Modeling Access Control Policy of a Social Network

Chaimaa Belbergui
STIC laboratory
Chouaib Doukkali University
El Jadida, Morocco

Najib Elkamoun
STIC laboratory
Chouaib Doukkali University
El Jadida, Morocco

Rachid Hilal
Presidency
Chouaib Doukkali University
El Jadida, Morocco

***Abstract*—Social networks bring together users in a virtual platform and offer them the ability to share -within the Community- personal and professional information's, photos, etc. which are sometimes sensitive. Although, the majority of these networks provide access control mechanisms to their users (to manage who accesses to which information), privacy settings are limited and do not respond to all users' needs. Hence, the published information remain all vulnerable to illegal access. In this paper, the access control policy of the social network "Facebook" is analyzed in a profound way by starting with its modeling with "Organization Role Based Access Control" model, and moving to the simulation of the policy with an appropriate simulator to test the coherence aspect, and ending with a discussion of analysis results which shows the gap between access control management options offered by Facebook and the real requirements of users in the same context. Extracted conclusions prove the need of developing a new access control model that meets most of these requirements, which will be the subject of a forthcoming work.**

Keywords—social network; Facebook; access control; OrBAC; study of coherence

I. Introduction

Facebook [1] is an online social network, free and very popular (1.65 billion users in 2016) allowing anyone to register, invite friends, exchange messages; share photos and videos, etc. After registration, the user owns an account that consists of a profile (personal information, professional information, photos, etc.) and a wall, which is powered by publications of friends, pages, groups and advertisers [2]–[4]. These publications can be a text, a photo or a video.

Facebook was invented by "Marc Zuckerburg" in 2004 in order to share information between Harvard University students and was put to use of the public on September 2006 [5]. Since then, it continues to expand to attract the largest number of users and offers them the means to manage access to their informations from the "Privacy Settings" interface. Yet, it is often the subject of debate [3], [4], [6]–[8], because of privacy issues that remains .That lead us to closely analyze this problematic using an access control model allowing the extracting of incoherence problems that exist in Facebook Access control policy to subsequently propose the most appropriate access management solution to resources .

Conventional access control models: Discretionary Access Control (DAC), Mandatory Access Control (MAC) [9], [10]. Role Based Access Control (RBAC) [9]–[11], and others are not suitable to the needs and requirements of social networks since they are often limited to the definition of positive permissions and cannot be used as part of a system that are no more interested in the permissions' definition than to prohibition's especially if it is contextual privileges (access rules based on conditions) [2]. Therefore, it is interesting to use the model: Organization Role Based Access Control (OrBAC) [9] ; This is an access control model focused on the organization and based on first-order logic. It meets all the previously mentioned requirements and adapts perfectly to the context of Facebook. Thanks to OrBAC, friends can be structured by role (friends, friends of friends, family, etc.), actions can be classified by activities (display, publish, etc.) And account owner's data can also be arranged by views (personal information, photos, etc.) [2].

Before suggesting the OrBAC's extension adapted to Facebook, it is essential to assimilate the use of Facebook and master its access control policy to clearly define the problem. In the same logic, this work is focused on the modeling and simulation of the entire policy as it is with the OrBAC model and MotOrBAC [12], software to edit all of the incoherencies detected in the policy, in addition, what the policy offers to the user as access control management features and the user's needs are compared in order to provide a more appropriate access control model using OrBAC and defining contextual rules to manage the policy of a finer way; This will be the subject of my forthcoming work.

II. A Review of Related Works

Few studies have focused on the problem of access control in the context of Facebook. Madejski, Johson and Belovin [13] and Brown, Hewe, Ihbe, Prakash and Borders [14]; used survey to study the main cause of access rights' violations. The results show that access control issues are due to the inability of proper management of privacy settings by the user. Therefore the proposed solution is recommending defensive strategies centered on the user. Masoumzadeh and Joshi [15], made the investigation based on the human aspect, they specifies that the conflicts of the access control policy are related to users owners of a same information, one of them wants to hide it and the other wants to publicize it. The solution was to suggest countermeasures implementation-wise and behavior-wise of the user. However, Yamada, Kim and Perrig [16], and Cheek and Shehab [17], specified that it is the implementation that must be developed to solve access control's problem. Toufik, Cousin, and Cuppens [2], proposed an OrBAC extension to control access into the Facebook context.

III. Preliminaries: Presentation of ORBAC

OrBAC [9], is an access control model based on the organization, using the first-order logic to define relations

between entities and access control policy. That policy is defined on two levels; the abstract one (role, activity, view) and the concrete one (subject, action, object).

A group of active entities is called "organization", each one playing a role within that organization. Therefore, each organization empowers subjects in roles. For example, the organization “faculty" may empower "Mary" in the role of "student". The concept of "role" enables dynamic management of security policy as long as the addition or deletion of a subject does not require a complete change of policy because it's only one relation that will be deleted (relation between this subject and the role). The notation is as following, if org is an organization, s is a subject and r is a role, then Empower (org, s, r) means that org empowers subject s to play the role r.

Every organization has objects representing passive entities. In order to structure the 'objects' entities satisfying a common property, and facilitate the management as mentioned previously, the entity "view" is used. Taking the example of the faculty, the view can for example be "course files", the objects will therefore be "computer courses, English courses, etc". The relation between the two entities is: If org is an organization, o is an object and v is a view, then Use (org, o, v) means that org uses object o in view v.

The entities “actions” define the way in which the subjects access to objects, it can be for example access to reading, writing, etc. The structuring of these entities is called "activities". The same activity can correspond to several actions in different organizations. The relation linking these entities is: If org is an organization, a is an action and a is an activity, then Consider (org, a, a) means that the organization org considers the action a as part of the activity a.

OrBAC also allows activation and deactivation of security rules based on concrete conditions of access called "contexts". Different types of situations exist: default context, temporal contexts, spatial contexts, composed contexts, etc. The used relation is: If org is an organization, s is a subject, a is an action, o is an object and c is a context, then Define (org, s, a, o, c) means that within the organization org, context c is true between subject s, the object o and action a. The context can be for example: Define (Faculty, John, consult, doc1, working_hours) that means that John can see the doc1 only during working hours.

The OrBAC access control policy is defined afterwards based on abstract level entities and presented relations. It consists of permissions, prohibitions, obligations and recommendations linking entities at the abstract level.

Notation is as follows: If org is an organization, r is a role, a is an activity and v is a view, then Permission (org, r, a, v, c) means that organization org allows role r to perform an activity on the view v in the context c.

The transition to the concrete level is done automatically afterwards: if s is a subject, a is an action and o is an object, then Is_permitted(s, a, o) means that the subject s has the permission to perform the action a on the object o. Other privileges Is_prohibited, Is_obligatory, and Is _recommended are defined in the same way.

OrBAC also offers the possibility to simulate and analyze security policies using the MotOrBAC simulator.

IV. Modeling and Simulation of Facebook Access Control Policy

This section presents the modeling of the security policy suggested by Facebook using OrBAC and subsequently the simulation of this policy using MotOrBAC simulator as follows:

Algorithm

Input: Facebook entities and access rules.

Output: security policy incoherencies.

Method:

1) Modeling of security policy with the OrBAC model:

- Inventory of roles (Friends, Family, etc.).
- Inventory of activities (create, consult, etc.).
- Inventory of views (personal_infos, etc.).
- Inventory of access rights (permissions).

2) Simulation of security policy with MotOrBAC simulator :

- Creating organizations (Facebook, U1, etc.).
- Adding of abstract entities (roles, activities, views).
- Adding of concrete entities (subjects, actions, objects).
- Adding of access rights.
- Simulation: Detection of conflicts.

A. The organization

The "Facebook" organization is defined as a central organization, "Users" as a sub-organization of Facebook, and users (accounts' owners) 1, 2, 3 and 4 as sub-organizations of "Users" (Fig. 1).

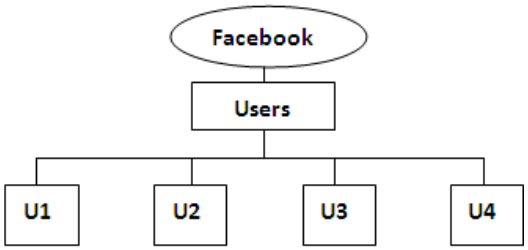


Fig. 1. The hierarchy of organizations

B. Subjects and roles

Roles are defined (what's written in black) at the central organization "Facebook" (Fig.2.), so they can be used by all users (principle of hierarchy). Among the "users" organizations, the organization "U1" is taking as an example, it empowers subjects (what's written in green) in roles that are classified as friends, family, study, etc. The diagram below summarizes all the roles and their hierarchy; associated with

subjects. The relation "empower" should be defined for all subjects and roles. Here is an example: Empower (U1, Alexander, public).

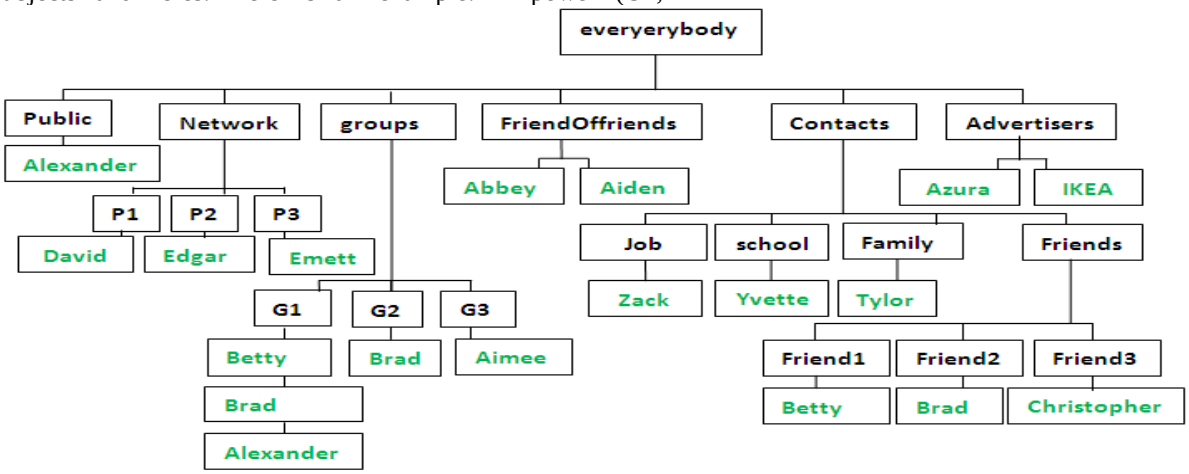


Fig. 2. The hierarchy of roles

C. Activities and actions

Every user in Facebook owns resources (photos, videos, etc.) and is permitted to control the access to these regarding members (friends, etc). Members perform actions like checking his pictures, etc. These actions can be structured in activities, the whole of it is presented in the Table below (TABLE I.):

- The activity "create" for example is an abstraction of the action 'open'.
- "Act.delete" and "modify" are sub-activities of "Act.manage" and associated respectively to actions "remove" and "change".

The relations "consider" has to be defined between all the activities and the actions. For instance: Consider (Facebook, create, open).

TABLE I. THE HIERARCHY OF ACTIVITIES

Activity	Sub-activities	Actions
Activity	Create	Open.
	Consult	View, search, read, see.
	Control_ Access -control_users_Access -control_Face_Access	Allow, oblige, prohibit.
	Publish -Publish_inmywall	Share, illustrate.
	Act.manage -Act.delete -modify	 Remove. Change.
	Organize	Conduct.
	Criticize -Comment -like	 State_opinion. Please.
	compose	Write, introduce.
	Use	Copy, store, archive.
	contact	Send_msg.
	Invite	Add.
	Join	Belong_to.
	Examine	Test.
	Block	Suspend.
	Accept	Approve.

D. Activities and Actions

In an account, many components exist (TABLE II.); photos, videos, personal informations, etc.

The relation between views and objects is defined as following: Use (Facebook, chaimaabelbergui, Full_name).

TABLE II. THE HIERARCHY OF VIEWS

View	Sub-views	Objects
Account (My_account)	About o Personal_infos ▪ Full_name ▪ gender ▪ birth_date ▪ family.situation ▪ political_opinions o Professional_infos ▪ Schooling ▪ Professional_skills ▪ work o View_Contact ▪ Mobile_phone ▪ Email ▪ Address ▪ website	 Chaimaa Belbergui Female March single nothing to report PhD student Nothing to report Nothing to report Number Email_address streetx site
	Parameters	friendRequests.Para notif.Para pub.Para app.Para profile.Para
	Favourites o Publications ▪ Photos -Photo_page -Photos_account Profile_photo Cover_photo Wall_photos ▪ Videos ▪ Status ▪ Comments o Wall o Messages o Friendrequests ▪ friendsOffriends_R ▪ public_R o Event o Identifications ▪ Photos_identif ▪ Status_identif ▪ Videos_identif o Likes o Relationships ▪ RelationU1_U4 o pages	 Photo1_page, photo2_page P_photo C_photo Wall_photo1, wall_photo2 Vidéo1, vidéo2 Statut1, statut2 Comment1, comment2 Journal_Users Message1, message2 R_friend_offriends Conference, travel. Identif_photo1, identif_photo2 Identif_statut1, identif_statut2 Identif_vidéo1, identif_vidéo2 like1, like2 friend Moroccan_cuisine
	Indentifiants o login o password	 Pseudo Pseudo
Groups		Group1, Group2

E. Access control policy

In this section access rights that Facebook (Face) gives to users and also those given by the account's owner to friends, family, etc. are detailed. The privileges are modeled next by OrBAC model.

- Facebook-User policy

Each person is permitted by Facebook to register; but before, he should choose and type his identifiants and some informations like : full name, gender, age, etc. By having an account, the user can exchange messages with friends, publish photos and videos, join groups, create events, etc.

Publications can be managed by the owner, or consulted and criticized by other persons belonging to Facebook.

When some users signal an account, this one cannot more be managed by owner. Facebook delete it automatically.

Here is Access rights:

Permission (Face,Userss,create, account)

Obligation (Face,Users,compose,identifiants)

Obligation (Face,Users,compose,About)

Permission (Face,Users,consult, About)

Permission (Face,Users, Act.manage, About)

Permission (Face,Users, Act.manage, identifiants)

Permission (Face,Users, Act.manage, parameters)

Permission (Face,Users, Act.manage, publications)

Permission (Face,Users, Act.manage, wall)

Permission (Face,Users, Act.manage, message)

Permission (Face,Users, Act.manage, identifiants)

Permission (Face,Users, criticize, publications)

Permission (Face,Users, criticize, wall)

Permission (Face,Users, criticize,events)

Permission (Face,Users, criticize, pages)

Permission (Face,Users, contact, account)

Permission (Face,Users, inviter, account)

Permission (Face,Users, adhérer, Groups)

Permission (Face,Users, publish, publications)

Permission (Face,Users, examine, identifications)

Permission (Face,Users, Accesscontrol, infosperso)

Permission (Face,Users, Accesscontrol, infospro)

Permission (Face,Users,Accesscontrol,viewcontact)

Permission (Face,Users, Accesscontrol,publications)

Permission (Face,Users, Accesscontrol, wall)

Permission (Face,Users, create, pages)

Permission (Face,Users, Act.manage, pages)

Permission (Face,Users, consult, pages)

Permission (Face,Users, accept, friend_requests)

Permission (Face,Users, block, account)

Permission (Face,Users, block, messages)

Permission (Face,Users, block, friend_requests)

Permission (Face,Users, block, events)

Permission (Face,Users, block, pages)

Permission (Face,Users, organize, applications)

Permission (Face,Users, organize, events)

Prohibition(Face,P1,comment,photosmypage)

Permission (Face, P1, comment, photos)

Permission(Face,advertisers,publishinmywall, publications)

Permission (Facebook,G3,consult, account)

Prohibition(Face,P1,Face_AccessControl, publications)

Permission(Face,P1,AccessControl, friend_requests)

Prohibition(Face,P3,AccessControl,profile_photo)

Permission(Face,P3,AccessControl, photos)

Prohibition(Face,P1,Face_AccessControl, publications)

Permission(Face,P1,AccessControl,publications)

Permission(Face,P2, consult, photos_account)

Permission(Face,friend3,publishinmywall,comment)

Prohibition(Facebook,P1,Act.manage,account, signaled_account)

Permission (Facebook,P1,Act.manage, account)

- User-User policy

Each user can manage access to his publications and informations. He can permit or prohibit access to friends, family, public,etc. As follows :

Permission (U1, friends, consult,publications)

Permission (U1, friends, consult, events)

Interdiction (U1, public, consult, publications)

Interdiction (U1, public, consult, events)

Permission (U1, friendOffriend, contact, account)

Interdiction (U1, public, contact, account)

Permission (U1, friends, consult, wall)

Interdiction (U1, public, consult, wall)

Permission (U1, friends, publish, wall)

Interdiction (U1, public, consult, identifications)

Interdiction (U1, friends, consult,personal_infos)

Permission (U1, friends, consult, pages)

Permission (U1, friends, criticize, publications)

Permission (U1, friends, criticize, wall)

Permission (U1, friends, criticize, events)

Prohibition (U1,everybody,consult,relation U1_U4)

Prohibition (U1, friend1, consult, photos)

Permission (U1, G1, consult, photos)

Prohibition (U1, G2, consult, photos)

Permission (U1, G1, consult, photos)

Prohibition(U1,public,consult, photos_account)

Prohibition(U1,P2,consult, photos_account)

Prohibition(U1,friend3,publishinmywall publications)

Prohibition(U1,advertisers,publishinmywall, publications)

Prohibition(U1,public,consult, account)

Permission (U4,everybody,consult,relation U1_U4)

Permission(U2,public, consult, photos_account) .

F. Simulation

The central organization and the sub-organizations are created (Fig.3).Then, all of the abstract entities in the Facebook organization are defined, beginning by roles (Fig.4). The concrete entities are specified in the organization U1 and assigned to the abstract ones. The figure (fig.5.) gives an example of this assignment linking the subjects and the roles. Finally the context "signaled account" is defined (Fig.6.) on which Facebook is based on to delete an account.

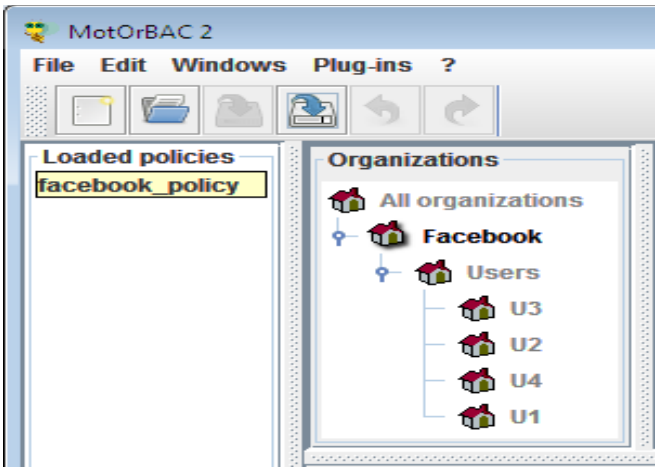


Fig. 3. The definition of organizations

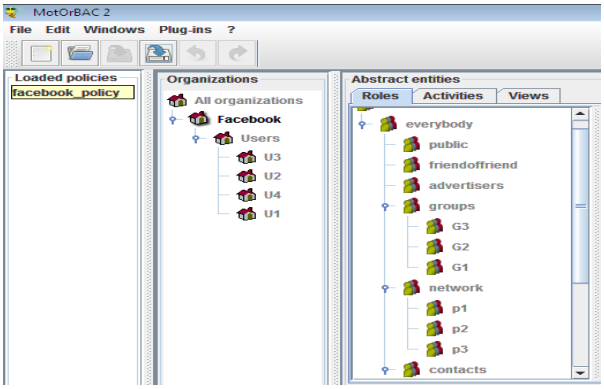


Fig. 4. The definition of roles

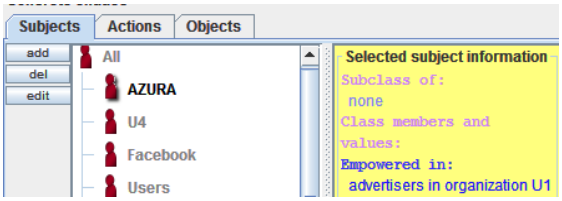


Fig. 5. The definition of subjects and their association to roles

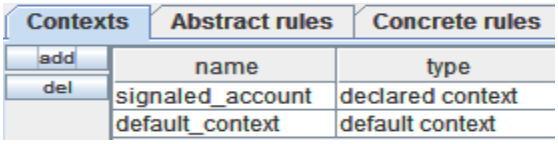
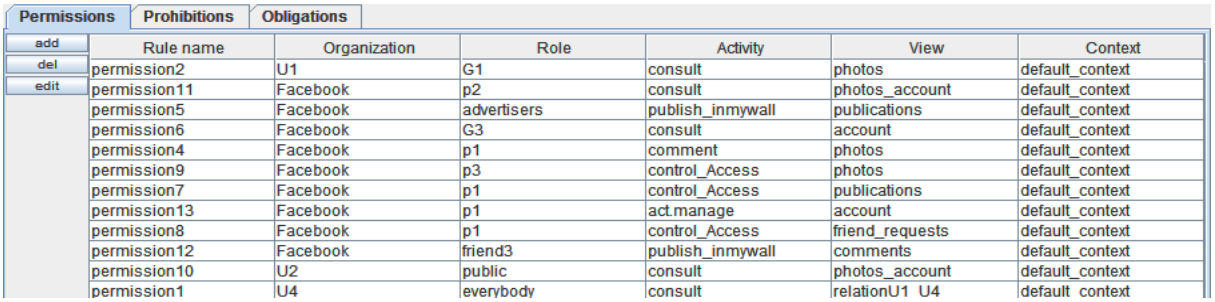
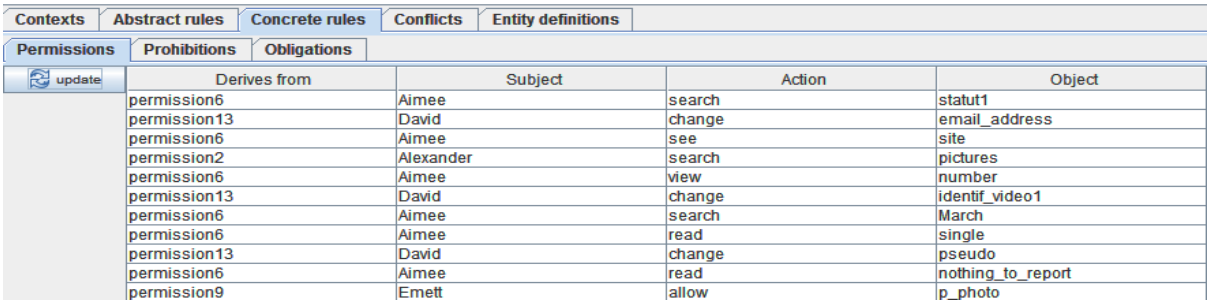


Fig. 6. The definition of the context



Rule name	Organization	Role	Activity	View	Context
permission2	U1	G1	consult	photos	default_context
permission11	Facebook	p2	consult	photos_account	default_context
permission5	Facebook	advertisers	publish_inmywall	publications	default_context
permission6	Facebook	G3	consult	account	default_context
permission4	Facebook	p1	comment	photos	default_context
permission9	Facebook	p3	control_Access	photos	default_context
permission7	Facebook	p1	control_Access	publications	default_context
permission13	Facebook	p1	act.manage	account	default_context
permission8	Facebook	p1	control_Access	friend_requests	default_context
permission12	Facebook	friend3	publish_inmywall	comments	default_context
permission10	U2	public	consult	photos_account	default_context
permission1	U4	everybody	consult	relationU1_U4	default_context

Fig. 7. The definition of permission at the abstract level



Derives from	Subject	Action	Object
permission6	Aimee	search	statut1
permission13	David	change	email_address
permission6	Aimee	see	site
permission2	Alexander	search	pictures
permission6	Aimee	view	number
permission13	David	change	identif_video1
permission6	Aimee	search	March
permission6	Aimee	read	single
permission13	David	change	pseudo
permission6	Aimee	read	nothing_to_report
permission9	Emett	allow	p_photo

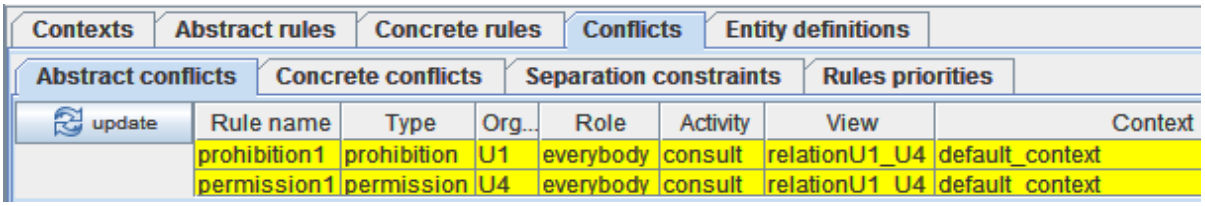
Fig. 8. The generation of permissions at the concrete level

The next step was to define all of the privileges in the abstract level: permissions, prohibitions and obligations that match to the policy of access control used by Facebook (Fig. 7). MotOrbac allows subsequently the automatic transition to the concrete level (Fig. 9) by the "update" tool.

- The detection of coherence

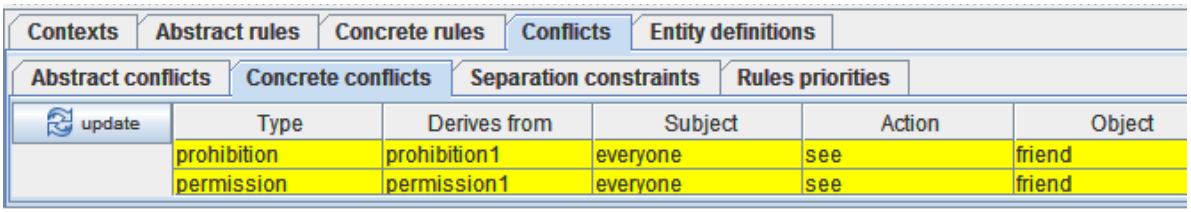
What is interesting about OrBAC is that it allows also to test the policy's coherence to count the conflicts in two levels; the abstract and concrete one.

Results show that 13 conflicts are present at the abstract level, which implies 122 at the concrete level. An example of the conflict is shown at the (Fig.9.) at the abstract level and it's translation to the concrete level (Fig.10.); the figure (Fig.11.) presents more examples of conflicts. By inadequacy of space, only some conflicts are presented.



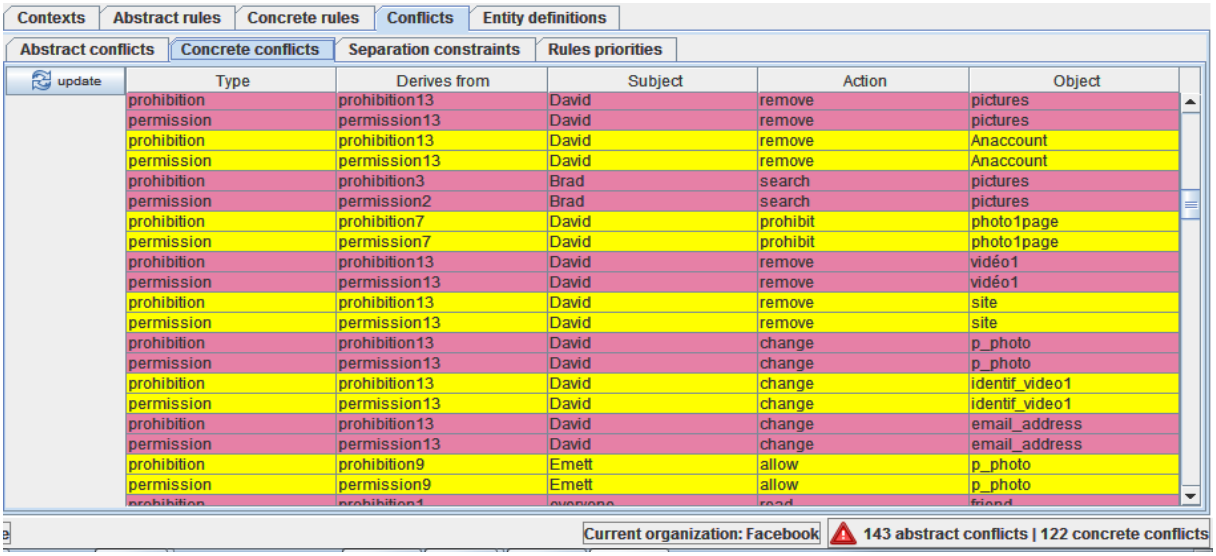
Rule name	Type	Org...	Role	Activity	View	Context
prohibition1	prohibition	U1	everybody	consult	relationU1_U4	default_context
permission1	permission	U4	everybody	consult	relationU1_U4	default_context

Fig. 9. Conflict's detection at the abstract level (between permission 1 and prohibition1)



Type	Derives from	Subject	Action	Object
prohibition	prohibition1	everyone	see	friend
permission	permission1	everyone	see	friend

Fig. 10. Conflict's detection at the concrete level (between permission 1 and prohibition1)



Type	Derives from	Subject	Action	Object
prohibition	prohibition13	David	remove	pictures
permission	permission13	David	remove	pictures
prohibition	prohibition13	David	remove	Anaccount
permission	permission13	David	remove	Anaccount
prohibition	prohibition3	Brad	search	pictures
permission	permission2	Brad	search	pictures
prohibition	prohibition7	David	prohibit	photo1page
permission	permission7	David	prohibit	photo1page
prohibition	prohibition13	David	remove	vidéo1
permission	permission13	David	remove	vidéo1
prohibition	prohibition13	David	remove	site
permission	permission13	David	remove	site
prohibition	prohibition13	David	change	p_photo
permission	permission13	David	change	p_photo
prohibition	prohibition13	David	change	identif_video1
permission	permission13	David	change	identif_video1
prohibition	prohibition13	David	change	email_address
permission	permission13	David	change	email_address
prohibition	prohibition9	Emett	allow	p_photo
permission	permission9	Emett	allow	p_photo

Fig. 11. Detection of conflicts at the concrete level

V. Discussion

The modeling and the simulation of the performed policy in the previous section confirm that the OrBAC model is very suitable to Facebook's context on the one hand, on the other hand they allowed to detail privileges given by Facebook to its users to be very detailed, and also those that every owner can give to his contacts, network, public, (Privacy settings) in order to correctly manage access to informations.

The most interesting is conflicts' analysis that allowed us to count coherence problems that exist in the access control policy defined by Facebook and which block the user to manage the entire privacy features. I sum them up in the following:

Conflicts between permissions and prohibitions defined by the two users:

- Coherence 1 between:

Prohibition (U1, everybody, consult, relation U1_U4)

Permission (U4, everybody, consult, relation U1_U4)

U1 and U4 are in friendship relation. When U1 prohibits to "everybody" to consult this relationship, while U4 allows them the access; that generates a conflict.

- Coherence10 between :

Prohibition (U1, public, consult, photos_account)

Permission (U2, public, consult, photos_account)

The access control to photos is limited because managing who copies them or shares them or even downloads them is impossible, that is why even if U1 does not allow the public to consult his photos, any friend can share them in public way.

Conflicts between permissions of Facebook and prohibitions of the user U1:

- Coherence 5 between :

Prohibition (U1,advertisers, publishinmywall, publications)

Permission(Face,advertisers,publishinmywall, publications)

Even if the user U1 chooses to not publish advertisements on his wall in privacy settings, Facebook obliges him to be contacted by advertisers.

- Coherence 6 between :

Prohibition (U1,public,consult, account)

Permission (Facebook, G3, consult, account)

Even though U1 chose not to be publicly listed in Facebook as soon as he join a group, all members of this group can view his profile and even see his account even if they are not members of his friends. In concrete level Aimee belongs to public, and both of them are members of group 3. Consequently, Facebook permit her to view U1 account.

- Coherence11 between :

Prohibition(U1,P2,consult, photos_account)

Permission(Face,P2, consult, photos_account)

Limiting access control to photos is a main cause of this incoherence. When U1 block someone (P2); Edgar in concrete level, U1 prohibit him to access his profile, his photos, his videos, etc. While, Facebook allows him to access them simply by typing "Photos of U1 full name" in the search bar.

- Coherence 12 between :

Prohibition (U1, friend3, publishinmywall, publications)

Permission (Face, friend3, publishinmywall, comment)

Even if U1 prohibit his friend3; Christopher in concrete level, from posting on his wall, there is another way to do it; it's to post it in a comment. Facebook does not give users the ability to manage "Likes" and "comments" on their publications.

Conflicts between permissions and prohibitions assigned by Facebook to users:

- Coherence 4 between :

Prohibition (Face, P1, comment, photosmypage)

Permission (Face, P1, comment, photos)

Facebook permit P1; David in concrete level, to comment on all his photos and prohibit him to comment it on his page. Actually, when P1 comments a post on his page he does it as a page, not as a person.

- Coherence 7 between :

Prohibition (Face, P1, Face_AccessControl, publications)

Permission (Face, P1, AccessControl, publications)

Facebook allows users (P1 for example) to control access to all of their posts but prohibit them from managing them compared to Facebook.

- Coherence 8 between :

Prohibition(Face,P1,AccessControl, friendsOffriends_requests)

Permission (Face,P1,AccessControl, friend_requests)

Facebook allows users (P1 for example) to choose who can contact them, but forces them to be contacted by friends of friends; which explains the detected conflict.

- Coherence 9 between :

Prohibition (Face, P3,AccessControl, profile_photo)

Permission (Face, P3, AccessControl, photos)

In the same logic, Facebook allows users to control access on all photos, but doesn't give them the same right on the profile picture; it is always public.

- Coherence 13 between :

Prohibition(Facebook,P1,Act.manage,account, signaled_account)

Permission (Facebook, P1, Act.manage, account)

Facebook prohibits users in some cases (signaled account) to manage them accounts while they have the right to do it habitually; which generates a conflict.

Conflicts between permissions and prohibitions assigned to people by the owner of the account U1:

- coherence 2 between :

Prohibition (U1, friend1, consult, photos)

Permission (U1, G1, consult, photos)

When U1 prohibits a friend from viewing photos that he posts; the prohibition is not necessarily taken into account if this friend is a member of one of U1 groups. For example, in concrete level, Betty is prohibited to access to photos in friend context but permitted to do it in group context.

- coherence 3 between :

Prohibition (U1, G2, consult, photos)

Permission (U1, G1, consult, photos)

When U1 allows to the group1 the access to his photos and he prohibit it to group2 knowing that some persons belong to both of the groups that create a conflict; in concrete level Brad belongs to both groups one and two.

As can be seen; Facebook does not suggest any solution to the listed problems and does not meet the needs of users.

Thereby, it is essential to use an access control model more detailed allowing to meet users' requirements.

VI. CONCLUSION

It is indisputable that Facebook continues to expand in all directions. Even though, the management of access control is still very limited compared to the needs of users who often claim problems. This finding is based on modeling and simulation of the security policy adopted by Facebook which have made, these are based on the use of the OrBAC model and MotOrBAC software. To the best of our knowledge, there is the first work that analyses coherence aspect of Facebook security policy.

The conclusion is that several coherences exist in this policy. Also, privacy settings are limited, for example: When user likes the photo of x, it is impossible to prohibit friends of x to see this "like". It is also impossible to make comments from our friends and my family private. Also, user do not necessarily trust the members belonging to the same class (eg. friends) with the same degree. Therefore, they should not have the same privileges; which is impossible on Facebook. Thus, there is no means to manage in a finer way access to resources.

Our next target is to develop a more complete model, suitable to the context of Facebook without incoherencies and that meets most of the requirements expressed by users of this social network.

REFERENCES

[1] A. F. J. G. M. à jour le 31/03/16 16:41, "Nombre d'utilisateurs de Facebook dans le monde." [Online]. Available: http://www.journaldunet.com/ebusiness/le-net/1125265-nombre-d-utilisateurs-de-facebook-dans-le-monde/. [Accessed: 29-May-2016].

[2] B. Toufik, M. E. Cousin, M. F. Cuppens, and M. N. Cuppens, Expression d'une politique de sécurité dans un réseau social, partie 2. Rapport de stage, Telecom Bretagne, 2010.

[3] M. Tremblay, M. Sc. , Analyse des impacts de la mondialisation sur la sécurité - Rapport 9, Septembre 2010

[4] B. Toufik, M. E. Cousin, M. F. Cuppens, and M. N. Cuppens, Expression d'une politique de sécurité dans un réseau social. Rapport de stage, Telecom Bretagne, 2010.

[5] "Facebook," Wikipédia. 29-May-2016.

[6] Y. Estienne, Un monde de verre: Facebook ou les paradoxes de la vie privée (sur) exposée. Lille, France: École supérieur de journalisme de Lille, 2011.

[7] T. Mendel, Étude mondiale sur le respect de la vie privée sur l'Internet et la liberté d'expression. Paris: Unesco, 2013.

[8] R. Ajami, N. Ramadan, N. Mohamed, and J. Al-Jaroodi, "Security challenges and approaches in online social networks: A survey," IJCSNS, vol. 11, no. 8, p. 1, 2011.

[9] A. A. El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miege, C. Saurel, and G. Trouessin, "Or-BAC: un modele de contrôle d'acces basé sur les organisations," Cah. Francoph. Rech. En Sécurité L'information, vol. 1, pp. 30–43, 2003.

[10] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," ArXiv Prepr. ArXiv09032171, 2009.

[11] D. Ferraiolo and D. Richard Kuhn, Role-based access control: features and motivations.Article, 1995.

[12] F. Autrel, F. Cuppens, N. Cuppens-Boulahia, and C. Coma, "MotOrBAC 2: a security policy tool," in 3rd Conference on Security in Network Architectures and Information Systems (SAR-SSI 2008), Loctudy, France, 2008, pp. 273–288.

[13] M. Madejski, M. Johnson, and S. M. Bellovin, "A study of privacy settings errors in an online social network," in Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on, 2012, pp. 340–345.

[14] G. Brown, T. Howe, M. Ihbe, A. Prakash, and K. Borders, "Social networks and context-aware spam," in Proceedings of the 2008 ACM conference on Computer supported cooperative work, 2008, pp. 403–412.

[15] A. Masoumzadeh and J. Joshi, "Ontology-based access control for social network systems," Int. J. Inf. Priv. Secur. Integr., vol. 1, no. 1, pp. 59–78, 2011.

[16] A. Yamada, T. H.-J. Kim, and A. Perrig, "Exploiting privacy policy conflicts in online social networks," CMU-CyLab-12-005 Carnegie Mellon Univ., 2012.

[17] G. P. Cheek and M. Shehab, "Policy-by-example for online social networks," in Proceedings of the 17th ACM symposium on Access Control Models and Technologies, 2012, pp. 23–32.