Jiajie Li

CSE 300

10 November 2016

Research Proposal: Combined RBAC and ABAC Model

In the field of computer security, access control is an important area of research. An efficient access control policy is crucial for organizations that manage and control large amounts of data on daily basis,because it guards and manages access to highly secured resources, and is responsible for granting permission to the right users. On the other hand, a flawed access control policy could cause some issues on security and performance especially. One typical security concern is that users could be given access to wrong resources, but modern policies rarely encounter this issue as it's the responsibility of administrators to define correct policies. Performance is instead a larger challenge, because nowadays organizations can have easily over millions of users and resources, and as the number grows it becomes more difficult and complicated to manage all the rules.Some traditional policy models including Access Control List(ACL), which have been widely adopted, havefaced the same issue and are no longer being used by organizations that manage large data sets. The new demands for efficient access control policies lead to the recent growth and development of two new models, Role-Based Access Control (RBAC) model and Attribute-Based Access Control (ABAC) model.

The two models are both invented as improvements of the traditional models that overcome the performance issue. RBAC model uses role assignments of users to determine permissions, and ABAC model uses attributes of users to determine permissions. Both models have their own advantages and disadvantages, and they have their own limitations when facing different situations. Researchers have suggested to combine the two to obtain a more efficient

model, which can be utilized in larger sets of cases. However, they only provided details on conceptual levels, and there isn't any implementation guidance or definition for this combined model. Another issue with this model is the difficulty of implementation. Implement a policy by administrators are time-consuming and error prone. In order to reduce the time and costs of implementation, it's possible to develop a mining algorithm that automate the process, which also makes it easier for organizations to adopt a new policy model. Therefore, in the proposed research, the goal is to define a new access control model, which combines both RBAC and ABAC models, and develop a mining algorithm for this new model to automate its implementation process.

The concepts of RBAC and ABAC models first came up around1990s, but they were officially recommended by the Federal Chief Information Officers Council (CIO) in the FICAM Roadmap and Implementation Guidance Version 2.0 (286-290) published in 2011. The recommendation displayed the confidence of the CIO, and that they had evaluated and considered themodels to be effectiveand trustworthy for government agencies to utilize in modern era. Following the government recommendation, many more studies and researches were conducted for the models. Since ABAC was relatively new compared to RBAC, there wasn't any definition for ABAC model until Hu, et al. published the guide and implementation definition for the model. In the document, Hu, et al. stated that RBAC was similar to ABAC in the sense that RBAC used the attribute of "role" (5). This showed that RBAC was actually compatible with ABAC, and as suggestedby the CIO, it was best to use a hybrid approach that combined different aspects of access control models to achieve the best result (290). The concept and idea to combine RBAC and ABAC models were given by Coyne and Weil. After the authors compared the advantages and disadvantages of the two models, they suggested to use a judicious

combination, and obtained a Role-Centric Access Control model, which was essentially a RBAC model extended with attributes. The reason behind this was that RBAC model could overcome the problem that ABAC couldn't audit user access to certain permissions, and the new model would reserve the flexibility of ABAC and auditing of RBAC (Coyne and Weil 15-16).However, the authors only provided conceptual details, and no implementation guidance was given. With the development of new models progressed, new mining algorithms for new models were invented as well. Stoller and Xu developed an algorithm for ABAC policy mining, which mined ABAC policies from existing old policies and RBAC policies, in hopes of overcoming the difficulty of implementing ABAC policies. Their algorithm was successful to transfer RBAC policies to ABAC policies, though it was difficult to evaluate its efficiency because according to Xu and Stoller it was the first known ABAC mining algorithm (13). RBAC and ABAC models both have limitations in different situations, and in the paper by Bogarerts, et al, they presented a case which ABAC couldn't be fully utilized. According to Bogarerts, et al, ABAC model had difficulty reflecting relationships (291), and therefore they proposed a new policy model that would work the best in their presented case. This showed that there wasn't any best access control model, and for different situations some models would be beneficial the most. Following this idea, the combined ABAC and RBAC models would also have its advantage in certain cases, that it could be utilized in its full potential.

The new access control model aims to combine ABAC model and RBAC model and reserve both of their benefits. This model follows the concept provided by Coyne and Weil, which extended RBAC model with attributes. Since Coyne and Weil only provided concepts for this model, first a concrete language needs to be defined. An access model rule typically contains users, resources, constraints and actions. Since RBAC is the main model, rules would also

contain role assignment and role permissions. Then with the extension of attributes, each rule would also have an attribute set that needs to be satisfied in order to grant the permission. After a language for the model is defined, then it's possible to develop the mining algorithm. This algorithm is based on the works of Stoller and Xu, and it is an extension of their ABAC mining algorithm. Since the algorithm by Stoller and Xu transfers RBAC to ABAC policies, this process can be modified and turned into transferring RBAC policy to the new combined Role-Centric ABAC policy. After the algorithm is finalized, it needs to be tested in real world cases, and it's important to find study cases that are most suitable for this model. To test the algorithm's efficiency and correctness, first manually create sample policy, then compare it with the result of the mining algorithm. If the results are similar, then it's possible to conclude that the algorithm is indeed correct. This research will be conducted by Master students ofComputer Science Department under the supervision of a CS Professor. The research will take place in Stony Brook main campus, and is expected to be finished in one academic semester.

The focus of the research is to create a new combined model of RBAC and ABAC based on the concept provided by Coyne and Weil, and also to develop a mining algorithm based on the study of Stoller and Xu. This research will further improve both RBAC and ABAC models, because it aims to create a more efficient model, by revealing their weaknesses but also searching for a possible solution to overcome both their disadvantages. Also it will provide more examples and solutions for access control mining problemsby developing an efficient mining algorithm for the new model.Following the suggestion of hybrid approach by the CIO, it will prove the possibility of combining models and reserving their benefits at the same time, and will in turn encourage more study and discovery of new access control models.

Bibliography

Federal Chief Information Officer Council and Federal Enterprise Architecture. “Federal Identity Credential and Access Management (FICAM) Roadmap and Implementation Guidance.” Version 2.0, 2 Dec. 2011.

Hu, Vincent, et al. “Guide to Attribute Based Access Control (ABAC) Definition and Considerations.” *NIST Special Publication 800-162*. National Institute of Standards and Technology, Jan. 2014.

Coyne, Ed and Timothy Weil. “ABAC and RBAC: Scalable, Flexible, and Auditable Access Management.”*IT Pro May/June 2013*. IEEE Computer Society, 2013, pp. 14-16.

Stoller, Scott and Zhongyuan Xu. “Mining Attribute-Based Access Control Policies.”*IEEE Transactions on Dependable and Secure Computing*.IEEE Computer Society, Sep. 2015.

Bogaerts, Jasper, et al.“Entity-Based Access Control: supporting more expressive access control policies.” *Proceedings of the 31st Annual Computer Security Applications Conference*. ACM, Dec. 2015, pp. 291-300.