RBAC in practice v7

Survey goal

You have been approached to participate on this study since you are active in the area of Identity and Access Management. The goal of this survey is to acquire facts and numbers about the use of the Role-Based Access Control (RBAC) model in practice, and it is part of an on-going empirical study conducted by the University of Twente and Novay (Enschede, The Netherlands).

According to our tests, this questionnaire will require a maximum of 30 minutes of your time.

Results can help you as a practitioner either to improve the use of RBAC in your organization, or can help you to learn whether pitfalls of RBAC you experienced in practice are echoed by the experience of other organizations. A summary of the results will be made public.

This survey is anonymous but you will have the choice, at the end, to determine if you would be willing to take part on its follow-up; in this case you must provide your email address.

About RBAC and overall instructions

This figure illustrates the basic feature of RBAC (NIST standard, 2004): the assignment of users to permissions to access information is performed exclusively via roles. We use the term RBAC, and sometimes "RBAC-compatible", in this survey to refer to access control which comply with this basic feature.

The content of this survey is structured in four parts containing questions to achieve the survey goal, preceded by a part containing demographic questions. Each part is composed of a set of closed questions, where you will be asked to select one or more appropriate options from a given list,

plus one optional open question where you will have the opportunity to add free text.

The RBAC model can be used to control access to information in at least:

1. **Support Applications: with coarse grained operating system-specific roles.**
2. **Stand-alone Business Applications: with application-specific roles.**
3. **Enterprise-wide Applications: with roles shared among several applications.**
4. **Cross-enterprise Applications: with roles shared among several enterprises/organizations.**

The four core parts of this survey refer to the above four types of applications. You should answer the questions based on your experience in practice, acquired from the companies you worked for or worked with. Please keep in mind that mandatory questions are marked with a red star.

Feel free to contact organizers of this survey via the emails: FranqueiraV <at> ewi.utwente.nl or N.CondoriFernandez <at> utwente.nl.

About yourself (preliminary)

1.) Do you have experience with RBAC?

( ) Yes (very experienced or experienced or somewhat experienced)

( ) No (not experienced or absolutely not experienced)

2.) Do you have experience with role engineering?

Role engineering is the process of defining and implementing roles.

( ) Yes (very experienced or experienced or somewhat experienced)

( ) No (not experienced or absolutely not experienced)

3.) Do you have experience with role management?

Role management is the process of keeping up-to-date the role structure, the assignment of users to roles, and the assignment of roles to permissions.

( ) Yes (very experienced or experienced or somewhat experienced)

( ) No (not experienced or absolutely not experienced)

About yourself

4.) What is your experience level with RBAC?

( ) Novice

( ) Low Experience

( ) Moderate Experience

( ) Experienced

5.) Your experience with RBAC in years falls within which range:

( ) > 10 years of experience

( ) > 7-10 years of experience

( ) > 5-7 years of experience

( ) > 3-5 years of experience

( ) 1-3 years of experience

6.) Your experience with RBAC comes MAINLY from activities as:

Select one or more most relevant.

[ ] Administrator

[ ] Decision Maker

[ ] Consultant

[ ] Vendor

[ ] Business Application Owner

[ ] Risk Manager

[ ] Information Security Officer

[ ] Developer

[ ] IT Architect

[ ] Requirements Engineer

) If your experience with RBAC did not fall under the activities listed in the previous question, please specify it here.

7.) Your experience with RBAC comes MAINLY from which types of applications:

[ ] Support Applications

[ ] Stand-alone Business Applications

[ ] Enterprise-wide Applications

[ ] Cross-enterprise Applications

8.) Your experience with RBAC comes MAINLY from which industrial sector:

[ ] Government

[ ] Technology

[ ] Finance

[ ] Education

[ ] Commerce

[ ] Health

9.) Your experience with RBAC comes MAINLY from relationship with organizations of which size:

[ ] Multinational enterprises

[ ] Large national enterprises

[ ] Small and medium enterprises

[ ] Government agencies

10.) Please describe briefly your experience with RBAC.

11.) Your experience with role engineering in years falls within which range:

( ) > 10 years of experience

( ) > 7-10 years of experience

( ) > 5-7 years of experience

( ) > 3-5 years of experience

( ) 1-3 years of experience

12.) Your experience with role engineering comes MAINLY from which types of applications:

[ ] Support Applications

[ ] Stand-alone Business Applications

[ ] Enterprise-wide Applications

[ ] Cross-enterprise Applications

13.) Please describe briefly your experience with role engineering.

14.) Your experience with role management in years falls within which range:

( ) > 10 years of experience

( ) > 7-10 years of experience

( ) > 5-7 years of experience

( ) > 3-5 years of experience

( ) 1-3 years of experience

15.) Your experience with role management comes MAINLY from which types of applications:

[ ] Support Applications

[ ] Stand-alone Business Applications

[ ] Enterprise-wide Applications

[ ] Cross-enterprise Applications

16.) Please describe briefly your experience with role management.

PART I

17.) We identified a set of eight relevant features of the RBAC model from theory.
How do you see these features being used in practice for the types of applications you have experience with?

1: Often used
2: Sometimes used
3: Seldomly used
4: Never used
5: Don't know

	Support Applications	**Stand-alone Business Applications**	**Enterprise-wise Applications**	**Cross-enterprise Applications**
F1: Permissions are assigned to users only via	___	___	___	___

roles, never directly to users.				
F2: There is a many-to-many relationship between users and roles.	___	___	___	___
F3: There is a many-to-many relationship between roles and permissions.	___	___	___	___
F4: Users do not need to have all their roles always activated.	___	___	___	___
F5: Users can have more than one role activated at the same time.	___	___	___	___
F6: It is possible to have an overview of all users assigned to a specific role.	___	___	___	___
F7: It is possible to have an overview of all roles assigned to a specific user.	___	___	___	___

F8: Roles can be organized in hierarchies, allowing inheritance of permissions.	___	___	___	___

) From your experience, do you see any other features of the RBAC model in practice?
If so, please mention feature, type of application, and illustrate with an example (if possible).

PART II

18.) This question presents a set of five assumptions of the RBAC model, collected from theory.
To which extent do you agree with these assumptions of RBAC for the types of applications you have experience with?

1: Agree
2: Undecided
3: Disagree
4: Don't know

	Support Applications	**Stand-alone Business Applications**	**Enterprise-wide Applications**	**Cross-enterprise Applications**
A1: Users should not acquire permissions because of individual attributes; they share profiles which determine their	___	___	___	___

roles, for example, based on responsibilities, duties, job functions, qualifications, authority.				
A2: The number of roles is at least an order of magnitude smaller than the number of users to be granted permissions; this means that several users get assigned to a same role.	___	___	___	___
A3: The role structure and the set of permissions assigned to each role are stable, therefore, they change slowly, over a period of time; what changes a lot is the set of users and their assignments to roles.	___	___	___	___
A4: There is agreement about the semantic of roles between those people involved with their	___	___	___	___

engineering and management.				
A5: Users and permissions are known in advance, before the access is evaluated as granted or denied.	___	___	___	___

19.) To which extent do you agree with the following theoretical strengths of the RBAC model in practice, considering the types of applications you have experience with?

1: Agree
2: Undecided
3: Disagree
4: Don't know

	Support Applications	**Stand-alone Business Applications**	**Enterprise-wide Applications**	**Cross-enterprise Applications**
S1: Efficient management of large scale users' permissions, both in terms of time and effort.	___	___	___	___
S2: Effective enforcement of the need-to-know access control principle, achievable by the	___	___	___	___

assignment of users to roles and by the assignment of roles to permissions.				
S3: Simplified auditing of users' permissions for regulatory compliance.	___	___	___	___
S4: Scalable assignment of permissions via inheritance of permissions in roles' hierarchies.	___	___	___	___
S5: Flexible semantics of roles and permissions.	___	___	___	___

) Do you recognize any other important assumption and/or strength of the RBAC model?
If so, please explain the assumption/strength, and relate it to the relevant type of applications.

PART III

20.) To which extent do you agree that each phenomenon below (in italic) reduces the strengths of the RBAC model in practice, considering the types of applications you have experience with?

1: Agree
2: Undecided
3: Disagree
4: Don't know

	Support Applications	**Stand-alone Business Applications**	**Enterprise-wide Applications**	**Cross-enterprise Applications**
P1: In RBAC all assignments of users to permissions need to be granted via roles; *this may give rise to roles with a few members, contributing to the phenomenon called 'role explosion'*.	___	___	___	___
P2: There may be many context-specific attributes which affect users' permissions; *coping with this contributes to the phenomenon of 'role explosion'* .	___	___	___	___
P3: Structuring and managing role hierarchies require a clear understanding	___	___	___	___

of the inheritance of permissions; *lack of this understanding causes unexpected side-effects resulting in under-entitlement or over-entitlement of users*.				
P4: The meaning of roles (in terms of terminology and permissions) across different departments, branches, or business partners has to be shared for RBAC to be effective; *reaching agreements about the semantic of roles may not be trivial, giving rise to interoperability problems* .	___	___	___	___
P5: RBAC is a complex and evolving model which leaves gaps not only at the level of design and implementation but also at	___	___	___	___

conceptual level; *this gives rise to different interpretations of the RBAC model also causing interoperability problems*.				
P6: Changes affecting the assignment of users to roles, and roles to permissions happen frequently; *access management based on roles may become either an overwhelming task or may lead to violations of need-to-know policies*.	___	___	___	___
P7: It may not be known in advance which permissions users should have until the need actually arises, and there are emergency situations which fall outside users' normal roles; *RBAC does not work well with such dynamics*.	___	___	___	___

) Do you see any other phenomenon happening in practice which reduces the strengths of RBAC?
If so, please explain the phenomenon and relate it to at least one type of applications.

PART IV

21.) It is often the case that other access control models are used in organizations, where permissions are not assigned via roles (i.e. outside the RBAC paradigm).
How do you perceive the usage of the RBAC model in practice, compared to non-RBAC models, based on the types of applications you have experience with?

1:RBAC is almost always used
2:RBAC is very much used
3: RBAC is equally used
4: RBAC is very much not used
5: RBAC is almost never used
6: Don't know

	Support Applications	**Stand-alone Business Applications**	**Enterprise-wide Applications**	**Cross-enterprise Applications**
Usage of RBAC	___	___	___	___

22.) Considering only RBAC-compatible applications in use in your organization, how do you perceive the usage of roles hierarchy, compared to its non-usage, for the types of applications you have experience with?

0: Don't know
1:Role hierarchy is almost never used
2: Role hierarchy is very much not used
3: Role hierarchy is equally used

4: Role hierarchy is very much used
5: Role hierarchy is almost always used

	Support Applications	Stand-alone Business Applications	Enterprise-wide Applications	Cross-enterprise Applications
Use of role hierarchy	___	___	___	___

23.) Select the MOSTLY used alternatives to the RBAC model based on the types of applications you have experience with.

	Support Applications	Stand-alone Business Applications	Enterprise-wise Applications	Cross-enterprise Applications
Access Control List	[ ]	[ ]	[ ]	[ ]
Mandatory Access Control (based on security clearance levels, for example, 'top secret', 'secret', 'confidential' or 'unclassified')	[ ]	[ ]	[ ]	[ ]
Attribute-Based Access Control (ABAC)	[ ]	[ ]	[ ]	[ ]
Task-Based Access Control (TBAC)	[ ]	[ ]	[ ]	[ ]
Location-Based Access Control	[ ]	[ ]	[ ]	[ ]

(LBAC)				

) Which other relevant alternatives to the RBAC model or RBAC developments do you recognize as in use in practice? Please relate them to their respective type of applications.

FOLLOW-UP

24.) Would you be willing to participate in a follow-up of this survey, for example, by taking part on another survey or interview?

( ) Yes

( ) No

) Your email is:

_____

25.) Feel free to add any feedback about the survey you think should be considered.

Thank You!

Your survey was successfully completed. Thank you very much for your participation.

Your response is really important to establish the state of practice of RBAC .