Providing Security in Granting Agency Using Workflow CRBAC Model

Marzieh Bahrami[†], Mohammad Reza Khayyambashi[††], and Seyed Ali Razavi Ebrahimi[†††]

[†] MS.C student computer, Payam Noor University, Tehran, Iran
[††] Department of Computer, Faculty of Engineering, University of Isfahan, Isfahan, Iran
[†††] Assistant Professor, Payam Noor University(PNU), Tehran, Iran

Summary
There have been many security solutions to secure representation in the work flow used in business processes and Grid Networks. Most of these solutions try to provide maximum security in workflow processes and most of them are used Role-Based Access Control model (RBAC). Capability Role-Base Access Control (CRBAC) is one of the models that are used to model RBAC which in this paper, we introduce these models and our proposed solution. Central idea of the model and the solution is secure Transfer ability of one user to other users within a safe and secure workflow.

Key words:
Capability, Delegation, Security, Workflow.

1. Introduction

Workflow systems are used to control the execution of business processes. In fact, a workflow system saves Features of a workflow and designs a series of tasks to provide a specific implementation. Workflow management systems (WFMS) commonly used by organizations to automate and verify their business processes. Success of a workflow depends on a secure implementation; So WFMS is responsible for security maintaining. Security in business processes is considered as a major issue and many research activities have been in this field. Naturally, a WFMS is a network-based application. In a WFMS, participate in various that can communicate with the workflow activities through one network system. This issue is needed to communication security. Processes should be changed in workflow networks, so it is required a WFMS based security network to implement security processes such as authentication, confidentiality, data integrity and non-repudiation [1]. Confidentiality includes Privacy against unauthorized disclosures of information such as workflow processes or external data. Thus, a WFMS usually should have an accessible mechanism to validate users. Access control is one of important technologies that should make it possible the data in the system can be accessed only by authorized users with valid roles. Although there are standards for security and access control services in distributed systems but still there is the lack of a comprehensive approach in access control services, especially job flows. In recent years, many attempts have been made to establish security in workflow systems. There are a variety of security models to create a flexible access control system to support workflow in business processes colleague. An access control model for workflow system architecture is workflow access control model based on service-oriented workflow access control (SOWAC) [2]. This model is based on SO architecture.
SOA provides the following:

- Services by reduce the complexity of service
- Service interfaces, able to function within the system architecture and the use of open standards
- Services support a weak coupling model that clients can be connected at runtime to Terminal servers

Compared to traditional systems, SOA is a distributed and dynamic environment, so to provide appropriate access control; access control model based on service-oriented (SOWAC) is proposed. In this model, the service access control is being licensed based on the work of replacing the unit, In fact, is described as a summary of a business service in the workflow. In state of workflow, logic business provides all their need to do and complete. In fact, these logic services can connect a variety of resources using other services to a workflow.
In SOWAC, access control of workflow is divided into two stages:
• Management
• implement or evaluate
Management Stage is included Security rules and policies, update and delete rules, use the security services and licensing policies. Stage implement evaluates Application access requirements of service providers, with security policies defined by the management Stage.
Implement Stage is divided into two parts:
The first part consists of licensing and the authenticity and consistency of privileges defined in the workflow model and The second part consists of evaluating access requests using security policies to be used when the need for services. Most of today's models for workflow access

Manuscript received November 5, 2013
Manuscript revised November 20, 2013

control model are based on RBAC [3]. An example of this model is shown in [4]. Another model uses RBAC access control model, the model is CRBAC. In fact CRBAC is developed of RBAC96 model [5]. One of the models for secure access control in workflow is Chinese wall security model (CWSM) that reduces the contradictions and inconsistencies in business organizations and it is appropriate for large-scale applications [3]. Model CWSM has been to establish controls to prevent conflicts and contradictions (COI) in business organizations. In this model data objects are owned by the companies. Access to data and information on this model depends on the rules of reading, writing, or reading – writing. The information of each company is divided into classes of COI. If the information belongs to the one class of COI, The information cannot be used in the classroom; conversely, the information cannot be applied to other classes. CWSM have set of rules to avoid conflicts and to read as follows:
• read rule: s can read o only if o is of the same company.
• Writing rule: s can write o only if s read o by reading rule and another object of the other companies could not read it.
In general, the following is done in a CWSM:

- Dynamic binding between objects and companies
- Dynamic Data Manipulation
- Privileged object management
- Run on Time

Generally implement a CWSM depends on the dynamic behavior of the workflow process.

2. CRBAC model

CRBAC is a mechanism of role-based access control that obtained from the RBAC and RBAC96. In this model, users use their roles and their ability to access objects and system components. In general, the ability is a unchangeable sign that contains An object and a list of authorized actions That can be imposed on the system and the corresponding object. In this model, the ability of a valid license to access a specific object are allowed between actions that This ability can be viewed as representing the user contingent and will be transferred to another user or users. So delegation will be realized by transferring the roles and capabilities.
Delegation will be awarding by two ways:
• Licensing agency representing the work done in each part of the workflow
• licensing to the representative of the state agency
In CRBAC model, agencies can be postponed by users without the interference of heads. CRBAC is an extension of RBAC96 model which obtained with community access control base mechanism that is able to model RBAC96.
In this model there are the following components:
• A set of Capabilities
• A set of tasks
• A mapping to identify its own strengths and abilities and assign roles and duties to others.
In this model, a set of domain is considered and users use of network and resource in the field and the domain. . In this model, the ability are resulted of and current roles and previous capabilities. What is important in workflow systems, is limiting their scope to the Capabilities. Overall CRBAC is shown in Fig 1.

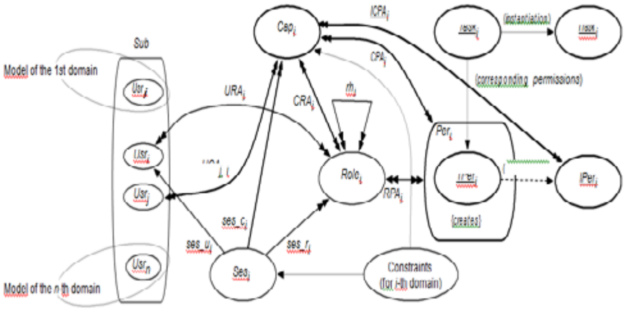

Fig1. View CRBAC

In this figure, there are the following basic components:
-Dom and sub, respectively represent the domain (domains), and a subset of the objects
- Roli– and Peri and Sesi and Capi respectively represent the set of roles, powers, and abilities meetings in my domain i for each Dom∈i
In addition to the above components, functions and relations are in the model:
- User: Dom→2 sub: Dom a function that i has a set of users in a domain can be specified for each Dom∈i
- Ses_ui: sesi→usri: a function mapping each session of the user in my domain i
- Ses_ri: sesi×2 Roli: a function mapping each session of the domain i into a set of roles that will be activated this session
- Cpa i ⊂cap i ×per i : An ability to communicate, even though the assignment of authority
In addition to the above functions, there are the terms and conditions:
- ses_ri⊂ {r| (ses_ui(s), r) ∈usri}: The active role of a session be attributed the user does it
S meeting have the following options:
- r∈ses, rj(s) {p|(r,p)∈peri}
- Ses_c i ⊂ {c| (ses_u i (s), c) ∈usr i }: Means that each activated own user ability with a session that does this session.
In addition, this model includes the following for workflow:

Workflow features: A feature of workflow w is a series of short works (taski) that taski= {t1…tm} is A collection of things Dom∈i

Sample workflow: An instance of workflow w, that w= (taski) is a sequence of pairs of objects such as {(t1, u1)…(tm, um)} so that Taski= {t1…tm}, {u1…um} ⊂sub

The grant process is represented as a sequence of three basic procedures is the following:

First

Create: a user creates a new ability.

Second

Assignment: a user, an assignment will have the ability.

Third

Transfer: Move the user the ability to send and assigned to another user.

Given the above definitions and the procedure, some rules is obtained that should be applied in the model.

The rules are as follows:

Creation rule: If user u, has be the role r or capability c, then he can create new ability of ci

Assignment rule: If user u has the role r with capability c, then can assign Authority of p to the ability of ci.

Transfer rule: New capabilities of ci in a specific area can be transferred of user u to another user ui.

3. Simulation and results

In the proposed solution, the Grid environment is simulated using the simulation software Grasim Then users with certain conditions have been enter in the environment and are examined with different way and methods of user access to resources. In addition, each user is given privileges and powers and According to our terms powers and abilities that can be transferred to another without having to compromise system security. It is used in all stages of a workflow that Users are logged in the workflow and use the resources and delegate or receive privileges and powers delegated to another or from one another Using CRBAC. In addition the security of the grid environment must be protected under the work flow. Overall, our proposed solution is based on the algorithm shown in Fig 2.

In this way, the Grady network with three users and resources R1, R2, R3 Grasim environment is created And each user is assigned a role and ability. Each user can then enter a workflow that The validity of them , is examined with the use of a central authentication system .It will be reviewed by the workflow After the security check if the user was safe then is entered into system and The Grid resources can be accessed either directly or indirectly. In direct access, users can use Grid environment and resources without interference workflow and Grid and resource security is achieved by the workflow. Three users U1 and U2 and U3 with capabilities and Cap3 Cap1 and Cap2 are entered Grid network. Here are the rules to create; transfer and assignment models used CRBAC. It is assumed that there are users with their own abilities and the creation of rule is not necessary.

To evaluate the proposed solution, we consider two cases, and we have evaluated. In the first case, no threat apply to the system and the system will continue to operate as normal And any attack threaten the system. In the latter case, the signal is entered into the system as a threat and Run times of assignments are obtained according to the Fig3.

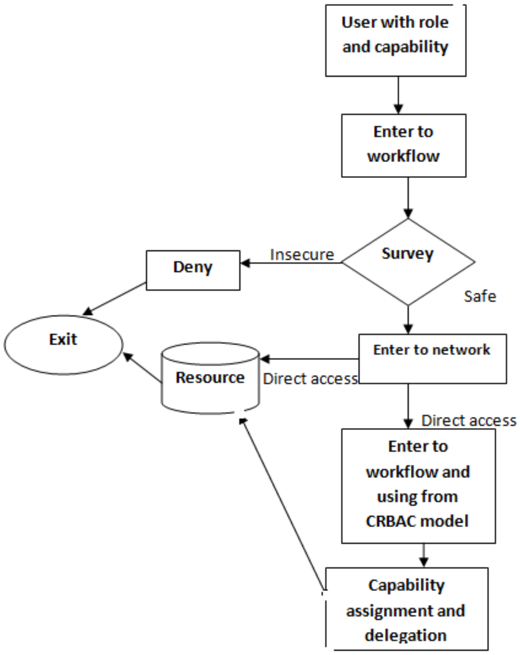
User with role and capability
Enter to workflow
Survey
Insecure
Safe
Deny
Exit
Enter to network
Resource
Direct access
Direct access
Enter to workflow and using from CRBAC model
Capability assignment and delegation

Fig2. Outline of proposed solution

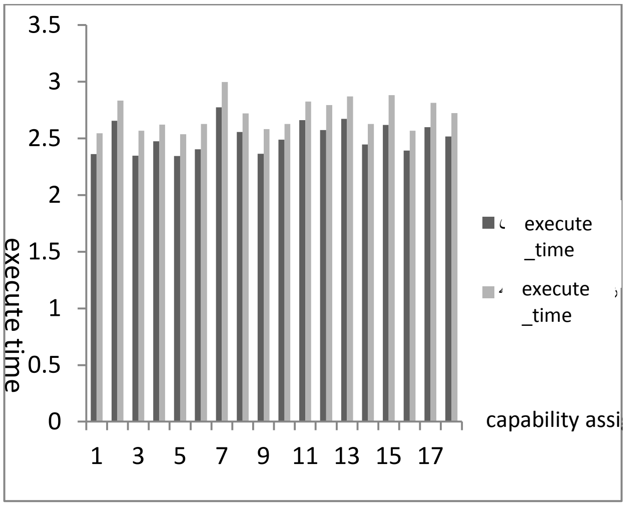

Fig3.result of proposed solution

To evaluate the performance of the security, three factors are considered and compared and analyzed for both cases. These three factors are:

- Runtime
- Cost
- Attack time

These three factors, in fact, play a major role in the process of evaluating and comparing and Based on these parameters in both phases of the scenarios can be compared and payments. Run time measured in seconds, time has shown millions of instructions per second, Running costs is obtained based on costs that are incurred each source. Effective time of the attack is the amount of time that the system suffered damage to the circumstances of the attack. In The obtained graph can be seen that when the change is small and insignificant; It is the resistance of the system against attacks. In fact, the running time of the attack has been little change the run-time before the attack. And can thus be deduced when the system is modeled using Assignment capabilities CRBAC, in the form and context of a workflow acts properly against possible threats of attacks.

4. Conclusions

With achieved results can be seen that Attacks against the system, affect system performance, and slow the system even when the system is disabled. What is important in system, first, to prevent attackers from entering the system and the second is to minimize the effects of the attack. In the proposed method, the system attempts to prevent attacks using relevant workflows and are also seen a user can even transfer it to another (delegation). As can be observed during the follow-up workflow, changes are much less after the attack. One advantage of using this workflow in Grid networks is security.

References

[1] Yu-Cheng Hsiao, Gwen-Hwan," implementing the Chinese Wall Security Model in Workflow Management Systems", 2010

[2] Yonghe Wei, Xiangtan Li," Oriented-Service Workflow Access Control Architecture", 2010

[3] R. Sandhog, E. Coyne, H. Feinstein, and C. Yeoman." Role- Based Access Control Models", IEEE Computer, vol.29, no.2, Pp.38-47, 1996.

[4] S. Kendal and R. Sandhogs. "Secure Role-Based Workflow Models", Database Security XV: Status and Prospects, pp.45- 58, 2002.

[5] K.Hasebe, M.Mabuchi, A.Matsushita, "Capability Based Delegation Model in RBAC"

[6] G.Jaspher Willkie Kathrine, Benson Edwin Raj, .Kirubakaran,"A Novel Security Framework for Computational Grid", 2011

[7] AstroGrid,"Virtual Observatory Software for Astronomers", vol.2009, 2009

[8] A.R-williams, s.sufi,"avern workflow Management System", July 2011

[9] Goodhue Liu,"Using Security Proxy based Trusted Computing Enhanced Grid Security Infrastructure", 2010

[10] I. Foster and C.Kesselman,"the grid blueprint for a new Computing infrastructure" 2nded.sanfransisco: Morgan Kaufmann, 2004

[11] Ian Foster," What is the Grid? A Three Point Checklist", 2002.

[12] "Grid computing security (A taxonomy)", published by the Computer Society, 2007

[13] Vserver,http://linux-vserver.org/documentation,accessed on 13th July, 2006.

[14] Yonghe Wei, Xingshan Li," Oriented-Service Workflow Access Control Architecture", 2010

[15] Xie Rui,"Grid Security Research Based on Middleware", 2010

[16] Victor Jose, M; Seenivasagam, V, "objects based grid Architecture for enhancing security in grid computing", September 2011, 414-417

[17] Jabri, M.A, Matsuoka, S, "Dealing with Grid-Computing Authorization Using Identity-Based Certificate less Proxy Signature", July 2011

[18] AstroGrid,"Virtual Observatory Software for astronomers", vol.2009, 2009

[19] http://forum.p30parsi.com/showthread.php,visited date: 5/16/2012

[20] "Workflow Management Coalition (WFMC), Workflow Management" Coalition: Terminology & Glossary Document Number WFMC-TC1011, 1999.

[21] Koji Hasebe and Mitsuhiro Mabuchi," Capability Role-Based Delegation in Workflow Systems", 2010

[22] Yu-Cheng Hsiao, Gwan-Hwan," implementing the Chinese Wall Security Model in Workflow Management Systems", 2010

[23] Yonghe Wei, Xingshan Li," Oriented-Service Workflow Access Control Architecture", 2010

[24] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman." Role-Based Access Control Models", IEEE Computer, vol.29, no.2, pp.38-47, 1996.

[25] K.Hasebe, M.Mabuchi, A.Matsushita, "Capability-Based Delegation Model in RBAC", pp, 109-118, 2010

[26] J. Crampton and H. Khambhammettu. "Delegation and Sat-Isfiability in Workflow Systems", Proceedings of the 13th ACM Symposium on Access Control Models and Technologies (SACMAT'08), pp.31-40, 2008.

[27] J.Crampton and H.Khambhammettu."On Delegation and Workflow Execution Models", Pp.2337-2144, 2008.

[28] K. Hasebe, M. Mabuchi, and A. Matsushita. "Capability-Based Delegation Model in RBAC", Proceedings of the 15th ACM Symposium on Access Control Models and Technologies (SACMAT'10), pp.109-118, 2010.

[29] J. Wainer, A. Kumar, and P. Barthelmess." DW-RBAC: A For- mal security model of Delegation and revocation in Workflow systems", Information Systems, vol.32, pp.365-384, 2007.

[30] Yu-Cheng Hsiao, Gwan-Hwan," implementing the Chinese Wall Security Model in Workflow Management Systems", 2010

[31] Koji Hasebe and Mitsuhiro Mabuchi,” Capability Role-Based Delegation in workflow Systems”, 2010

[32] Jabri, M.A, Matsuoka, S, “Dealing with Grid-Computing Authorization Using Identity Based Certificate less Proxy Signature”, July 2011

[33] G.Neiger, A.Santani, F.leung, D.Rodgers and R.Uhlig,”Intel Virtualization Technology: Hardware Support for efficient Processor virtualization”, 2011

[34] Massoud Amin, “Guaranteeing the Security of an Increasingly stressed grid”, 2011

Marzieh Bahrami MS.C student computer, Payam Noor University, Tehran, Iran. Received the B.S. and degrees in computer engineering from payam noor university of Isfahan-iran in 2004. During 2004-2009, she has worked in Institute for Higher Education of najaf abad,isfahan,iran. Her interest clude: Service Oriented Architecture, Semantic Web, Information Security, Empirical Research in Software

Mohammad-Reza Khayyambashi was born in Isfahan, Iran in 1961. He received the B.Sc. degree in Computer Hardware Engineering from Tehran University, Tehran, Iran in 1987. He received his M.Sc. in Computer Architecture from Sharif University of Technology (SUT), Tehran, Iran in 1990. He got his Ph.D. in Computer Engineering, Distributed Systems from University of Newcastle upon Tyne; Newcastle upon Tyne, England in 2006. He is now working as a lecturer at the Department of Computer, Faculty of Engineering, University of Isfahan, Isfahan, Iran. His research interests include Distributed Systems, Networking, Web Services, Fault Tolerance and E-Commerce.

`Seyed Ali Razavi Ebrahimi Born in Bam, Iran, received his BS in Electronic Engineering from Tehran University and MSc degree in System Control Engineering from Sharif University, Iran. He received his PhD degree in Computer Graphics from Ecole des Mines de Nantes (EMN), France in 1997 and currently is assistant professor at Payam Noor University (PNU), Tehran, Iran. His research interests include software engineering, intelligent interaction, CG. and distributed systems