Author copy - In Proceedings of the 2012 International Conference on Software Engineering (ICSE 2012).
DOI: 10.1109/ICSE.2012.6227053

Application of Self-Adaptive Techniques to Federated Authorization Models

Christopher Bailey
School of Computing
University of Kent
Canterbury, UK
c.bailey@kent.ac.uk

***Abstract*—Authorization infrastructures are an integral part of any network where resources need to be protected. As organisations start to federate access to their resources, authorization infrastructures become increasingly difficult to manage, to a point where relying only on human resources becomes unfeasible. In our work, we propose a Self-Adaptive Authorization Framework (SAAF) that is capable of monitoring the usage of resources, and controlling access to resources through the manipulation of authorization assets (e.g., authorization policies, access rights and sessions), due to the identification of abnormal usage. As part of this work, we explore the use of models for facilitating the autonomic management of federated authorization infrastructures by 1) classifying access behaviour exhibited by users, 2) modelling authorization assets, including usage, for identifying abnormal behaviour, and 3) managing authorization through the adaptation and reflection of modelled authorization assets. SAAF will be evaluated by integrating it into an existing authorization infrastructure that would allow the simulation of abnormal usage scenarios.**

***Keywords*-self-adaptation; model driven engineering; model transformation; authorization; computing security**

I. INTRODUCTION

Organisations use authorization infrastructures to protect, control and monitor access to electronic resources. There exist a variety of approaches to authorization, such as, role based access control (RBAC) [1], and attribute based access control (ABAC) [2]. Each rely upon traditional methods of management, whereby human administrators monitor audit logs, and make changes to access control rules or user access rights manually (and reactively) based on what they observe. Administrators analyse audit logs, primarily conveying usage statistics of user access requests, to ensure access is being used as expected.

As organisations federate their access, by which they share their resources with other organisations across a distributed infrastructure, the number of users with access increases dramatically. This enforces the need for more efficient management of access control, as it is known that an authorized user can cause far greater damage in comparison to an external attacker, due to their access rights [3]. As exhibited through the use of alternative solutions aimed at improving authorization management, such as usage control (UCON) [4] and intrusion detection systems (IDSs) [5], human controllers alone are not capable of effectively managing authorization infrastructures. Despite these solutions, few automated mechanisms exist, such as, active IDSs [5], for mitigating, or preventing further abnormal usage. In these cases, the extent of what can be done is minimal compared to the full scope of an authorization infrastructure.

Autonomic management has been identified as a potential solution for improving traditional authorization management. It reduces the need for human controllers by automating management activities, such as, identifying misuse of access rights and responding appropriately, assessing the state of the authorization infrastructure, and ensuring sufficient and relevant access is available to its users. We propose a model for facilitating autonomic management of authorization activities. This is achieved by modelling of authorization assets (e.g., access control rules, access rights, and access sessions), modelling usage, and controlling authorization through autonomic management decisions. The use of models allows an autonomic controller to reason about the state of authorization (such as, current active access control rules and any abnormal usage attributed to them) by, guiding how the authorization infrastructure should be adapted in order to manage access to resources.

This research investigates the role of models when automating the management of federated authorization infrastructures. The motivation for using models is that these infrastructures provide opportunities for modelling complex adaptation situations where the need for autonomic management is significant. This research will be performed in the context of the Self-Adaptive Authorization Framework (SAAF) [6] whose objective is to monitor and control the assets of federated authorization infrastructures.

The rest of the paper is structured as follows. In Section 2, we identify the research problem and our expected contribution. Section 3 describes our proposed approach, including methodologies and evaluation plan. Section 4 outlines our current work. In Section 5, we comment upon related work, and finally, Section 6 concludes by summarising what has been achieved so far, and indicates lines for future research.

Author copy - In Proceedings of the 2012 International Conference on Software Engineering (ICSE 2012).
DOI: 10.1109/ICSE.2012.6227053

II. Research Problem and Expected Contribution

As identified in the introduction, there is motivation to improve traditional management of federated authorization by automating management activities. The concept of federated authorization implies organisations that share access conform to one authorization model, however each organisation will implement that authorization model differently, utilising their own formats for authorization policies, and store user access rights in their own way. The research problem can be split into two parts: 1) how to manage authorization over a federated infrastructure, regarding what can be controlled and what can be used to assess the need for change, and 2) how autonomy can be integrated with the management of a federated authorization infrastructure, considering the various underlying technologies and implementations employed by the participating organisations.

Our contribution is the definition of a model that represents a federated RBAC/ABAC authorization infrastructure, extended to classify adaptation situations (modelling unexpected behaviour) and controls to govern adaptations (adaptation goals). Through modelling the target infrastructure, we capture the authorization state, and assess such state against expected usage in order to trigger the need for adaptation. Modelling also provides support for reasoning about the target infrastructure by separating the different adaptation activities from its application specific implementation. This can be achieved through model transformation, which also allows the usage of specific techniques and tools that are associated with different adaptation activities. These activities include the detection of abnormal behaviour, the analysis of the alternative solutions, the decision of what measures to take, and the execution of these adaptations in a federated authorization infrastructure.

III. Proposed Approach

The proposed approach involves the design and development of a Self-Adaptive Authorization Framework (SAAF) [6] that implements the MAPE-K feedback control loop [7][8]. The aim of SAAF is to manage RBAC/ABAC authorization infrastructures by monitoring and controlling authorization assets. SAAF builds a model of usage patterns collected by monitoring user access requests. It identifies abnormal behaviour when patterns of usage no longer conform to what is expected (such as, rates of requests over time). As a response, SAAF adapts manageable authorization assets in order to react to abnormal behaviour, and manage future access control decisions.

SAAF is positioned to work with a distributed RBAC/ABAC authorization infrastructure in order to encompass federated access. This presents an opportunity to model the state of authorization in a distributed environment, and apply SAAF in a decentralised manner [9], as multiple sensors and effectors will be required to interface with various authorization services.

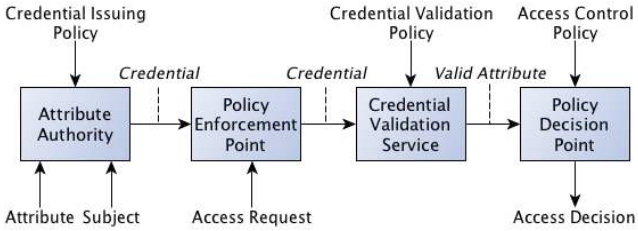

Figure 1. Conceptual Model for Distributed RBAC/ABAC Infrastructure

A. Conceptual Model

The conceptual model (figure 1) provides an abstraction of a federated RBAC/ABAC authorization infrastructure [10]. It captures the necessary authorization services (such as the Policy Decision Point) and authorization assets (such as policies) that enable a subject (an authenticated user) to gain access to an organisation's resources. A subject's access rights is managed by their organisation's Attribute Authority (AA), which assigns attributes (such as the role of 'Staff') and generates credentials for its subjects. A credential is a signed declaration of a subject's access right, providing information about who assigned this subject access. The AA's credential issuing policy governs which attributes a subject within their organisation can have. When a subject wishes to access a resource they request access through the resource's Policy Enforcement Point (PEP). The PEP communicates with the Credential Validation Service (CVS) and Policy Decision Point (PDP) in order to be informed if the subject can have access. The role of the CVS is to identify if a trusted AA has signed the subject's credential. It validates the credential against its credential validation policy and returns any valid attributes the subject has. The PDP then uses these valid attributes to assess if the subject has the necessary rights to access the resource, in accordance to its access control policy.

With respect to SAAF, the conceptual model identifies what can be controlled to realise management decisions, and what can be used to assess the need for management decisions. There are 3 services that can be controlled: Attribute Authorities (AA), Credential Validation Services (CVS) and the Policy Decision Points (PDP). By adapting an AA's credential issuing policies, SAAF can manage an individual subject's access rights. Adaptation of a CVS's credential validation policies allows SAAF to control what AAs can be trusted to manage access. Finally, adaptation of a PDP's access control policies allows SAAF to control the specific attributes needed for any subject, from any organisation, to access any resource. To assess the need for management decisions there are two types of assets that must exist, these being user access requests and the corresponding access control decisions. These assets allow for the analysis of user behaviour, through relating requests by a subject, over time.

Author copy - In Proceedings of the 2012 International Conference on Software Engineering (ICSE 2012).
DOI: 10.1109/ICSE.2012.6227053

B. Autonomic Management

A solution to automated management relies on 4 activities. The first activity is *Trigger Adaptation* that identifies the need for a change to the target authorization infrastructure. This is achieved through monitoring usage of the authorization infrastructure and modelling user behaviour in conjunction with behavioural rules. For example, a behaviour rule might state that no subject may request access to a particular resource beyond a given threshold, related to the frequency of access requests. Should this threshold be violated abnormal behaviour is identified.

The second activity is *Generate Solutions*, whereby multiple solutions are generated to address the identified abnormal behaviour. Within the scope of the conceptual model, there is a finite set of actions that can be executed against an authorization infrastructure. The actions can be modelled in a decision tree, where actions are grouped to form solutions. For example, remove rule from policy and revoke credential from subject.

The *Solution Selection* activity identifies the most relevant solution for the abnormal behaviour, as each solution will have varying degrees of cost, considering a single attribute decision maker. For example, removing all access control rules will prevent a user from continuing malicious activity, however, it will also impact the entire user base unnecessarily. An alternative solution whereby only the user's access is impacted would be more relevant since the incurring cost would be lower. However, this selection has to be considered in the context of allowing the behaviour to continue.

Finally, *Plan Generation* is the process of creating a step-by-step plan that can be executed in order to realise the chosen solution against the authorization infrastructure. The plan is executed with the use of multiple effectors that can control authorization services, such as, updating an access control policy used by a Policy Decision Point.

C. Evaluation Plan

SAAF's ability to manage an authorization infrastructure will be evaluated using heuristics and measurements by executing expected/unexpected usage scenarios. The scenarios may capture the time required to identify abnormal usage, the time required to react to abnormal usage, and the impact that the adaptation might have upon the infrastructure. For example, measuring the number of subjects belonging to an authorization infrastructure that have been impacted unnecessarily. Success will be achieved through comparison against traditional management techniques, where a human operator attempts to identify and resolve the same scenarios observed by SAAF.

To ensure results are valid, the evaluation scenarios applied to SAAF are modelled on real world events where it is known users have carried out abnormal or malicious usage. The historic actions of the human operators will be simulated against the same usage scenarios, and compared against SAAF's own actions. Each controller will be assessed using the same heuristics and measurements.

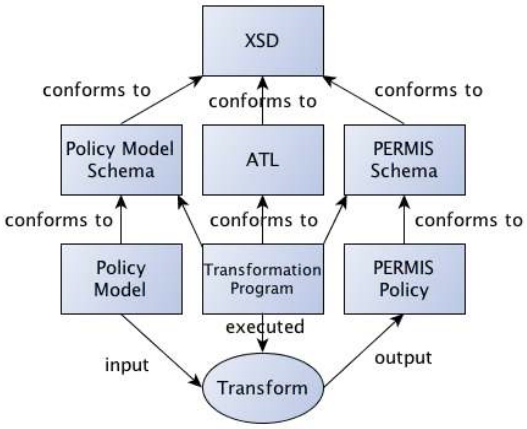

Figure 2. Applying model transformation to generate PERMIS policies

IV. CURRENT WORK

A. PERMIS Integration

Our current work is focused on the design and development of SAAF and integration into the PERMIS [10] authorization infrastructure, which is based on a distributed RBAC/ABAC model. PERMIS is chosen due to its ability to operate with various technologies and different policy formats, allowing for simulation of multiple implementations of RBAC/ABAC. It also provides the necessary effectors for SAAF to control authorization services, such as, a policy manager to activate and deactivate authorization policies that belong to the credential validation service and policy decision point.

B. Model Transformation

SAAF's integration into PERMIS requires the target authorization infrastructure, like PERMIS (or any RBAC/ABAC authorization infrastructure), to be modelled in order to reason and manipulate its state. Model driven engineering (MDE) [11] presents a favourable option in order to model authorization assets, manipulate these models at run-time, and reflect [12] eventual changes into authorization infrastructure (through model transformation).

Figure 2, based on the MDE model transformation process [11], explores one aspect of model transformation in which we transform SAAF's view of the authorization infrastructure, with respect to SAAF's *policy model*. The policy model provides an abstraction of implemented RBAC/ABAC authorization policies, allowing SAAF to carry out management decisions without knowledge of implementation. Once SAAF has analysed the state of the authorization infrastructure in accordance to the policy model, the policy model is adapted as a result of SAAF reacting to abnormal behaviour. This requires the policy model to be reflected against the target authorization infrastructure. A transformation program generates a policy

in the target authorization infrastructure's own policy format (in this case PERMIS), from the SAAF policy model. As part of the transformation the generated policy is validated against the target's policy schema (i.e., the PERMIS policy schema). With regards to SAAF, this activity is carried out as part of the plan execution, which uses effectors to activate policies generated through model transformation.

V. Related Work

To the best of our knowledge, we are not aware of any other work that utilises self-adaptation as a means for managing authorization infrastructures. However, there are several techniques that improve upon traditional authorization management. Usage control (UCON) extends traditional authorization in order to limit what a user can do in terms of requesting access [4]. As a proactive means for limiting abnormal behaviour, the approach does not support any type of run-time adaptation to an authorization infrastructure, such as, active response when abnormal behaviour is detected. For example, if one user continually reaches their usage limit this violation could be considered as malicious behaviour, requiring the need for permanent removal of the user's access rights. UCON remains static in this case, whereas self-adaptation would identify the need for access right removal, and modify the infrastructure accordingly. Intrusion detection systems (IDSs) also can be used to improve traditional authorization management techniques [5]. These identify when and where malicious usage has taken place. Some IDSs actively react to these attacks in a minimalistic manner, for example, by adding firewall rules in light of an identified attack. IDSs are limited in terms of the input criteria to assess attacks, such as, network traffic. Our solution differs as it operates at a higher level, where more meaningful information can be analysed to produce clearer and precise decisions, within the full scope of authorization infrastructures.

Our proposal builds upon several other related works, although not necessarily directly connected to autonomic authorization management. One of these contributions is the UML representation of RBAC, which provides a re-usable RBAC model [13]. It incorporates OCL constraints, and RBAC policy patterns to allow instantiation of polices into an RBAC system. Although, primarily aimed for supporting design at development-time, it nevertheless provides a good basis for defining a model that can be used with SAAF. There is also SECTET-PL [14], a policy language interpreted as UML, to be used with model driven engineering. The goal is to align security business objectives (seen as our behavioural rules) with a target system through model transformation, which shares some similarities with our work.

VI. Conclusion

In the context of our Self-Adaptive Authorization Framework (SAAF), this paper has proposed the use of models as a means for automating the management activities of authorization infrastructures. The modelling of federated authorization infrastructures and their usage, allows SAAF to reason about the state of the authorization infrastructure, in order to assess if the state of authorization must change. For example, if a number of users carry out malicious behaviour against the authorization infrastructure (exhibited through their access requests), the state of authorization must change to further prevent such behaviour. Our current work is focused on integrating SAAF with a federated authorization infrastructure by using model driven engineering to facilitate reasoning about the state of authorization, and providing seamless interaction with multiple organisations. The use of models will be evaluated through the implementation of SAAF, where autonomic management can be demonstrated against a federated authorization infrastructure.

References

[1] ANSI. "Information technology – Role Based Access Control". ANSI INCITS 359-2004.

[2] ITU-T Rec X.812 (1995) | ISO/IEC 10181-3:1996 "Security Frameworks for open systems: Access control framework".

[3] A.P. Moore, D.M. Cappelli, T.C. Caron, E. Shaw, D. Spooner and R.F. Trzeciak, "A preliminary model of insider theft of intellectual property," In Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 2, 2011.

[4] R. Sandu and J. Park, "Usage Control: A Vision for Next Generation Access Control," In Computer Network Security 2776, Springer-Verlag, 2003.

[5] H. Debar, M. Dacier and A. Wespi, "Towards a taxonomy of intrustion-detection systems," Comput. Netw 31, Apr 1999, pp. 805-822.

[6] C. Bailey, D.W. Chadwick and R. de Lemos, "Self-Adaptive Authorization Framework for Policy Based RBAC/ABAC Models," Proc. 9th Internationl Conference on Dependable, Autonomic and Secure Computing, (DASC 11), 2011, pp. 37-44.

[7] J.O. Kephart and D.M. Chess, "The Vision of Autonomic Computing," Computer 36, Jan. 2003, pp. 41-50.

[8] Y. Brun, G. M. Serugendo, C. Gacek, H. Giese, and H. Kienle, "Engineering Self-Adaptive Systems through Feedback Loops. In Software Engineering for Self-Adaptive Systems, Lecture Notes in Computer Science, Vol. 5525. Springer Verlag, Berlin, Heidelberg. 2009, pp. 48-70.

[9] R. de Lemos, H. Giese, H. A. Müller, and M. Shaw, "Software engineering for self-adaptive systems," In Dagstuhl Seminar 10431 Proceedings. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany. Dagstuhl Germany. May 2011.

[10] D.W. Chadwick, G. Zhao, S. Otenko, R. Laborde, L. Su and T.A. Nguyen, "PERMIS: A modular Authorization Infrastructure," Concurrency and Computation: Practice and Experience 20, Aug. 2008, pp. 1341-1357.

[11] J. Bézlvin, "Model Driven Engineering: An Emerging Technical Space," In Generative and transformational techniques in software engineering, GTTSE 2005, LNCS 4143, 2006, pp. 36-64.

[12] J. Andersson, R. de Lemos, S. Malek and D. Weyns, "Reflecting on self-adaptive software systems," in Software Engineering for Adaptive and Self-Managing Systems, SEAMS, 2009, pp. 38-47.

[13] D. Kim, I. Ray, R. France, and N. Li, "Modeling Role-Based Access Control Using Parameterized UML Models," Proc. of Fundamental Approaches to Software Engineering, 2004, pp. 180-193.

[14] M. Alam, R. Breu and M. Hafner, "Model-Driven Security Engineering for Trust Management in SECTET," Journal of Software Vol. 2, No. 1, 2007, pp. 47-59.