Information Assurance through Access Control Policies: A Comprehensive Study

[1]R.GnanaJeyaraman Dr. D. Gunaseelan[2], P.K. Kumaresan[3]
[1]*Asso. professor, Department of computer Science and Engineering, SBM College of Engineering & Technology, Dindigul, Tamilnadu, India*
[2]*Professor, College of Computer Science, JAZAN University, JAZAN, Kingdom of Saudi Arabia,*
[3] *Professor, Department of Information Technology, VMKV Engineering College, Vinayaka Missions Univerisity, Periyaseeragapadi, Salem, India*

***Abstract*—** *The real essence of information sharing is to let the correct information timely reach the appropriate receiver, at the right place and in an understandable format. The objective of this paper is to study about the different Access control policies that have been proposed so far for the static and dynamic environment to ensure secured information sharing.*
Keywords *Access control, Access control policies, tacp, Information sharing*

Introduction

Information assurance is the process of ensuring that the right people get the right information at the right time. It includes information security, managing relevance, integrity, accuracy, authentication, confidentiality and non-repudiation. Information sharing is a fundamental component of a successful security program. In today's information technology, authorization is concerned with the ways in which users can access resources in the computer system, or informally speaking, with "who can do what."

II ACCESS CONTROL MECHANISMS

Access control:
Access control is the fundamental security mechanism in use today. Access control shows up in virtually all systems and imposes great architectural and administrative challenges at all levels of enterprise computing. Access control refers to any method or mechanism by which the access of principals to resources is regulated.

Access control Matrices:
Access control can be simply implemented through a access control matrix which specifies which principal can do what actions to which objects. But this approach suits only for isolated or small-scale IT systems and works poor for distributed, federated, large scale or complex systems.

Access Control Policies:
It is more standard tool for specifying and deciding access requests. Policies should capture the intended behavior of an access-control system. Policy analysis has to be done for conflict detection, gap detection, safety problem and refinement. The policies are expressed in policy languages and the methods for policy analysis depend on the concrete representation of the policies.

A. RBAC:
Discretionary access control (DAC) restricts access to objects based on the identity of the subject and/or groups to which they belong. Role-based access control (RBAC)[2], a realization of DAC, regulates a user's access to certain resources based on a *user role*. A user role is a collection of permissions the user needs to accomplish that role. A user may have multiple roles, with each role having a set of permissions. By controlling access using roles and permissions, a security policy can be realized that limits access to the need-to-know information/resources. Using RBAC raises some difficult issues when dealing with coalitions such as: who creates the roles? Who determines permissions (access)? Who assigns users to roles? Are there constraints placed on users within those roles? There are different RBAC approaches that allow for fine-grained role definition.

B. ABAC:
Attribute-based access control [12] defines a new access control paradigm in which the access rights are granted to the users through the use of policies combined with attributes. The policies can use any type of attributes (user attributes, resource attribute, etc...). Attributes are like static values and they enable relation-based access control. XACML, the eXtensible Access Control Markup Language is a standard that implements attribute-based and policy-based access control.

C. RISK-AWARE ROLE-BASED ACCESS CONTROL:
Liang Chen and Jason Crampton [11] propose risk-aware access control and the core goal is to provide a mechanism that can manage the trade-off between the risks of allowing an unauthorized access with the cost of denying access when the inability to access resources may have profound consequences. When a user makes a request to access some resources, a risk-aware access control mechanism will evaluate the request by estimating the expected costs and benefits of granting access: the request might be denied if the

risk is above some system-defined threshold; alternatively, the request might be denied if the cost exceeds the expected benefit.

D. RBAC-A:

D. Richard Kuhn et al., [14]propose a model which combines the best features of Role Based Control (RBAC) with Attribute Based Access control (ABAC) to design a simple and flexible model. RBAC controls all access through roles assigned to users. Each role assigns a collection of permissions to users. Roles are structured hierarchically and some roles inherit permissions for others. Once roles are structured, the users are assigned roles as authorized by the management. RBAC requires the domain to be single administrated or slowly changing across multiple domains. To extend RBAC for dynamically changing domain, ABAC model which is flexible but lack RBAC's clarity can be merged with RBAC. This approach might be more flexible than RBAC because it does not require separate roles for relevant sets of subject attributes, and rules can be implemented quickly to accommodate changing needs. RBAC-A uses three approaches to handle the relationship between roles and attributes namely: Dynamic roles, Attribute-centric and Roles-centric.

E. BtG:

Most traditional policies do not allow for overriding. A policy that allows for "Break-The-Glass (BTG)"[9] was implemented in order to override access control whilst providing for non-repudiation mechanisms for its usage. The policy was easily integrated within the model confirming its modularity and the fact that user intervention in defining security procedures is crucial to its successful implementation and use. The purpose of break-glass is to allow operators emergency access to the system in cases where the normal authentication cannot be successfully completed or is not working properly. Break-glass is based upon pre-staged "emergency" user accounts, managed in a way that can make them available with reasonable administrative overhead. The break-glass solution is time-tested, robust, and does not require additional automated technology. The break-glass solution is based on pre-staged emergency user accounts, managed and distributed in a way that can make them quickly available without unreasonable administrative delay. This solution follows the guideline that contingency plans should be simple, effective, and reliable. According to this paradigm, when a subject requests an access, the system checks regular access control policies. In case the request is denied, the system verifies whether this decision can be overridden by a BtG policy and, in such a case, the subject is notified and asked to confirm.

F. dRBAC:

Eric Freudenthal et al., [8]propose Distributed Role-Based Access Control (dRBAC). dRBAC is a scalable, decentralized trust-management and access control mechanism for systems that span multiple administrative domains.The three striking features of dRBAC are three features:

(1) third-party delegation of roles from outside a domain's namespace, relying upon an explicit delegation of assignment;

(2) Modulation of transferred permissions using scalar valued attributes associated with roles; and

(3) Continuous monitoring of trust relationships over long-lived interactions.

The authors claim that dRBAC defines a complete system that can be used to distribute, locate, validate and revoke role-based delegations in a larger security context.

G. GSRBAC:

Generalized Spatial RBAC[7] (GSRBAC), a model that extends RBAC and SRBAC to incorporate location information associated with roles and services in order to permit location-based definition of security and energy related policies. In the GSRBAC model, permissions are dynamically assigned to the role depending on location of a user and may be granted if in addition location of the requested service satisfies specified spatial constraints. Incorporating spatial information in RBAC as proposed in GSRBAC would enable RBAC to define more elaborated and fine-grained security policies with requirements to implement both more secure and green (energy-efficient) future mobile applications.

H. ARBAC:

An administrative role based access control (ARBAC) [15] policy specifies how each administrator may change the RBAC policy. It is often difficult to fully understand the effect of an ARBAC policy by simple inspection, because sequences of changes by different administrators may interact in unexpected ways. ARBAC policy analysis algorithms can help by answering questions, such as user-role reach ability, which asks whether a given user can be assigned to given roles by given administrators.

I. I-RBAC:

In I-RBAC[10], the operation on an object by the role is executed inside isolation environment if the role or the operation is predefined to be isolated. The key idea is to ensure system availability at all times for all the roles, while simultaneously ensuring the system integrity and security.

Another main advantage is that, it would be a cost-effective alternative to building a separate RBAC system to enable otherwise disallowed accesses, such as the training roles. It is an extension to the basic RBAC model in an effort to address the usability issues of RBAC under various conditions.

J. TEMPORARY ACCESS CONTROL POLICIES:

Barbara Carminati et al [5] propose a system that is based on context aware accesss control. In this strategy, when an access is denied by a regular policy, the system checks if this decision can be overridden by a temporary access control policy activated by the emergency and, in this case, the access is granted.

It seem similar to BtG, but there are important differences:

- BtG policies are always active, whereas the proposed emergency policies are active only during emergencies and this allows a more precise tuning of normal policy overriding.
- a user can decide when to use a BtG policy to override a regular one, whereas in our proposal only the system can override a regular policy.
- An important advantage of this schema is in term of security, because a user cannot decide whether to break the glass, rather only the system can override a regular policy and only during an emergency.
- Another advantage is the rapidity in emergency management.

The authors propose a novel notion of *emergency policies* able to manage flexible and secure information sharing during emergency situations. *Emergency policies* are capable of expressing complex emergency situations, override regular policies with *temporary access control policies* during these situations and support obligations.

K. RABAC :

Xin Jin et al.,[16] propose Role-centric Attribute Based Access Control that extends the RBAC model with permission filtering policies. It is a novel extension to the NIST RBAC model in an effort to address the role explosion problem of RBAC without modifying significant components of RBAC model and retaining the static relationships between roles and permissions. It is the first model to integrate roles and attributes using the role centric approach.

III CONCLUSION AND FUTURE WORK:

This paper is the initial work towards understanding the existing access control policies. In this paper, we have presented all the well-known access control policies. The paper gives a basic idea of so-far proposed access control policies though an in-depth citation has not been presented. As a future work, we intend to present a new access control policy that well suits for secured information sharing during emergency situations.

REFERENCES:

[1] Anna Ferrreira, Ricardo Joao Cruz Correia, Luis Antunes 002, Pedro Farinha, E. Oliveira-Palhares, David W.Chadwick, Altamiro da Costa Pereira", How to Break Access Control in a Controlled Manner" 2006 Proceedings 19th IEEE International Symposium on Computer-Based Medical Systems (CBMS)

[2] Anna Lisa Ferrara , P. Madhusudan, and G. Parlato *Policy Analysis for Self-Administrated Role-Based Access Control*, 19th Int'l Conference on Tools and Algorithms for the Construction and Analysis of Systems - TACAS 2013, Rome, Italy, 2013.

[3] Brucker, Achim D.; Petritsch, Helmut (2009). "Extending Access Control Models with Break-glass.". ACM symposium on access control models and technologies (SACMAT). ACM Press. pp. 19706

[4] Carminati, B.; Ferrari, E.; Guglielmi, M. "SHARE: Secure information sharing framework for emergency management", Data Engineering (ICDE), 2013 IEEE 29th International Conference on,On page(s): 1336 - 1339

[5] Carminati, B.; Ferrari, E.; Guglielmi, M. "Secure Information Sharing on Support of Emergency Management", Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom), On page(s): 988 – 995

[6] J. Crampton and G. Loizou. Administrative scope: A foundation for role-based administrative models. *ACM Transactions on Information and System Security*, 6(2):201–231, 2003.

[7] M.L. Damiani, E. Bertino, C. Silverstri, " Spatial Domains for the Administration of Location-based Access control Policies", Journal of Network and System Management, Springer, Sept 2008.

[8] Eric Freudenthal, Tracy Pesin, Lawrence Port, Edward Keenan, and Vijay Karamcheti , "dRBAC: Distributed Role-based Access Control for Dynamic Coalition Environments ", ICDCS '02 Proceedings of the 22 nd International Conference on Distributed Computing Systems (ICDCS'02) Page 411

[9] Ferreira, A. and Chadwick, D.W. and Farinha, P. et al. (2009) How to securely break into RBAC: the BTG-RBAC model. In: Computer Security Applications Conference, 2009. ACSAC'09. Annual, December 7–11, 2009, Honolulu, Hawaii, USA.

[10] Gunti, N.; Weiqing Sun; Niamat, M. "I-RBAC: Isolation enabled role-based access control", Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on, On page(s): 79 – 86

[11] Liang Chen, Jason Crampton, "Risk-Aware Role-Based Access Control" 7th International Workshop, STM 2011, Copenhagen, Denmark, June 27-28, 2011 .

[12] Lingyu Wang, Duminda Wijesekera†, and Sushil Jajodia "A logic-based framework for attribute based access control", Proceedings of the 2004 ACM workshop on Formal methods in security Engineering Pages 45 - 55

[13] Ngajyothi Gunti, *Weiqing Sun*, and Mohammed Niamat , "I-RBAC: Isolation Enabled Role-Based Access Control", Ninth Annual Conference on Privacy, Security and Trust (PST 2011) Montreal, Quebec, Canada, July 19-21, 2011.

[14] Richard Kuhn, Edward J. Coyne, Timothy R. Weil, "Adding Attributes to Role-Based Access Control," *Computer*, vol. 43, no. 6, pp. 79-81, June 2010, doi:10.1109/MC.2010.155

[15] Scott D. Stoller, Ping Yang, Mikhail Gofman, and C. R. Ramakrishnan. Symbolic Reachability Analysis for Parameterized Administrative Role Based Access Control. Computers & Security 30(2-3):148-164, March-May 2011, Elsevier.

[16] Xin Jin, Ravi Sandhu and Ram Krishnan, RABAC: Role-Centric Attribute-Based Access Control. In Proceedings 6th International Conference, on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2012, St. Petersburg, Russia, October 17-20, 2012, pages 84-96.