composed of domains which have their own attributes. Roles and attributes are reflected in the access control of each domain.

3.3 Combination View

Because smart gird is a complex system, unexpected problems can occur. So coping with such situations is critical. Combination view enables detailed access control. It regards that task in smart grid is compound of resources. Resources and tasks are differ from domain to domain. For example, resources and tasks are operations and services in service domain(Fig.4) but in management domain they are operations and commands. Thus if unexpected problem occurs in specific task, we can transform the task into different combination of resources flexibly.

4 Access Control Policies in Domains

In this section, we define policies for smart grid system with improvements that we explained before. Service, database and management domain which are belonged to system need the policies matching for each of the features. According to their functions, we define access tables using for access control.

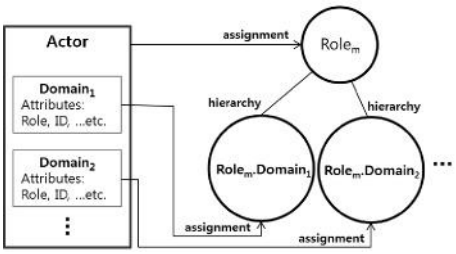

Fig. 3. Role-Attribute Assignment on Actor

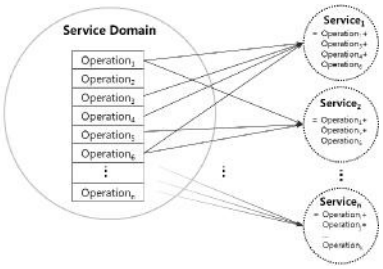

Fig. 4. Combination View Applied to Service Domain

4.1 Service Domain

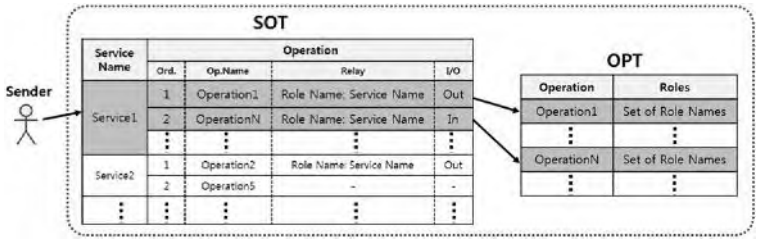

Fig. 5. Access Control Flow in Service Domain

Fig.5 shows the access control flow in service domain when service request occurs to it. SOT(Service Operation Table) has information on operations which are the elements of service. It consists of name of service which can be dealt within this domain, order of operations for service, operation name, destination for operation delay and flag which means whether the destination is in or out of this system. OPT(Operation Permission Table) denotes the roles which have permission for operation at work. Following are access control policies in service domain.

- Check the line of SOT where the requested service name is exist.
- Deal with the operations by their order before check if the role of sender is in OPT for each operation.
- If the roles for operation in OPT has no matched role of sender, then alarm sender that it has no permission to process it.
- When if the access is accepted, the operation works.
- If the operation should be delayed to inter-system-domain, system performs the operation and responds the result to sender.
- If the operation should be relayed to external-system, it goes to the service domain in external-system followed by the relay field of SOT.

4.2 Database Domain

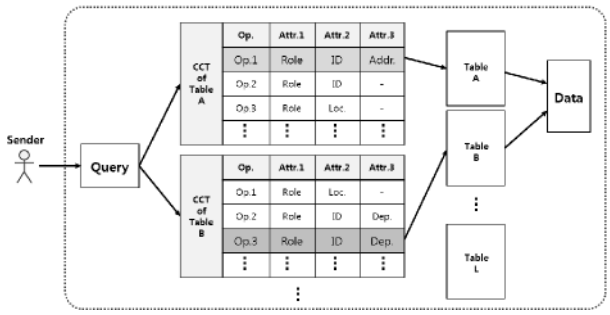

Fig. 6. Access Control Flow in Database Domain

Fig.6 shows the access control flow in database domain when query occurs to it. Each database table has a CCT(Claim Check Table) which consists of claims for each operation and policy which meets the claims. Claim is a requirements to acquire the access authority in respect of the resource. Following are access control policies in database domain.

- If the sender who requests service for receiving data has the attributes matching the claim for access authority, database domain returns the result of the operation.
- If the attributes of the sender are not sufficient for claim, then database domain returns the denying message.

4.3 Management Domain

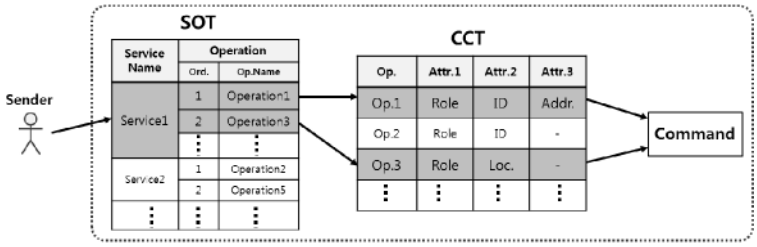

Fig. 7. Access Control Flow in Management Domain

Fig.7 shows the access control flow in management domain when request for command occurs to it. Each operation has a line in CCT and policy which fills the claims. Following are access control policies in management domain.

- Sender can perform the command if and only if the initial requester meets the claims for carrying requested operations defined by CCT out.
- Management domain returns the result of requested command if and only if the initial requester's attributes satisfy the claims.

5 Conclusion

Since the smart grid system is composed of many kinds of subjects(i.e., user, service provider, service component, etc.) and objects(i.e., service system, smart meter, etc.), it needs different kinds of access control policy to each smart grid component. After our analyzing existing access control policies, we have found that a novel access control mechanism should be developed for providing access control policies to complex smart grid system. Therefore, in this paper, we first analyzed the features and security requirements of smart grid system. From our analysis, we came to know that scalability, flexibility, interoperability are most crucial requirements for smart grid access control mechanism.

To develop a proper access control mechanism for smart grid system, we defined a DoD concept which gives scalability by making an extended domain in a way that one domain combines other domains. In addition, interoperability was satisfied by using a proposed communication model which enables communication between heterogeneous networks. And we proposed how RABAC access control mechanism can be applied to such a complex smart grid system. RABAC can manage the numerous smart grid subjects in detail due to following the advantages of RBAC and ABAC. For assigning flexibility, we defined a combination view. It enables reconstructing task in domain thus this feature can cope with occurrence of the unexpected problem properly. As a result, our model satisfies all requirements what we analyzed, therefore we expect our proposed access control mechanism will contribute to the realization of smart grid.

References

1. Farhangi, H.: The path of the smart grid. Power and Energy Magazine, IEEE 8(1) (january-february 2010) 18 –28
2. H. Khurana, M. Hadley, N.L.D.A.F.: Smart-grid security issues. In: IEEE Security and Privacy, vol. 8. (2010) 81–85
3. NIST: Nist framework and roadmap for smart grid interoperability standards, release 2.0. (2012)
4. Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R., Chandramouli, R.: Proposed nist standard for role-based access control. ACM Trans. Inf. Syst. Secur. 4(3) (August 2001) 224–274
5. Lang, B., Foster, I., Siebenlist, F., Ananthakrishnan, R., Freeman, T.: Attribute based access control for grid computing. Math. Comput. Sci.(MCS) Div., Argonne Nat. Lab (2006)
6. Kuhn, D.R., Coyne, E.J., Weil, T.R.: Adding attributes to role-based access control. Computer 43(6) (june 2010) 79 –81
7. B. Aboba, L. Blunk, J.V.J.C., Levkowetz, H.: **Extensible authentication protocol (eap). (2004)**