A Role-based Access Control Model Supporting Regional Division in Smart Grid System

Daniela Rosic, Imre Lendak, Srdjan Vukmirovic

Faculty of technical sciences, University of Novi Sad
Trg Dositeja Obradovica 6, 21000 Novi Sad, Serbia
E-mail: drosic@uns.ac.rs; lendak@uns.ac.rs; srdjanvu@uns.ac.rs

Abstract: Smart grids are modern electric power infrastructures, which incorporate elements of traditional power systems and information and communication technology (ICT), with the aim to improve the reliability, efficiency and safety requirements of critical infrastructure systems. Due to its reliance on ICT, the Smart Grid exposes electrical power systems to new vulnerabilities and security issues. Therefore, security is becoming an ever increasing concern, in the physical and ICT domain as well. Access controls are one of the most important aspects of information security and a vital element of a layered security strategy. The role-based access control (RBAC) model is widely used in complex enterprise systems which are characterized by many participants accessing the system, but with different levels of access rights depending on their specific duties and responsibilities. The existing security models, which are primarily role-based, are usually not tailored for critical infrastructure systems with specialized features, such as high numbers of equipment and devices dispersed over vast geographical regions. In order to meet the security requirements of smart grids, it is important to manage their assets on a fine level of granularity. This paper proposes an access control management system for smart grids by considering the regional division of critical assets and concept of areas of responsibility (AOR). To this end, the standardized RBAC model was extended with the aim to improve the existing access control policy with greater level of granularity from the aspect of managing electrical utilities. In this paper, we propose the RBACAOR model, which was developed and tested on the Windows operating system platform using .NET Framework role-based security, with the use of different data stores for the RBACAOR configuration, namely Active Directory (AD), AD Lightweight Directory Services (AD LDS) and Microsoft SQL Server.

Keywords: smart grid; role-based access control; regional division; area of responsibility;

1 Introduction

Smart grids are modern electric power infrastructures which incorporate elements of traditional electric power grids and information and communication technology (ICT), with the aim to improve the reliability, efficiency and safety as crucial requirements of critical infrastructure systems. As complex systems of systems, which are integrated and interconnected over the communication network, smart grids brought along substantial benefits relating to the automation, supervision and real-time monitoring and control throughout the electric power grid, modern communications infrastructure and modern energy management techniques [1][2].

In order to provide greater reliability, efficiency and effectiveness of operations, the Smart Grid relies on a complex information and communication infrastructure to establish interconnections between different smart grid components. This complexity and the numerous interconnections (e.g. utility field crew for accessing critical operations data, control center inter-connections, etc.), make the Smart Grid a prime target of cyberattacks. Deliberate attacks are not the only threats to modern critical infrastructures (smart grids included), which might jeopardize the reliable and safe operation of these complex systems [3][4], illegitimate access and malicious attacks against smart grids can also cause data latency or data loss, thus negatively affecting operation capabilities, e.g. decision making and timely and correct responses to system events. The privacy of users might also be compromised as consumer data is now stored in business systems, which are often accessible from the Internet [5].

Because of the above listed threats, security is becoming a growing concern in smart grids, and the protection of the system and its resources from unauthorized access is of critical importance. Strict access control systems are a vital element of a layered security strategy, especially in mission-critical systems and services, where they represent a significant step towards eliminating single points of failure.

This paper proposes the $RBAC_{AOR}$ access control management system, which addresses the specific requirements of smart grids. The existing role-based access control (RBAC) model [6] will be extended to support features and security requirements specific to the smart grid environment. These specific features and requirements are analyzed in Section 2. The extended $RBAC_{AOR}$ model is discussed in Section 3. The proposed $RBAC_{AOR}$ model is applied in a smart grid environment in Section 4.

2 Security Requirements and Features of Smart Grid

2.1 Security Requirements of Smart Grids

A conventional power grid is composed of dedicated power devices which form isolated networks, with reliable and predictable communication links. In contrast, smart grids expose electrical power systems to new vulnerabilities and security issues through the introduction of complex communication networks and information systems. In order to effectively protect smart grids from cyberattacks, strong and robust security controls are needed. Access control is one of the most important aspects of information security, critical in preserving the confidentiality, integrity and availability of information [7]. Availability might be the most important security objective in critical infrastructure systems, as a measure towards ensuring continuous, uninterrupted, real-time monitoring and control. While information integrity is an increasingly critical requirement, confidentiality was historically the least critical for electric power grids. The latest trends show, that it is becoming more significant as personal information (such as customer energy consumption data) might be available on networks and disclosure of sensitive data can lead to serious concerns regarding user privacy.

In order to meet security challenges, the National Institute of Standards and Technology (NIST) specified the following security requirements for smart grids [7]:

- Availability refers to ensuring timely and reliable access to and use of system and data. Malicious attacks targeting availability can be considered as Denial-of-Service (DoS) attacks, which intend to delay, block, or even corrupt the communication channels in the system.

- Integrity refers to guarding against information modification or destruction by unauthorized users or systems. Malicious attacks targeting the integrity of a smart grid attempt to manipulate or corrupt critical data, such as meter readings, billing information, or control commands, thus leading to the ability to negatively impact operations or even service disruption and system instability.

- Confidentiality, refers to protecting sensitive data from unauthorized access. Although malicious attacks targeting confidentiality have negligible effects on the operation of the system, serious privacy issues arise from a disclosure of customer personal information and may lead to a variety of severe consequences in the Smart Grid.

In order to address these challenging security issues in a Smart Grid, various cyber security controls are specified by the NIST. Access controls ensure confidentiality, integrity and availability of system and data by employing identification, authentication and authorization mechanisms as follows:

- Identification & Authentication: the information system(s) incorporated into smart grids have to uniquely identify and authenticate all participants (users, devices, systems) requiring access to the system.

- Authorization: the information system(s) incorporated into smart grids have to enforce authorization checks for valid users, who request access to resources within the system or between interconnected systems. Authorization may be achieved by various mechanisms to meet the needs of businesses. Different access control models are discussed in the following section.

2.2 Access Control Model Overview

The existing access control models can be classified into three broad categories: mandatory access control (MAC), discretionary access control (DAC) and role-based access control (RBAC). The MAC policy relies on security labels which have to be assigned to all users and resources in the system by system administrators, making the MAC inflexible for large systems. On the other hand, the DAC policy is based on object ownership, in which resource owners define the access privileges associated with their resources. Access control lists (ACL) are a commonly used DAC policy, enforcing specific entities attached to resources to define resource access to objects on a per user basis. Decentralized administration, as well as difficult and costly maintenance of large numbers of ACLs make the DAC less suitable for large systems.

The RBAC model was introduced as an alternative to MAC and DAC, as a model which meets the security requirements of complex enterprise systems with many participants. In RBAC, access decisions are based on the user's privileges obtained through the roles the user is authorized for. It offers easier access management, and reduces complexity and the cost of administration. These positive characteristics make RBAC suitable for systems with large numbers of users [8].

2.3 RBAC96 Model

The RBAC96 [9] is a family of role-based access control (RBAC) models which defines the scope of RBAC features included in the NIST standard. The Core RBAC (RBAC$_0$) defines a minimum collection of RBAC entities and entity relationships which have to be supported by any RBAC compliant system. Core RBAC elements and relations are listed below (RBAC abbreviations are enclosed in brackets):

- Users *(USERS)* are subjects (a person, computer, network) which directly interact with the system,
- Objects *(OBS)* are physical or information assets, i.e. any system resource which needs to be protected,
- Operations *(OPS)* are active processes or actions invoked by a user,
- A permission *(PRMS)* is an operation defined on an object – access right (privilege) for a resource in the system,
- A role *(ROLES)* is a job function or responsibility in the context of the system,
- User Assignments *(UA)* define user-role relations. Users are assigned to roles according to their responsibilities. Each user can be assigned one or many roles, and each role can be assigned to one or many users.

- Permission Assignments *(PA)* define permission-role relations. A role is a collection of permissions and each permission can be assigned to one or many roles. Permissions are not assigned to users directly. Instead, users obtain permissions implicitly through their roles.

The set of entities and static relations in the $RBAC_0$ model is represented in Fig. 1. The entity relationship diagram implies that a user can have one or many roles. A role is a collection of one or many permissions. Every permission is determined as a privilege needed to perform a certain operation on an object.

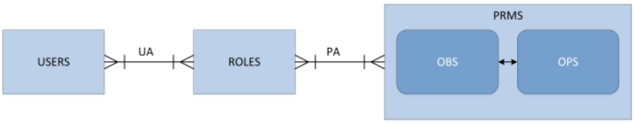

Figure 1

$RBAC_0$ Entity Relationships Diagram

2.4 Authorization Challenges in the Smart Grid

The Smart Grid is a collection of information systems with different operational and functional requirements [10]. The operational system represents a real-time environment for monitoring and control of Industrial Control Systems (ICS), such as a Supervisory Control and Data Acquisition (SCADA) or Distributed Control System (DCS). Beside SCADA/DCS, smart grids usually contain enterprise systems as well, which are intended for business and engineering operations, as well as to provide access from the Internet using common functions like e-mail and web services. The SCADA/DCS and the various enterprise systems are often interconnected, thereby allowing data exchange, as well as efficient operational and maintenance activities. Therefore, strict access controls are crucial for a reliable and secure integration of ICSs in corporate business processes, ensuring that all users are restricted only to the functionalities needed to accomplish their duties, as well as to disable illegitimate users from accessing the system.

Smart grids are very complex interconnected systems. For example, statistics [1] showed that there are over 2000 power distribution substations, about 5600 distributed energy facilities, and more than 130 million customers all over the US. From this it follows that smart grids are characterized by large numbers of users, critical assets and functionalities which need to be properly managed, controlled and made available to appropriate users and applications across the system. Hundreds of thousands of pieces of equipment and devices are deployed over a very large geographical area and the separation of duties and responsibilities with respect to the electricity network (e.g. by voltage level, by substation, by feeder, or by device) significantly simplifies the management of these systems.

Furthermore, sharing responsibilities among users who are assigned the same role reduces a likelihood of (configuration) errors in the system.

The RBAC96 is a rather generic access control model and does not fully meet all the security requirements of critical infrastructure systems, such as the separation of users' duties and responsibilities according to regional division of critical assets. To this end, the notion of an area of responsibility (AOR) is introduced as another level of access control in the Smart Grid environment [11]. The AOR refers to a collection of electric power system resources in a common geographic area, usually managed together. Depending on the assigned AORs, a user can be allowed to monitor, control and/or modify only certain parts of the system. Fig. 2 illustrates the relationships between electric power system resources, users and AORs. The resources belong to AORs as geographical areas, which are comprised of one or more logical areas. Users are never assigned to geographical areas directly. Instead, users are assigned to AORs as logical areas, thus obtaining a certain level of responsibility for geographical areas associated with these logical areas. In doing so, a finer granularity of access rights is allowed for users belonging to the same role. Hereafter, the notion of AOR configuration refers to both geographical areas and logical areas, as well as the relationships between them.

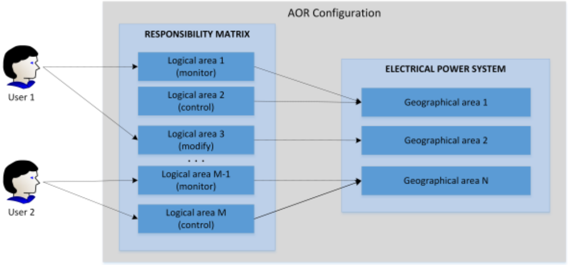

Figure 2
Area of Responsibility Configuration

3 The Formal Definition of RBACAOR Model

This sections contains a formal definition of $\mathrm{RBAC}_{\mathrm{AOR}}$, which extends the RBAC model and thereby meets the security requirements of smart grids discussed in Section 2. The model changes put forward in this paper propose to extend the basic set of RBAC_0 entities and static relations to incorporate the concept of AORs. Only the static (i.e. configuration time) entity relationships are considered, i.e. any aspect of dynamic (i.e. on-the-fly) AOR assignment is outside our scope.

3.1 The Extended Set of RBACAOR Entities and Relations

$RBAC_{AOR}$ extends the basic set of $RBAC_0$ entities with the concept of AORs [11]. The AOR entity is introduced to establish another level of access control with respect to the regional division of smart grid assets. The entity relationship diagram of the $RBAC_{AOR}$ model is represented in Figure 3. The $RBAC_{AOR}$ specific entities and relationships (marked in red) are summarized below:

- User-AOR Assignments *(UAA)* are introduced to define relationships between users and AORs. A user can be assigned zero, one or many AORs. On the other hand, an AOR can be assigned to one or many users. An AOR should not remain unassigned, as in that case a part of the Smart Grid would be unsupervised.
- Object-AOR Assignments *(OAA)* are introduced to define relationships between the smart grid assets (OBS) and AORs in the $RBAC_{AOR}$ model. Depending on the structure of the electric power system, each asset can belong to one or many AORs. One example of one-to-many relation is for assets (e.g. switchgear) placed on (or near) the boundary between the high-voltage (HV) energy management and medium-voltage (MV) distribution management system. For OBSs which are assigned to zero AORs, AOR level of access control is not considered. Similarly, an AOR can be associated with an arbitrary set of objects, depending on the business logic.

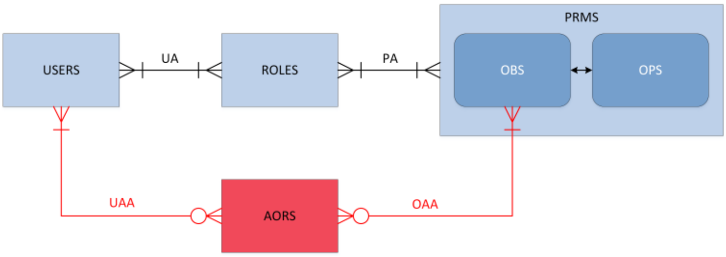

Figure 3
$RBAC_{AOR}$ Entity Relationships Diagram

3.2 AOR Responsibility Matrix for the Operation of the Smart Grid

To support different levels of responsibilities for the operation of electric power systems, the AOR entity is extended with the property *LevelOfResponsibility* which can take any of the following values: MONITORING, CONTROL and CONFIGURATION. AOR levels of responsibility are closely related to different types of operations in the Smart Grid, which can be grouped into the below listed three categories [12][13]:

- MONITORING – Smart grid monitoring (such as equipment status, power flow, outage information, etc.) delivers situational awareness about power system components and performance in near real time, based on which potential problems might be identified (overloads, high/low voltage conditions, fault and outage locations) and premature equipment failures might be predicted.
- CONTROL – Smart grid control (i.e. operations) involves response to situations needing immediate actions in a timely and correct manner, e.g. the control of substations, transformers or feeders, configuration of different operational parameters which influence the behavior of the Smart Grid, managing incidents, etc. Control activities are usually carried out by human operators who analyze data (e.g. in the form of events and alarms in different systems) and decide which protective, preventive or corrective action should be taken.
- CONFIGURATION – Smart grid configuration covers activities related to modifying feeders, transformers, and other components of electric power systems, and their connectivity in the network model. Importing feeders from a Geographical Information System (GIS) might be regarded as a configuration activity in the Smart Grid.

The AOR responsibility matrix, namely the AOR Policy, is introduced to define the required level of responsibility for different types of smart grid operations. The AOR Policy is determined by the following rule: a user is allowed to execute an operation on an OBS (i.e. smart grid asset belonging to a particular AOR) only if the category of the requested operation corresponds to the AOR level of responsibility the user is assigned to. Otherwise, the user is restricted to read-only access to the requested smart grid asset.

Introducing different categories of smart grid operations does not require any additional changes to the Operation entity defined in $RBAC_0$. Instead, requiring a certain level of responsibility for the operation is accomplished by employing the AOR's property *LevelOfResponsibility* based on the (logical) category of every smart grid operation.

3.3 Class Diagram of $RBAC_{AOR}$ Authorization Framework

The set of entities and static relations in the $RBAC_{AOR}$ model is represented in Figure 4. The $RBAC_{AOR}$ class diagram is given in the context of the Microsoft Windows operating systems. A security principal is any entity which can be authenticated by the system, e.g. users and user groups. A security identifier (commonly abbreviated SID) is used as a unique, immutable identifier of users, roles, permissions and AOR entities.

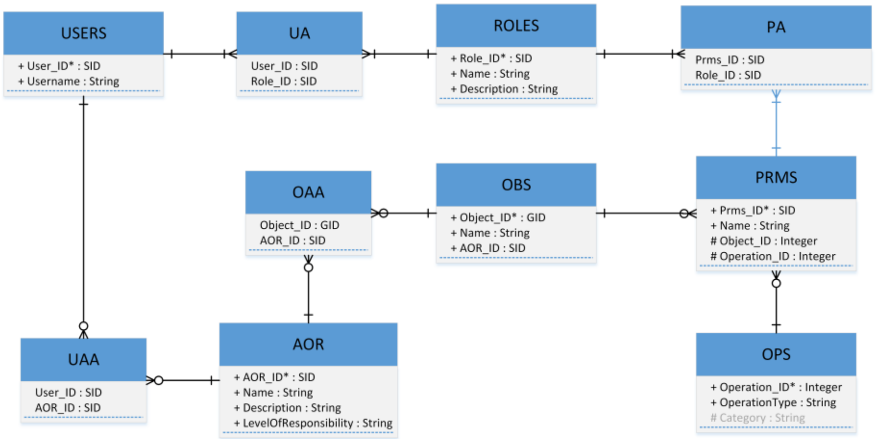

Figure 4
RBAC_{AOR} Class Diagram

4 RBAC_{AOR} Implementation

The proposed RBAC_{AOR} access control management system was implemented with Microsoft's Identity and Access Management (IAM) system and the .NET programming framework. The core component of Microsoft's IAM system is the Active Directory Domain Services (AD DS) which provides a centralized and secure identity storage and services for authentication and authorization, compliant with the Lightweight Directory Access Protocol (LDAP) protocol. Kerberos is a trusted third party authentication protocol natively included in the Active Directory (AD) environment, it ensures mutual authentication of principals and provides them with a shared session key (symmetric cipher key) to protect the confidentiality and integrity of communication channels.

The authorization mechanism ensures control of privileged operations based on information contained in a centralized identity storage. For applications running within the enterprise boundary (and having access to the AD over LDAP) the .NET authorization framework enables role-based access control mechanism in which roles are defined as AD security groups representing the relationship between users and access rights to resources in the system. Our initial analyses showed that using AD for storing the entire RBAC_{AOR} configuration would incur significant performance issues. Furthermore, AD schema changes, required to support new RBAC_{AOR} entities, would result in a significant and costly administrative burden. Furthermore, errors in AD schema changes might result in data loss or corruption. Therefore, we suggest storing the RBAC_{AOR} configuration in different types of data stores, depending on the type of data and how applications use them.

A single smart grid system was modeled in a single AD domain with its own identity storage, thus ensuring separation of users' responsibilities between different systems. However, a controlled communication must be established between systems to accomplish different business needs as discussed in Section 2. A secure integration of multiple systems occurs through the AD trust mechanism which establishes a trust relationship between identity stores, allowing for users in one domain to access resources in another domain. The remainder of this section describes details regarding the RBAC_{AOR} configuration data storage and the RBAC_{AOR} access control system.

4.1 RBAC_{AOR} Configuration Storages

Two different types of databases were used for storing RBAC_{AOR} configuration. A directory database was used for storing relatively static data which needs to be distributed among applications in a single system or between systems. A relational database was used for storing frequently changing data on a per-application basis. Figure 5 shows how the different databases were used for storing the RBAC_{AOR} entities.

Active Directory (AD) was used as a directory database to provide a centralized storage of system-specific information, such as users, roles and user-role membership, which needs to be used across the enterprise and between systems. However, AD could provide more complex access controls based on other data, including user attributes, time, data or other environmental attributes, thus allowing for a higher degree of control and more flexibility to meet the specific needs of enterprise systems.

Application-specific data (permissions, AORs and group memberships related to RBAC_{AOR}) were stored in the Active Directory Lightweight Directory Services (AD LDS). The AD LDS is a service-architected implementation of AD which runs on every machine in the system, thus alleviating run-time loads on AD and reducing network traffic. RBAC_{AOR} application data require directory schema extensions to include definitions of custom objects and attributes and storing application-specific data in AD LDS allows for flexible access control mechanism which can be extended with new application-specific entities without incurring significant risks, costs, or burdens.

Electric power system resources change more frequently compared to other RBAC_{AOR} entities (users, roles, permissions, AORs). These changes are related to creating, editing and deleting electric network elements, their connectivity and AOR memberships when the smart grid's network model is configured or integrated with other IT systems. Accordingly, Microsoft's SQL Server was used as a relational database, to store information about OBS entities, as well as, relationships between OBS and AORs.

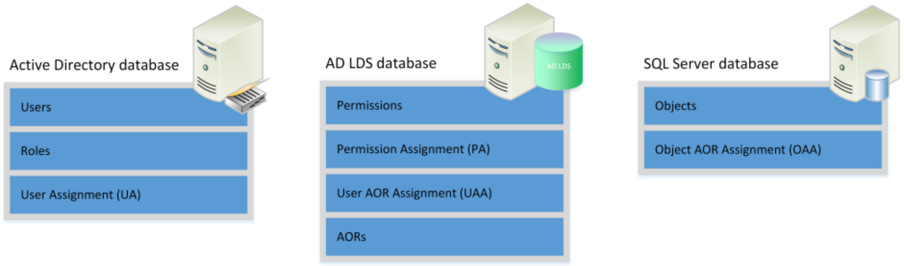
Active Directory database
Users
Roles
User Assignment (UA)
AD LDS database
AD LDS
Permissions
Permission Assignment (PA)
User AOR Assignment (UAA)
AORs
SQL Server database
Objects
Object AOR Assignment (OAA)

Figure 5
RBAC$_{AOR}$ Data Storages

4.2 RBAC$_{AOR}$ Access Control System

As presented in Figure 6, the RBAC$_{AOR}$ access control system is comprised of two processes, authentication and authorization, which are combined to ensure that resources are accessed only by authorized users.

The RBAC$_{AOR}$ authentication framework utilizes .NET Integrated Windows authentication (IWA) as a first step toward gaining access to the system. IWA is based on the Secure Protocol Negotiation (SPNEGO) security package embedded in the Windows operating systems. Although the SPNEGO can interface with both the Kerberos and the NTLM authentication protocols, Kerberos was chosen as the best suited authentication protocol for intranet environments where both clients and servers are in the same domain or trusted domains. Kerberos is a widely-adopted network authentication protocol, in which client and server mutually authenticate each other based on a reliable third-party. Kerberos ensures session confidentiality and integrity by using session keys [14].

The RBAC$_{AOR}$ security principal is a result of successful authentication and consolidates identity information from multiple data storages (AD and AD LDS) which are combined in real-time. The RBAC$_{AOR}$ authorization framework is based on .NET Framework role-based security which has been adapted to specific data stores of system and applications, such as AD, AD LDS and SQL Server. The RBAC$_{AOR}$ authorization framework is comprised of two independent authorization processes which are combined to determine the final access control decision based on information encapsulated into the RBAC$_{AOR}$ security principal:

1. The Role-Based Access Control flow is executed by a user request to execute operation Op on an OBS. A RBAC access decision is determined by checking whether the RBAC$_{AOR}$ security principal has a permission which defines the privilege for the required resource.
2. The AOR access control flow is executed by a user request to access OBS, belonging to an area of responsibility AOR. An AOR access decision is determined by checking whether the RBAC$_{AOR}$ security

principal is a member of at least one logical area associated with the AOR to which the object (OBS) belongs.

The final access control decision is determined based on the RBAC access decision and AOR access decision so that access is authorized only when both RBAC and AOR access decisions are determined as allowed. For authorized users, the level of responsibility is further considered based on the AOR Policy. As explained in Section 3, a user is allowed to execute an operation Op on an object (OBS) only if the user is assigned to at least one logical area (related to the AOR to which object belongs) with the level of responsibility which corresponds to the category of the requested operation. Otherwise, the user is restricted to read-only access to the requested operation on the smart grid asset.

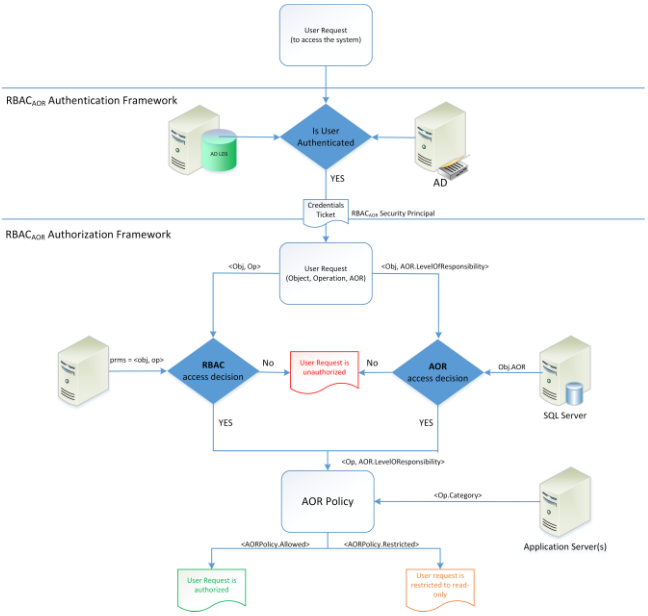

Figure 6

RBAC$_{AOR}$ Access Control System

Conclusions

This paper addresses the problem of access control in smart grids, as one of the most important aspects in preserving the confidentiality, integrity and availability of smart grid (and critical infrastructure systems in general) assets. First, we analyzed features and security requirements specific to smart grids, in order to define the strengths and weaknesses of the existing access control models, with emphasis on the RBAC model, as the most commonly used model in large enterprise systems. While analyzing the security requirements of smart grids, we deduced that the existing access control model based on a user's roles and responsibilities within the system does not cover every security requirement of modern electric power grids with large numbers of equipment and heterogeneous devices dispersed over vast geographical regions. Therefore, this paper presents an extension to the standard RBAC_0 model with the concept of the area of responsibility (AOR). The proposed RBAC_{AOR} model is comprised of two separate components: role-based access control flow and AOR-based access control flow. Both components check independently whether users have appropriate access rights, and make the final access decision based on the combination of access decisions made by each subcomponent.

The RBAC_{AOR} model extends the currently available role-based access controls, to provide an efficient and highly secure access control method designed specifically for smart grids. The proposed access control model was implemented with Microsoft technologies and can be easily integrated into existing role-based access control systems which are based on Active Directory security services.

Hierarchical RBAC or constrained RBAC were outside the scope of this research, i.e. only the Core RBAC features and the set of static relationships were taken into consideration. Making access control decisions based on user and/or session attributes to enforce different constraints depending on the context in which limitations are imposed was (also) outside of the scope of this paper. Some examples include roles and AORs which can be activated/deactivated for a given user, depending on the workstation the user has logged into, or dynamic AOR assignment to support transfer of duties during regular system activities. Activities related to real time simulation in smart grids in order to analyze the behavior of a network which evolves might also require specific authorization policies. The authors intend to explore these questions as part of their future research. It is important to note that the RBAC_{AOR} model proposed in this paper is flexible and extensible, and the authors are confident that it will easily incorporate solutions for these additional requirements.

References

[1] Xu Li, Xiaohui Liang, RongXing Lu, Xuemin Shen, Xiaodong Lin, Haojin Zhu: “Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges”, IEEE Communications Magazine, August 2012, pp. 38-45

[2] Wenye Wang, Zhuo Lu: “Survey Cyber Security in the Smart Grid: Survey and Challenges”, Computer Networks: The International Journal of Computer and Telecommunications Networking, April 2013, pp. 1344-1371

[3] H. Melvin: “A Role of ICT in Evolving SmartGrids”, 10th International Conference on Digital Technologies (DT), July 2014, pp. 235-237

[4] Ruofei Ma, Hsiao-Hwa Chen, Yu-Ren Huang, Weixiao Menart: “Smart Grid Communication: Its Challenges and Opportunities”, IEEE Transactions on Smart Grid, February 2013, pp. 36-46

[5] Zhang Zhigang, Liu Hao, Niu Shuangxia, Mo Jiansong: “Information Security Requirements and Challenges in Smart Grid”, 6th IEEE Joint International Information Technology and Artificial Intelligence Conference (ITAIC), August 2011, pp. 90-92

[6] National Institute of Standards and Technology (NIST): “Role-based Access Control”, 2003

[7] National Institute of Standards and Technology (NIST), NISTIR 7628: “Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements”, 2010

[8] Maria B. Line, Inger Anne Tondel, Martin G. Jaatun: “Cyber Security Challenges in Smart Grids”, 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe), December 2011, pp. 1-8

[9] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, Ramaswamy Chandramouli: “Proposed NIST Standard for Role-based Access Control”, ACM Transactions on Information and System Security, August 2001, pp. 224-274

[10] J. Zerbst, M. Schaefer, I. Rinta-Jouppi: “Zone Principles as Cyber Security Architecture Element for Smart Grids”, IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe), October 2010, pp. 1-8

[11] D. Rosic, U. Novak, S. Vukmirovic: “Role-based Access Control Model Supporting Regional Division in Smart Grid System”, 5th International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), June 2013, pp. 197-201

[12] A. P. S. Meliopoulos, G. J. Cokkinides, Renke Huang, E. Polymeneas, P. Myrda: “Grid Modernization: Seamless Integration of Protection, Optimization and Control”, 47th Hawaii International Conference on System Sciences (HICSS), January 2014, pp. 2463-2474

[13] Applied Communication Sciences: “Smart Grid – Leveraging Distributed Operations Capabilities”, 2012

[14] Dahui Hu, Zhiguo Du: “An Improved Kerberos Protocol Based on Fast RSA Algorithm”, IEEE International Conference on Information Theory and Information Security (ICITIS), December 2010, pp. 274-278