Report on the Survey of Role-Based Access Control (RBAC) in practice

Authors: Nelly Condori Fernandez, Virginia N. L. Franqueira, Roel Wieringa

Date: February, 2012

Technical Report nr: TR-CTIT-12-06

University of Twente (the Netherlands)

Contents

Introduction

Since the Role-Based Access Control (RBAC) model was first introduced, it evolved into probably the most discussed and researched access control model in academia [1]. In an earlier literature study, we collected: (a) a set of core features of the RBAC model, according to the ANSI/INCITS 359:2004 RBAC standard [2], (b) implicit assumptions, (c) a set of strengths, and (d) a set of phenomena which may limit these strengths in practice, therefore, representing possible weaknesses. This previous study revealed that RBAC can be used to control access to information in:

- support applications, with operating system specific roles,
- stand-alone business applications, with application-specific roles,
- enterprise-wide applications, with roles shared among several applications, and
- cross-enterprise applications, with roles shared among several organizations.

However, little is known about the extent these **features**, **assumptions**, **strengths** and **phenomena** are recognized by practitioners and important in practice. To acquire insights about these four elements and complement our initial set of strengths and phenomena, a survey was designed by the Information Systems Group from the University of Twente and Novay (http://www.novay.nl/) and launched online between June and July 2011.

Executive Summary

- Respondents of the survey could be clustered in two groups based on location: National (practitioners from the Netherlands) and International (practitioners from elsewhere). However, no significant difference among these groups was observed in respect to the questions related to the RBAC model. Therefore, the analysis reported considers respondents not clustered.

- The majority of practitioners from the National group had more than 5 years experience with RBAC, acquired mainly as consultants and IT architects in large national enterprises from the finance and government sectors. While the majority of practitioners from the International group had 5 or less years of experience with RBAC, acquired also as consultants and IT architects in multinational or large national enterprises from the technology or finance sectors. Regardless of group, respondents had sufficient experience with support applications and cross-enterprise applications. Therefore, we drew conclusions in this report only related to stand alone and enterprise applications (conclusion 5).

- Although the survey results are not statistically significant due to a low response rate, responses allowed us to uncover patterns of RBAC usage and relationships between features, assumptions, strengths and phenomena which weakness some strengths of RBAC. These patterns and relationships appear in the report in the format of conclusions. Some highlights are:

  - Surprisingly, respondents perceived the overall usage of the RBAC model as more *unused* than *used* (conclusion 21).

  - Agreement about the semantics of roles is not trivial, according to respondent's perception about phenomenon P4 (conclusion 18). This is explained by an obtained disagreement with the assumption that there is consensus about the semantic of roles in practice (assumption A4 - conclusion 10), and a low agreement with the flexibility that semantics of roles and permissions can bring (strength S5 - conclusion 15).

  - Role hierarchy which allow inheritance of permissions (feature F8) is seldomly or never used in practice (conclusion 7). This is explained by a high agreement that the inheritance of permission is not well-understood in practice (phenomenon P3 - conclusion 17). No use of role hierarchy is reflected on the low perception of survey respondents about the scalability of permission assignments in RBAC (strength S4 - conclusion 14).

  - Results obtained for features F2 (there is a many-to-many relationship between users and roles) and F4 (users do not need to have all their roles always activated) suggest that the concept of *session*, useful for the activation of different roles by a same user, is not very often used in practice. As a consequence, dynamic separation of duty policies, that constrain session-role assignments, is also not reality in RBAC implementations either (conclusions 1 and 6).

  - Results about feature F1 (permissions are assigned to users only via roles, never directly to users) and about assumption A2 (number of roles is much smaller than the number of users to be granted access) suggest the use of hybrid implementations of RBAC. In fact, several practitioners mentioned in the open questions such hybrid RBAC (e.g., combining RBAC and ABAC) are gaining momentum as a more effective IAM strategy,

1- Methodology

The following venues were used to distribute the survey.

- **LinkedIn Professional Social Network** (http://www.linkedin.com)

  A. Group: Identity & Access Management

  Type of Group: Professional

  Group Objective: The purpose of this group is for all professionals who work within the IdAM business domain, commercial or government, to be able to easily find each other and increase collaboration.

  B. Group: Platform Identity Management Nederland & ECP EPN IdM

  Type of Group: Networking

  Translated Group Objective: This group provides a network for professionals with an interest in identity management and authentication on a national (macro) level for the Netherlands.

- **Mailing Lists**

  C. mail@pimn.nl (Platform Identity Management Nederland - PIMN)

  D. l.trax.nl (internal list from Traxion - Nederland)

Response rate

Potentially, a total of 3801 practitioners were invited to take part on the survey via venues A-D. The actual response rate was 0.74%, calculated based on complete surveys. A survey is considered "complete" when all questions related to the RBAC model were answered. Refer to Appendix A1 for more details.

2- About the Survey Design

The survey consisted of 25 questions, in which 16 questions were related to the demographic characteristics of the respondent practitioners, 7 questions were related to the survey content and 2 questions were related to follow-up and feedback.

Content questions followed a non-trivial table format where we aimed to validate perceived usage and extent of agreement with features, assumptions, strengths and limiting phenomena identified in the previous study, for each type of application (also identified in pre-study). Such tables used Likert scales with four or five points.

The survey combined both closed and open questions. Features, assumptions, strengths and phenomena used in the closed questions are listed next for reference.

- **RBAC features**
  - 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 roles always activated.
  - F5: Users can have more than 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.
- **Assumptions of RBAC**
  - 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.

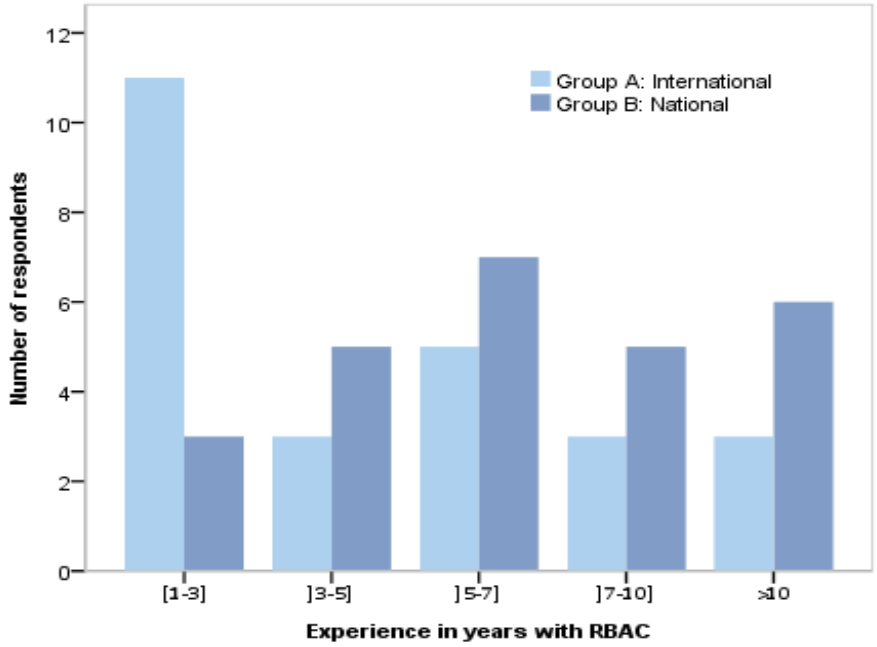
- **Strengths of RBAC**
  - S1: Efficient management of large scale users' permissions, both in terms of time and effort.
  - S2: Effective enforcement of the need-to-know access control principle, achievable by the assignment of users to roles and by the assignment of roles to permissions.
  - S3: Simplified 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.

- **Phenomena in the RBAC context of use which limits its strengths**
  - 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.

3- About the Respondents

3.1 Distribution of respondents per years of experience with RBAC

The analysis of responses for question 5 of the survey is reported in the following graph. It shows two equally representative groups composed of practitioners from the Netherlands (group B – National) and of practitioners from outside the Netherlands (group A – International).



		Group		Total
		A	B	
Experience in years with RBAC	[1-3]	11	3	14
		44,0%	11,5%	27,5%
	]3-5]	3	5	8
		12,0%	19,2%	15,7%
	]5-7]	5	7	12
		20,0%	26,9%	23,5%
	]7-10]	3	5	8
		12,0%	19,2%	15,7%
	>10	3	6	9
		12,0%	23,1%	17,6%
Total		**25**	**26**	**51**

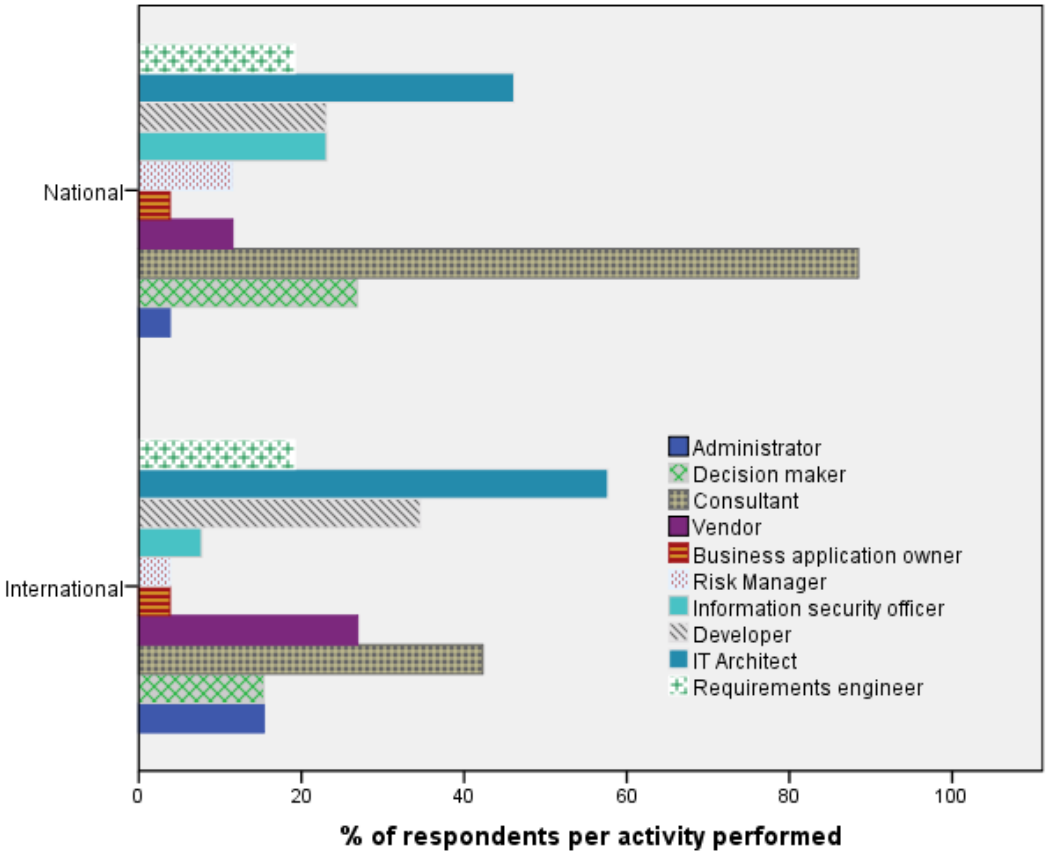
While 69.2% of respondents in the National group (group B) reported to have an experience greater to 5 years with RBAC, 56% of respondents in the International group (group A) reported to have 5 years or less of experience with RBAC.

3.2 Distribution of respondents' experience with RBAC per activity performed

The distribution of responses for question 6 of the survey is shown below. More than one activity could be selected by participants; therefore, responses for each group do not add up to 100%.

Almost 90% of respondents in the National group gained experience with RBAC via consultancy work, while, in the International group, RBAC experience via consultancy amounts to just over 40%. Equally representative in both groups is RBAC experience acquired as IT architect: 46.2% (National group) and 57.7% (International group). The third higher representation among the groups diverge: 34.6% of RBAC experience in the International group comes from development and 26.9% in the National group comes from decision making.

Significant differences among groups are: the representation of RBAC experience as vendor is around 10% in the National group, and almost 27% in the International group; RBAC experience as administrator is insignificant in the International group, but represents over 18% in the National group; and RBAC experience gained as Information Security Officer, while around 5% for the International group, amounts to over 20% in the National group.

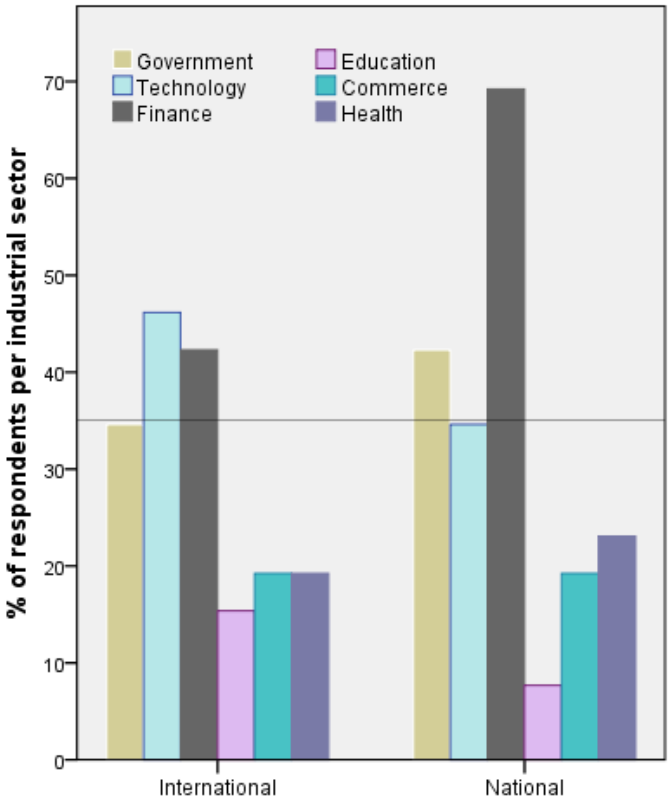


3.3 Distribution of respondents' experience with RBAC per industrial sector

The distribution of responses for question 8 of the survey is shown below. More than one sector could be selected by participants; therefore again, responses for each group do not add up to 100%.

The top three most represented sectors from which respondents acquired experience with RBAC, regardless of group, are government, finance and technology. However, the order in which these sectors appear in the top-three list varied per group; the order for the National group is (1) finance, (2) government, and (3) technology, while the order for the International group is (1) technology, (2) finance, and (3) government. Moreover, for the International group the distribution of these top three sectors is in range of 10%, between 35% (government) to 45% (technology), but for the National group the range is 35%, from 35% (technology) to 70% (finance).

The representation of practitioners' experience acquired from the finance sector in the National group is a positive outlier (70%) and acquired from the education sector is a negative outlier (7,7%).



3.4 Distribution of respondents' experience with RBAC per organization size

The following table relates respondents' declared level of experience with RBAC (question 4) to the size of organizations in which RBAC experience was mainly acquired (question 9), per group.

This table confirms previous graph on years of experience with RBAC (section 3.1) for group B (National). This previous graph showed that 69.2% of respondents in group B had 5 years or more of experience with RBAC. Here, we see that 81% of group B respondents declared themselves as having moderate to high experience (experienced) with RBAC, with predominance for experience acquired with large national enterprises. However, experience gained from government agencies in question 9 (around 15%) contradicts the graph from section 3.3, where the government sector had a representation of 40%+ for the National group B.

For group A (International), respondents declared predominance of experience with RBAC acquired from multinational enterprises. In terms of the level of expertise with RBAC among respondents of group A, respondents claimed equally (around 30%) low experience, moderate experience and high experience (experienced).

Distribution of respondents per company size

Group			Company size				Total
			Multinational enterprise	Large national enterprise	Small and medium enterprises	Government agencies	
A	RBAC experience	Novice	0	0	1	0	1
		Low experience	4	6	0	1	9
		Moderate experience	5	5	0	2	8
		Experienced	7	4	1	3	8
	Total		16	15	2	6	26
B	RBAC experience	Novice	0	1	1	0	1
		Low experience	1	2	0	1	4
		Moderate experience	3	2	0	0	4
		Experienced	9	13	9	3	17
	Total		13	18	10	4	26

4- Analysis of Survey Results

Since no significant difference was found between groups A (International) and B (National) in terms of results obtained (see more on that in Appendix A2), we report our analysis of the survey data in terms of the sample as a whole.

In this section, structured in sub-sections 4.1-4.4, we analyse RBAC features, assumptions, strengths and phenomena in the RBAC context of use in terms of frequency of use (e.g., feature “x” is often used) or in terms of frequency of agreement (e.g., I agree with assumption “y” of RBAC).

4.1 To which extent the RBAC basic features are found in access control mechanisms implemented in practice?

Features F1 to F8 were collected from the Core RBAC and its Hierarchical RBAC extension, described in the ANSI/INCITS 359:2004 RBAC standard. These two components (Core and Hierarchical) become visible in the set of strengths and weaknesses (phenomena observable in RBAC context of use), analyzed sub-sections to follow.

We start with the extremes "never used" (Figure 1) and "often used" (Figure 2) for a pre-analysis of RBAC features. The first graph points to F1, F4 and F8 as high frequency features never used. For features F4 and F8, this seems to be confirmed in the second graph of most often used features, since both have more or less consistently low frequencies there. However, the second graph suggests that the frequency of use for F1 is very sensitive to different types of application. Comparing the frequency of use for F1 among the 4 type of applications, it is most used for stand-alone and enterprise applications.

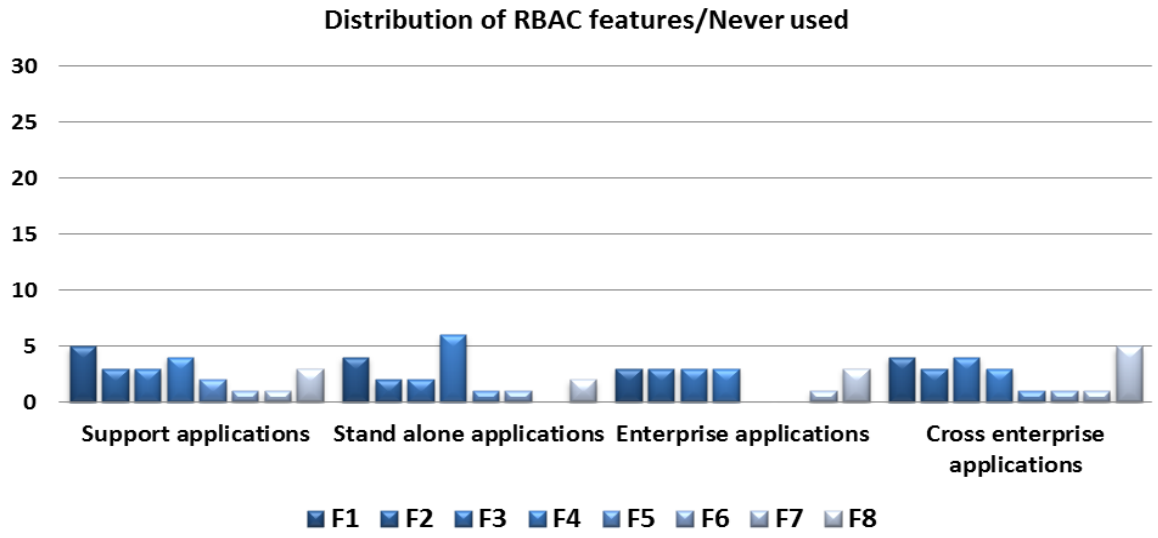


Figure 1. Distribution of features never used per application type

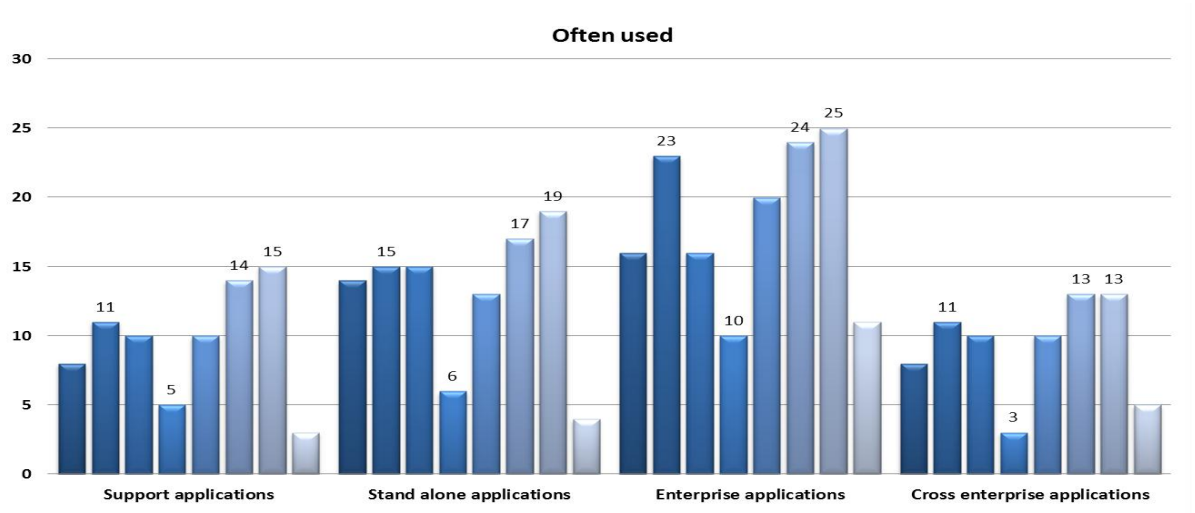


Figure 2. Distribution of RBAC features often used per application type

If we take another perspective and analyze the second graph (Figure 2) of often used features first, the ones which strike as the three most often used features of RBAC are: F2, F6 and F7. When we turn back to the "never used" graph, F2, F6 and F7 really stand out as the least represented features, reinforcing the "often used" graph.

One would expect that feature F3 ("There is a many-to-many relationship between roles and permissions) would follow the same pattern as feature F2 ("There is a many-to-many relationship between users and roles"), since they complement each other and, together, allow the achievement of a many-to-many relationship between users and permissions. It is interesting to notice, however, that respondents had a different perception of usage for both in enterprise applications (only).

From these observations, we draw the following conclusions before we carry on with further analysis of features F1, F2 and F8.

Conclusions

Conclusion 1:

Feature F4 (users do not need to have all their roles always activated) has been reported consistently by the survey respondents as not used in practice. One possible explanation is that users do indeed need to have all their roles activated at all times, suggesting that the concept of *session,* which makes it possible for a user to activate a sub-set of the roles assigned to him, is often absent from RBAC implementations according to respondents.

The inexistence of feature F4 means that an important part of the RBAC flexibility is lost. It also means that dynamic separation of duty policies, that constrain session-role assignments, is not reality in RBAC implementations either.

Conclusion 2:

Basic review functions of the Core RBAC, i.e. features F6 (it is possible to have an overview of all users assigned to a specific role) and F7 (it is possible to have an overview of all roles assigned to a specific user) were consistently indicated by the survey respondents as features of RBAC often used in practice. In fact, these features are fundamental to materialize strength S3 of RBAC (simplified auditing of user's permissions for regulatory compliance) and collect its rewards. We return to this when analysing survey results for strengths of RBAC.

Conclusion 3:

Features F2 (there is a many-to-many relationship between users and roles) and F3 (there is a many-to-many relationship between roles and permissions) were not perceived as having the same pattern of usage by respondents for enterprise applications; F2 was perceived as more used than F3.

Since results indicated F2 as used, i.e., a user can have many roles, the interpretation of the results for F3 suggest a many-to-one relationship between roles and permissions. This would mean that each role would have a single permission only in enterprise applications, and this is very restrictive. To confirm or reject this requires further investigation.

Feature F1: permissions are assigned to users only via roles, never directly to users.

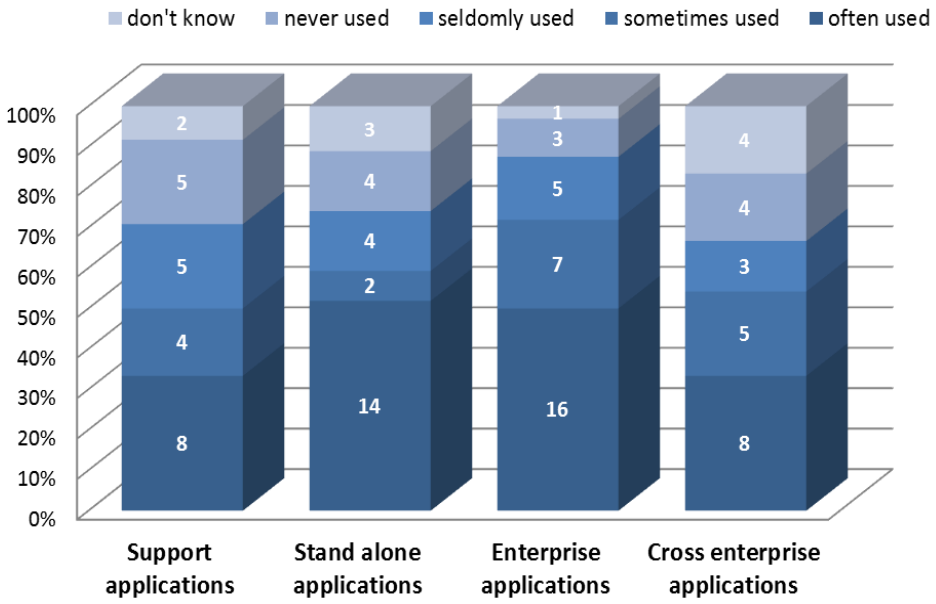


Figure 3. Stacked Bar Chart with distribution of frequency of use for feature F1

As we can see in the Figure 3, 52% of 27 cases affirm that the feature F1 is often used in stand alone applications, although 30% of these 27 respondents perceive it as seldomly or never used. Similar perception was evidenced in enterprise applications (50% of 32 respondents perceived feature F1 as often used) although one quarter (25% of cases) of respondents affirm that the feature F1 is seldomly or never used in this type of applications.

The perception of use in support and cross enterprise applications is the opposite. In both, 42% of respondents (10 out of 24) point this feature as seldomly or never used, while 33% indicate that feature F1 is often used.

This result suggests that only up to half of the practitioners participating in the survey perceive permission in practice acquired strictly via roles. This means that they either see permissions assigned via roles but with the possibility of direct assignments of permissions to users, or they don't see permissions assigned via roles all together. An explanation for the first situation is the fact that role is an informal and frequently used concept often adopted in general terms, not necessarily adherent to the RBAC standard. This result also suggests that support and cross enterprise applications were the types of application where the perception of often used permissions assigned strictly via roles was lower (33%).

Next, we analyze the frequency of use in stand-alone and enterprise applications along with the actual experience of respondents with each one of these two application types, as indicated by answers to question 7.

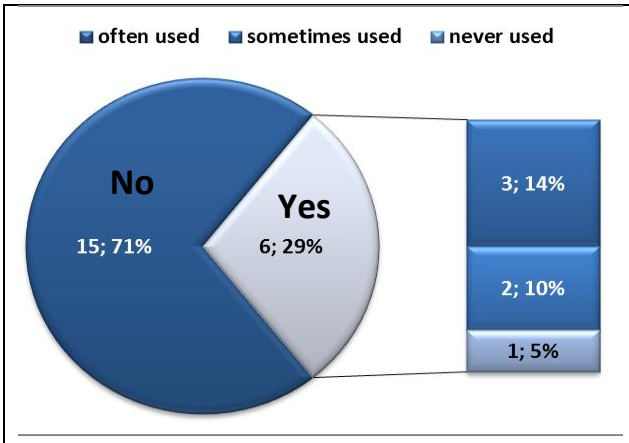


Figure 4(a). Frequency of use of feature F1 by respondents' experience with support applications

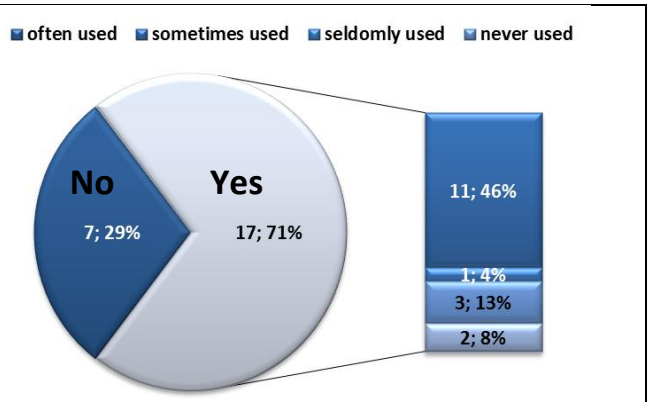


Figure 4(b). Frequency of use of feature F1 by respondents' experience with stand alone applications

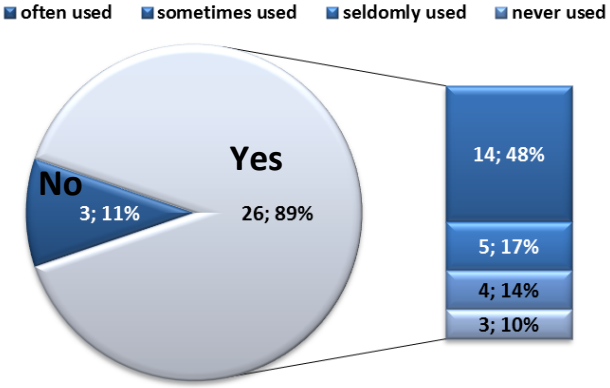


Figure 4(c). Frequency of use of feature F1 by respondents' experience with enterprise applications

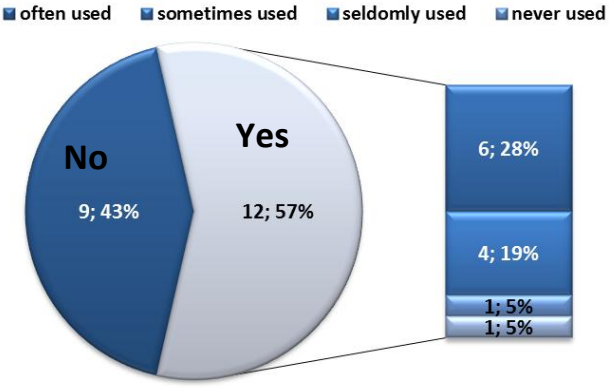


Figure 4(d). Frequency of use of feature F1 by respondents' experience with cross-enterprise applications

Figure 4. Cross-analysis of results for question 7 about experience with RBAC for each type of application against results for question 17 about perception of use for feature F1

The pie charts in Figure 4 show that, based on answered for question 7, respondents' experience with RBAC originated mainly from stand alone applications (71%, 17 out of 24 – figure 4b) and enterprise applications (89%, 26 out of 29 – figure 4c). Just above half of respondents (57%, 12 out of 21 – figure 4d) acquired experience with RBAC from cross-enterprise applications and below one third of respondents (29%, 6 out of 21 – figure 4a) acquired it from support applications.

The stacked bar in each subfigure of Figure 4 show the distribution of perception of use for feature F1 in details, based on answers for question 17. As we can see in these stacked bars, respondents with experience with RBAC selected one of the four options: often used, sometimes used, seldomly used or never used for feature F1. This means that respondents who indicated that they "don't know" the frequency of use of feature F1 are, in fact, part of those respondents without experience with RBAC. This information threatens the validity (relevant sample) of the perception of use for feature F1,

especially for support applications and cross-enterprise applications where the percentage of respondents without experience is significant. Figure 4(a) shows that 71% of respondents did not have experience with RBAC from support applications and figure 4(d) shows that 43% of respondents did not have experience with RBAC from cross-enterprise applications.

Similar analysis for all the other features F2-F8 indicated the same pattern as the one illustrated by the stacked bars in Figure 4 in respect to feature F1. They consistently showed that "don't know" answers for the perception of use of each feature were provided by respondents who indicated no experience with RBAC in a certain type of application; however, those respondents without RBAC experience provided other perceptions as well. This represents a threat to the validity of this survey results especially for support applications and cross-enterprise applications.

Conclusions

Conclusion 4:

Core RBAC feature F1 (permissions are assigned to users only via roles, never directly to users) was perceived as often used in stand alone applications and enterprise applications by 52% and 50% of respondents. However, for enterprise applications a quarter of respondents indicated that this feature is never or seldomly used, and more than a quarter (30%) of respondents indicated this for stand alone applications. Therefore, this result is not very conclusive: half of respondents confirmed that F1 is used in practice but as much as a quarter indicated the opposite. This suggests that hybrid implementations of RBAC (as opposed to pure implementations according to RBAC standard), which combine, e.g., RBAC and ABAC, are often found in practice. Comments collected in the open questions made by several respondents, in fact, confirm that; see item 1 in Section 4.7.

Conclusion 5:

Our respondents sample did not have equal experience with all types of applications where RBAC can be used. A cross analysis of feature F1 against respondents' RBAC experience indicated that too few respondents had sufficient experience with support applications and cross-enterprise applications to conclude anything about the use of RBAC with those applications. We will continue presenting our analysis for all four types of applications, but we will draw conclusions only about stand alone and enterprise applications.

Feature F2: there is a many-to-many relationship between users and roles.

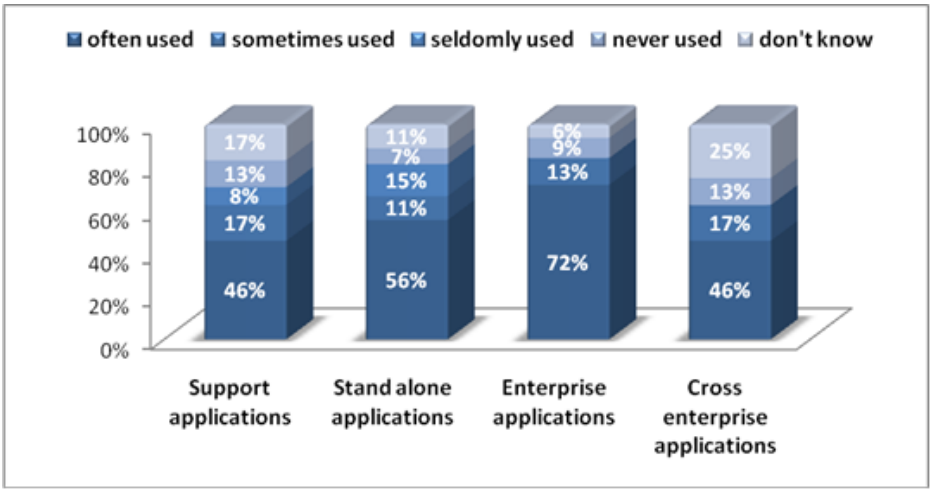


Figure 5. Stacked bar chart with distribution of frequency of use for feature F2

Figure 5 shows the frequency of use for feature F2 in respect to each type of application, as perceived by respondents. Enterprise applications were the type of applications where most respondents perceive feature F2 as most used (72%), and the less respondents perceive it as seldomly or never used (9%). This gap is reduced for stand-alone applications, where 56% of respondents perceive F2 as often used while 22% perceive it as seldomly or never used.

For cross-enterprise and support applications, a significant percentage of respondents (25% and 17%, respectively) indicated they don't know whether F2 is or not often used. This gap between often used and seldomly/never used is more visible in stand-alone applications, where 56% of respondents perceive feature F2 as often used but 22% of respondents perceive it as never or seldomly used. A similar, although less strong, pattern happens with support applications, where 46% of respondents perceive feature F2 as often used while 13% perceive it as never used.

Conclusions

Conclusion 6:

Feature F2 (there is a many-to-many relationship between users and roles) was perceived as often used by 56% of respondents for stand alone applications, but more than one fifth of respondents (22%) perceived it as seldomly or never used. This result suggests restrictive RBAC implementations in practice, in which either a user cannot assume several roles or a role cannot be assigned to several users. Since the second option does not make much sense, the first possibility is probably true. But if users cannot assume more than one role, then the concept of *session*, useful for the activation of different roles by a same user, as defined in the RBAC ANSI/INCITS 359:2004 standard, loses its purpose completely. From the logical truth that single user-role assignments → no session, evidence collected by the survey indicate that the concept of session is not very often used in practice.

Feature 8: roles can be organized in hierarchies, allowing inheritance of permissions.

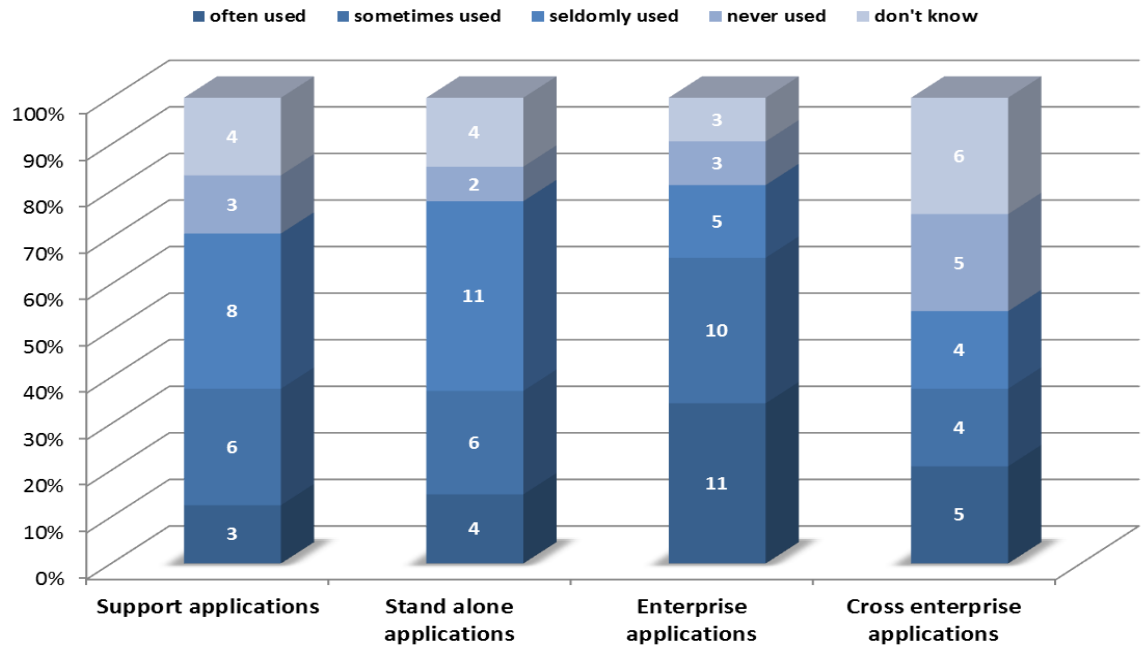


Figure 6. Stacked bar chart with distribution of frequency of use for feature F8

As shown in Figure 6, feature F8 has a high perception rate of seldomly used and never used, according to respondents, with a pick of 48% (13 out of 27) in stand alone business applications, followed by 46% (11 out of 24) in support applications, 37.5% (9 out of 24) for cross-enterprise applications and 25% (8 out of 32) for enterprise applications. Furthermore, it has a low perception rate of often used: 12.5% (3 out of 24) in support applications, 14.8% (4 out of 27) in stand alone applications and 21% (5 out of 24) in cross-enterprise applications. For enterprise applications, although not so low, only 34% (11 out 32) perceive feature F8 as often used.

Conclusions

Conclusion 7:

Feature F8 (roles can be organized in hierarchies, allowing inheritance of permissions) was perceived as seldomly or never used in stand alone applications by 48% of respondents. Only 14.8% perceived F8 as often used in this type of applications.

But if feature F8 is not used, then this means that some strengths of RBAC (e.g., strength S4 - scalable assignment of permissions) will be affected. This is consistent with the frequently observed phenomenon P3 (inheritance of permission is not well-understood in practice) as reported in the literature.

Therefore, from the literature and from evidence collected about F8 in this survey, we expect to confirm survey results about S4 and P3 which confirm the causal relationships: no use of F8 (roles can be organized in hierarchies, allowing inheritance of permissions) → decreased strength S4 (scalable assignment of permissions). Phenomenon P3 (inheritance of permission is not well-understood in practice) explains low use of F8.

4.2- Which assumptions of the RBAC model hold in practice?

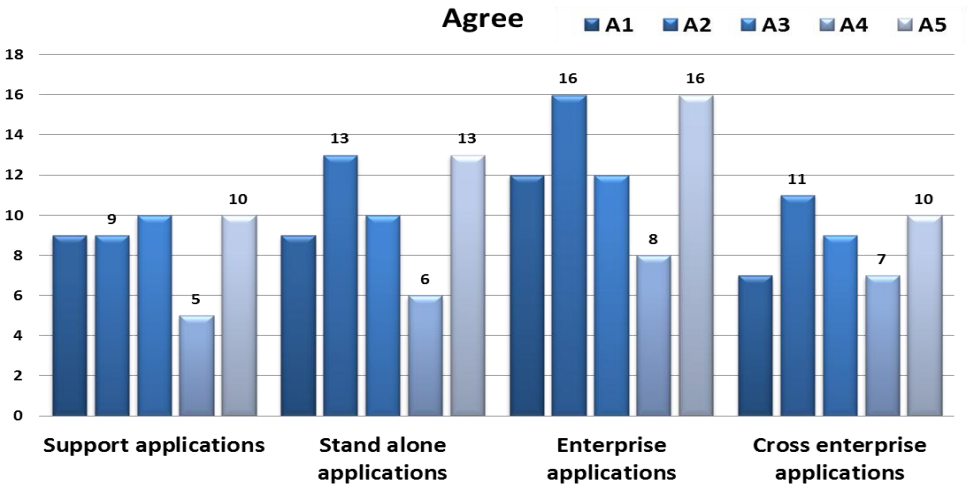


Figure 7(a). Perception of agreement

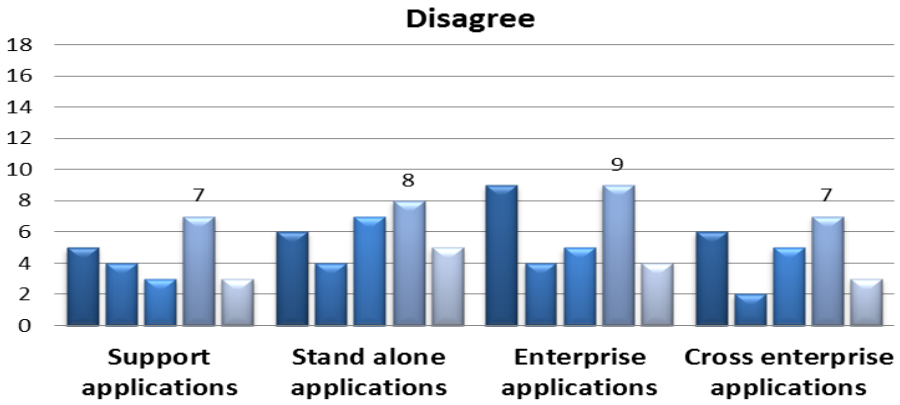


Figure 7(b). Perception of disagreement

Figure 7. Respondents' agreement and disagreement with assumptions A1-A5 by type of application

Figure 7 shows the frequency of agreement and disagreement with assumptions A1-A5, according to respondent's perception. According to figures 7(a) and 7(b), respondents consistently agreed with assumption A2 and A5, i.e., a high frequency of agreement and a low frequency of disagreement across all four types of applications. A2 refers to the assumption which says that there is a much smaller number of roles compared to the number of users to be granted access, and A5 refers to the assumption which says that users' identity and permissions are known in advance, before access is evaluated as granted or denied. Furthermore, respondents consistently disagreed with assumption A4, since the frequency of disagreement was the highest for all four types of application, according to figure 7(b), and the frequency of agreement was the lowest also for all types of applications, according to figure 7(a). Assumption A4 refers to the existence of an agreement about the semantic of roles, therefore, respondents did not think such agreement exist in practice.

Before we have a closer look at responses for assumptions A2, A4 and A5, we draw the following conclusions.

Conclusions

Conclusion 8:

For assumptions A1 (users should not acquire permissions due to individual attributes but based on shared profiles) and A3 (the role structure and permissions assigned to roles are stable), responses indicated an inconsistent frequency among agreement and disagreement.

For A1, this inconsistency is more evident for enterprise applications; agreement was high but disagreement was also high. This suggests that the very basic assumption of the RBAC standard, that users acquire permissions via roles only, may not be a consensus in practice. A probable explanation is the fact that, since *role* is such a widely used term outside the RBAC model, different interpretations of role-based access control exist in practice, not necessarily compliant with the ANSI/INCITS 359:2004 RBAC standard.

For A3, this inconsistency is more evident for stand alone applications where agreement was high and disagreement was also high. This suggests that there is no consensus in practice that either the role structure or the permissions assigned to roles is stable (or both), especially for this type of application. Further investigation is needed to reveal what is the case.

Assumption 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.

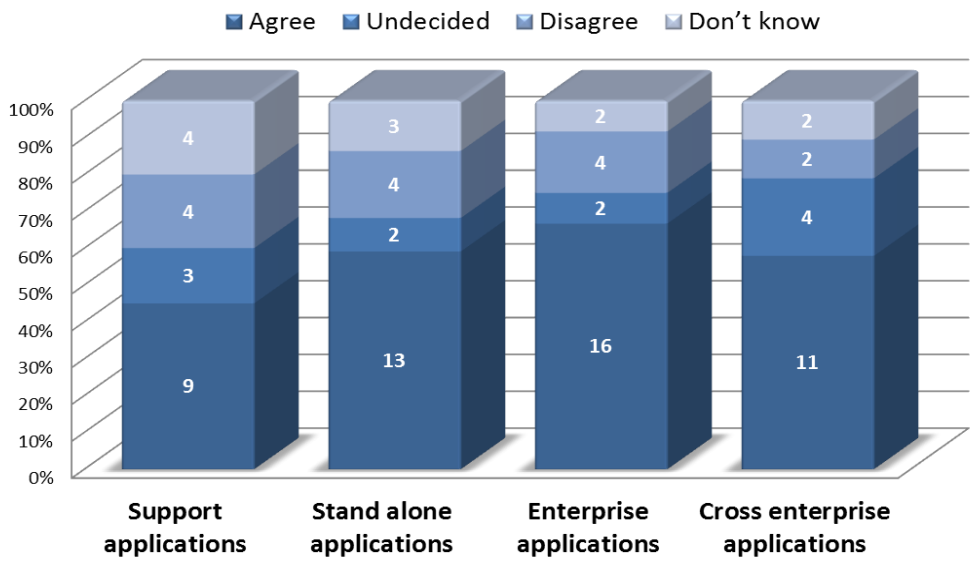


Figure 8. Respondents' agreement and disagreement with assumptions A2 by type of application

Figure 8 shows that the level of agreement with assumption A2 is more evident for enterprise applications, where 67% of respondents agree and 17% disagree with it. For stand alone applications this pattern also happens: 59% of respondents agree and 18% disagree with it. The percentage of undecided or don't know is 17% and 23% respectively for enterprise and stand alone applications. Surprising here is the level of disagreement (around 20%) and the level of undecided/don't know which reaches more than 20% in stand alone applications (23%); we expected this to be much lower since this assumption, together with assumption A1, allows several strengths of RBAC to be achieved, such as strengths S1-S3.

Conclusions

Conclusion 9:

A relatively high percentage of respondents agreed with assumption A2 (number of roles is much smaller than the number of users to be granted access). For enterprise applications agreement reached 67% and for stand alone applications it reached 59%. A relatively low percentage of disagreement was observed for enterprise applications (17%) and stand alone applications (23%), although these percentages are still high, given the fact that some strengths of RBAC depend on this assumption being fulfilled.

An explanation for respondents agreement about A2 in practice would be the use of hybrid implementations of RBAC, which combine, e.g., RBAC and ABAC. Such a hybrid implementation would be a way to fulfil A2 by keeping the number of roles to a manageable size. Inconclusive results obtained for feature F1 (permissions are assigned to users only via roles, never directly to users) suggested the same direction (conclusion 4).

Another possible explanation for respondents agreement about A2 in practice would be that permissions in enterprise applications are not very sensitive to context factors, such as users' individualities, particularities and localities, a sensitivity that normally lead to role explosion. If this explanation was true, we would have observed a low perception about phenomena P1 (individual context factors lead to roles with few members) and P2 (context dynamics impacts user permissions) for enterprise applications. However, evidence from survey responses pointed to an inconsistent result for P1 and P2 (conclusion 16).

Assumption A4: there is agreement about the semantic of roles between those people involved with their engineering and management.

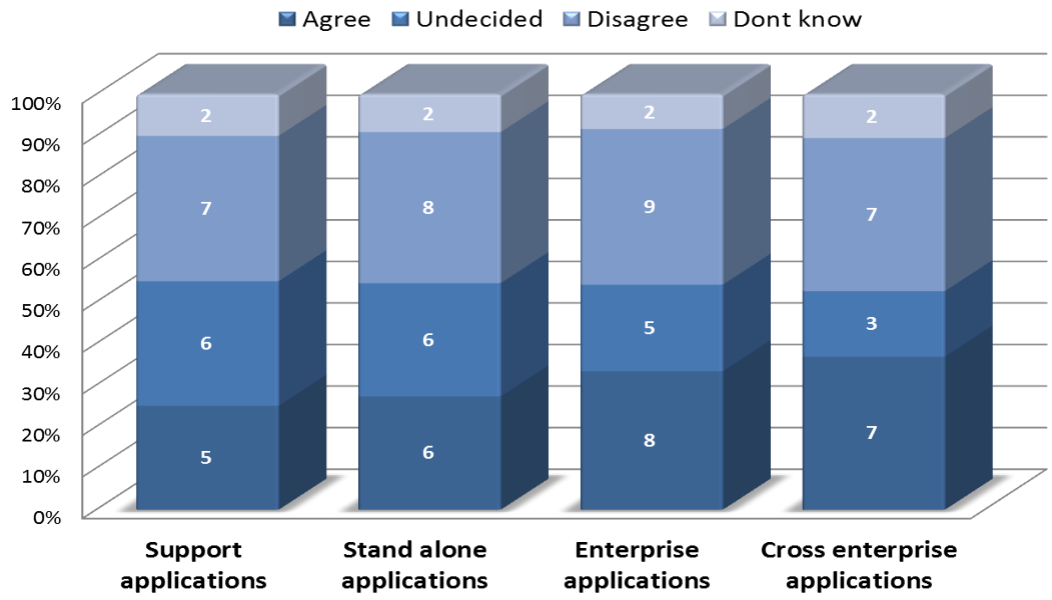


Figure 9. Respondents' agreement and disagreement with assumptions A4 by type of application

Figure 9 shows a very low agreement with assumption A4 among all types of applications, as perceived by respondents: support applications (25%), stand alone applications (27%), enterprise applications (33%) and cross enterprise applications (37%). Consistently, figure 9 also shows a high level of disagreement with A4 , regardless of the type of application: support applications (35%), stand alone applications (36%), enterprise applications (37.5%), and cross enterprise applications (37%).

Conclusions

Conclusion 10:

Respondents consistently disagreed with assumption A4 (there is an agreement about the semantic of roles) probably because this agreement is not trivial in practice. Without this agreement about the semantics of roles, the flexibility it can bring to RBAC implementations (strength S5) cannot be achieved. We will see that the analysis of the responses about S5 is consistent with this.

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

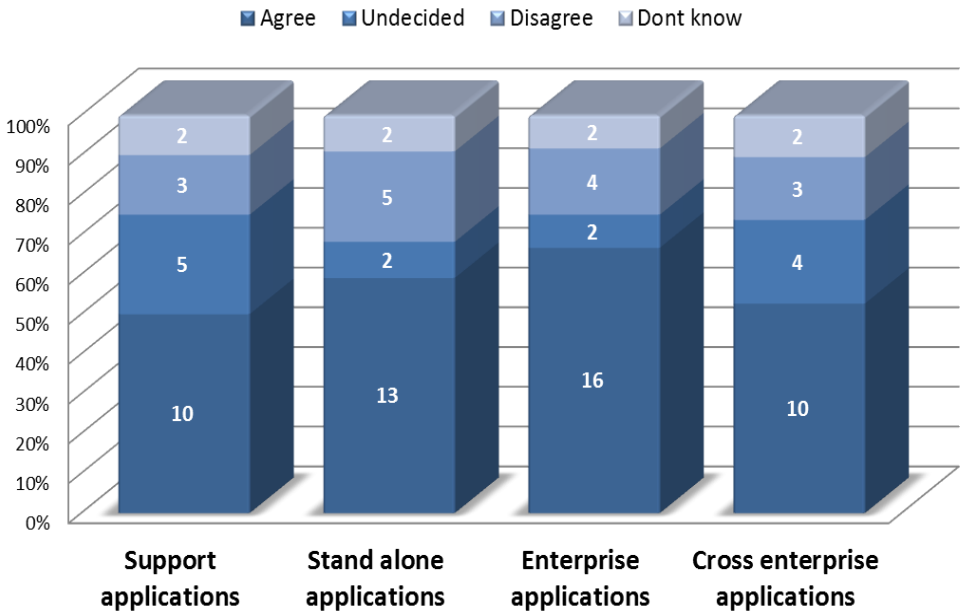


Figure 10. Respondents' agreement and disagreement with assumptions A5 by type of application

Figure 10 shows agreement with assumption A5 along all types of applications. This agreement is most visible in enterprise applications where 67% of respondents agreed and 17% disagreed with A5. For stand alone applications 59% agreed and 23% disagreed, for cross enterprise applications 53% agreed and 16% disagreed, and for support applications 50% agreed and 15% disagreed with A5 as an assumption of RBAC in practice. The lower agreement difference for cross enterprise applications was expected therefore a more interesting result was the higher than 20% disagreement with A5 for stand alone applications since it was expected that owners of such applications had a pretty clear understanding of all roles that users could assume beforehand. A possible explanation might be the multitude of dynamic context attributes, individualities, localities and particularities which interfere with the assignments of users to permissions via known roles.

Conclusions

Conclusion 11:

A consistent high level of agreement with A5 (users and their permissions are known before access is evaluated) as an assumption of RBAC in practice was indicated by respondents. This agreement was more visible for enterprise applications but could be observed for the other types of applications as well.

4.3- Which theoretical strengths of the RBAC model hold in practice?

Figure 11 shows the frequency of agreement and the level of respondents "undecided" about strengths S1 to S5 considering RBAC as defined in the ANSI/INCITS 359:2004 RBAC standard.

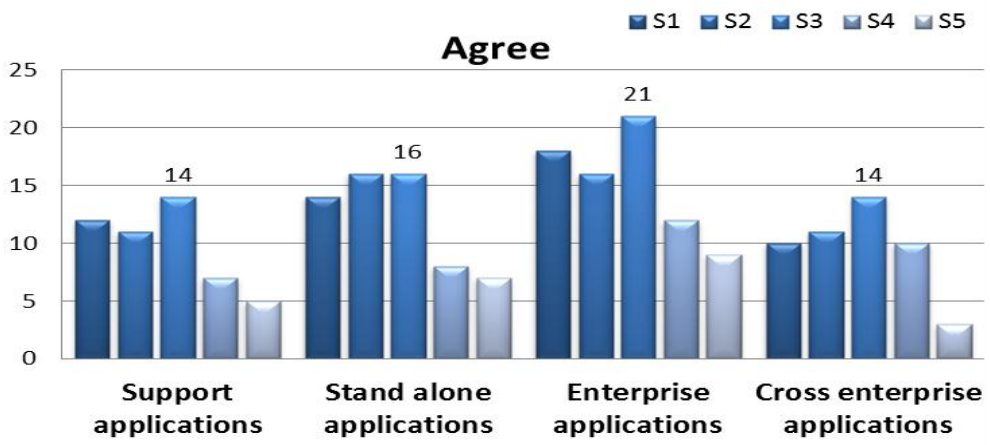


Figure 11(a): Perception of agreement

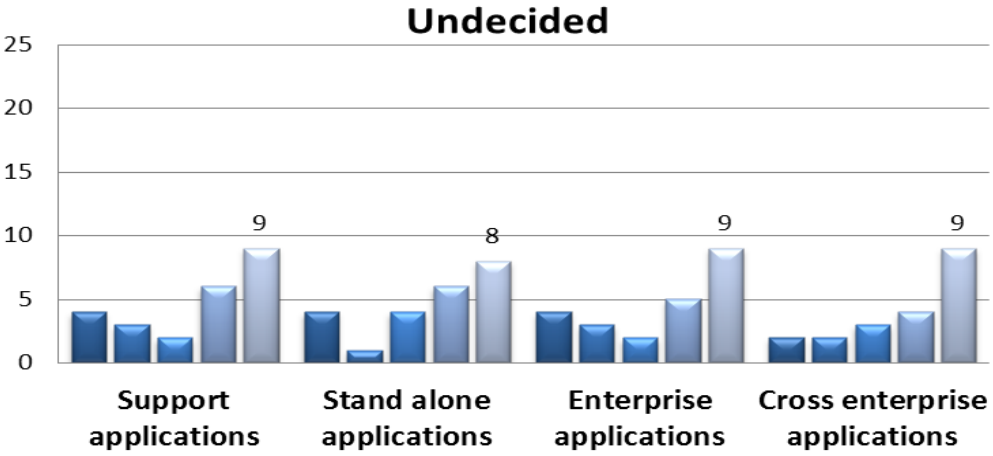


Figure 11(b): Level of indecision

Figure 11. Perception of RBAC strengths S1-S5

According to figures 11(a) and 11(b), strengths S1 (efficient management of users' permissions), S2 (effective enforcement of need-to-know) and S3 (simplified auditing for regulatory compliance) were the ones with higher level of agreement for all types of applications. S3 was the strongest strength recognized in practice. On the other hand, agreement with strengths S4 and S5 were very low and the level of indecision about them was remarkably high.

Before we have a closer look at responses for strengths S3, S4 and S5, we draw the following conclusions.

Conclusions

Conclusion 12:

Respondents consistently indicated agreement with S1 (efficient management of users' permissions) and S2 (effective enforcement of need-to-know) as strengths of RBAC in practice.

Despite a high agreement level with strengths S1 and S2, they are harvested when both RBAC assumptions A1 and A2 are satisfied, i.e., A1, A2 → S1, S2 (refer to reference [3]). From respondents, we obtained a consistently high agreement with A2 (the number of roles is much smaller than the number of users; conclusion 9) for enterprise applications, which enforces this relationship. However, the inconsistent agreement about A1 (no permissions due to individual attributes - users share profiles; conclusion 8) may be an explanation why these percentages obtained for S1 and S2 were not as high as the one obtained for strength S3 or even higher (see analysis for S3 next).

Strength S3: Simplified auditing of users' permissions for regulatory compliance.

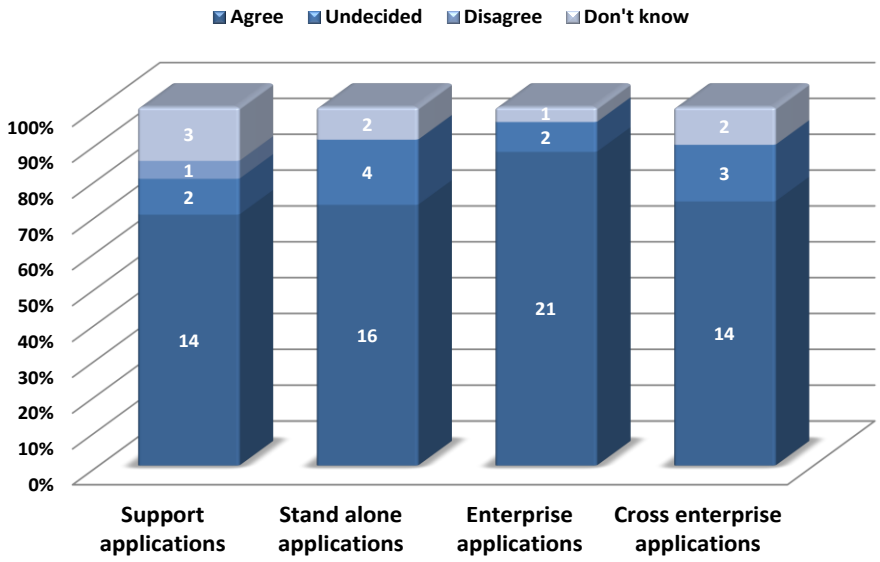


Figure 12. Respondents' agreement and disagreement with strength S3 by type of application

Figure 12 shows an agreement of 70%+ with strength S3 for all types of applications: 70% for support applications, 73% for stand-alone applications, 87.5% for enterprise applications and 74% for cross-enterprise applications. This strength depends on the presence of core RBAC features (F1 to F5) but, most importantly, with the presence of review functions F6 and F7. Therefore, since per conclusion 2, F6 and F7 were recognized as often used in practice, this result is not surprising and just provides an explanation why S3 is achievable. Strength S3 is a very appealing strength of RBAC both for companies to show compliance and to regulatory bodies to demand compliance.

Interesting though was the inconsistency between agreement and disagreement obtained for assumption A1 which is also fundamental for the achievement of strength S3. If users can acquire permissions not always via roles, but also via individual attributes, then features F6 and F7 will not be sufficient to harvest strength S3, and additional review of individual permissions must happen as well.

Conclusions

Conclusion 13:

Agreement about RBAC strength S3 (simplified auditing for regulatory compliance) was confirmed for all types of applications. This was more visible for enterprise applications, and is consistent with results for features F6 and F7 (conclusion 2).

Strength S4: Scalable assignment of permissions via inheritance of permissions in roles' hierarchies.

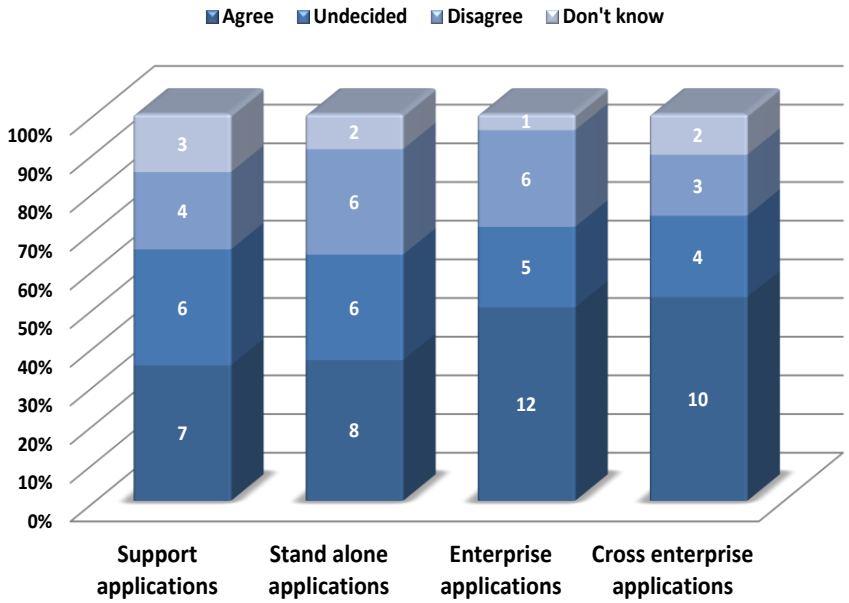


Figure 13. Levels of agreement with strength S4 by type of application

Figure 13 shows a low level of agreement and a high level of disagreement with S4, as strength of RBAC. This is more visible for support applications for which 35% of respondents agreed with S4 while 20% disagreed, for stand alone applications for which 36% of respondents agreed with S4 while 27% disagreed, and for enterprise applications for which half of respondents agreed but one quarter disagreed with S4. Also remarkable is the high level of indecision about this strength (although not comparable with S5 analyzed next), ranging from 21% (for enterprise and cross-enterprise applications) to 27% (for stand alone applications) and 30% (for support applications).

It is interesting to observe that, since feature F8 is fundamental for achieving strength S4 and this was perceived as the most seldomly or never used feature of RBAC by respondents (conclusion 7), we expected that S4 would be the least agreed strength (instead of S5) without a significant level of indecision.

Conclusions

Conclusion 14:

A low level of agreement (53% or less), a high level of disagreement (16% or more) and also a high level of indecision (21% or more) about strength S4 (scalable assignment of permissions via inheritance of permissions in roles' hierarchies) was observed for all types of applications. This can be explained by the fact that this strength only materializes if feature F8 (inheritance hierarchies) is present and, as we saw in conclusion 7, that F8 is seldomly or never used in practice.

Strength S5: Flexible semantics of roles and permissions.

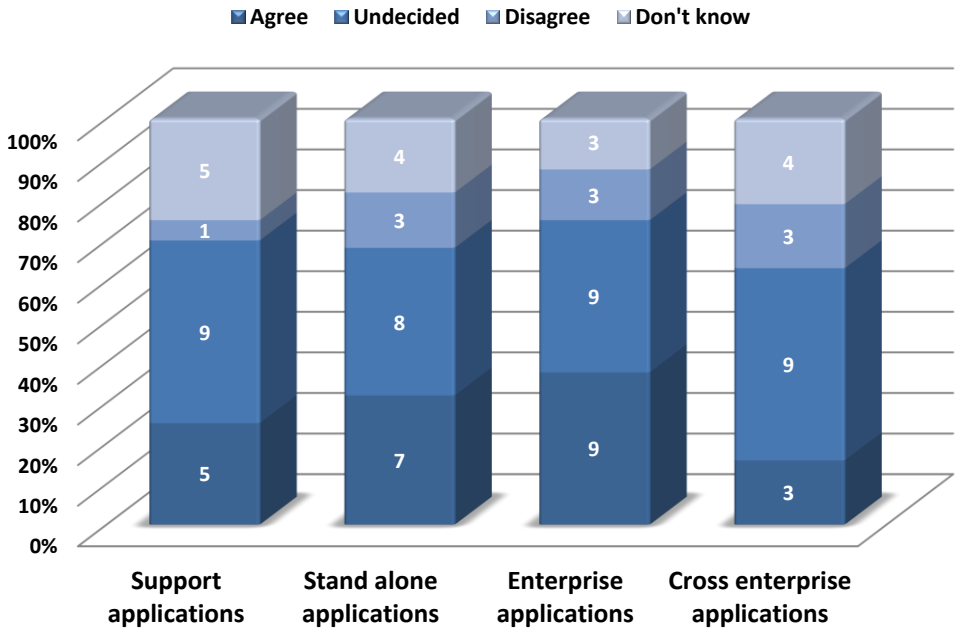


Figure 14. Levels of agreement with strength S5 by type of application

Figure 14 shows a very low level of agreement with S5, as strength of RBAC. Consistently along all types of applications, respondents indicated low agreement and high level of indecision or "don't know": for support applications, 70% of respondents were undecided or didn't know about S5 in practice and only 25% agreed with S5, for stand alone applications, 54.5% indicated they were undecided or didn't know and 32% agreed with S5, for enterprise applications, 50% indicated they were undecided or didn't know and 37.5% agreed with S5, for cross-enterprise applications, 68% indicated they were undecided or didn't know and 16% agreed with S5. This result is consistent with the consistent high level of disagreement with assumption A4 (conclusion 11). If reaching an agreement about the semantics of roles is not trivial in practice (assumption A4) then one cannot expect the benefits derived from this flexibility of roles and permissions (strength S5).

Conclusions

Conclusion 15:

A low level of agreement (37.5% or less) and high level of indecision or "don't know" (50% or more) for strength S5 (flexible semantics of roles and permissions) was observed for all types of applications. This is consistent with the disagreement with assumption A4 (there is agreement about the semantics of roles), per conclusion 10.

4.4- Which phenomena found in practice invalidate or rebut the claimed strengths of the RBAC model?

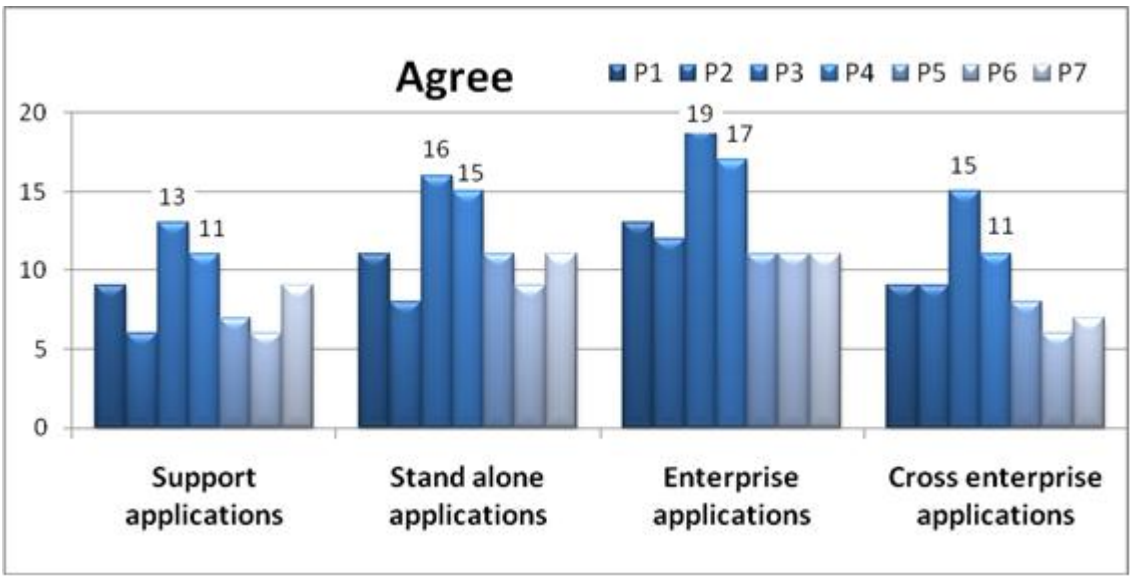


Figure 15 (a): Level of agreement with the phenomena recognized by the respondents

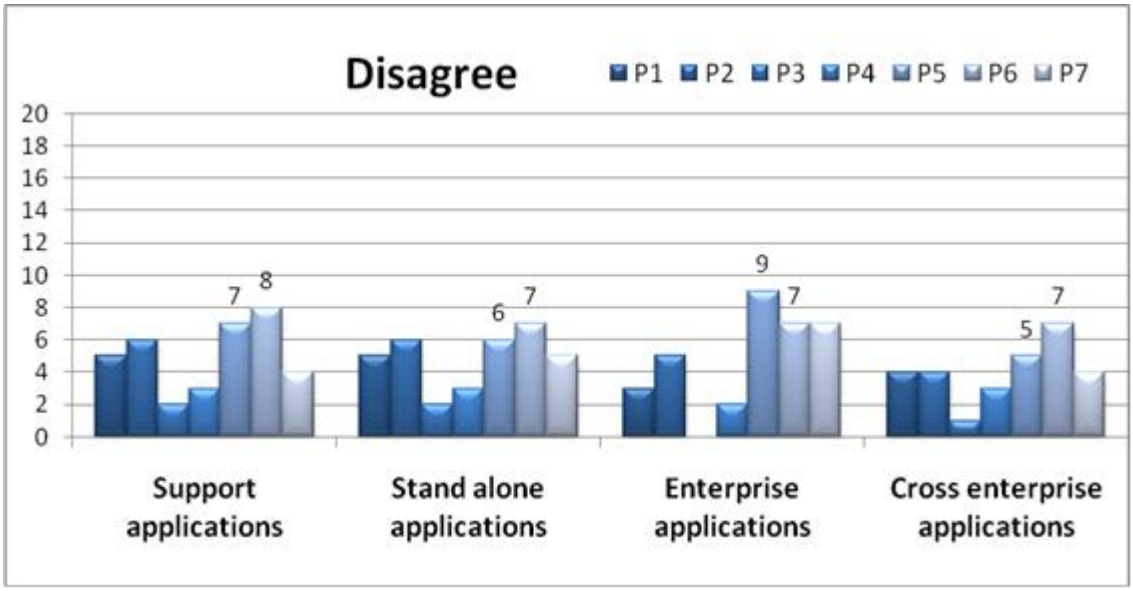


Figure 15 (b): Level of disagreement with the phenomena recognized by the respondents

Figure 15. Perception of phenomena found in RBAC context of use

Figures 15(a) and 15(b) show that respondents consistently agreed with phenomena P3 and P4, as weaknesses of RBAC. For both, respondents indicated a high percentage of agreement and a low level of disagreement.

These figures also indicate a consistent high level of disagreement with phenomena P5 and P6, compared to a relatively low percentage of agreement.

Before we have a closer look at responses for phenomena P3, P4, P5 and P6, we draw the following conclusions.

Conclusions

Conclusion 16:

Responses about phenomena P1 (individual context factors contribute to role explosion), P2 (context dynamics contribute to role explosion), and P7 (it may not be known in advance which permissions users should have and emergency situations may fall outside users' normal roles; rigidity of RBAC does not cope well with modern business dynamics) were in the borderline, with a scattered frequency among agreement and disagreement. A potential inconsistency is clearer for P2 in respect to stand alone and for P7 in respect to enterprise (and cross-enterprise) applications.

P1 and P2 are causes of *role explosion*, and if they happen, then assumptions A1 (users do not acquire permissions due to individual attributes – they share profiles which determine roles) and A2 (the number of roles is much smaller than the number of users to be granted access) are not satisfied. Conclusions 8 and 9 show that total consensus about the truth of A1 and A2 is lacking; our explanation is that P1 and P2 do happen sometimes (but not always).

The observed lack of consensus about phenomenon P7 can be explained in two ways: (i) permissions may not be known in advance and (ii) emergency situations may fall outside users' normal roles. Explanation (i) would violate assumption A5 (users and permissions are known in advance, before access is granted). But respondents consistently agreed with A5 (conclusion 11). So we conclude that the probable explanation is (ii), i.e., RBAC is too rigid to deal with emergency situation. The only way to find out is to investigate this further.

Phenomenon 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.*

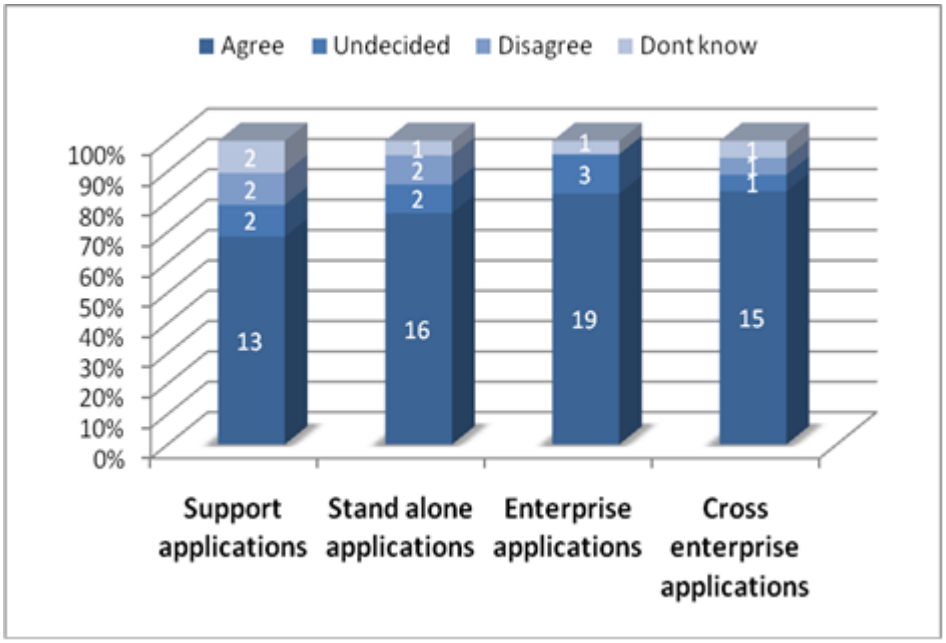


Figure 16. Levels of agreement for the phenomena P3 by type of application

Figure 16 shows a consistent agreement with phenomenon P3.

- Support applications: 68% agreement, 10.5% disagreement and 10.5% undecided;
- Stand alone applications: 76% agreement, 9.5% disagreement and 9.5% undecided;
- Enterprise applications: 83% agreement, no disagreement and 13% undecided;
- Cross-enterprise applications: 83% agreement, 5.5% disagreement and 5.5% undecided.

Conclusions

Conclusion 17:

There is consistent agreement about phenomenon P3 (structuring and managing role hierarchies require a clear understanding of the inheritance of permissions), stronger in respect to enterprise (and cross-enterprise) applications (83%), and stand-alone applications (76%). This result is consistent with conclusion 7.

Phenomenon 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 agreement about this semantic of roles may not be trivial, giving rise to interoperability problems.*

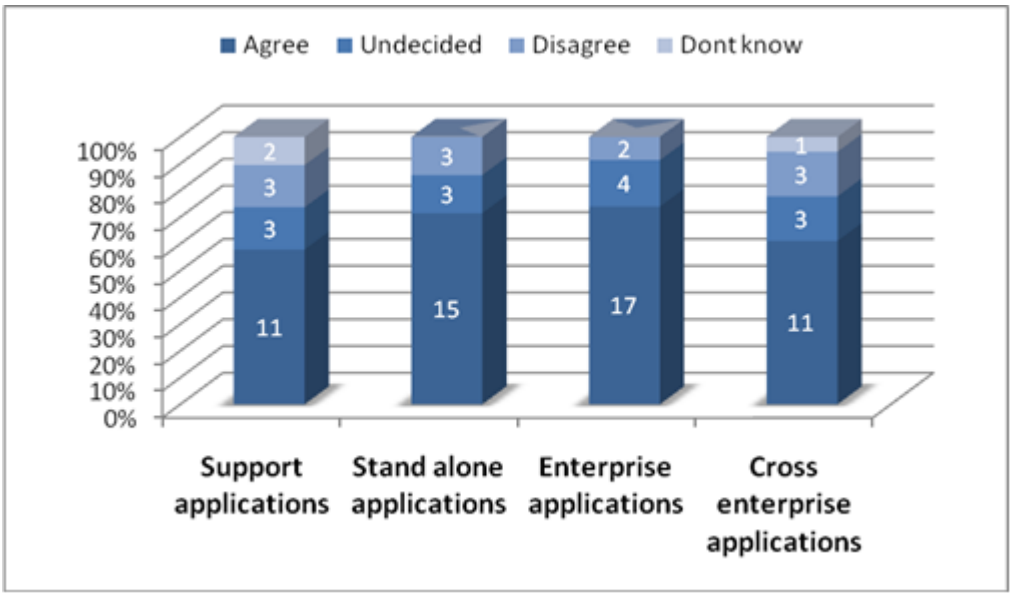


Figure 17. Levels of agreement for the phenomena P4 by type of application

Figure 17 shows a consistent agreement with phenomenon P4, although not as strong compared to P3.

- Support applications: 58% agreement, 16% disagreement and 16% undecided;
- Stand-alone applications: 71% agreement, 14% disagreement and 14% undecided;
- Enterprise applications: 74% agreement, 9% disagreement and 17 % undecided;
- Cross-enterprise applications: 61% agreement, 17% disagreement and 17% undecided.

Conclusions

Conclusion 18:

Consistent agreement about phenomenon P4 (reaching agreements about the semantic of roles may not be trivial) is more visible for stand alone applications (71%) and enterprise applications (74%). This result is consistent with previous conclusions 10 and 15 (high P4 → low A4 → low S5).

Phenomenon 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.*

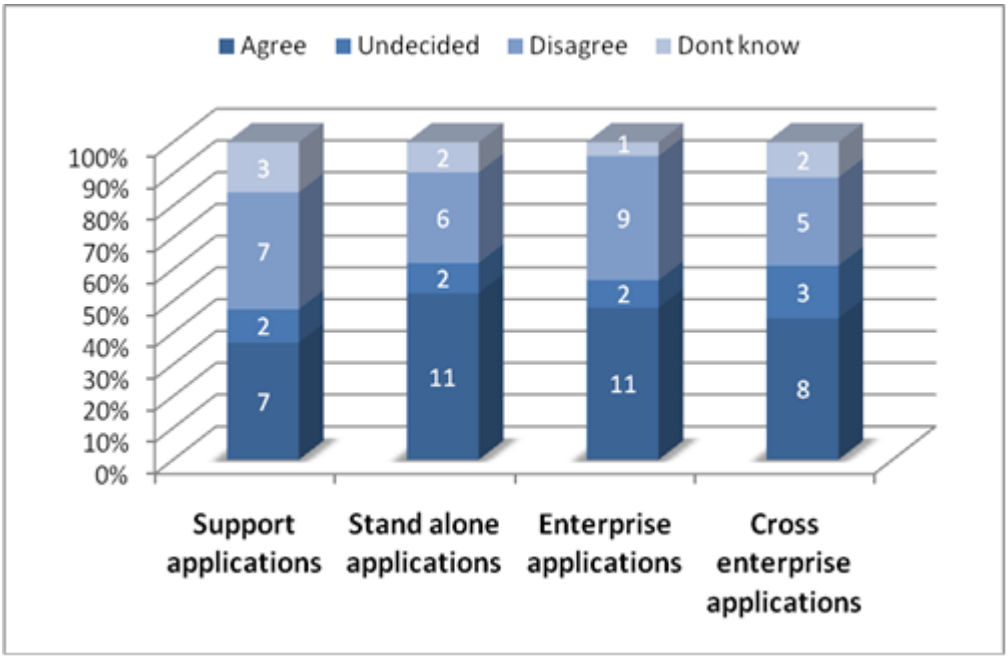


Figure 18. Levels of agreement for the phenomena P5 by type of application

Figure 18 shows a level of agreement below 53% and a level of disagreement above 27% for all types of applications.

- Support applications: 37% agreement, 37% disagreement and 10.5% undecided;
- Stand-alone applications: 52% agreement, 29% disagreement and 9.5% undecided;
- Enterprise applications: 48% agreement, 39% disagreement and 8.7 % undecided;
- Cross-enterprise applications: 44% agreement, 28% disagreement and 17% undecided.

Conclusions

Conclusion 19:

Responses for phenomenon P5 (RBAC is a complex and evolving model which leaves interpretation gaps, potentially causing interoperability problems) showed a consistent low agreement (52% and 48% for stand alone and enterprise applications, respectively) and high disagreement (29% and 39% for the same types of applications). This suggests that, among interoperability issues in RBAC caused by phenomena P4 and P5, the most problematic in practice is P4 (see conclusion 18).

Phenomenon 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*.

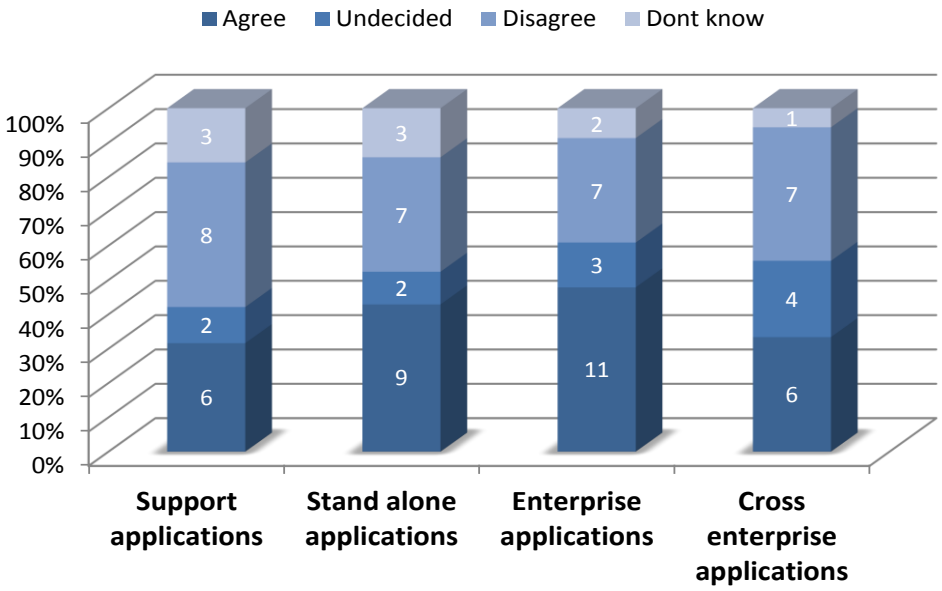


Figure 19. Levels of agreement for the phenomena P6 by type of application

Figure 19 shows a level of agreement below 48% and a level of disagreement above 30% for all types of applications.

- Support applications: 32% agreement, 42% disagreement and 11% undecided;
- Stand alone applications: 43% agreement, 33% disagreement and 10% undecided;
- Enterprise applications: 48% agreement, 30% disagreement and 13% undecided;
- Cross-enterprise applications: 33% agreement, 39% disagreement and 22% undecided.

Conclusions

Conclusion 20:

Responses showed a consistent low level of agreement (43% for stand-alone and 48% for enterprise applications, respectively) and high level of disagreement (33% and 30% for the same types of applications) about phenomenon P6 (frequent changes may cause access management based on roles to become either an overwhelming task or lead to violations of need-to-know policies). Although agreement is higher than disagreement, the gap between them is not enough to draw conclusions.

4.5- 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?

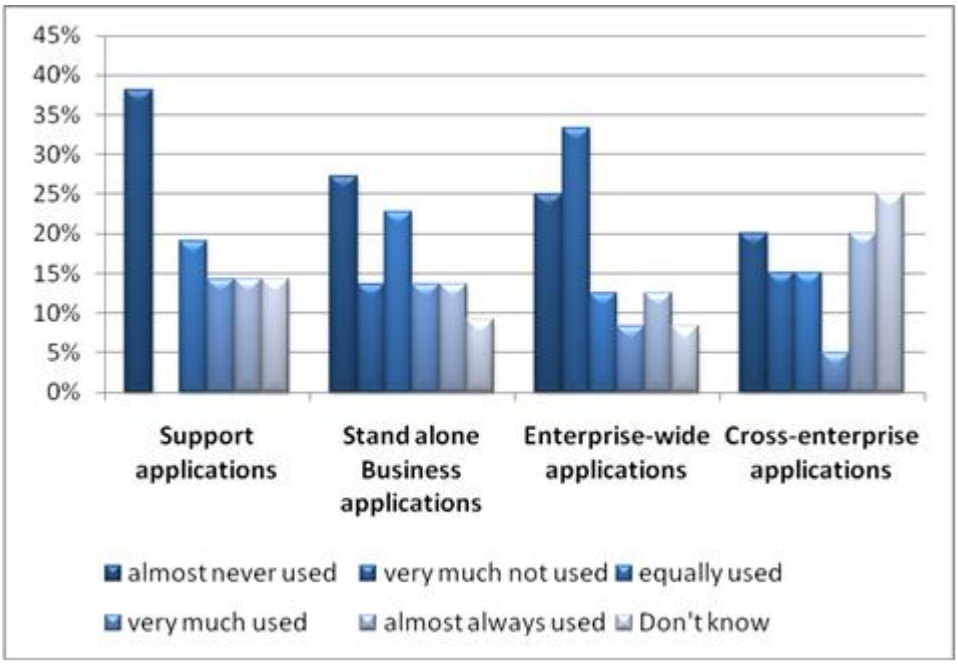


Figure 20. Perception of usage of the RBAC model in practice

The analysis of figure 20 resulted in the percentages shown in table 1.

	Almost never used	Very much never used	Equally used	Very much used	Almost always used	Don't know
Support applications	38%	0%	19%	14%	14%	14%
Stand alone applications	27%	14%	23%	14%	14%	9%
Enterprise applications	25%	33%	13%	8%	13%	8%
Cross-enterprise applications	20%	15%	15%	5%	20%	25%

Table 1. Perceived usage of the RBAC model in percentages

Per table 1, we see that the percentages of answers “don’t know” were higher for support applications (14%) and cross-enterprise applications (25%). This is coherent with conclusion 5 since respondents indicated more experience with stand alone and enterprise applications.

Table 1 also shows that practitioners perceived the RBAC model as more unused than used in practice. By grouping “almost never used” with “very much never used” as an indication of *unused*, and “very much used” with “almost always used” as an indication of *used*, we have the following.

- Stand alone applications: 41% unused and 28% used;
- Enterprise applications: 58% unused and 21% used.

Conclusions

Conclusion 21:

Responses about the perceived usage of the RBAC model in practice indicated a surprising *unused* rate higher (41% for stand alone applications and 58% for enterprise applications) than the *used* rate (28% and 21%, respectively). Previous conclusions put this observation in perspective.

4.6- How do you perceive the usage of roles hierarchy, compared to its non-usage, for the types of applications you have experience with?

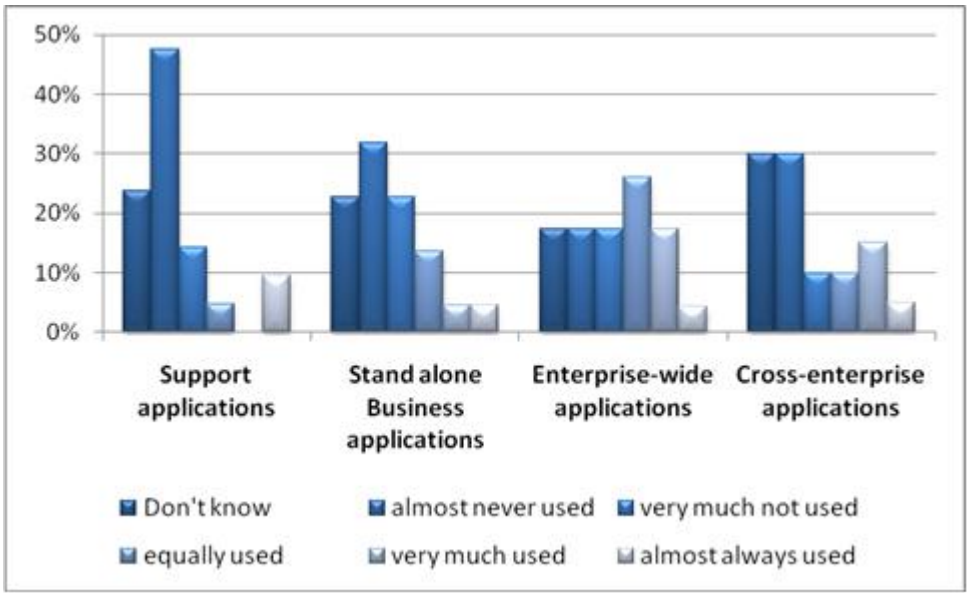


Figure 21. Perception of usage of roles hierarchy in practice

The analysis of figure 21 resulted in the percentages shown in table 2.

	Almost never used	Very much never used	Equally used	Very much used	Almost always used	Don't know
Support applications	48%	14%	5%	0%	10%	24%
Stand alone applications	32%	23%	14%	5%	5%	23%
Enterprise applications	17%	17%	26%	17%	4%	17%
Cross-enterprise applications	30%	10%	10%	15%	5%	30%

Table 2. Perceived usage of roles hierarchy in percentages

Table 2 shows that roles hierarchy is perceived as highly unused for all types of applications. This is corroborated with the also high percentage of "don't know" responses regardless of the type of applications (between 17% and 30%). Performing the same grouping as we did for the previous question (section 4.5) to partition the responses in terms of *unused* and *used*, we obtain the following.

- Support applications: 62% unused and 10% used;
- Stand alone applications: 55% unused and 10% used;
- Enterprise applications: 34% unused and 21% used;
- Cross-enterprise applications: 40% unused and 20% used.

Conclusions

Conclusion 22:

Responses about the perceived usage of roles hierarchy in practice were consistent with previous conclusion 7 about feature F8. The gaps between *unused* and *used* rates for all types of applications were significant. For example, for stand alone applications the difference was 45% between the perception of *unused* (55%) and the perception of *used* (10%).

As for conclusion 7, it showed that the practice of flat roles prevails in practice, suggesting that the benefits that a hierarchical structure may bring (e.g., strength S4) are not enough to overcome its complexity (e.g., phenomenon P3).

4.7- Results from open questions

This list summarizes free-text comments obtained from the survey open questions.

1. Several practitioners mentioned that, in practice, a hybrid approach mixing RBAC and ABAC (Attribute-Based Access Control) is gaining momentum as a more effective IAM strategy.

   In fact, the new RBAC model will take this direction (see our recent publication [3]) to overcome some of the phenomena we used in the survey. This is consistent with conclusions 4 and 9.

2. Several practitioners mentioned the features Static Separation of Duty and Dynamic Separation of Duty as additional features of RBAC.

   We acknowledge them and thank to respondents for pointing this out; these are the features of constrained RBAC. We decided not to include them since our list of features was already quite long.

3. Some practitioners mentioned that as long as – every user has only one role –, RBAC works.

   This is an amazing restriction; it is hard to understand how it can be practical. However, it is consistent with results obtained by the survey about feature F2, summarized in conclusion 6.

4. Several practitioners mentioned the need to allow users to acquire exceptional permissions, outside their roles. However, they all pointed out that exceptions should be logged and the persons responsible for authorizing them should be clearly identified for auditing.

   This looks like a combination of RBAC and audit-based access control. Our paper [3] also mentions this as a solution direction for dealing with phenomenon P7.

5. Some practitioners mentioned that the enormous effort required for designing the role structure and populating role data as an inhibitor of RBAC.

6. Some practitioners mentioned the need to educate asset owners to cope with complexities of RBAC theory and role design.

7. Some practitioners mentioned the need of delegation to easy maintenance of the role structure and role assignments. The suggestion was to creating of an Application Owner Role for every application. Users assigned to that role would be able create new permissions.

8. Some practitioners mentioned that technical (IT) role names need to be translated to business role names for asset owners to understand them. A solution to this problem, suggested by another practitioner, is to design a role structure based on a business model.

Note

We ignored responses to question 23 (about most used alternatives to RBAC) because respondents identified a problem with the question itself.

References

[1] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 1st ed. John Wiley & Sons, Inc., 2001.

[2] ANSI/INCITS 359:2004, “Information Technology - Role Based Access Control,” American National Standards Institute (ANSI), International Committee for Information Technology Standards (INCITS), February 2004.

[3] V. N.L. Franqueira and R. J. Wieringa, “Role-Based Access Control in Retrospective”, Computer (in-press), IEEE. January 2012. Available online via IEEE Xplore

Appendix A

A1- More information about the response rate

An overlap of 100 subscribers of the PIMN mailing list, estimated to be also part of the EPC EPN LinkedIn group, was considered in the calculations of the response rate, as shown below.

Distribution venues*	Invited	Responses	% response per venue
LinkedIn: Identity & Access Management	2885	12	0.004159
PIMN mailing list	355	12	0.033803
LinkedIn: PIMN & ECP EPN idM	626	1	0.001597
Taxion mailing list	35	3	0.054545
Total without estimated overlap	3901	28	0.094105
Overlap	100	-	-
Total with estimated overlap	3801	28	-
Response rate	**0.736648 %**		

* We also launched the survey in the LinkedIn group "Identity and Access Management (IAM)". However, since we had none respondents, this venue were ignored.

We had a high rate of partial responses which were discarded in the analyses described in section 4 of this report (refer to table below). The reason why this happened was not evident during the analysis of responses. However, the complexity of questions related to RBAC features, assumptions, strengths and phenomena might have put off many participants who started the survey all right but felt it became too time consuming to evaluate table-like questions with many items to evaluate. In fact, this survey was really more complex than the average surveys, and we would like to warmly thank those who completed it from start to end!

Survey completion	Number of respondents
Complete responses	28
Partial responses	81
Total	107

A2- Why respondents grouping into National and International were ignored in the analysis of results

Applying a chi-square test, shown in the following table, we corroborated that there is no significant difference in the frequency with which both groups (International and National) report their experience level with RBAC. This is because the value obtained (0,142) is higher than conventional criteria for statistical significance (0.001–0.05).

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6,888	4	,142
Likelihood Ratio	7,205	4	,125
Linear-by-Linear Association	4,557	1	,033