International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:1, No:8, 2007

Role-based Access Control Model in Home Network Environments

Do-Woo Kim, Geon Woo Kim, Jun-Ho Lee, and Jong-Wook Han

***Abstract*—**The home in these days has not one computer connected to the Internet but rather a network of many devices within the home, and that network might be connected to the Internet. In such an environment, the potential for attacks is greatly increased. The general security technology can not apply because of the use of various wired and wireless network, middleware and protocol in digital home environment and a restricted system resource of home information appliances. To offer secure home services home network environments have need of access control for various home devices and information when users want to access. Therefore home network access control for user authorization is a very important issue. In this paper we propose access control model using RBAC in home network environments to provide home users with secure home services.

***Keywords*—**Home Network, Access Control, RBAC, Security.

I. Introduction

THE home in these days has not one computer connected to the Internet but rather a network of many devices within the home, and that network might be connected to the Internet. In such an environment, the potential for attacks is greatly increased.

The general security technology can not apply because of the use of various wired and wireless network, middleware and protocol in digital home environment and a restricted system resource of home information appliances. Also the users of a home environment are mostly lacking awareness and knowledge on security and network management [1,2].

Access is the ability to do something with a system resource (e.g., use, change, or view). Access control is the means by which the ability is explicitly enabled or restricted in some way. Computer-based access controls can prescribe not only who or what process may have access to a specific system resource, but also the type of access that is permitted. With role-based access control, access decisions are based on the roles that individual users have as part of an organization. Users take on assigned roles (such as doctor, nurse, teller, manager). The use of roles to control access can be an effective means for developing and enforcing enterprise-specific security policies, and for streamlining the security management process [3].

To offer secure home services home network environments have need of access control for various home devices and information when users want to access. Therefore home network access control for user authorization is a very important issue. In this paper we propose access control model using RBAC in home network environments to provide home users with secure home services.

The rest of the paper is organized as follows. In Section 2, we provide some background information on DAC, MAC, and RBAC. The need of security in Home network environments is given in Section 3. The proposed RBAC model in Home network environments is presented in Section 4. Conclusion is in Section 5.

II. Preliminaries

A. DAC and MAC

DAC(Discretionary Access Control) is a means of restricting access to objects based on the identity of users or groups to which they belong, or both. The controls are discretionary in the sense that a user or subject given discretionary access to a resource is capable of passing that information along to another subject. To provide this discretionary control, DAC mechanisms usually include a concept of object ownership, where the object's "owner" has control permission to grant access permission to the object for other subjects [5].

MAC (Mandatory Access Control) is a technique to protect and contain computer processes, data, and system devices from mis-use. MAC mechanisms assign a security level to all information, assign a security clearance to each user, and ensure that all users only have access to that data for which they have a clearance. This may extend or replace discretionary access control for file system permissions and the concepts of users and groups. The most important feature is that the user can not fully control the access to resources that they create. The system security policy (as set by the administrator) entirely determines the access that is to be granted and a user is not permitted to grant less restrictive access to their resources than

Do-Woo Kim is with the Electronics and Telecommunication Research Institute, Daejeon, Korea (phone: 82-42-860-1351; fax: 82-42-860-5611; e-mail: dwkim@etri.re.kr).

Geon Woo Kim is with the Electronics and Telecommunication Research Institute, Daejeon, Korea (phone: 82-42-860-5427; fax: 82-42-860-5611; e-mail: kimgw@etri.re.kr).

Jun-Ho Lee is with the Electronics and Telecommunication Research Institute, Daejeon, Korea (phone: 82-42-860-1331; fax: 82-42-860-5611; e-mail: jhlee7@etri.re.kr).

Jong-Wook Han is with the Electronics and Telecommunication Research Institute, Daejeon, Korea (phone: 82-42-860-4940; fax: 82-42-860-5611; e-mail: hanjw@etri.re.kr).

the administrator specifies. Discretionary access control systems permit users to entirely determine the access granted to their resources which means that they can through accident or malice give access to unauthorized users [5].

B. RBAC

In Role-Based Access Control (RBAC), access decisions are based on an individual's roles and responsibilities within the organization or user base. The process of defining roles is usually based on analyzing the fundamental goals and structure of an organization and is usually linked to the security policy. For instance, in a medical organization, the different roles of users may include those such as doctor, nurse, attendant, nurse, patients, etc. Obviously, these members require different levels of access in order to perform their functions, but also the types of web transactions and their allowed context vary greatly depending on the security policy and any relevant regulations.

As shown in Fig. 1, a user is associated with a role, and roles are associated with permissions. A user has permission only if the user has an authorized role that is associated with that permission [3,5].

With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by people in particular jobs and assigning members of the workforce to the proper roles [4].

RBAC grants rights and permissions to roles rather than individual users. Users then acquire the rights and permissions by being assigned to appropriate roles. By grouping individuals with other individuals who have similar access rights, RBACs can provide significant security management efficiencies.

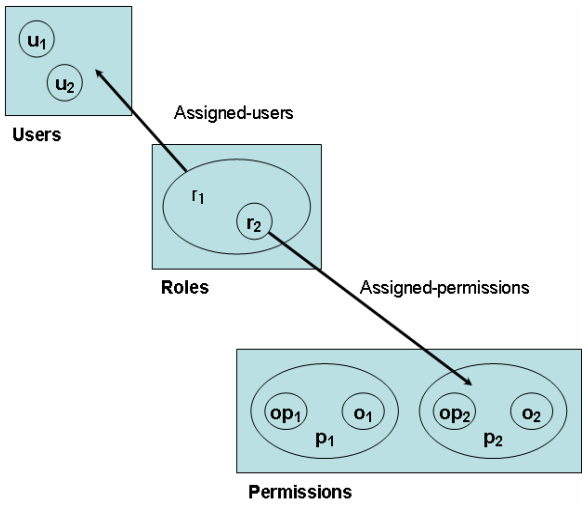


Fig. 1 User, role, permission relationships

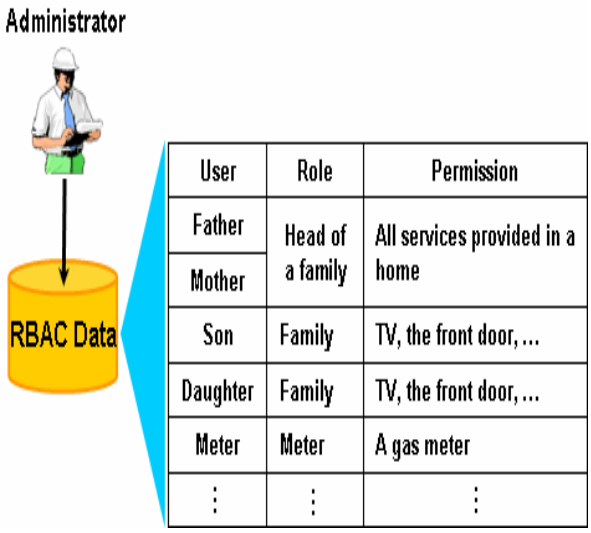
III. RBAC in Home Network Environments

To offer secure home services home network environments have need of access control for various home devices and information when users want to access. RBAC is a promising technology for managing and enforcing security in large-scale-enterprise system, we were motivated by the need to manage and enforce the strong access control technology of RBAC in home network environments [7-11]. RBAC is applied to the home network because RBAC have flexibleness to adapt easily to all access control domain. The access control domain of RBAC can be various service and resource such as information appliances, sensor.

Almost any access control model can be stated formally using notions of *users*, *objects*, *operations*, and *permissions*, and the relationships between these entities. In home network environments, the term *user* refers to people who interface with the home network system. An *object* can be any resource accessible on a home network environment, including information home appliances, home network services, information such as files, databases. An *operation* is an active process invoked by user. *Permission* is authorizations to perform some action on the object.

The term permission refers to some combination of object and operation. A particular operation used on two different objects represents two distinct permissions, and similarly, two different operations applied to a single object represent two distinct permissions.

A role is a job function within the organization that describes the authority and responsibility conferred on a user. With RBAC, A home network system administrator can create roles according to the job functions performed in a home. Therefore it can be defined a grandfather, a grandmother, a father, a mother, a son, a daughter and a meter as a user by RBAC in home network environments. Also, it can be defined the head of a family, the family, the adult, the student, the teenager and the meter as a role in the home network environments.



User	Role	Permission
Father	Head of a family	All services provided in a home
Mother		
Son	Family	TV, the front door, …
Daughter	Family	TV, the front door, …
Meter	Meter	A gas meter
⋮	⋮	⋮

Fig. 2 Definition of roles and permissions for RBAC

As shown in Fig. 2, we can assign a father and mother to the head of a family or the adult role. A son and daughter can be assigned as the family or the teenager role. Also we can assign a grandfather and grandmother to the family role.

IV. The Application of RBAC in Home Network Environments

It is also desired in some scenarios that the need of access control be enforced especially for critical devices such as the home security alarm, or the front door.

Generally an access control system based on RBAC in home network environments is embedded in a home server and a home gateway. In some case it is embedded in information home appliances, and son on. An access control system based on RBAC verifies the access right on each service provided in home network. Fig. 3 shows the control service of access right using RBAC in home network environments.

A user can be a member of many roles, and a role can have many users. Also, a role can have many permissions and the same permission can be assigned to many roles. Let us suppose that a home network administrator assigned a meter to the meter role and assigned a son to the family role. If the meter role has only the permission to the gas meter and the family role have permissions to the CD player and gas meter, a meter can access the gas meter but cannot access the CD player. But a son can access both the CD player and gas meter.

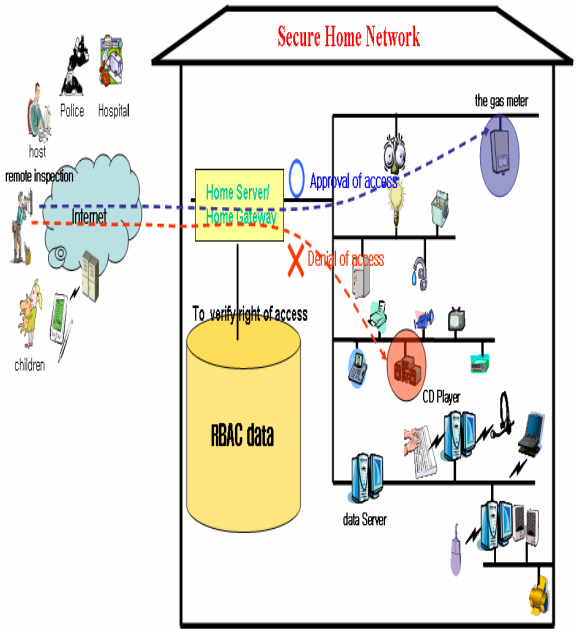


Fig. 3 The control service of access right using RBAC in home network

V. Conclusion

The home computing environment is evolving into a home network of multiple devices, which will also need to be secured. The security of the home environment means that all unauthorized access to various devices and systems is denied and the data is well protected.

To offer secure home services we have presented the access control model using RABC in home network environments. We are developing a access control system suitable for home network environments. And we will make a research into secureing home network environments such as authentication, authorization and confidentiality.

References

[1] Carl M. Ellison, *Home Network Security*, Intel Technology Journal, 2002.
[2] Guoyou He, *Requirements for Security in Home Environments*, Residential and Virtual Home Environments Seminar on Internetworking, Spring 2002.
[3] David F. Ferraiolo, R.S. Sandhu, Serban Gavrila, D.Richard Kuhn and Ramaswamy Chandramouli, *Proposed NIST Standard for Role-Based Access Contro*", ACM Transactions on Information and Systems Security (TISSEC), Volume 4, Number 3, August 2001.
[4] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, *Role based access control model*", IEEE Computer, 29 February 1996.
[5] David F. Ferraiolo, D Richard Kuhn, *Role-Based Access Control*, Artech House Inc, 2003
[6] Matthew J. Brodeur, *Security Concerns In Home Automation Technologies*, 2001.
[7] David Ferraiolo and Richard Kuhn. *Role-based access control*, In 15th NIST-NCSC National Computer Security Conference, pages 554-563, Baltimore, MD, October 13-16 1992.
[8] Kim Thomas, *Building a Secure Home Network*, SANS Institute, 2001
[9] Stallings William, *Network Security Essentials: Applications and Standards*, Prentice Hall, 2000.
[10] Gerard O'Driscoll, *Essential Guide to Home Networking Technologies*, Prentice Hall, 2000.
[11] http://www.iec.org/online/tutorials/home_net/