ACCESS CONTROL SYSTEM FOR DISTRIBUTED NETWORKS

Giorgi Iashvili
Georgian Technical University

Abstract

Access control models for electronic information flow control have existed for decades and have been developed over time to support a range of applications and uses. In this work we are summarizing the existing literature on access control models and proposing a new combination of rules and methods that are best suited to the changing security threats introduced by the move to mobile collaborative working and de-perimeterization.

Keywords: Access control systems. Distributed networks. Co-located. De-perimeterization. Context aware.

1. Introduction

Existing access control models for electronic information flow have been supporting a range of different applications for several decades. But nowadays, when doing a business, according to El Kalam & Deswarte [1] ''usually requires collaboration between different organizations'' and even in one organization the business process is getting more and more depended on distributed and mobile collaborative work from different locations and different devices, access control models have to be transformed in such way to provide appropriate access to the data and restrict unauthorized attempts. And one of the most important things is the flexibility of the model – how easily can be managed the access control in organization. Everything what used to work well in one co-located domain is not working when the information flow is out of the boundary of the domain because it is getting harder to control the access to the data using heuristic approaches while moving to de-perimeterization. [2,3] In the figure below we can see the template of access control system, where the proper access is granted by special smart cards.

Figure 1. Access control system with smart cards

When access control model was working in one domain there were no problems with enforcing the security policy, authorization and etc. Now on a large scale when data is going beyond the perimeter, access control systems have to overcome the difficulties related with time, geographical and sociocultural differences.

According to all these, we think that the main challenges for the modern access control systems are the problems related with sociocultural and geographical differences between the distributed mobile working employees and before proposing our view of the ideal access control model, let us make a short review of existing models.

2. Main part - Review of some existing access control models

2.1. Mandatory Access Control (MAC)

This model is based on the concept that the system assigns different levels of classification to each user and each resource in organizational network and the access is defined and granted after ensuring that the entity who is asking for the access of a certain data has level at least as high as the classification of the data itself. The decision about the access is made only by the system owner (administrator) and no one from the end users is allowed to provide any type of privileges to anyone. [4, 5].

That is why MAC is considered as most secure and restrictive access control model and basically it is used in military applications or governmental services. (However, a variation of MAC model is used in Microsoft Vista Operation System)

2.2. Discretionary Access Control (DAC)

In contrast of MAC model in DAC we have completely different approach – where user decides himself who can access his data and what type of privileges can be granted to other users for the certain resources (owned by him) This issue makes the DAC model least restrictive to compare with other ones. In other words, DAC model can be known as ''who can access my data''. The access types are managed on the certain resource and it is not centralized. One of the most spread examples of DAC is incorporated in Linux systems.

2.3. Role-based access control model (RBAC)

In this model there is no any access defined to certain users – the access is granted only to the certain roles that exist in organization. For example, there are no users like Giorgi Iashvili or Gigi Tsereteli – for them there will be one role – PhD Student and any student which will be associated with this role will be granted with same access. The decision about access is made by system owner (administrator).

The role based approach brought simplicity in administration – cause the number of users is depended on number of roles, positions in organization and it is definitely less than the number of employees. But on the other hand it means that there is no granularity – because it is not possible to give some privileges to certain users. According to Desmond [6] the main challenge of this model is that what you choose – strong security which involves more granularities for each role or easier administration which means fewer roles in the system.

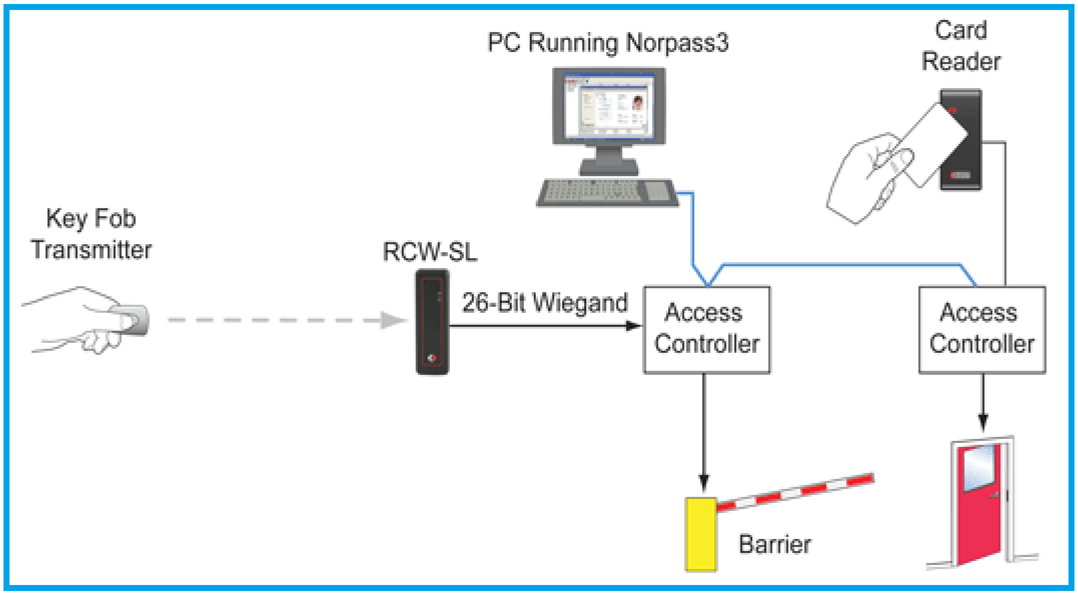

Figure 2. Sample of access control system with multiple check points

2.4. Rule-based access control model (RuBAC)

This model is based on the principle that we have one (at least) appropriate rule for each user in the system. Unlike to the Role-based model this approach gives granularity in the rules and it makes the model more accurate. But on the other hand, if consider how often employees are coming and leaving the company it will be clear that administration of RuBAC model in a large organization will be inefficient.

2.5. Context aware access control model

Very good explanation of this model is provided by Zhang & Parashar [7] According to them, in distributed environment where lot of users access resources from different devices, "granting a user access without taking the user's current context into account" can occur serious problems related with security "as the user's privileges not only depend on "who the user is" but also on "where the user is" and etc." Context can be environmental, personal, spatio-temporal, social and etc. We consider that nowadays, in the world of mobile devices the most important context properties are geolocation and social ones and it should be considered while modifying existing access control models.

From the figure 3 we can see the template scheme of access control system with biometric authentication.

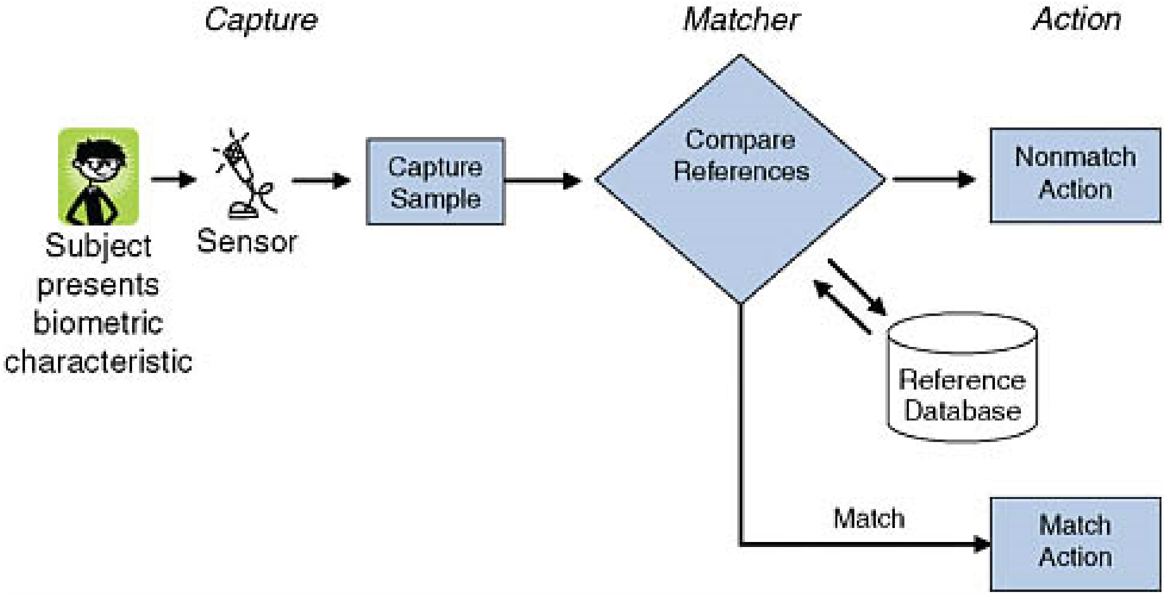

Figure 3. Scheme of access control system with biometric authentication

3. Conclusion

Solution – RuMRoDCaP access control model

As a solution we propose a new access control model – RuMRoDCaP which involves the best properties of all abovementioned models and we think this model will overcome all problems related with sociocultural and geographical issues. We suggest maintaining a centralized security policy for the whole organization and each employee has to access any organizational data with the rights defined by this policy no matter they are in or out of the organizational boundary. Our model is MAC based and decision about the access is made only by the system owner (administrator) cause in case of DAC the security would be compromised and access would not be controlled by the system owner. But we think that in some cases user can ask for higher access privileges to his superior and superior makes decision whether send request to the central system administrator for access elevation or not. This issue makes our policy more reliable and restrictive. Due to the fact that initiation about the elevation of the access privileges is from the user side we can say that RuMRoDCaP is partially using DAC model also.

Based on existing positions in organization we define the roles and will use these roles in our model – creating rules for these roles. The roles will be defined in more details – so it brings more complexness in administration but also more granularity and better security what is the main reason of our choice.

But we also define a number of certain users (Top-management, branch managers and some key people in organization) which will have personal rules. It brings more accuracy in access control decisions.

One of the main important things in our model will be the context property – basically the geolocation of the device (GPS) from which the user tries to access the data. There will be different rules for different locations based on pre-defined assumptions. We say that we have centralized security policy for everyone but when user access the data from different geolocation there can be some local regulations and policies which will be mandatory for the user or device. On this issue we have the approach that only those regulations can be taken into account which provide higher security than our centralized policy and not the vice versa.

We can see that in our model the final decision is made only by the system owner on the central site and we think this is the most key issue in our model. Also one of the serious problems for access control model in distributed environment is how to enforce the centralized security policy into distributed areas. For this problem we suggest very intensive real time centralized monitoring of the distributed systems and devices which will reduce the risk of such case when some device or user is out of the central security policy.

References:

1. El Kalam A.A.. Deswarte Y. (2006). *Multi-OrBAC: a New Access Control Model for Distributed, Heterogeneous and Collaborative Systems,* s.l.: s.n.

2. Bertino E., Kirkpatrick M.S. (2011). *Location-Based Access Control Systems for Mobile Users,* Chicago: s.n.

3. Demchenko Y., Gommans L., Laat C. (2006). *Extending Role Based Access Control Model for Distributed Multidomain Applications,* s.l.: s.n.

4. Anderson R.J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems.* 2 ed. Indianapolis: Wiley Publishing.

5. Gentry S. (2012). *Access Control: Models and Methods,* s.l.: s.n.

6. Desmond J. (2003). *Roles or Rules: The Access Control Debate,* s.l.: s.n.

7. Zhang G., Parashar M. (2004). *Context-aware Dynamic Access Control for Pervasive Applications,* s.l.: s.n.

ᲓᲐᲨᲕᲔᲑᲘᲡ ᲙᲝᲜᲢᲠᲝᲚᲘᲡ ᲡᲘᲡᲢᲔᲛᲐ ᲒᲐᲜᲐᲬᲘᲚᲔᲑᲣᲚᲘ ᲥᲡᲔᲚᲔᲑᲘᲡᲐᲗᲕᲘᲡ

გიორგი იაშვილი
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

დაშვების კონტროლის სისტემები ელექტრონულ მონაცემთა ნაკადის კონტროლისათვის უკვე რამდენიმე ათწლეულია ფართოდ გამოიყენება და ვითარდება. ნაშრომში მიმოვიხილავთ დაშვების კონტროლის სისტემებზე არსებულ ლიტერატურას და დასკვნის სახით ვთავაზობთ წესებისა და მეთოდების ახალ კომბინაციას, რომელიც შესაძლებელია გამოყენებული იქნას დეპერიმეტრიზაციისას წარმოქმნილი ახალი საფრთხეების თავიდან ასაცილებლად.

СИСТЕМА КОНТРОЛЯ ДОСТУПА ДЛЯ РАСПРЕДЕЛЕННЫХ СЕТЕЙ

Иашвили Г.Н.
Грузинский Технический Университет

Резюме

В последние десятилетия находят все более широкое применение системы контроля доступа потока электронных данных и они постоянно совершенствуются. В работе дан обзор существуюшей литературы о системах контроля доступа. В качестве вывода предложена новая комбинация правил и методов, применение которой позволит избежать новые угрозы, возникшие при депериметризации.