Meta-heuristics Based Multi-Layer Access Control Technique (MBMAC)

Oluwafemi S. Ogunseye, Julius O. Okesola
Tai Solarin University of Education, Ijebu-Ode, Ogun State, Nigeria

ABSTRACT. Access control is a major preventive measure for sensitive resources. Most access control techniques have been found to be inadequate in providing sufficient security to KMS which houses the sources of competitive advantage for many organizations today. However, current research showed that combining access control techniques can help provide better security. In this work a meta-heuristic strategy for access control technique combination that is both more effective than previous methods of combination but also more resource friendly is presented. The new method applies access control technique with human reasoning in a multilayer architecture ensuring that malicious users are prevented access and the misuse or abuse of privileges common to other methods is stemmed.
KEYWORDS: Access Control, Metaheuristics, Knowledge Management Systems, Security

Introduction

Knowledge Management was initially defined as the process of applying a systematic approach to the capture, structure, management, and dissemination of knowledge throughout an organization in order to work faster, reuse best practices and reduce costly rework from project to project ([NT95], [PV98], [PS99], [RH99]). Many documents tend to be warehoused, sophisticated search engines are then used to try to retrieve some of these contents, and fairly large-scale and costly KM systems are built. Knowledge Management has proven to be most successful in the capture, storage, and subsequent dissemination of knowledge that has been rendered explicit-particularly lessons learned and best practices. Knowledge

Management (KM) entails the capturing of knowledge from past decision making for application to current decision making with the express purpose of improving organizational performance ([Jen05]) and has been recognized as a critical management strategy in generating competitive advantage for the organization ([Gra96]). Knowledge has become increasingly more valuable than the more traditional physical or tangible assets.

KM's importance has increased in intensity because of the Globalization of businesses which has encouraged multicultural, multilingual and multisite companies. A second reason for this increased intensity is the speed of today's business world, people have to do more and do it faster to keep up, this forces down the time to learn and has put more pressure on KM. Organizations now realize that labour can be very mobile and a need to preserve the knowledge of good labour for continued performance is essential. And lastly the advances in technology have encouraged dependence on IT for solution to many business problems.

These needs have propelled the wide spread adoption of KM and major development of KMS in organizations of the world. This rise in online knowledge is gradually increasing the likelihood of KM unauthorized access and abuse by both employees and outsiders. Anything of value must be protected and since knowledge is fast becoming one of the most valued asset and a major source of competitive edge within an enterprise, its security is essential. Since knowledge is not needed by everyone, Knowledge management activities should be carried out in such a way that the right knowledge becomes available to only the right person at only the right time. This is a task that can be tackled by a sufficiently adequate Access Control Technique.

1. State of the art & related work

Access control is usually the frontline defense for KMSs. They are sometimes categorized as discretionary or non-discretionary. The three most widely recognized models are Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC). MAC and RBAC are both non-discretionary. The focus will be on Non-discretionary access control techniques for this work looking at current and widely used access control methods and their downsides. Some of these are:

- Role-based access control (RBAC) models are receiving increasing attention as a generalized approach to access control [Atl99], [Osb00], [San95], [San97], [San98a]. In an RBAC model, roles represent functions within a given organization. Authorizations are then granted to roles, rather than single users. The authorizations granted to a role are strictly related to the data objects and resources that are needed for exercising the functions associated with the role. Because of its relevance, RBAC has been widely investigated [Atl99], [Osb00], [San95], [San97], [San98a]. However, even though RBAC has reached a good maturity level, there are still significant application requirements not addressed by current RBAC models. One such requirement is related to the roles' temporal dimension. In many organizations, functions may have limited or periodic temporal duration such as part-time or temporary functions. To cope with these requirements, [BBF01] proposed Temporal-RBAC (TRBAC), an extension of RBAC models that supports temporal constraints on the enabling/disabling of roles. TRBAC supports periodic role enabling and disabling, and temporal dependencies among such actions. As organizations merge, globalize or grow, managing roles become cumbersome creating loopholes for security breaches and misuse. Role engineering is a major problem. It is however still the most used and most secure Access control technique, the major downside is its susceptibility to abuse of privileges.
- Lattice-based access control models were described in [McC00] and [PP03]. In Lattice-based models, subjects and objects are assigned security labels from a partially ordered universe, which is a lattice. Nowadays, lattice-based access control is not widely used because the practical implementation is difficult as the size of the security lattice increases (OKE09].
- Perimeter-Based access Control was proposed by Scott-Chapman ([Sco06]), in his thesis he modeled a perimeter based community-centric, access control system that makes use of an access control tree to represent privileges. The tree is rendered in such a way that the location based relationships of the objects in their respective security perimeters are preserved. Objects are represented by nodes and access operations are represented by branches. The access control tree is able to dynamically determine capability by consolidating security information from external data sources,

software agents, and location based sensors. The strategies he described focused on physical access control.

- Two Level Access Control was proposed by Menzel ([MWM07]), the idea is a Two Level Access Control (2LAC) architecture for cross organizational federated service composition independent from local access control models. The aim is to prevent information leakage but focuses on composite web service frameworks categorizing existing SOA security frameworks and their capabilities to support cross-organizational federated composite services. It does not really focus on strengthening the core information server as against the ability to securely share information in distributed environments.
- Component-Based Access Control by Sodiya and Onashoga in 2009 suggested an access control scheme that adopts the techniques of Role-Based Access Control (RBAC), Purpose-Based Access Control (PBAC), Time-Based Access Control (TBAC) and History-Based Access Control (HBAC) as components to form an integrated Components-based Access Control Architecture (CACA). This combination of access control techniques provided a very impressive level of security. This technique though strong is inadequate for a KMS because the components do not provide a sufficiently accurate judge of access rights and ends up putting up many false positives denying access to legitimate users of the system. Take a case where a legitimate user urgently needs a knowledge resource at an odd time (relative) and that resource has not been accessed before. It implies that he scores zero (0) in both instances. His total score using Sodiya and Onosoga's formula is therefore 1/3 which denies him access to the resource. The model is not suitable for a global KMS where users are dispersed across varied locations and time. The system also scores zero to users requesting knowledge that has never been accessed. Since knowledge is generated regularly, it implies that even old users accessing knowledge that was just uploaded by another user or administrator gets penalized and could even be denied access. The method is also resource intensive as the user must be tested on all the components before access is granted or denied. The system is not intelligent.

  The real strength of the system was considered to be its use of more than one access control technique and its weakness as the strategy used in combination.

2. The proposed model

From the CACA, we see the strength in combination of access control techniques; we see that proper combination of access control techniques can provide a synergy of strength for access control techniques. However the combination strategy was considered as the cause of the unsuitability of the model for use in KMS. A proper synergy of access control techniques cannot be achieved by a scoring system as used in Sodiya & Onasoga ([SO09]), as this method is too rigid. The application of heuristics is proposed to suitably combine different technique in ways that will save resources and also be more effective.

2.1. Design method

The Access control technique will comprise of layers of other access control techniques working together to ensure competence.

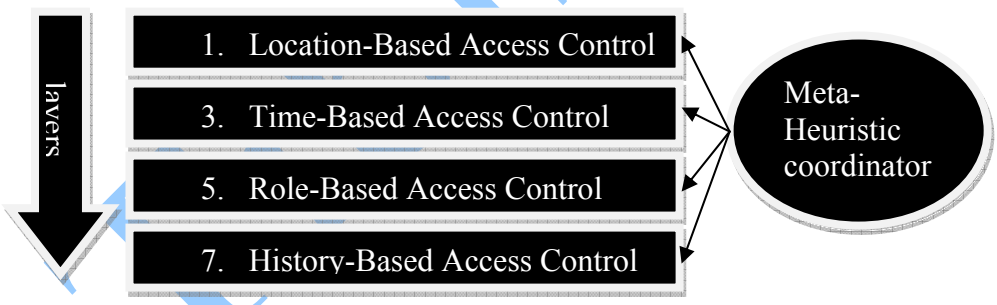

Figure 1. The Meta-heuristic coordination process for the KMS

When a user attempts to access the KMS, the first step is to determine their location. Depending how sensitive the system is, if the request is from an outsider and it is against security policy then the access is denied at that layer without having to use more computational resources.
However there are several way malicious users use to beat such access control technique, like masquerading.

In event the user scales through the first layer, they are immediately probed on the second layer. For the second layer the metaheuristics coordination engine test time based on two factors:
i. Subject-Based Restriction (SBR):- This states that a subject must request an object at a particular period of time. It is represented as
Ai: (t1..t11) --- for single period definition
and Ai: (t1..t11, t2..t22… tn..tnn) --- for multiple periods definition
where (t1..t11, t2..t22… tn..tnn) represents periods
ii. Object-Based Restriction (OBR):- This states that a particular operation must be performed on an object at a particular period. It is represented as
Oi: (t1..t11) --- for single period definition
and Oi: (t1..t11, t2..t22… tn..tnn) --- for multiple periods definition

The period adapts to locale time differences in zones by using the user's location in a distributed KMS.

When the timing is wrong, access is denied but if right the next layer is employed, RBAC helps define what resources the user can access and privileges they might have as assigned by the system administrator. This is what is mostly used by systems for access control, its main demerit is the abuse of privileges where authorized user can perform privileged actions at wrong times and locations to the detriment of the organization.

In event the user is allowed to access the resource then the usage history of the resource comes into question. This last layer is not designed to debar the user directly but immediately flags the site officer/ system administrator if the resource had not been used before or the frequency is low and a user is the first to request it after a long while of existence.

2.1.1. High Points & Possible Low Points of the model

High Point: Through the layers, a synergy is formed among the access control methods. The weaknesses of individual methods/layers are covered by the subsequent layers/methods. The layers therefore stand-in for the security loop-holes of the previous ones. The system reduces resource usage by only employing a layer when it is needed.

Low Point: The model would theoretically tend to delay legitimate users through the multilayer processing. This would however not be obvious in today's mostly high capacity computers. This is therefore not expected to be an issue with current and continuous advancement in computer hardware technology especially the areas of processing power and memory.

3. Model testing

A prototype KMS was with this model of access for a client Audit firm to manage knowledge over its various audit challenges. Presentation Layer was basic MXML, on an Adobe Air environment, designed with Flex. The Logic Layer was with PHP and the Data layer was with Oracle 11g.

The Access Control module was however made to be a consumed as a service i.e. it was enveloped in its own class library and the methods exposed through web services.

By consuming the access control techniques as a service we are able to choose which access control method to employ per time just for the sake of testing. Hence, the CACA, RBAC and MBMAC where options for our application and we could choose the access control method t employ.

We carried out a usability test on the system after allowing it to run for three months with the Audit firm while other phases of deployment and customization were going on. The results confirm that MBMAC effectively controlled 98.2% of Access control issues on KMS, and all the loopholes created by RBAC and CACA where addressed. The system outperformed the CACA and RBAC and with a little fine-tuning of our model, we should accomplish 100%.

The system was also very easy to use as the access control MBMAC was abstracted, The user does not know the method off access control being employed as the interfaces where similar to the ones they are use to.

Conclusion

The security of knowledge resources is paramount for any wise organization. Adopting the right access control technique can go a long way in saving KM stakeholders a lot of stress and provide a high degree of security against malicious users regardless of whether they are internal or external to the organization. RBAC is one of the most prominent access control methods applied in systems today. This work and other previous work show its downside and shortcomings. The CACA model showed the advantage of combining access control techniques to cover for the shortcomings of individual access control techniques and form a stronger access control technique altogether. CACA's success is however short-

circuited by the blind side of its methodology-a scoring system. In this work, Instead of the rigid scoring system of CACA we apply a human based thinking and problem solving algorithm-heuristics, to combine the access control techniques. The result is a better Access control model that is more resource friendly and accurate than the CACA model providing the strengths of the CACA without the weaknesses of the CACA.

References

[Atl99] **V. Atluri (ED.)** - *Proceedings of the Fourth ACM Workshop on Role-Based Access Control* (Fairfax, Va.). 1999

[BBF00] **E. Bertino, P. A. Bonatti, E. Ferrari -** TRBAC: *A Temporal Role-based Access Control Model*. Proc. of the 5th ACM RBAC Workshop, July 26-28, 2000, Berlin.

[Gra96] **Grant** - *Future of KM available online at* http://www.igiglobal.com/files/prefaces/IJKM%20preface%203(1).pdf 1996

[Jen05] **E. Jennex Murray** - *Internet Support for Knowledge Management Systems.* Encyclopedia of Information Science and Technology (III) 1640-1644 2005

[McC00] **A. McCue** - *LloydsTSB to offer smartcard security.* Retrieved from http://www.vnunet.com/vnunet/news/2118641/lloydstsb-offer-smartcard-security 2000

[MWM07] **M. Menzel, C. Wolter, C. Meinel** - *Access control for cross-organisational web service.* Journal of Information Assurance and Security, 2. 2007

[NT95] **Ikujiro Nonaka, Hirotaka Takeuchi** - *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation* by Oxford University Press, 1995

[OKE09] **S. Obedkov, D. G. Kourie, J. H. P. Eloff -** *Building access control models with attribute exploration*. Elsevier Journal of Computers and Security, 28, 2-7. 2009

[Osb00] **S. Osborn (ED.) -** *Proceedings of the Fifth ACM Workshop on Role-Based Access Control*(Berlin). 2000

[OSM00] **S. Osborn, R. Sandhu, Q. Munawer -** *Configuring role-based access control to enforce mandatory and discretionary access control policies*. ACM Trans. Inf. Syst. Sec. 3, 2, 85–106. 2000

[PP03] **P. Pfleeger, S. T. Pfleeger -** *Security in computing*. Prentice Hall. 2003

[PS99] **J. Pfeffer, R. I. Sutton -** *Knowing 'What' to do is not enough: turning knowledge into action*, Carlifonia Management Review 1999.

[PV98] **B. Pasternack, A. Visco -** *The centerless corporation*, Simon and Schuster, New York. 1998

[RH99] **R. Ruggles, D. Holtshouse -** *The Knowledge Advantage*. NH-US Capstone US 1999

[San91] **R. Sandhu -** *Separation of duties in computerized information systems. In DatabaseSecurity IV*: *Status and Prospects*, North Holland, Amsterdam, the Netherlands, 179–189. *1991*

[San95] **R. Sandhu (ED.) -** *Proceedings of the First ACM Workshop on Role-Based Access Control* (Fairfax, Va.). *1995*

[San96] **R. Sandhu -** *Role hierarchies and constraints for lattice-based access controls*. In *Computer 1996 Security—Esorics '96* (Rome), E. Bertino, H. Kurth, G. Martella, and E. Montolivo, Eds., LectureNotes in Computer Science, vol. 1146, Springer-Verlag, New York.

[San97] **R. Sandhu (ED.) -**.*Proceedings of the Second ACM Workshop on Role-Based Access Control* (Fairfax, Va.). 1997

[San98a] **R. Sandhu (ED.) -** *Proceedings of the Third ACM Workshop on Role-Based Access Control* (Fairfax, Va.). 1998a

[San98b] **R. Sandhu -** *Role-based access control*. Advances in Computers, *46*, Academic Press.

[Sco06] **A. Scott-Chapman -** *A dynamic, perimeter based, community-centric access control system*. Msc. Thesis, Florida State University.2006

[SO09] **A. S. Sodiya, S. A. Onashoga -** *Components-based Access Control Architecture*, Journal of Issues in Informing Science and Information Technology, USA, Vol. 6, 2009, pp 53-61.