Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Μοντέλα Ελέγχου Πρόσβασης και Υλοποίηση RBAC με Ενσωμάτωση Χρονικών Περιορισμών στο Περιβάλλον των Windows**
Ονοματεπώνυμο Φοιτητή	**Καλλιάνη Ευαγγελία του Νικολάου**
Αριθμός Μητρώου	**ΜΠΣΠ08008**
Ονοματεπώνυμο Φοιτητή	**Ξέρα Αθανασία του Δημητρίου**
Αριθμός Μητρώου	**ΜΠΣΠ08007**
Κατεύθυνση	**Δικτυοκεντρικά Πληροφοριακά Συστήματα**
Επιβλέπων	**Χρήστος Δουληγέρης, Καθηγητής**

Ημερομηνία Παράδοσης **Οκτώβριος 2010**

Τριμελής Εξεταστική Επιτροπή

Χρήστος Δουληγέρης Καθηγητής	Χαράλαμπος Κωνσταντόπουλος Λέκτορας	Παναγιώτης Κοτζανικολάου Λέκτορας

ΠΕΡΙΛΗΨΗ

Κοινή απαίτηση όλων των σύγχρονων πληροφοριακών συστημάτων είναι η προστασία της πληροφορίας κατά τη διακίνησή της μέσα σε αυτά. Ο έλεγχος πρόσβασης απαιτεί την ύπαρξη μιας σειράς μηχανισμών που εξασφαλίζουν την ακεραιότητα, την εμπιστευτικότητα και την εξουσιοδότηση. Στην παρούσα μεταπτυχιακή διατριβή παρουσιάζονται οι Βασικές Αρχές Ασφάλειας καθώς και οι Βασικές Δομές Ελέγχου Πρόσβασης (όπως Πίνακες Ελέγχου πρόσβασης, Λίστες Ελέγχου Πρόσβασης, Λίστες Δυνατοτήτων) που τις εξασφαλίζουν. Επίσης παρουσιάζεται και μια σειρά πολιτικών ελέγχου πρόσβασης που κινούνται στην ίδια κατεύθυνση. Συγκεκριμένα, παρουσιάζονται μοντέλα όπως ο Διακριτικός Έλεγχος Πρόσβασης (DAC), ο Υποχρεωτικός Έλεγχος Πρόσβασης (MAC), το μοντέλο Bell – La Padula, το μοντέλο Biba, η πολιτική ασφάλειας Κινέζικου Τείχους, το μοντέλο Harrison- Ruzzo-Ullman, το μοντέλο Clark Wilson και το μοντέλο Domain – Type Enforcement. Ειδική έμφαση δίνεται στο Μοντέλο Ελέγχου Πρόσβασης Βασισμένο σε Ρόλους (RBAC). Αναλύονται οι τέσσερις βασικές του συνιστώσες (βασικό RBAC, ιεραρχικό RBAC, περιορισμένο RBAC και συμμετρικό RBAC) καθώς και τέσσερις επεκτάσεις του βασικού μοντέλου: Μοντέλο Ελέγχου Πρόσβασης Βασισμένο Σε Ρόλους με Χρονικούς Περιορισμούς (TRBAC), Γενικευμένο Μοντέλο Ελέγχου Πρόσβασης Βασισμένο Σε Ρόλους με Χρονικούς Περιορισμούς (GTRBAC), Γενικευμένο Μοντέλο Ελέγχου Πρόσβασης Βασισμένο Σε Ρόλους (GRBAC) καθώς και το και Μοντέλο Ελέγχου Πρόσβασης Βασισμένο Σε Ρόλους Με Επίκεντρο Την Ποιότητα Υπηρεσιών (QRBAC).

Τέλος παρουσιάζεται η υλοποίηση και λειτουργικότητα εφαρμογής η οποία υλοποιεί το βασικό μοντέλο RBAC καθώς και συνιστώσες των επεκτάσεών του TRBAC και GTRBAC. Η φιλική προς χρήστη διεπαφή αναδεικνύει τα πλεονεκτήματα που προσφέρει η χρήση του RBAC ακόμα και σε ένα μικρό αυτόνομο σύστημα τοπικού υπολογιστή. Η εφαρμογή αφορά τη διαχείριση πρόσβασης σε υπολογιστή σχολικού περιβάλλοντος με δυνατότητα προσαρμογής των παραμέτρων της (ρόλοι και δικαιώματα) ώστε να είναι δυνατή η ενσωμάτωσή της και σε άλλα συστήματα αντίστοιχων απαιτήσεων.

ABSTRACT

The common requirement of all modern information systems is the protection of information during its distribution in them. Access control requires the existence of a series of mechanisms that ensure Integrity, Confidentiality and Authorization. In this thesis, we present the Basic Principles of Information Protection and the Basic Access Control Structures that ensure them (e.g. Access Control Matrixes, Access Control Lists – ACLs, Capability Lists) as well as a series of access control policies towards the same direction. Specifically, we present models such as the Discretionary Access Control (DAC), the Mandatory Access Control (MAC), the Bell – La Padula Model, Biba's Model, the Chinese Wall Security Policy, the Harrison-Ruzzo-Ullman model, the Clark Wilson model and the Domain – Type Enforcement model. Special emphasis is given to the Role Based Access Control Model (RBAC). The four main components of the basic model (Core RBAC, Hierarchical RBAC, Constrained RBAC, Symmetric RBAC) are analyzed along with four of its extensions: Temporal Role Based Access Control (TRBAC), Generalized – Temporal Role Based Access Control (GTRBAC), Generalized Role-Based Access Control (GRBAC) and Quality of Service Role Based Access Control (QRBAC).

Finally, we present the implementation and functionality of an application which implements the core RBAC model along with some components of TRBAC and GTRBAC extensions. The user-friendly interface highlights the advantages of RBAC even in a small, autonomous local computing system. The application is about the administration of access rights in a computer that is employed in school environment. Of course, after some minor parameter adjustment, it can also be incorporated into other local computing systems that have the same or similar requirements.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα θέλαμε να ευχαριστήσουμε θερμά τον επιβλέποντα καθηγητή μας κ. Χρήστο Δουληγέρη που δέχτηκε να αναλάβει την επίβλεψη της μεταπτυχιακής μας διατριβής καθώς και για την ουσιαστική καθοδήγηση που μας προσέφερε.

Ιδιαίτερες ευχαριστίες θα θέλαμε να απευθύνουμε στον υποψήφιο Διδάκτορα κ. Μάνο Γεωργακάκη για τη βοήθεια στην επιλογή του θέματος καθώς και για την καθοριστική συμβολή του στην ολοκλήρωση της διατριβής, μέσω των σημαντικών παρατηρήσεών του καθ' όλη τη διάρκεια εκπόνησης αυτής.

Επίσης, θα θέλαμε να ευχαριστήσουμε τους φίλους και συμφοιτητές μας Μιχάλη Κίτσιο, Απόστολο Λεβέντη και Αντώνη Γιαννόπουλο για τις πολύτιμες παρατηρήσεις τους καθώς και τη βοήθεια που μας προσέφεραν συντελώντας σημαντικά στην υλοποίηση της εφαρμογής που αναπτύξαμε. Ακόμη θα θέλαμε να ευχαριστήσουμε τη Μελίνα Εσόγλου για τη βοήθειά της στη διαμόρφωση και διόρθωση της παρούσας αναφοράς.

Τέλος, ευχαριστούμε ιδιαίτερα τις οικογένειές μας και τους φίλους μας για την ηθική και ψυχολογική υποστήριξη που μας παρείχαν.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ i
ABSTRACT i
ΕΥΧΑΡΙΣΤΙΕΣ ii
1. ΕΙΣΑΓΩΓΗ 1
1.1. Ασφάλεια και Απαιτήσεις Ασφάλειας 1
1.2. Έλεγχος Πρόσβασης 1
1.3. Αντικείμενο Διατριβής 2
2. ΜΗΧΑΝΙΣΜΟΙ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ 3
2.1. Εισαγωγή 3
2.2. Βασικές Έννοιες 3
2.3. Βασικές Αρχές Ασφάλειας 4
2.4. Βασικές Δομές Ελέγχου Πρόσβασης 6
2.4.1. Πίνακες Πρόσβασης 6
2.4.2. Λίστες Ελέγχου Πρόσβασης (Access Control Lists) 7
2.4.3. Λίστες Δυνατοτήτων (Capability Lists) 8
2.5. Πολιτικές Ελέγχου Πρόσβασης 9
2.5.1. Διακριτικός Έλεγχος Πρόσβασης (Discretionary Access Control - DAC) 9
2.5.2. Υποχρεωτικός Έλεγχος Πρόσβασης (Mandatory Access Control – MAC) 12
2.5.3. Μοντέλο Bell – La Padula 13
2.5.4. Μοντέλο Biba 14
2.5.5. Πολιτική Κινέζικου Τείχους (Chinese Wall Security Policy) 15
2.5.6. Μοντέλο Harrison, Ruzzo, Ullman 17
2.5.7. Μοντέλο Clark Wilson 19
2.5.8. Μοντέλο Domain-Type Enforcement (DTE) 21
2.6. Επίλογος 21
3. ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ ΒΑΣΙΣΜΕΝΟΣ ΣΕ ΡΟΛΟΥΣ 23
3.1. Αντί Εισαγωγής… 23
3.2. Το RBAC στον Άξονα του Χρόνου 23
3.3. Μοντέλο Ελέγχου Πρόσβασης Βασισμένο σε Ρόλους (Role Based Access Control – RBAC) 24
3.3.1. Βασικό RBAC 25
3.3.2. Ιεραρχικό RBAC 27
3.3.3. Περιορισμένο RBAC 31
3.3.4. Συμμετρικό RBAC 35
3.4. Αντί Επιλόγου… 36
4. ΕΠΕΚΤΑΣΕΙΣ RBAC 38
4.1. Εισαγωγή 38

4.2. Μοντέλο Ελέγχου Πρόσβασης Βασισμένο Σε Ρόλους με Χρονικούς Περιορισμούς - Temporal Role Based Access Control (TRBAC) 38
4.3. Γενικευμένο Μοντέλο Ελέγχου Πρόσβασης Βασισμένο Σε Ρόλους με Χρονικούς Περιορισμούς Generalized – Temporal Role Based Access Control (GTRBAC) 40
4.4. Γενικευμένο Μοντέλο Ελέγχου Πρόσβασης Βασισμένο Σε Ρόλους – Generalized Role-Based Access Control (GRBAC) 43
4.5. Μοντέλο Ελέγχου Πρόσβασης Βασισμένο Σε Ρόλους Με Επίκεντρο Την Ποιότητα Υπηρεσιών – Quality of Service Role Based Access Control (QRBAC) 44
4.6. Επίλογος 45
5. ΥΛΟΠΟΙΗΣΗ ΕΦΑΡΜΟΓΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ ΒΑΣΙΣΜΕΝΟΥ ΣΕ ΡΟΛΟΥΣ ΓΙΑ ΤΙΣ ΑΝΑΓΚΕΣ ΥΠΟΛΟΓΙΣΤΗ ΣΕ ΣΧΟΛΙΚΟ ΕΡΓΑΣΤΗΡΙΟ 46
5.1. Εισαγωγή 46
5.2. Σκοπός Εφαρμογής - Απαιτήσεις 46
5.3. Εργαλεία Ανάπτυξης – Δομή Εφαρμογής 49
5.4. Βάση Δεδομένων 49
5.5. Εφαρμογή Ανάθεσης Ρόλων και Δικαιωμάτων (RBACProject) 52
5.5.1. Καρτέλα Διαχείρισης Χρηστών 54
5.5.2. Καρτέλα Διαχείρισης Ρόλων 63
5.5.3. Καρτέλα Μηνυμάτων 76
5.6. Εφαρμογή Υλοποίησης Δικαιωμάτων (RBACStartUp) 78
5.7. Επίλογος 84
6. ΣΥΝΟΛΙΚΗ ΕΠΙΣΚΟΠΗΣΗ 85
7. ΒΙΒΛΙΟΓΡΑΦΙΑ 87

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

Εικόνα 2.1: Πίνακας Πρόσβασης 6
Εικόνα 2.2: Λίστα Ελέγχου Πρόσβασης 8
Εικόνα 2.3: Λίστα Δυνατοτήτων 9
Εικόνα 2.4: Το «κενό» της Απλής Ιδιότητας 14
Εικόνα 2.5: Σύνθεση εταιρικών πληροφοριών στο Μοντέλο Κινέζικου Τείχους 16
Εικόνα 3.1: Βασικές Συνιστώσες Μοντέλου RBAC 25
Εικόνα 3.2: Βασικό RBAC 26
Εικόνα 3.3: Ιεραρχικό RBAC 28
Εικόνα 3.4: Ιεραρχία Ρόλων με τη Μορφή Ανεστραμμένου Δένδρου 29
Εικόνα 3.5: Ιεραρχία Ρόλων με Χρήση Ιδιωτικού Ρόλου 30
Εικόνα 3.6: Περιορισμένο RBAC με Στατικό Διαχωρισμό Καθηκόντων 33
Εικόνα 3.7: Περιορισμένο RBAC με Ιεραρχίες και Δυναμικό Διαχωρισμό Καθηκόντων 34
Εικόνα 3.8: Συμμετρικό RBAC 36
Εικόνα 4.1: Καταστάσεις Ρόλων και Μεταβάσεις Μεταξύ Αυτών στο μοντέλο TRBAC 39
Εικόνα 4.2: Καταστάσεις Ρόλων και Μεταβάσεις Μεταξύ Αυτών στο GTRBAC 41
Εικόνα 5.1: Δομή Εφαρμογής Ανάθεσης Ρόλων και Δικαιωμάτων RBACProject 53
Εικόνα 5.2: Λειτουργίες Καρτέλας Διαχείρισης Χρηστών 55
Εικόνα 5.3: Λειτουργίες Καρτέλας Διαχείρισης Ρόλων 63
Εικόνα 5.4: Δομή Εφαρμογής Υλοποίησης Δικαιωμάτων (RBACStartUp) 79
Εικόνα 5.5: Αλγόριθμος Ενεργοποίησης/ Απενεργοποίησης Ρόλων και Δικαιωμάτων Βάσει των Χρονικών Περιορισμών 82

1. ΕΙΣΑΓΩΓΗ

1.1. Ασφάλεια και Απαιτήσεις Ασφάλειας

Η συνεχής ανάπτυξη της τεχνολογίας οδήγησε στη δημιουργία μεγάλων πληροφοριακών συστημάτων τα οποία διαχειρίζονται και χρησιμοποιούνται από μεγάλο αριθμό χρηστών. Το γεγονός αυτό σε συνδυασμό με τον όγκο αλλά και τη σημαντικότητα των πληροφοριών που διακινούνται πλέον μέσα από αυτά τα συστήματα θέτει σε πρώτο πλάνο την ανάγκη για την προστασία της ροής της πληροφορίας και της λειτουργίας των συστημάτων γενικά. Δεν είναι τυχαίο άλλωστε ότι ένας από τους τομείς της επιστήμης της πληροφορικής που γνωρίζει ιδιαίτερα μεγάλη άνθιση στις μέρες μας είναι αυτός της Ασφάλειας.

Οι βασικότερες απαιτήσεις Ασφάλειας που κρίνεται απαραίτητο να ικανοποιούνται είναι οι εξής:

- Αυθεντικοποίηση (Authentication)
- Εξουσιοδότηση (Authorization)
- Εμπιστευτικότητα (Confidentiality)
- Ακεραιότητα (Integrity)
- Διαθεσιμότητα (Availability)
- Μη - Άρνηση Ευθύνης (Non- Repudiation)

Με λίγα λόγια σε κάθε περίπτωση πρέπει να εξασφαλίζουμε ότι γνωρίζουμε ποιος είναι αυτός που επικοινωνεί με το σύστημά μας (Αυθεντικοποίηση), ποια δικαιώματα και ρόλους έχει (Εξουσιοδότηση) και δεδομένου ότι έχει πραγματοποιήσει μία ενέργεια ότι υπάρχουν οι κατάλληλοι μηχανισμοί ώστε να μην μπορεί μετέπειτα να την αρνηθεί (Μη - Άρνηση Ευθύνης). Σε επίπεδο πληροφορίας χρειάζεται να διασφαλίσουμε τη μη αλλοίωση της πληροφορίας κατά τη διακίνησή της στο σύστημα (Ακεραιότητα) καθώς και την προστασία της σε ότι αφορά την προσπέλασή της από μη εξουσιοδοτημένους χρήστες του συστήματος (Εμπιστευτικότητα). Τέλος, στα πλαίσια της ασφάλειας εντάσσεται και η διαθεσιμότητα του συστήματος που αφορά τρόπους και μηχανισμούς συνεχούς λειτουργίας αυτού καθώς επίσης και σχέδια ανάκαμψης σε περιπτώσεις καταστροφών.

Οι δύο έννοιες που συχνά συγχέονται είναι αυτές της αυθεντικοποίησης και της εξουσιοδότησης. Πρόκειται για δύο εντελώς διαφορετικές λειτουργίες που ο συνδυασμός τους αποτελεί τον κύριο άξονα εφαρμογής του ελέγχου πρόσβασης. Η σχέση τους έγκειται στο ότι η σωστή εξουσιοδότηση βασίζεται και εξαρτάται από τη σωστή αυθεντικοποίηση. Για παράδειγμα, αν σε ένα σύστημα δεν εξασφαλίσουμε μηχανισμούς που θα ελέγχουν την ταυτότητα του χρήστη δεν μπορούμε έγκυρα και σωστά να καθορίσουμε σε ποιους πόρους του συστήματος αυτός τελικά θα έχει πρόσβαση.

1.2. Έλεγχος Πρόσβασης

Ο έλεγχος πρόσβασης (ή και έλεγχος προσπέλασης) αφορά λειτουργίες και διεργασίες βάσει των οποίων οι πόροι και οι χρήστες του συστήματος αλληλεπιδρούν μεταξύ τους. Αποτελεί θεμελιώδη μηχανισμό των σύγχρονων υπολογιστικών συστημάτων προκειμένου να ικανοποιηθούν οι βασικές απαιτήσεις ασφάλειας. Χρησιμοποιείται για την εξασφάλιση της ακεραιότητας και της εμπιστευτικότητας των πληροφοριών καθώς και της διαχείρισης των πόρων του συστήματος προϋποθέτοντας ότι έχει προηγηθεί ο σχεδιασμός και η εφαρμογή κατάλληλων διαδικασιών αυθεντικοποίησης και εξουσιοδότησης των χρηστών.

Σκοπός είναι ο περιορισμός της πρόσβασης σε πόρους και δεδομένα από μη εξουσιοδοτημένους χρήστες αλλά και η μη απόκτηση απεριόριστης πρόσβασης σε ήδη εξουσιοδοτημένους χρήστες. Ξεφεύγοντας από τη συστημική ορολογία και βλέποντας την επιχειρηματική εικόνα του ελέγχου πρόσβασης, μπορούμε να πούμε ότι μέσω αυτού επιτυγχάνεται η βέλτιστη κατανομή των πόρων και των πληροφοριών στους χρήστες με απώτερο στόχο την αύξηση της παραγωγικότητας. Στην αντίπερα όχθη, η επιβολή του έλεγχου πρόσβασης μπορεί να αυξήσει σημαντικά το κόστος λειτουργίας της επιχείρησης δεδομένου ότι η διαχείριση ενός συστήματος ελέγχου προϋποθέτει την επένδυση σε υλικό, λογισμικό και ανθρώπινο δυναμικό.

1.3. Αντικείμενο Διατριβής

Στόχος της παρούσας διατριβής αποτελεί η μελέτη και συνοπτική παρουσίαση των αρχών ασφάλειας καθώς και των βασικότερων πολιτικών και μοντέλων ελέγχου πρόσβασης. Ειδικότερη έμφαση δίνεται στο μοντέλο ελέγχου πρόσβασης βασισμένο σε ρόλους καθώς θεωρείται ένα από τα πιο δημοφιλή και ευρέως χρησιμοποιούμενα μοντέλα τα οποία υλοποιούνται σήμερα στον εμπορικό κόσμο.

Για την περαιτέρω κατανόηση της λειτουργικότητας και ευκολίας στη διαχείριση της πρόσβασης που προσφέρει το μοντέλο αυτό παρουσιάζεται στο τελευταίο κεφάλαιο της Διατριβής η ανάπτυξη εφαρμογής υλοποίησής του για το λειτουργικό σύστημα των Windows σε τοπικό Ηλεκτρονικό Υπολογιστή.

Αναλυτικότερα η εργασία μας δομείται ως εξής:

- Στο Κεφάλαιο 2, το οποίο οργανώνεται σε 4 ενότητες, περιγράφονται οι βασικές έννοιες οι οποίες είναι χρήσιμες για την κατανόηση του υπολοίπου της εργασίας, οι βασικές αρχές ασφάλειας που πρέπει να διέπουν τους μηχανισμούς ελέγχου καθώς και οι βασικές δομές ελέγχου πρόσβασης (πίνακες, ACLs κλπ). Στην τελευταία ενότητα του κεφαλαίου, παρουσιάζονται οι κυριότερες πολιτικές και μηχανισμοί ελέγχου πρόσβασης όπως είναι ο Διακριτικός Έλεγχος Πρόσβασης, ο Υποχρεωτικός Έλεγχος Πρόσβασης, το μοντέλο Clark-Wilson κλπ.
- Στο Κεφάλαιο 3, αναλύεται εκτενώς ο έλεγχος πρόσβασης βασισμένος σε ρόλους (RBAC) παρουσιάζοντας τις τέσσερις βασικές συνιστώσες του RBAC και τα χαρακτηριστικά τους.
- Στο Κεφάλαιο 4, παρουσιάζονται κάποιες από τις επεκτάσεις του μοντέλου RBAC που εισάγουν νέες λειτουργικότητες στο βασικό μοντέλο.
- Στο Κεφάλαιο 5, παρουσιάζεται αναλυτικά η ανάπτυξη εφαρμογής υλοποίησης του μοντέλου ελέγχου πρόσβασης βασισμένο σε ρόλους για τις ανάγκες Ηλεκτρονικού Υπολογιστή σε περιβάλλον σχολικού εργαστηρίου.

2. ΜΗΧΑΝΙΣΜΟΙ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ

2.1. Εισαγωγή

Στο κεφάλαιο αυτό γίνεται περιγραφή των βασικών δομών ελέγχου πρόσβασης (όπως πίνακες, ACLs κλπ). Επιπλέον, αναλύονται οι κυριότερες πολιτικές και μηχανισμοί ελέγχου πρόσβασης. Πριν την παρουσίαση των πρωταρχικών μηχανισμών ελέγχου πρόσβασης κρίνεται απαραίτητος ο ορισμός κάποιων βασικών εννοιών που χρησιμοποιούνται κατά κόρον στη συνέχεια και οι οποίες θα βοηθήσουν στην καλύτερη κατανόηση των μοντέλων και των αρχών που τα διέπουν. Επίσης, περιγράφονται οι βασικές αρχές ασφάλειας που πρέπει να ικανοποιούνται σε ένα πληροφοριακό σύστημα.

Πιο συγκεκριμένα το Κεφάλαιο 2 αποτελείται από τις εξής ενότητες:

- Βασικές Έννοιες
- Βασικές Αρχές Ασφάλειας
- Βασικές Δομές Ελέγχου Πρόσβασης
  - Πίνακες Πρόσβασης
  - Λίστες Ελέγχου Πρόσβασης (Access Control Lists)
  - Λίστες Δυνατοτήτων (Capability Lists)
- Πολιτικές Ελέγχου Πρόσβασης
  - Διακριτικός Έλεγχος Πρόσβασης (Discretionary Access Control - DAC)
  - Υποχρεωτικός Έλεγχος Πρόσβασης (Mandatory Access Control – MAC)
  - Μοντέλο Bell – La Padula
  - Μοντέλο Biba
  - Πολιτική Κινέζικου Τείχους (Chinese Wall Security Policy)
  - Μοντέλο Harrison, Ruzzo, Ullman
  - Μοντέλο Clark Wilson
  - Μοντέλο Domain-Type Enforcement (DTE)
- Συνολική Επισκόπηση

2.2. Βασικές Έννοιες

Χρήστης

Αναφέρεται σε πρόσωπα που αλληλεπιδρούν με ένα υπολογιστικό σύστημα.

Υποκείμενο

Αφορά τις ενεργές οντότητες ενός υπολογιστικού συστήματος που προκαλούν είτε τη ροή της πληροφορίας είτε την αλλαγή της κατάστασης του συστήματος. Ως υποκείμενο μπορεί να χαρακτηριστεί ένας χρήστης, μία διεργασία ή ένα νήμα. Τις περισσότερες φορές η έννοια του υποκειμένου ταυτίζεται με αυτή του χρήστη. Αυτό όμως δεν είναι απόλυτο καθώς ένας χρήστης μπορεί να έχει σε λειτουργία εκ μέρους του περισσότερα του ενός υποκείμενα. Σε αυτή την περίπτωση η έννοια του υποκείμενου αφορά την εκάστοτε διεργασία-πρόγραμμα που εκτελείται στο σύστημα εκ μέρους του χρήστη.

Αντικείμενο

Πρόκειται για τις παθητικές οντότητες ενός υπολογιστικού συστήματος που είτε περιλαμβάνουν είτε δέχονται πληροφορίες. Ως αντικείμενα νοούνται οι πόροι του συστήματος όπως για

παράδειγμα αρχεία, ευρετήρια, περιφερειακές συσκευές, διεργασίες, προγράμματα κα. Αποτελούν τις οντότητες πάνω στις οποίες μπορεί να εκτελεστεί μία λειτουργία. Σε αυτό το σημείο αξίζει να αναφέρουμε ότι μία ενεργή οντότητα μπορεί να πάρει τη θέση του αντικειμένου (ένας χρήστης ενεργεί πάνω σε έναν άλλο χρήστη).

Λειτουργία

Είναι μια ενεργή διεργασία η οποία προκαλείται από ένα υποκείμενο πάνω σε μία παθητική οντότητα.

Δικαίωμα Πρόσβασης

Η εξουσιοδότηση ενός υποκειμένου να εκτελέσει μια λειτουργία στο σύστημα. Πιο συγκεκριμένα είναι ο συνδυασμός ενός αντικειμένου και της λειτουργίας που μπορεί να εκτελεστεί σε αυτό. Χαρακτηριστικά, μία συγκεκριμένη λειτουργία που χρησιμοποιεί δύο διαφορετικά αντικείμενα αντιπροσωπεύει δύο διαφορετικά δικαιώματα και αντίστοιχα δύο διαφορετικές λειτουργίες πάνω στο ίδιο αντικείμενο αντιπροσωπεύουν και πάλι δύο ξεχωριστά δικαιώματα.

Πολιτική

Η πολιτική είναι στη ουσία μία δήλωση για το τι θεωρείται επιτρεπτό να γίνεται και τι όχι. Έτσι στον τομέα της ασφάλειας μία πολιτική ασφάλειας είναι ο ορισμός του τι ακριβώς θεωρούμε ως ασφαλές σύστημα και τι επιτρέπεται να γίνεται έτσι ώστε αυτό να παραμένει ασφαλές.

Μηχανισμός - Μοντέλο

Ο μηχανισμός ή μοντέλο ασφάλειας είναι μέθοδοι, εργαλεία ή διαδικασίες που υλοποιούν μία πολιτική ασφάλειας. Οι μηχανισμοί μπορεί να είναι και μη-τεχνικοί όπως για παράδειγμα το να απαιτείται η απόδειξη της ταυτότητας του χρήστη πριν αυτός αλλάξει τον κωδικό εισόδου του στο σύστημα. Χρησιμοποιείται για να ορίσει αλλά και να ελέγξει ως προς την ορθότητα μια πολιτική ελέγχου πρόσβασης.

Ρόλος

Ο ρόλος είναι ένα σύνολο από συμπεριφορές, δικαιώματα και υποχρεώσεις που συνδέονται με μια συγκεκριμένη δραστηριότητα. Θα πρέπει να σημειωθεί ότι ο ρόλος δεν ταυτίζεται πάντα με το άτομο αφού μία οντότητα μπορεί να έχει πολλούς διαφορετικούς ρόλους.

2.3. Βασικές Αρχές Ασφάλειας

Το 1975 οι Salzer και Schroeder δημοσίευσαν ένα άρθρο στο οποίο παρουσίαζαν βασικές αρχές για το σχεδιασμό και την υλοποίηση μηχανισμών ασφάλειας προκειμένου να μην παραβιάζονται οι καθορισμένοι σ' ένα πληροφοριακό σύστημα περιορισμοί πρόσβασης [5].

Οι βασικές αυτές αρχές ενισχύουν τις έννοιες της απλότητας του συστήματος και του περιορισμού πρόσβασης σε αυτό. Σε ό,τι αφορά στην απλότητα είναι προφανές ότι όσο πιο απλό είναι ένα σύστημα τόσο πιο εύκολα κατανοητό είναι και επιπλέον μειώνονται οι πιθανότητες λάθους και έλλειψης σταθερότητας. Αντίστοιχα, με τον περιορισμό επιτυγχάνεται ελαχιστοποίηση της πρόσβασης και περιορισμός της κάθε οντότητας του συστήματος στα δεδομένα που χρειάζεται για την ορθότερη λειτουργία αυτού [1].

Οι βασικές αυτές αρχές ασφαλείας παρουσιάζονται παρακάτω [5]:

1. Αρχή του ελαχίστου δικαιώματος (Least Privilege)

Σε κάθε πρόγραμμα και χρήστη θα πρέπει να δίνονται ο ελάχιστος αριθμός δικαιωμάτων πρόσβασης που είναι απαραίτητα για να ολοκληρώσει την εργασία του. Με την υλοποίηση της αρχής αυτής επιτυγχάνεται ο περιορισμός της ζημιάς που θα προκύψει σε περίπτωση

συστημικού λάθους ή κακόβουλης ενέργειας. Έτσι, όταν ένα υποκείμενο προκειμένου να πραγματοποιήσει μια εργασία χρειάζεται κάποια επιπλέον δικαιώματα πρόσβασης πέραν αυτών που διαθέτει, αυτά θα πρέπει να του ανατίθενται προσωρινά και αφού ολοκληρώσει την εργασία του θα πρέπει και πάλι να του αφαιρούνται. Η ανάθεση των δικαιωμάτων πρόσβασης θα πρέπει να γίνεται πολύ προσεκτικά και επιλεκτικά στους χρήστες ανάλογα με τις λειτουργικές τους ανάγκες και θα πρέπει περιοδικά να ελέγχονται προκειμένου να ικανοποιείται η αρχή του ελαχίστου δικαιώματος.

2. Αρχή της οικονομίας του μηχανισμού (Economy of Mechanism)

Ο σχεδιασμός των μηχανισμών ασφάλειας θα πρέπει να είναι όσο πιο μικρός και απλός γίνεται προκειμένου ο έλεγχος και η αξιολόγησή τους να γίνονται πιο εύκολα και γρήγορα. Μέσω της απλότητας επιτυγχάνεται εύκολος εντοπισμός και διόρθωση πιθανών λαθών πρόσβασης που θα προκύψουν και τα οποία θα απαιτούσαν την γραμμή-προς-γραμμή εξέταση του κώδικα και του υλικού που υλοποιούν το μηχανισμό ασφάλειας. Η εφαρμογή αυτής της αρχής υλοποιείται κυρίως στα κατώτερα και πιο προστατευμένα επίπεδα του συστήματος.

3. Αρχή της προεπιλογής ασφάλειας (Fail-safe Defaults)

Σύμφωνα με την αρχή αυτή, η προεπιλεγμένη κατάσταση σε ένα σύστημα είναι η άρνηση πρόσβασης σε ένα αντικείμενο και ο μηχανισμός ασφάλειας είναι αυτός που καθορίζει πότε είναι επιτρεπτή η πρόσβαση. Αν ο μηχανισμός ασφάλειας του συστήματος αποτύχει για κάποιο λόγο, τότε θα απαγορευτεί κάθε πρόσβαση, είτε νόμιμη είτε παράνομη, διατηρώντας πλήρως προστατευμένο το σύστημα. Συνήθως γίνεται κάποιος συμβιβασμός (trade-off) μεταξύ της αρχής αυτής και της απαίτησης της διαθεσιμότητας ανάλογα με το είδος του συστήματος.

4. Αρχή της πλήρους μεσολάβησης (Complete Mediation)

Κάθε αίτημα ενός υποκειμένου για πρόσβαση σε ένα αντικείμενο θα πρέπει να ελέγχεται για εξουσιοδότηση και κατόπιν να παραχωρείται το δικαίωμα πρόσβασης σε αυτό. Αυτή η διαδικασία θα πρέπει να επαναλαμβάνεται κάθε φορά που κάποιος θέλει να αποκτήσει πρόσβαση σε κάποιο αντικείμενο ακόμα και αν το έχει προσπελάσει νωρίτερα. Δε θα πρέπει το σύστημα να βασίζεται σε μια κρυφή μνήμη και να επιτρέπει τη νέα προσπέλαση λόγω της ύπαρξης της προηγούμενης γιατί στο ενδιάμεσο μπορεί να έχουν τροποποιηθεί τα δικαιώματα πρόσβασης.

5. Ανοικτή Σχεδίαση (νόμος του Kerckhoff – Open Design)

Η επιτυχία των μηχανισμών ασφάλειας δεν πρέπει να έγκειται στο γεγονός ότι η σχεδίασή τους είναι κρυφή. Αν οι σχεδιαστές «μοιράζονται» με τους χρήστες όλη τη γνώση τότε τόσο πιο ασφαλείς αισθάνονται οι χρήστες για το σύστημά τους. Επιπλέον ισχύει η λογική του ότι όσο περισσότεροι βλέπουν κάτι τόσο περισσότερες είναι οι πιθανότητες αυτό να έχει τελικά επιτυχία αφού καθένας θα μπορεί να το βελτιώνει. Αυτή η αρχή τηρείται κατά παράδοση στα κρυπτογραφικά συστήματα όπου οι αλγόριθμοι εξετάζονται λεπτομερώς από το ευρύ κοινό.

6. Διαχωρισμός του δικαιώματος (Separation of Privilege)

Μία άλλη αρχή που θα πρέπει να ακολουθείται όταν και όπου αυτό είναι δυνατό, είναι να στηρίζεται ο μηχανισμός ασφάλειας σε μία σειρά από συνθήκες με τέτοιο τρόπο που για να ικανοποιηθούν να πρέπει να συμβάλουν δύο ανεξάρτητες οντότητες.

7. Λιγότερο συνήθης μηχανισμός (Least Common Mechanism)

Σύμφωνα με αυτή την αρχή θα πρέπει να αποφεύγεται ο διαμοιρασμός των μηχανισμών σε πάρα πολλούς χρήστες. Στα πλαίσια αυτού εντάσσεται ο διαχωρισμός του συστήματος είτε φυσικά (διαφορετικά υποσυστήματα) είτε λογικά μέσω εικονικών μηχανών.

8. Ψυχολογική Αποδεκτικότητα (Psychological Acceptability)

Αυτό που είναι επίσης μεγάλης σημασίας είναι οι μηχανισμοί ασφάλειας να είναι τελικά αποδεκτοί από τους χρήστες. Η όποια πολυπλοκότητα των μηχανισμών δε θα πρέπει σε καμία

περίπτωση να φτάνει στο χρήστη και να τον επιβαρύνει. Επιπλέον, θα πρέπει να λαμβάνονται υπόψη όλες οι συνθήκες που αφορούν το εργασιακό περιβάλλον του χρήστη και το πώς αυτές μπορούν να επηρεάσουν την πολιτική ασφάλειας που θα ακολουθηθεί.

2.4. Βασικές Δομές Ελέγχου Πρόσβασης

2.4.1. Πίνακες Πρόσβασης

Ένας θεμελιώδης τρόπος απεικόνισης των δικαιωμάτων πρόσβασης είναι ο πίνακας ή μήτρα πρόσβασης (access control matrix). Για πάνω από 30 χρόνια ο πίνακας πρόσβασης έχει συμβάλει στη μελέτη των δικαιωμάτων των υποκειμένων στην προσπέλαση των αντικειμένων αποτελώντας ένα εννοιολογικό πρότυπο στην ανάλυση των ιδιοτήτων πρόσβασης [1]. Η απλή δομή των δύο διαστάσεων και η ευκολία κατανόησής της είναι το βασικό πλεονέκτημά του.

Στον πίνακα, λοιπόν, περιγράφονται με ακρίβεια όλες οι πιθανές καταστάσεις του ελέγχου πρόσβασης. Κάθε σειρά του πίνακα αποτελεί ένα υποκείμενο ενώ κάθε στήλη αντιπροσωπεύει ένα αντικείμενο. Θα πρέπει εδώ να σημειωθεί ότι σε πολλές περιπτώσεις στις στήλες του πίνακα απεικονίζονται επιπλέον και υποκείμενα εάν το σύστημα που περιγράφεται επιτρέπει διαδικασίες αλληλεπίδρασης μεταξύ υποκειμένων. Στα κελιά που δημιουργούνται αναφέρονται τα δικαιώματα. Ο πίνακας μπορεί να περιγραφεί με ένα σύνολο τριπλετών [2]. Μια τριπλέτα (Υ,Α,Δ) περιγράφει μία κατάσταση όπου Υ είναι το υποκείμενο το οποίο έχει το δικαίωμα Δ στο αντικείμενο Α. Τα δικαιώματα που καταγράφονται σε ένα πίνακα πρόσβασης είναι για παράδειγμα δικαιώματα Ανάγνωσης (Read), Γραφής (Write), Εκτέλεσης (Execute) και Ιδιοκτησίας (Ownership). Τα τρία πρώτα δικαιώματα είναι ξεκάθαρο το τι περιγράφουν και δε χρήζουν περαιτέρω ανάλυσης. Το δικαίωμα της Ιδιοκτησίας καθορίζει τη δυνατότητα ενός υποκειμένου να αλλάξει τα δικαιώματα πρόσβασης σε ένα αντικείμενο. Φυσικά ανάλογα με το σύστημα τα δικαιώματα που περιγράφονται μπορεί να ποικίλουν.

Στο παρακάτω σχήμα (Εικόνα 2.1), παρουσιάζεται ένα παράδειγμα πίνακα πρόσβασης.

Εικόνα 2.1: Πίνακας Πρόσβασης

	Αντικείμενο 1	Αντικείμενο 2	Αντικείμενο 3	Υποκείμενο 1	Υποκείμενο 2
Υποκείμενο 1	R,W	O	E		
Υποκείμενο 2	R	R,W,E		R	
Υποκείμενο 3	O	E,R			W

Η κατάσταση ενός πίνακα πρόσβασης είναι ουσιαστικά η εικόνα που αυτός παρουσιάζει μία δεδομένη χρονική στιγμή [2]. Σε ένα σύστημα μπορεί να συμβούν πολλές μεταβάσεις από μία κατάσταση του πίνακα σε μία άλλη. Οι μεταβάσεις περιγράφονται με εντολές. Οι εντολές αποτελούνται από μία σειρά πρωτογενών λειτουργιών οι οποίες έχουν ως τελικό αποτέλεσμα την αλλαγή του πίνακα πρόσβασης και τη μετάβαση σε άλλη κατάσταση [1]. Παραδείγματα τέτοιων λειτουργιών είναι:

- Δημιουργία Αντικειμένου (Create Object)
- Καταστροφή Υποκειμένου (Destroy Subject)
- Προσθήκη Δικαιώματος (Add Access Right) κλπ

Σύμφωνα με τους Harrison, Ruzzo και Ullman, το μοντέλο των οποίων περιγράφεται αναλυτικά σε επόμενη ενότητα, η δομή μίας εντολής αποτελείται από την ύπαρξη ή όχι συνθηκών που η ικανοποίησή τους οδηγεί στην εκτέλεση μιας ή περισσοτέρων πρωτογενών λειτουργιών. Ειδικότερα η δομή μίας εντολής command c με παραμέτρους X_1, X_2, …, X_n είναι ως έξης:

command c(x_1, … , x_n)

If r_1 in A[x_{s1} , x_{o1}] and

r_2 in A[x_{s2} , x_{o2}] and . . .

r_n in A[x_{sn} , x_{on}]

Then

op_1

op_2

. . .

op_n

όπου τα Xs_1,Xs_2, … ,Xs_n είναι το σύνολο των υποκειμένων, τα Xo_1,Xo_2, … ,Xo_n είναι τα αντικείμενα, r_1,r_2, … , r_n το σύνολο των δικαιωμάτων και op_1,op_2, … ,op_n πρωτογενείς λειτουργίες.

Με τις εντολές και ακολουθώντας πάντα τους βασικούς κανόνες Ιδιοκτησίας, τα υποκείμενα μπορούν να παραχωρήσουν αλλά και να ανακαλέσουν δικαιώματα πρόσβασης άλλων υποκειμένων [1]. Έτσι δίνεται η δυνατότητα της προσαρμογής του πίνακα πρόσβασης στις εκάστοτε συνθήκες και απαιτήσεις του συστήματος.

Ο πίνακας ελέγχου πρόσβασης που περιγράφηκε παραπάνω δεν προσαρμόζεται εύκολα σε αύξηση του μεγέθους των χρηστών ή και των πόρων του συστήματος. Σ' ένα μεγάλο σύστημα με πολλούς χρήστες και πολλά αντικείμενα, ο πίνακας ελέγχου πρόσβασης θα ήταν πολύ μεγάλος σε μέγεθος και θα περιείχε πολλά άδεια κελιά. Εξαιτίας αυτής της μη προσαρμοστικότητάς του και της δυσκολίας διαχείρισης του σε αλλαγές μεγέθους (non Scalability), χρησιμοποιούνται στην πράξη κάποιες άλλες προσεγγίσεις υλοποίησής του πίνακα πρόσβασης, οι οποίες παρουσιάζονται παρακάτω.

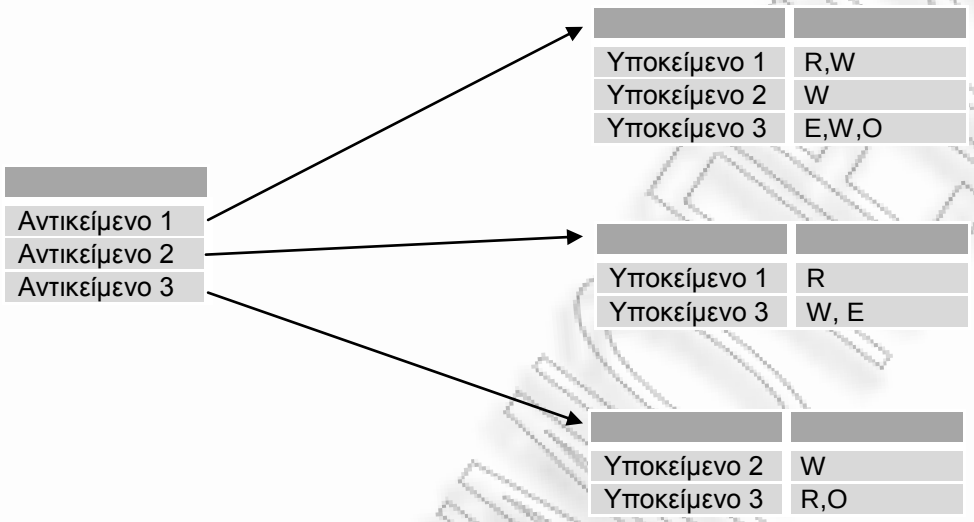
2.4.2. Λίστες Ελέγχου Πρόσβασης (Access Control Lists)

Μια δημοφιλής προσέγγιση υλοποίησης του πίνακα ελέγχου πρόσβασης είναι με τη βοήθεια των λιστών ελέγχου πρόσβασης που αποτελούν λίστες με δικαιώματα που χαρακτηρίζουν κάποιο συγκεκριμένο αντικείμενο. Κάθε αντικείμενο συνδέεται με μια λίστα ελέγχου πρόσβασης (ACL) η οποία περιλαμβάνει τα υποκείμενα καθώς και τις άδειες που αυτά έχουν πάνω στο αντικείμενο [1][4]. Επομένως, σε μια λίστα, κάθε καταχώριση περιλαμβάνει δύο πεδία: το υποκείμενο και τις προσβάσεις-λειτουργίες που είναι εξουσιοδοτημένο να εκτελέσει στο αντικείμενο [1].

Το βασικό πλεονέκτημα των λιστών ελέγχου πρόσβασης είναι ότι καθιστούν εύκολη και γρήγορη την εύρεση των χρηστών που έχουν πρόσβαση σε ένα αντικείμενο, καθώς και των λειτουργιών που οι τελευταίοι μπορεί να επιτελέσουν πάνω στο αντικείμενο, ελέγχοντας τη λίστα του αντικειμένου. Μειονεκτούν όμως σε σχέση με τους πίνακες στην περίπτωση που θέλουμε να προσδιορίσουμε όλες τις προσβάσεις ενός υποκειμένου στο σύστημα οπότε και θα πρέπει να ελεγχθεί η ACL κάθε αντικειμένου. Επιπλέον, επιτρέπουν την εύκολη ανάκληση της πρόσβασης σε ένα αντικείμενο μέσω της απλής διαγραφής της αντίστοιχης καταχώρισης της λίστας [1][3].

Στο παρακάτω σχήμα, Εικόνα 2.2, παρουσιάζεται μια απεικόνιση μιας λίστας ελέγχου πρόσβασης.

Εικόνα 2.2: Λίστα Ελέγχου Πρόσβασης



Ένα επιπλέον πλεονέκτημα που προσφέρουν οι λίστες ελέγχου πρόσβασης είναι ότι μπορεί να περιοριστεί το μέγεθός τους συνδέοντας το κάθε αντικείμενο με ομάδες χρηστών που έχουν κοινή πρόσβαση σε αυτό αντί με κάθε έναν μεμονωμένους τους χρήστες της ομάδας. Στην περίπτωση αυτή βέβαια χρειάζονται επιπλέον διαχειριστικές λειτουργίες προκειμένου να διαχειριστούμε τις συμμετοχές των υποκειμένων στις ομάδες [1].

Όλα τα παραπάνω πλεονεκτήματα των λιστών ελέγχου πρόσβασης τις καθιστούν κατάλληλες για την υλοποίηση αντικειμενοστρεφών (object- oriented policies) πολιτικών όπως ο διακριτικός έλεγχος πρόσβασης (Discretionary Access Control).

2.4.3. Λίστες Δυνατοτήτων (Capability Lists)

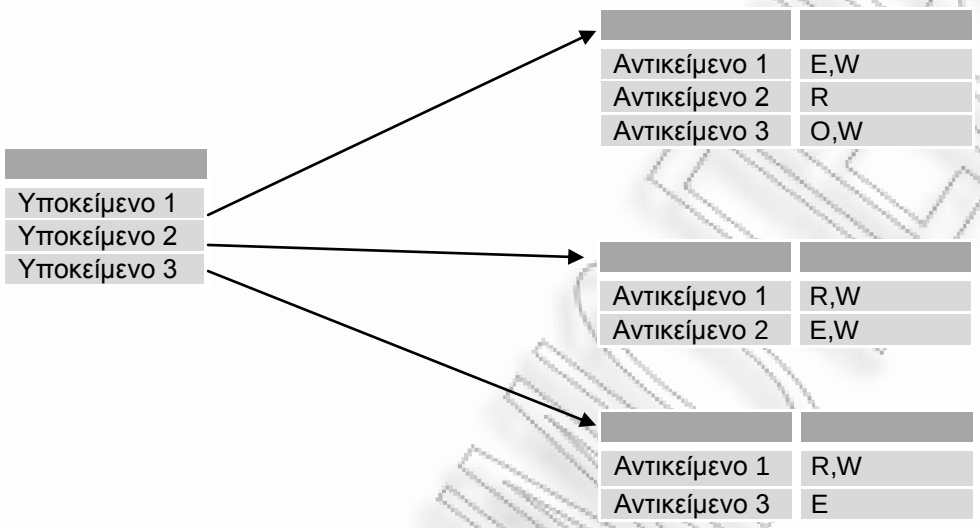
Ο δεύτερος τρόπος προσέγγισης βασίζεται στην αποθήκευση του πίνακα ελέγχου πρόσβασης ανά γραμμή οπότε και έχουμε όλα τα δικαιώματα πρόσβασης ενός υποκειμένου συγκεντρωμένα. Η δομή αυτή καλείται λίστα δυνατοτήτων και κάθε στοιχείο της, που λέγεται δυνατότητα (προσδιοριστής δικαιωμάτων), προσδιορίζει ένα αντικείμενο και όλα τα δικαιώματα πρόσβασης που έχει το υποκείμενο πάνω σε αυτό [1]. Επομένως, κάθε υποκείμενο συνδέεται με μια λίστα δυνατοτήτων που αποθηκεύει για κάθε αντικείμενο στο σύστημα τις λειτουργίες που το υποκείμενο είναι εξουσιοδοτημένο να εκτελέσει σε αυτό [4]. Η πρόσβαση σε ένα αντικείμενο λοιπόν επιτρέπεται μόνο αν το υποκείμενο το οποίο τη ζητά έχει δυνατότητα για το αντικείμενο αυτό.

Η υλοποίηση αυτή προσφέρει μεγάλη ευκολία στην επισκόπηση και την εύρεση όλων των προσβάσεων που έχει ένα υποκείμενο με απλή εξέταση της λίστας δυνατοτήτων του. Δε συνίσταται στις περιπτώσεις που χρειάζεται να εντοπιστούν όλοι οι χρήστες που έχουν πρόσβαση σε ένα αντικείμενο αφού απαιτείται έλεγχος της λίστας δυνατοτήτων κάθε

υποκειμένου. Επιπρόσθετα, είναι δύσκολη η ανάκληση της άδειας πρόσβασης σε ένα αντικείμενο [1][3].

Μία απεικόνιση της λίστας δυνατοτήτων παρουσιάζεται στην παρακάτω Εικόνα 2.3.

Εικόνα 2.3: Λίστα Δυνατοτήτων



Είναι πιθανό σε πολλές περιπτώσεις να συνδυαστούν οι λίστες ελέγχου πρόσβασης (ACLs) και οι λίστες δυνατοτήτων. Η κατοχή μιας δυνατότητας από ένα υποκείμενο αρκεί ώστε το υποκείμενο να λάβει πρόσβαση εξουσιοδοτημένη από τη δυνατότητα. [1]Σε ένα κατανεμημένο σύστημα, η προσέγγιση αυτή έχει το πλεονέκτημα να μη χρειάζεται επαναλαμβανόμενη πιστοποίηση αυθεντικότητας. Αυτό επιτρέπει σε ένα υποκείμενο να πιστοποιήσει την αυθεντικότητά του μία μόνο φορά, να λάβει τις δυνατότητές του και μετά να τις παρουσιάζει για να λάβει υπηρεσίες από διάφορους εξυπηρετητές (server) του συστήματος [3]. Ο κάθε εξυπηρετητής (server) μπορεί να χρησιμοποιήσει περαιτέρω λίστες ελέγχου πρόσβασης (ACLs) προκειμένου να πετύχει ένα πιο διαβαθμισμένο έλεγχο (finer-grained access control).

2.5. Πολιτικές Ελέγχου Πρόσβασης

Η πρώτη προσπάθεια κωδικοποίησης των μοντέλων ελέγχου πρόσβασης έγινε το 1983 από το Υπουργείο Άμυνας των Ηνωμένων Πολιτειών με την έκδοση του “Trusted Computer System Evaluation Criteria (TSEC), γνωστού και ως «Πορτοκαλί Βιβλίο» (“Orange Book”) εξαιτίας του πορτοκαλί εξώφυλλού του. Το πρότυπο αυτό όριζε δύο πολιτικές ελέγχου πρόσβασης για στρατιωτικές εφαρμογές: το διακριτικό έλεγχο πρόσβασης (Discretionary Access Control) και τον υποχρεωτικό έλεγχο πρόσβασης (Mandatory Access Control).

2.5.1. Διακριτικός Έλεγχος Πρόσβασης (Discretionary Access Control - DAC)

Σύμφωνα με το TSEC, η πολιτική του διακριτικού ελέγχου πρόσβασης ορίζεται ως εξής: η πολιτική DAC αποτελεί ένα μέσο περιορισμού της πρόσβασης στα αντικείμενα με βάση την ταυτότητα των υποκειμένων ή και των ομάδων στις οποίες αυτοί ανήκουν. Οι έλεγχοι πρόσβασης είναι διακριτικοί με την έννοια ότι ένα υποκείμενο που έχει συγκεκριμένη άδεια

πρόσβασης σε ένα αντικείμενο, μπορεί να μεταβιβάσει την άδεια αυτή(άμεσα ή έμμεσα) σε οποιοδήποτε άλλο χρήστη [6].

Πρόκειται για τον πιο συνηθισμένο μηχανισμό ελέγχου πρόσβασης που δίνει τη δυνατότητα στους χρήστες του συστήματος να επιτρέπουν ή να απαγορεύουν την πρόσβαση των υπολοίπων χρηστών στους πόρους που αυτοί ελέγχουν. Επομένως στην πολιτική DAC έχουμε ελεύθερη διακίνηση της πληροφορίας και οι κανόνες αυτής καθορίζονται αποκλειστικά και μόνο από τους ιδιοκτήτες της πληροφορίας [1][7]. Όπως προκύπτει από τα παραπάνω, για να μπορέσουμε να παρέχουμε το μηχανισμό DAC χρειαζόμαστε την έννοια της «ιδιοκτησίας» των αντικειμένων όπου «ιδιοκτήτης» ενός αντικειμένου είναι αυτός που μεταβιβάζει ή ανακαλεί δικαιώματα προσπέλασης σε άλλους χρήστες-υποκείμενα. Συνήθως, «ιδιοκτήτης» ενός αντικειμένου είναι ο δημιουργός του ο οποίος έχει και τον πλήρη έλεγχο της πρόσβασης σε αυτό [1].

Ένας μηχανισμός DAC αφήνει στη διακριτική ευχέρεια του χρήστη που έχει κάποιο συγκεκριμένο δικαίωμα προσπέλασης πάνω σε ένα αντικείμενο τη δυνατότητα να το μεταβιβάσει σε κάποιο άλλο χρήστη ή να το ανακαλέσει από αυτόν χωρίς να απαιτείται η διαμεσολάβηση του διαχειριστή του συστήματος [7]. Ο πιο συνηθισμένος μηχανισμός για την υλοποίηση της πολιτικής DAC είναι μέσω της χρήσης των λιστών ελέγχου πρόσβασης (ACLs). Ειδικότερα, κάθε αντικείμενο συνδέεται με μια ACL που βασίζεται στο διακριτικό έλεγχο πρόσβασης δηλ περιέχει τους χρήστες και τις ομάδες των χρηστών στις οποίες έχει επιτρέψει πρόσβαση ο ιδιοκτήτης του αντικειμένου καθώς και τις επιτρεπτές λειτουργίες που μπορούν να επιτελέσουν σε αυτό [1].

Τύποι DAC

Μερικοί από τους τύπους DAC που έχουν προτείνει οι ερευνητές παρουσιάζονται παρακάτω [1]:

Αυστηρό DAC (Strict DAC)

Σε αυτόν τον τύπο DAC μόνο ο «ιδιοκτήτης» του αντικειμένου μπορεί να παραχωρήσει άδεια πρόσβασης στο αντικείμενο. Η ιδιοκτησία δε μπορεί να μεταβιβαστεί σε άλλο χρήστη.

Φιλελεύθερο DAC (Liberal DAC)

Σε αυτό τον τύπο DAC επιτρέπεται στον ιδιοκτήτη του αντικειμένου να αναθέτει την «εξουσία»-ιδιότητα που έχει να παραχωρεί άδεια προσπέλασης και σε άλλους χρήστες. Το φιλελεύθερο DAC χωρίζεται σε περαιτέρω κατηγορίες ανάλογα με την κλίμακα που μπορεί να ανατεθεί η εξουσία της πρόσβασης.

One-level grant

Ο ιδιοκτήτης του αντικειμένου μπορεί να μεταβιβάσει τη δυνατότητα που έχει να παραχωρεί άδεια προσπέλασης στο αντικείμενο σε ένα άλλο χρήστη ο οποίος όμως δεν μπορεί να τη μεταβιβάσει περαιτέρω.

Two- level grant

Ένας χρήστης που έχει λάβει από τον ιδιοκτήτη του αντικειμένου άδεια προσπέλασης σε αυτό μπορεί να την μεταβιβάσει σε ένα τρίτο χρήστη. Δε μπορεί να γίνει όμως επόμενη μεταβίβαση.

Multilevel grant

Οποιοσδήποτε χρήστης έχει λάβει άδεια προσπέλασης σε ένα αντικείμενο μπορεί να την μεταβιβάσει σε οποιοδήποτε άλλο χρήστη χωρίς να υπάρχει περιορισμός στις μεταβιβάσεις.

Παραπάνω παρουσιάσαμε τους τύπους μεταβίβασης της άδειας πρόσβασης σε ένα αντικείμενο. Σημαντική όμως είναι και η ανάκληση των δικαιωμάτων πρόσβασης στο DAC.

Οι δύο πιο σημαντικοί τύποι ανάκλησης είναι [1]:

Ανάκληση εξαρτώμενη από αυτόν που την παραχώρησε (Grant-dependent revocation)

Μόνο ο χρήστης που παραχώρησε την άδεια προσπέλασης στο αντικείμενο έχει δικαίωμα να την ανακαλέσει.

Ανάκληση ανεξάρτητη από αυτόν που την παραχώρησε (Grant-independent revocation

Επιτρέπει στον οποιοδήποτε χρήστη να ανακαλέσει τα δικαιώματα πρόσβασης κάποιου άλλου χρήστη.

Οι πολιτικές DAC αποτέλεσαν την πλέον διαδεδομένη μέθοδο ελέγχου πρόσβασης κατά τη δεκαετία 1980-1990 εξαιτίας της μεγάλης ευελιξίας που προσφέρουν και της εύκολης εξοικείωσης των χρηστών με αυτές. Αυτή η μεγάλη ευελιξία που παρέχουν οδήγησε στην ευρεία χρήση τους σε διάφορους τομείς.

Παρά, όμως, τη μεγάλη εμπορικότητά τους, οι πολιτικές DAC είναι γνωστό ότι παρουσιάζουν δύο αρκετά σημαντικά μειονεκτήματα. Το πρώτο είναι ότι δε μπορούν να ελέγξουν και να ασφαλίσουν τη ροή της πληροφορίας σ' ένα σύστημα καθώς η παραχώρηση του δικαιώματος ανάγνωσης είναι μεταβατική [1]. Για παράδειγμα έστω ότι έχουμε ένα χρήστη Α ο οποίος παραχωρεί το δικαίωμα που έχει να διαβάζει δεδομένα σε ένα χρήστη Β. Δεν υπάρχει κάτι που να εμποδίζει το χρήστη Β από το να αντιγράψει τα δεδομένα του χρήστη Α σε ένα αρχείο που αυτός ελέγχει και στη συνέχεια να παραχωρήσει σε οποιοδήποτε άλλο χρήστη πρόσβαση ανάγνωσης στο αντίγραφο των περιεχομένων του χρήστη Α εν αγνοία του. Ο λόγος που συμβαίνει αυτό είναι ότι στο διακριτικό έλεγχο πρόσβασης η διάδοση της πληροφορίας δεν ελέγχεται, δηλαδή δεν επιβάλλεται κανένας περιορισμός στη χρησιμοποίηση της πληροφορίας από τη στιγμή που κάποιος χρήστης την έχει στα χέρια του [3].

Επιπρόσθετα, οι πολιτικές DAC είναι ιδιαίτερα ευάλωτες σε επιθέσεις Δούρειου Ίππου (Trojan horse attacks). Ο Δούρειος Ίππος είναι κακόβουλο λογισμικό που εκτός από κάποιες «καλοήθεις» και χρήσιμες ενέργειες που διενεργεί φανερά, πραγματοποιεί ταυτόχρονα κρυφές-κακόβουλες πράξεις [9]. Στέλνοντας ένα Trojan horse, αυτός που πραγματοποιεί την επίθεση αποκτά πρόσβαση σε πόρους που σύμφωνα με την πολιτική DAC δε θα ήταν εξουσιοδοτημένος να έχει και στη συνέχεια μπορεί να εκμεταλλευτεί με αρνητικό τρόπο αυτή την πληροφορία που αποκτά από την παράνομη πρόσβαση [1] [9].

Ένα τέτοιο παράδειγμα παρουσιάζεται παρακάτω [7]:

Έστω ένας «έντιμος» χρήστης Α που είναι ιδιοκτήτης ενός ευαίσθητου πόρου, του αρχείου Α, στο οποίο μόνο αυτός έχει πρόσβαση και ένας «μη έντιμος χρήστης» Β ο οποίος θέλει να αποκτήσει πρόσβαση στο αρχείο αυτό. Ο χρήστης Β φτιάχνει ένα πρόγραμμα το οποίο φανερά υλοποιεί κάποιες χρήσιμες λειτουργίες για τον Α ενώ παράλληλα έχει ενσωματώσει σε αυτό μια κακόβουλη συνάρτηση η οποία κρυφά διαβάζει και αντιγράφει σε ένα αρχείο που μόνο ο Β ελέγχει (το αρχείο Β) τα περιεχόμενα του αρχείου Α. Ο χρήστης Α τρέχει το πρόγραμμα αυτό το οποίο υπογείως και κρυφά αντιγράφει τις πληροφορίες του αρχείου Α στο αρχείο Β ενεργώντας καθόλα νόμιμα με το μηχανισμό DAC.

Από το προαναφερθέν παράδειγμα διαπιστώνουμε την ανεπάρκεια του μηχανισμού DAC να παρέχει προστασία από τον κακόβουλο χρήστη που επιθυμεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε δεδομένα. Ο μηχανισμός του Διακριτικού Ελέγχου πρόσβασης δε μπορεί να χρησιμοποιηθεί σαν ο μοναδικός μηχανισμός προστασίας στα σύγχρονα υπολογιστικά περιβάλλοντα υψηλού κινδύνου στα οποία μπορούμε να θεωρήσουμε ότι κάθε μη ελεγμένο λογισμικό μπορεί να περιέχει Trojan Horse [1]. Στα σύγχρονα συστήματα επομένως προτείνεται ο συνδυασμός του Διακριτικού Ελέγχου Πρόσβασης ταυτόχρονα με τον Υποχρεωτικό Έλεγχο Πρόσβασης που περιγράφεται παρακάτω.

2.5.2. Υποχρεωτικός Έλεγχος Πρόσβασης (Mandatory Access Control – MAC)

Μία άλλη από τις πολιτικές ελέγχου που αναπτύχθηκαν είναι η Πολιτική Πολλών Επιπέδων (Multi-Level Security Policy) ή αλλιώς Πολιτική Υποχρεωτικού Ελέγχου Πρόσβασης (Mandatory Access Control). Σύμφωνα με το TCSEC οι πολιτικές ασφάλειας που ορίζονται για συστήματα που χρησιμοποιούνται για την προσπέλαση απόρρητων ή άλλων ειδικά κατηγοριοποιημένων ευαίσθητων πληροφοριών θα πρέπει να προβλέπουν τρόπους εφαρμογής κανόνων υποχρεωτικού ελέγχου πρόσβασης.

Αυτό σημαίνει ότι θα πρέπει να περιέχουν σύνολα κανόνων για τον έλεγχο προσπέλασης που θα βασίζονται:

- άμεσα στη σύγκριση της άδειας χρήσης ή της εξουσιοδότησης του χρήστη σε ότι αφορά την πληροφορία που ζητά να έχει πρόσβαση καθώς και της ταξινόμησης ή του βαθμού ευαισθησίας της πληροφορίας,
- και έμμεσα σε φυσικούς ή άλλων περιβαλλοντολογικούς παράγοντες ελέγχου.

Οι κανόνες υποχρεωτικού ελέγχου πρόσβασης πρέπει να εκφράζουν με ακρίβεια τους νόμους, κανονισμούς και γενικές πολιτικές από τις οποίες παράγονται [6].

Η εφαρμογή της πολιτικής αυτής είναι υποχρεωτική για όλες τις οντότητες του πληροφοριακού συστήματος. Στην πολιτική MAC αυτό που ουσιαστικά υλοποιείται είναι ότι για όλους τους πόρους και τις πληροφορίες του συστήματος καθορίζονται ετικέτες ασφάλειας που δηλώνουν το βαθμό ευαισθησίας ή δημιουργούνται τάξεις σύμφωνα με τη σημαντικότητά τους ή την εμπιστευτικότητά τους [8].

Οι πολιτικές MAC λόγω του «αυστηρού» και πολύ τυπικού ύφους του ελέγχου πρόσβασης που παρέχουν χρησιμοποιούνται κατά κύριο λόγο σε εφαρμογές που διαχειρίζονται κρίσιμα και ιδιαίτερα σημαντικά δεδομένα (κυβερνητικού τομέα) ή σε στρατιωτικά πληροφοριακά συστήματα ασφάλειας, συστήματα δηλαδή όπου βρίσκει κατά κόρον εφαρμογή η αρχή του «γνωρίζω-ότι-χρειάζεται» (need-to-know) [1][8].

Στα συστήματα αυτά η πληροφορία χαρακτηρίζεται ως αταξινόμητη (unclassified –U), εμπιστευτική (confidential – C), μυστική (secret –S), πολύ μυστική (top secret – TP). Οι χαρακτηρισμοί αυτοί αποτελούν τα στοιχεία ενός ιεραρχικού μοντέλου που μπορεί να απεικονιστεί με την εξής συσχέτιση επιπέδων: TS ≥ S ≥ C ≥ U καθορίζοντας με αυτό τον τρόπο τα επίπεδα ασφάλειας [1]. Πέραν αυτών αναφέρονται και μη ιεραρχικοί χαρακτηρισμοί (κατηγορίες) και παραδείγματα είναι οι “NATO” και “NUCLEAR”. Μία ετικέτα, λοιπόν, αποτελείται από ένα επίπεδο ασφάλειας και μία κατηγορία ενώ μπορούμε να πούμε ότι υπερτερεί μιας άλλης στην περίπτωση που το επίπεδο ασφάλειας της είναι μεγαλύτερο ή ίσο από αυτό της άλλη ετικέτας και ο χαρακτηρισμός κατηγορίας περικλείει την κατηγορία της άλλης [1].

Αντίστοιχα ορίζονται και επίπεδα ασφάλειας για τους χρήστες του συστήματος που αναφέρονται ποιες πληροφορίες και πόρους έχει άδεια να προσπελάσει. Η πρόσβαση επιτρέπεται μόνο σε οντότητες με συγκεκριμένα διακριτά επίπεδα εξουσιοδότησης ή άδειας χρήσης και μόνο εφόσον ικανοποιούνται βασικοί κανόνες [8]:

- Το επίπεδο ασφάλειας που αντιστοιχεί στο χρήστη που ζητά άδεια πρόσβασης θα πρέπει να είναι τουλάχιστον ίσο με το βαθμό ευαισθησίας της πληροφορίας.
- Η άδεια προσπέλασης της πληροφορίας δε θα οδηγήσει σε υποβιβασμό της ετικέτας ασφάλειας της πληροφορίας. Δηλαδή δε θα δοθεί η δυνατότητα αυτή να εγγραφεί σε πληροφορία χαμηλότερου επιπέδου με αποτέλεσμα να αλλάξει ο βαθμός ευαισθησίας της.

Οι κανόνες της πολιτικής υποχρεωτικού ελέγχου πρόσβασης εφαρμόζονται από το λειτουργικό σύστημα ή το κεντρικό πυρήνα ασφάλειας. Έτσι αλλαγές στις ετικέτες ευαισθησίας

μπορούν να κάνουν μόνο οι διαχειριστές του συστήματος και όχι οι ιδιοκτήτες των αρχείων. Με αυτό τον τρόπο το επίπεδο ασφάλειας σε ότι αφορά την προσπέλαση της πληροφορίας από τους χρήστες είναι το μέγιστο δυνατό αφού περιορίζονται κατά πολύ οι ενέργειες που μπορούν τελικά να κάνουν οι χρήστες [1].

Αντιπροσωπευτικότερο μοντέλο της πολιτικής του Υποχρεωτικού Ελέγχου Πρόσβασης αποτελεί το μοντέλο Bell – La Padula.

2.5.3. Μοντέλο Bell – La Padula

Το μοντέλο Bell – La Padula είναι φορμαλιστικό μοντέλο που αποτυπώνει την πολιτική Υποχρεωτικού Ελέγχου Πρόσβασης. Το μοντέλο αναπτύχθηκε από τους David Elliot Bell και Len La Padula στα πλαίσια ενός ευρύτερου έργου της MITRE Corporations την περίοδο 1972-1975 με κύριο αντικείμενο την ασφάλεια. Σκοπός ήταν η αποτύπωση ενός μαθηματικού μοντέλου που θα περιγράφει την έννοια της ασφάλειας σε ένα σύστημα [10][11].

Το μοντέλο βασίζεται στην αρχή του ότι το σύστημα βρίσκεται σε μία ασφαλή κατάσταση όπου ικανοποιούνται όλοι οι κανόνες που ορίζει η πολιτική και κάθε μετάβαση του συστήματος σε μία άλλη κατάσταση εξασφαλίζει ότι και η νέα κατάσταση θα είναι επίσης ασφαλής. Έτσι το σύστημα παραμένει ασφαλές σε κάθε περίπτωση.

Το μοντέλο Bell – La Padula ορίζει δύο ιδιότητες υποχρεωτικού ελέγχου και μία ιδιότητα διακριτικού ελέγχου:

Απλή Ιδιότητα Ασφάλειας

Ένα υποκείμενο επιτρέπεται να έχει δικαίωμα ανάγνωσης ενός αντικειμένου αν η ετικέτα ασφάλειας του υποκειμένου υπερτερεί της ετικέτας ασφάλειας του αντικειμένου [11].

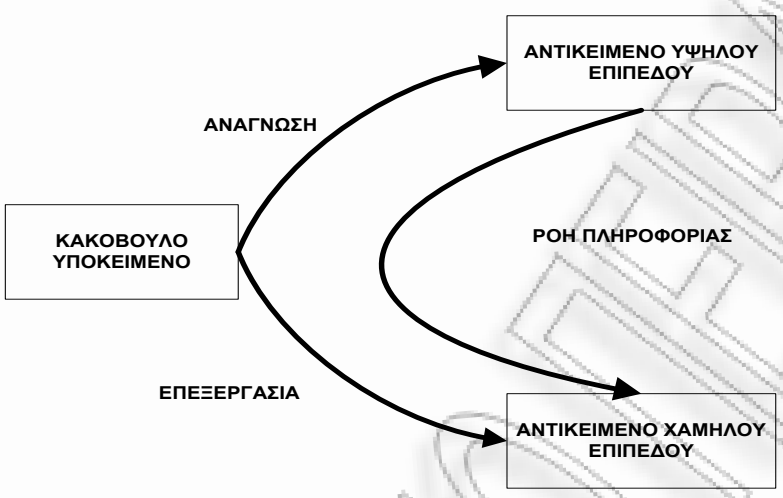
Αρχικά η ιδιότητα αυτή φαινόταν αρκετή ώστε να εξασφαλίσει την ασφάλεια του συστήματος. Αυτό που δεν προβλέπεται όμως στην απλή ιδιότητα ασφάλειας είναι η περίπτωση όπου ένα υποκείμενο μπορεί να «διαβάσει» μία πληροφορία (αντικείμενο) ενός επιπέδου ικανοποιώντας τη συνθήκη που θέσαμε με τις ετικέτες και στη συνέχεια να τη «γράψει» ως περιεχόμενο σε ένα αντικείμενο χαμηλότερου επιπέδου. Με αυτό τον τρόπο η πληροφορία πλέον αλλάζει επίπεδο ασφάλειας και μπορεί να είναι προσβάσιμη από χρήστες που κανονικά δε θα έπρεπε να έχουν αυτή τη δυνατότητα [1]. Γραφική απεικόνιση αυτής της διαδικασίας παρουσιάζεται στην Εικόνα 2.4. Αυτό ακριβώς το κενό έρχεται να καλύψει η επόμενη ιδιότητα.

Ιδιότητα*

Ένα υποκείμενο επιτρέπεται να έχει δικαίωμα εγγραφής σε ένα αντικείμενο αν η ετικέτα ασφάλειας του αντικειμένου υπερτερεί της ετικέτας ασφάλειας του υποκειμένου. Η ιδιότητα * ικανοποιείται όταν σε κάθε κατάσταση αν ένα υποκείμενο έχει άδεια ανάγνωσης σε ένα αντικείμενο επιπέδου ασφάλειας A και ταυτόχρονα άδεια εγγραφής σε ένα αντικείμενο επιπέδου ασφάλειας B (όπου A>B) τότε το επίπεδο B υπερισχύει του A [11].

Αυτό που θα πρέπει να σημειωθεί σε αυτό το σημείο είναι ότι η Ιδιότητα * δεν αφορά έμπιστα υποκείμενα, τα οποία θεωρείται ότι δεν πρόκειται να μεταβιβάσουν πληροφορία σε χαμηλότερα επίπεδα ακόμη κ αν αυτό είναι δυνατό [10]. Επίσης πρέπει να υπογραμμιστεί το γεγονός ότι οι δύο αυτές ιδιότητες που αναφέραμε πρέπει να εφαρμόζονται ταυτόχρονα και πως καμία από τις δύο ξεχωριστά δεν εξασφαλίζει την ασφάλεια πρόσβασης στα αντικείμενα του συστήματος [10][11]. Με την ικανοποίηση και των δύο ιδιοτήτων αυτό που πετυχαίνουμε είναι να έχουμε εγγραφή-προς-τα-επάνω (write-up) και ανάγνωση-προς-τα-κάτω (read-down) και κατά συνέπεια αποτρέπεται η διαρροή κακόβουλου λογισμικού (malicious software) προς τα λιγότερο ασφαλή επίπεδα.

Εικόνα 2.4: Το «κενό» της Απλής Ιδιότητας



Διακριτική Ιδιότητα Ασφάλειας

Για την εφαρμογή της ιδιότητας αυτής χρησιμοποιείται μήτρα προσπέλασης για το διακριτικό έλεγχο της προσπέλασης. Η πρόσβαση επιτρέπεται μόνο αν υπάρχει αντίστοιχη εγγραφή στη μήτρα πρόσβασης [11].

Τα μειονεκτήματα που εμφανίζει το μοντέλο Bell – La Padula έγκεινται κυρίως στο ότι δεν είναι ευέλικτο αλλά ούτε και εύκολα προσαρμόσιμο σε εμπορικές εφαρμογές. Επιπλέον δεν εξασφαλίζει την ασφάλεια στην περίπτωση μεταφοράς κακόβουλου λογισμικού προς τα πιο πάνω επίπεδα αφού ένας χρήστης μπορεί να μεταφέρει πληροφορία σε ανώτερα επίπεδα η οποία όμως μπορεί να είναι απλά κακόβουλο λογισμικό. Όντας ένα ιεραρχικό μοντέλο αντιμετωπίζει τα αντίστοιχα προβλήματα και δεν ικανοποιείται πάντα η αρχή του «γνωρίζω-ότι-χρειάζεται» [2]. Χαρακτηριστικό παράδειγμα αποτελεί ότι κάθε χρήστης γνωρίζει την ύπαρξη κάθε αντικειμένου, ασχέτως των δικαιωμάτων πρόσβασης που έχει σε αυτό, πράγμα το οποίο δεν είναι επιθυμητό σε πολλές περιπτώσεις. Τέλος, το μοντέλο αυτό όπως και γενικά η πολιτική πολλών επιπέδων ασφάλειας δεν προβλέπει την προστασία από τη μη εξουσιοδοτημένη αλλαγή της πληροφορίας, παρά μόνο την εμπιστευτικότητα της πληροφορίας [1].

Τη λύση έρχεται να δώσει το μοντέλο ακεραιότητας Biba.

2.5.4. Μοντέλο Biba

Μετά την ολοκλήρωση του μοντέλου των Bell – La Padula και την εφαρμογή του διαπιστώθηκε ότι ήταν απαραίτητη η δημιουργία ενός νέου μοντέλου που δε θα εστιάζει απλά στην προστασία της εμπιστευτικότητας αλλά θα εμποδίζει τη μη εξουσιοδοτημένη τροποποίηση της πληροφορίας και κατά συνέπεια την προστασία της ακεραιότητάς της. Την τελευταία αυτή απαίτηση ασφάλειας δεν την εξασφαλίζει η πολιτική πολλών επιπέδων. Έτσι σχεδόν ένα χρόνο μετά την παρουσίαση του Bell – La Padula η MITRE Corporations το 1977 παρουσίασε ένα καινούριο μοντέλο [30]. Το όνομά του οφείλεται στον Kenneth J. Biba ο οποίος και το ανέπτυξε και αναφέρεται στη βιβλιογραφία ως μοντέλο ακεραιότητας Biba (Biba Integrity Model). Στην πραγματικότητα το μοντέλο αυτό αποτελεί συμπλήρωμα στο μοντέλο Bell – La Padula και όχι κάτι εναλλακτικό.

Κατ' αντιστοιχία με το Bell – LaPadula, τόσο τα υποκείμενο όσο και τα αντικείμενα χαρακτηρίζονται από ετικέτες ακεραιότητας. Το μοντέλο Biba ορίζει και αυτό περιορισμούς στα δικαιώματα ανάγνωσης και γραφής ανάλογα με την ιεραρχία των επιπέδων ακεραιότητας των οντοτήτων. Συγκεκριμένα ορίζονται η Ιδιότητα Απλής Ασφάλειας και η Ιδιότητα* καθώς και οι ιδιότητες Ενεργοποίησης του επεκτεταμένου μοντέλου και η ιδιότητα του δακτυλίου [2] [8][30]:

Απλή Ιδιότητα Ασφάλειας

Ένα υποκείμενο επιτρέπεται να έχει δικαίωμα ανάγνωσης ενός αντικειμένου αν η ετικέτα ακεραιότητας του αντικειμένου υπερτερεί της ετικέτας ασφάλειας του υποκειμένου.

Ιδιότητα*

Ένα υποκείμενο επιτρέπεται να έχει δικαίωμα εγγραφής σε ένα αντικείμενο αν η ετικέτα ακεραιότητας του υποκειμένου υπερτερεί της ετικέτας ασφάλειας του αντικειμένου.

Ιδιότητα ενεργοποίησης του επεκτεταμένου μοντέλου

Ένα υποκείμενο μπορεί να ενεργοποιήσει ένα άλλο υποκείμενο μόνο αν η ετικέτα ακεραιότητάς του υπερτερεί.

Ιδιότητα δακτυλίου

Ένα υποκείμενο έχει δικαίωμα ανάγνωσης για όλα τα αντικείμενα, ανεξαρτήτως της ετικέτας ακεραιότητάς του. Μπορεί όμως να τροποποιεί αντικείμενα για τα οποία η ετικέτα ακεραιότητας του υπερτερεί των αντικειμένων καθώς και να ενεργοποιεί υποκείμενα των οποίων η ετικέτα ακεραιότητας υπερτερεί της δικής του.

Ειδικότερα η ετικέτα ακεραιότητας μπορεί να έχει τις τιμές Κρίσιμη (Crucial – C), Πολύ Σημαντική (Very Important – VI), Σημαντική (Important) και οι οποίες ακολουθούν τη συσχέτιση C >VI> I. Έτσι, τα δικαιώματα ανάγνωσης και εγγραφής παρέχονται σε ένα υποκείμενο αν ικανοποιούνται οι ιδιότητες που αναφέρθηκαν και πετυχαίνουμε εγγραφή-προς-τα-κάτω (write-down) και ανάγνωση-προς-τα-επάνω (read-up) [1].

Αυτό που θα πρέπει να σημειωθεί είναι ότι οι ετικέτες ασφαλείας που αναφέρθηκαν προηγουμένως (μοντέλο Bell – La Padula) και οι ετικέτες ακεραιότητας δεν είναι το ίδιο πράγμα. Οι πρώτες καθορίζουν τα επίπεδα εμπιστευτικότητας περιορίζοντας τη ροή των πληροφοριών ενώ οι τελευταίες κυρίως αναστέλλουν την τροποποίηση αυτών.

Στην πραγματικότητα το μοντέλο Biba υποστηρίζει τόσο πολιτικές υποχρεωτικού όσο και διακριτικού ελέγχου. Η πολιτική που αναφέρθηκε παραπάνω αποτελεί την Αυστηρή Πολιτική Ακεραιότητας (Strict Integrity Policy) [2].

2.5.5. Πολιτική Κινέζικου Τείχους (Chinese Wall Security Policy)

Οι David Brewer και Michael Nash παρουσίασαν μία θεωρία που μπορούσε να χρησιμοποιηθεί για υλοποίηση δυναμικά μεταβαλλόμενων δικαιωμάτων πρόσβασης και η οποία ονομάζεται Πολιτική Κινέζικου Τείχους. Πρόκειται για μία πολιτική που αφορά εμπορικές εφαρμογές και διαχειρίζεται θέματα σύγκρουσης συμφερόντων που σχετίζονται με αναλυτές που παρέχουν συμβουλευτικές υπηρεσίες σε μια επιχείρηση.

Ένας τέτοιος σύμβουλος που εργάζεται για λογαριασμό μιας εταιρείας, αποκτά πρόσβαση σε ευαίσθητες και σημαντικές πληροφορίες της εταιρείας και οφείλει να διατηρήσει την εμπιστευτικότητα των πληροφοριών αυτών [12]. Αυτό σημαίνει ότι δεν πρέπει να έχει τη δυνατότητα να παρέχει συμβουλευτικές υπηρεσίες σε μία ανταγωνιστική της πρώτης εταιρεία. Αν αποκτήσει πρόσβαση σε σημαντικές και κρίσιμες πληροφορίες και της ανταγωνιστικής εταιρείας τότε αποκτά ένα σημαντικό ανταγωνιστικό πλεονέκτημα το οποίο μπορεί να χρησιμοποιήσει για προσωπικό του όφελος, γεγονός το οποίο δεν είναι θεμιτό[1][12].

Στόχος επομένως της πολιτικής του Κινέζικου Τείχους είναι ο εντοπισμός και η προφύλαξη της ροής πληροφοριών που μπορούν να οδηγήσουν σε συγκρούσεις συμφερόντων. Σε αντίθεση με το μοντέλο Bell – LaPadula η πρόσβαση στις πληροφορίες δεν περιορίζεται από τα ίδια τα χαρακτηριστικά της πληροφορίας [12].Τα δικαιώματα πρόσβασης του χρήστη δημιουργούνται δυναμικά ανάλογα με τις πληροφορίες στις οποίες έχει ήδη πρόσβαση.

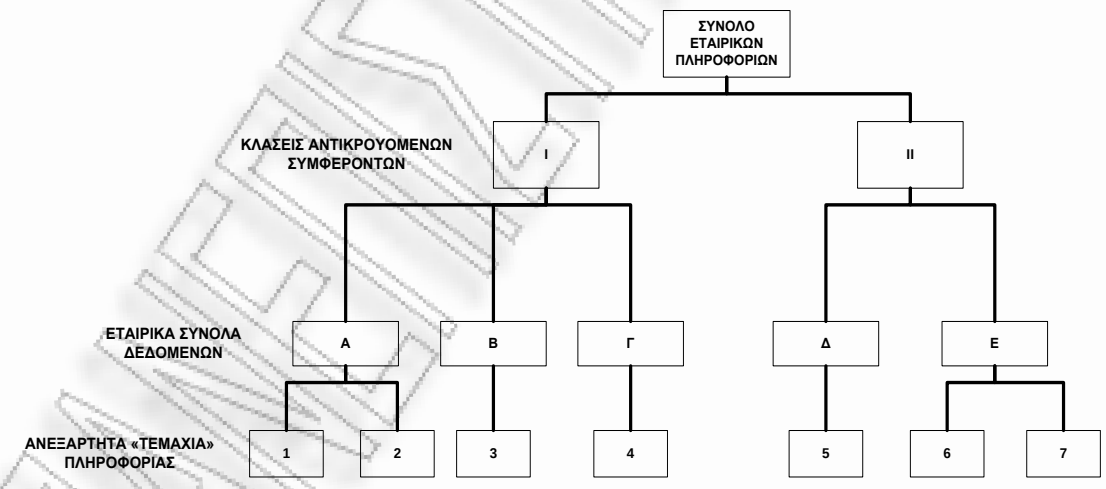
Μοντέλο Κινέζικου Τείχους ή Μοντέλο Brewer Nash

Το Μοντέλο Κινέζικου Τείχους ή Μοντέλο Brewer Nash αποτελεί την υλοποίηση της Πολιτικής Κινέζικου Τείχους. Με βάση το μοντέλο αυτό όλες οι εταιρικές πληροφορίες ταξινομούνται ιεραρχικά στα παρακάτω τρία επίπεδα [12]:

1) Στο χαμηλότερο επίπεδο βρίσκονται τα αντικείμενα τα οποία είναι ανεξάρτητα «τεμάχια» πληροφορίας που το καθένα αφορά μία εταιρεία
2) Στο ενδιάμεσο επίπεδο βρίσκονται τα Εταιρικά Σύνολα Δεδομένων (company datasets). Ως εταιρικό σύνολο δεδομένων ορίζεται το σύνολο των αντικειμένων που ανήκουν σε έναν οργανισμό/εταιρεία.
3) Στο ανώτερο επίπεδο εμφανίζονται οι Κλάσεις Αντικρουόμενων Συμφερόντων (Conflict of Interest Class –COI). Σε κάθε τέτοια κλάση ανήκουν όλα τα εταιρικά σύνολα δεδομένων που αφορούν επιχειρήσεις που είναι ανταγωνιστικές μεταξύ τους, περιλαμβάνει δηλαδή το σύνολο των ανταγωνιστικών οργανισμών. Οι κλάσεις αντικρουόμενων συμφερόντων είναι αμοιβαία αποκλειόμενες μεταξύ τους. Κάθε εταιρεία ανήκει μόνο σε μία κλάση και κάθε κλάση περιλαμβάνει τουλάχιστον δύο εταιρείες.

Τα επίπεδα στα οποία ταξινομούνται ιεραρχικά όλες οι εταιρικές πληροφορίες στο Μοντέλου Κινέζικου Τείχους παρουσιάζονται σχηματικά στην παρακάτω Εικόνα 2.5.

Εικόνα 2.5: Σύνθεση εταιρικών πληροφοριών στο Μοντέλο Κινέζικου Τείχους



Αποστειρωμένη πληροφορία

Η πληροφορία που δε θεωρείται ευαίσθητη για μια εταιρεία και γι αυτό και μπορεί να είναι προσπελάσιμη από οποιοδήποτε υποκείμενο.

Αρχικά ο σύμβουλος εφόσον δεν έχει διαβάσει κάποια πληροφορία για κάποιον οργανισμό είναι ελεύθερος να αποκτήσει πρόσβαση σε οποιαδήποτε πληροφορία επιθυμεί και για οποιοδήποτε οργανισμό αφού δεν υπάρχει σύγκρουση συμφερόντων, εκτός κι αν περιορίζεται από κάποια άλλη πολιτική όπως πχ από την πολιτική MAC. Μετά την αρχική του επιλογή για πρόσβαση στα αντικείμενα μιας εταιρείας, δημιουργείται για το σύμβουλο ένα Κινέζικο Τείχος για όλα τα dataset που βρίσκονται στην ίδια κλάση αντικρουόμενων συμφερόντων με το dataset που βρίσκεται εντός του Τείχους του [1]. Ο σύμβουλος έχει παρόλα αυτά τη δυνατότητα να αποκτήσει πρόσβαση σε οποιοδήποτε άλλο dataset ανήκει σε διαφορετική κλάση, μεταβάλλοντας έτσι το Κινέζικο Τείχος του ώστε να περιλαμβάνει και το νέο dataset.

Όπως και στο μοντέλο Bell – La Padula έτσι και στο Μοντέλο Κινέζικου Τείχους ορίζονται οι παρακάτω δύο ιδιότητες οι οποίες προσδιορίζουν τα δικαιώματα ανάγνωσης και γραφής.

Απλή Ιδιότητα Ασφάλειας

Ένα υποκείμενο επιτρέπεται να έχει πρόσβαση σε ένα αντικείμενο μόνο αν ισχύουν τα παρακάτω [12]:

Το αντικείμενο ανήκει στο ίδιο σύνολο εταιρικών δεδομένων με ένα αντικείμενο που ήδη έχει προσπελάσει το υποκείμενο

Το αντικείμενο ανήκει σε μια διαφορετική κλάση δηλαδή το υποκείμενο δεν έχει ήδη προσπελάσει ένα άλλο αντικείμενο της ίδιας κλάσης αντικρουόμενων συμφερόντων.

Φυσικά η αποστειρωμένη πληροφορία μπορεί να «διαβαστεί» από οποιοδήποτε υποκείμενο.

Ιδιότητα*

Ένα υποκείμενο μπορεί να έχει δικαίωμα εγγραφής σε ένα αντικείμενο αν [12]:

Επιτρέπεται η πρόσβαση σε αυτό σύμφωνα με την Απλή Ιδιότητα Ασφάλειας

Δεν επιτρέπεται η ανάγνωση κάποιου μη αποστειρωμένου αντικειμένου το οποίο ανήκει σε διαφορετικό σύνολο εταιρικών δεδομένων με αυτό στο οποίο ζητάμε δικαίωμα εγγραφής. Αυτό εξασφαλίζει ότι η ευαίσθητη πληροφορία μπορεί να ρέει από ένα αντικείμενο σε ένα άλλο αν και τα δύο ανήκουν στην ίδια εταιρία.

2.5.6. Μοντέλο Harrison, Ruzzo, Ullman

Το μοντέλο των Bell – La Padula που περιγράφηκε παραπάνω δεν είναι ένα δυναμικό μοντέλο. Ο ορισμός του δεν περιέχει μεθόδους για την αλλαγή των δικαιωμάτων προσπέλασης, τη δημιουργία ή τη διαγραφή υποκειμένων και αντικειμένων. Τον Αύγουστο του 1976 οι M. A. Harrison, W. L. Ruzzo and J. D. Ullman παρουσίασαν ένα νέο μοντέλο που επικεντρώνεται ακριβώς σε αυτές τις διαδικασίες ορίζοντας συστήματα εξουσιοδότησης. Αποτελεί ένα φορμαλιστικό μοντέλο που βασίζεται στον πίνακα πρόσβασης [2].

Τα στοιχεία του μοντέλου είναι ένα σύνολο αντικειμένων (O), ένα σύνολο υποκειμένων (S), ένας πίνακας πρόσβασης (A), ένα σύνολο εντολών (C) και ένα σύνολο διαδικασιών – λειτουργιών (P). Η κατάσταση του συστήματος σε κάθε δεδομένη στιγμή καθορίζεται από τα στοιχεία των (S,O,A) ενώ οι αλλαγές στην κατάσταση και η μετάβαση σε μία άλλη γίνονται μέσω των εντολών του συνόλου C.

Το μοντέλο ορίζει έξι πρωτογενείς διαδικασίες [14]:

- Δημιουργία Αντικειμένου (Create Object)

  Ένα υποκείμενο μπορεί να δημιουργήσει ένα νέο αντικείμενο

- Δημιουργία Υποκειμένου (Create Subject)
  Ένα υποκείμενο μπορεί να δημιουργήσει ένα νέο υποκείμενο
- Καταστροφή Αντικειμένου (Destroy Object)
  Ένα αντικείμενο μπορεί να διαγράψει ένα αντικείμενο
- Καταστροφή Υποκειμένου (Destroy Subject)
  Ένα υποκείμενο μπορεί να διαγράψει ένα υποκείμενο
- Προσθήκη Δικαιώματος (Add Access Right)
  Ο ιδιοκτήτης ενός αντικειμένου καθορίζει τα δικαιώματα προσπέλασης οποιουδήποτε υποκειμένου επί του αντικειμένου.
- Διαγραφή Δικαιώματος (Delete Access Right)
  Με τη διαδικασία αυτή ο ιδιοκτήτης ενός αντικειμένου διαγράφει τα δικαιώματα προσπέλασης οποιουδήποτε υποκειμένου επί του αντικειμένου.

Μία εντολή command c με παραμέτρους X_1, X_2, …, X_n δομείται ως έξης:

command c(x_1, … , x_n)
If r_1 in A[x_{s1} , x_{o1}] and
r_2 in A[x_{s2} , x_{o2}] and . . .
r_n in A[x_{sn} , x_{on}]
Then
op_1
op_2
. . .
op_n

όπου τα Xs_1,Xs_2, … ,Xs_n είναι το σύνολο των υποκειμένων, τα Xo_1,Xo_2, … ,Xo_n είναι τα αντικείμενα, r_1,r_2, … , r_n το σύνολο των δικαιωμάτων και op_1,op_2, … ,op_n πρωτογενείς λειτουργίες.

Με άλλα λόγια η δομή της ορίζει μία σειρά από ελέγχους – υποθέσεις προκειμένου να εκτελεστεί η διαδικασία (ή οι διαδικασίες) που ορίζει το κυρίως μέρος της εντολής [14].

Πρώτος Ορισμός (Διαρροή ενός δικαιώματος): Λέμε ότι μία εντολή c διαρρέει το δικαίωμα r από μία κατάσταση, αν κατά τη διάρκεια της εκτέλεσης της c για κάποιες αρχικές παραμέτρους της κατάστασης, η εκτέλεση της βασικής λειτουργίας που ορίζει η εντολή (προφανώς της μορφής Add Access Right) προσθέτει το δικαίωμα r στο κατάλληλο κελί του πίνακα πρόσβασης, το οποίο δεν περιείχε το r ακριβώς πριν την εκτέλεση της πρωτογενούς λειτουργίας [13].

Δεύτερος ορισμός: Δεδομένου ενός πίνακα A και μίας αρχικής κατάστασης αυτού, λέμε ότι ο A δεν είναι ασφαλής ως προς το δικαίωμα r αν και μόνο αν υπάρχει σειρά εντολών που να επιτρέπουν τη μετάβαση του A σε μία νέα κατάσταση στην οποία το r διαρρέει [13].

Το πιο προφανές παράδειγμα διαρροής δικαιώματος είναι αν η ίδια η εντολή περιέχει μία διαδικασία που αναιρεί την εισαγωγή του δικαιώματος στον πίνακα πρόσβασης (Delete Access Right). Φυσικά θα πρέπει να υπάρχουν δικαιώματα που διαρρέουν διαφορετικά ο πίνακας δε θα άλλαζε ποτέ [1]. Το πρόβλημα της ασφάλειας στο μοντέλο των Harrison – Ruzzo – Ullman έγκειται στο να αποδειχθεί τελικά αν ο πίνακας πρόσβασης A είναι ασφαλής ως προς ένα δικαίωμα r για σύνολο εντολών C. Το πρόβλημα αυτό έχει αποδειχθεί ότι είναι υπολογιστικά

δύσκολο στη γενική περίπτωση. Μπορεί να λυθεί μόνο για την περίπτωση που η εντολή περιέχει στο κυρίως μέρος της μία μόνο λειτουργία.

2.5.7. Μοντέλο Clark Wilson

Τα μοντέλα που είχαν αναπτυχθεί ως το 1987 και βασίζονταν στα κριτήρια ασφαλείας του TCSEC αφορούσαν κυρίως στρατιωτικές εφαρμογές. Το κενό που εμφανίζονταν ήταν ότι δεν ήταν αρκετά για να καλύψουν τις απαιτήσεις ασφάλειας που προέκυπταν στις εμπορικές εφαρμογές. Τη λύση ήρθε να δώσει ένα νέο μοντέλο που παρουσιάστηκε το 1987 σε μια δημοσίευση από τους David D.Clark και David R.Wilson.

Το μοντέλο Clark-Wilson προορίζεται για εμπορικά συστήματα και παρέχει μια δομημένη μεθοδολογία για έλεγχο προσπέλασης. Οι Clark και Wilson διαπίστωσαν ότι η εμπιστευτικότητα είναι μεν αρκετά σημαντική για τις εμπορικές εφαρμογές αλλά ιδιαίτερο βάρος σε τέτοιου τύπου εφαρμογές πρέπει να δίνεται στην ακεραιότητα. Με τον όρο ακεραιότητα αναφερόμαστε στην ποιότητα, την ορθότητα, την αυθεντικότητα και την ακρίβεια των πληροφοριών-δεδομένων που είναι αποθηκευμένες σε ένα πληροφοριακό σύστημα. Με την ακεραιότητα επιτυγχάνεται ότι τα δεδομένα τροποποιούνται με «σωστό» τρόπο μόνο από εξουσιοδοτημένους χρήστες. Έτσι σκοπός του μοντέλου είναι να διασφαλίσει ότι η πληροφορία του συστήματος είναι συνεπής ως προς το τι προσδοκούν οι χρήστες.

Το μοντέλο ορίζει δύο ειδών δεδομένα: τα δεδομένα περιορισμένου τύπου (Constrained Data Items – CDI) και τα δεδομένα μη περιορισμένου τύπου (Unconstrained Data Items – UDI). Επίσης ορίζει δύο ειδών διαδικασίες: τις διαδικασίες επαλήθευσης ακεραιότητας (Integrity Verification Procedures – IVP) και τις διαδικασίες συναλλαγής (Transaction Procedures) [2].

Οι Clark και Wilson στα πλαίσια της εξασφάλισης της ακεραιότητας της πληροφορίας προτείνουν δύο βασικές αρχές στις οποίες στηρίζουν και το μοντέλο τους [1]:

Η αρχή της καλά σχηματισμένης συναλλαγής (Well-formed Transaction)

Κάθε ολοκληρωμένη ενέργεια αποτελείται από διαδικασίες που εκτελούνται από εξουσιοδοτημένους χρήστες με τέτοιο τρόπο ώστε το σύστημα να μεταβαίνει από μία συνεπή κατάσταση σε μία νέα επίσης συνεπή. Ένας χρήστης δε θα πρέπει να διαχειρίζεται τα δεδομένα αυθαίρετα αλλά μόνο με περιορισμένους τρόπους που εξασφαλίζουν την ακεραιότητά τους [15].

Η αρχή του διαχωρισμού των καθηκόντων (Separation of Duty – SoD)

Σύμφωνα με αυτή την αρχή σκοπός είναι να εξασφαλιστεί η εξωτερική συνέπεια των δεδομένων: η συμφωνία του αντικειμένου-δεδομένου του συστήματος με το αντικείμενο του πραγματικού κόσμου που αυτό αντιπροσωπεύει. Έμμεσα, αυτό μπορεί να επιτευχθεί με το χωρισμό των διαδικασιών σε τμήματα όπου το κάθε ένα από αυτά εκτελείται από διαφορετικό πρόσωπο [15].

Ίσως το πιο χαρακτηριστικό παράδειγμα εφαρμογής για την κατανόηση του μοντέλου αυτού είναι μία τραπεζική εφαρμογή όπου καταγράφονται διάφορες συναλλαγές. Έτσι η αρχή της καλά σχηματισμένης συναλλαγής έγκειται στο ότι πρέπει να χρεώνονται και να πιστώνονται σωστά τα ποσά έτσι ώστε να μην υπάρχουν διαφορές ενώ ο διαχωρισμός των καθηκόντων επιτυγχάνεται με την απαίτηση να πραγματοποιήσει μέρος της συναλλαγής (ή έστω την τελική έγκρισή της) ο προϊστάμενος του εκάστοτε χρήστη- υπαλλήλου της τράπεζας.

Σύμφωνα με το μοντέλο θα πρέπει να ακολουθούνται οι παρακάτω εννιά κανόνες για τη διασφάλιση της ακεραιότητας των δεδομένων [15]:

Κανόνες Επικύρωσης (Certification Rules)

Κανόνας Επικύρωσης 1 (Certification Rule 1 – CR1)

Όλες οι διαδικασίες επαλήθευσης ακεραιότητας θα πρέπει κατάλληλα να εξασφαλίζουν ότι όλα τα δεδομένα περιορισμένου τύπου παραμένουν έγκυρα όταν εκτελείται η διαδικασία επαλήθευσης ακεραιότητας.

Κανόνας Επικύρωσης 2 (Certification Rule 2 – CR2)

Όλες οι διαδικασίες συναλλαγής θα πρέπει να είναι πιστοποιημένα έγκυρες. Δηλαδή θα πρέπει να μετασχηματίζουν ένα δεδομένο περιορισμένου τύπου σε μία έγκυρη τελική κατάσταση, δεδομένου ότι αυτό αρχικά ήταν επίσης σε έγκυρη κατάσταση. Για κάθε μία διαδικασία συναλλαγής και για κάθε μία ομάδα δεδομένων περιορισμένου τύπου που αυτή υπάρχει πιθανότητα να διαχειριστεί κατά την εκτέλεσή της, ο υπεύθυνος ασφάλειας του συστήματος θα πρέπει να καθορίσει τη σχέση που θα ορίζει αυτή την εκτέλεση καθορίζοντας ποια δεδομένα περιορισμένου τύπου μπορεί τελικά αυτή η συναλλαγή να επηρεάσει. Οι σχέσεις αυτές είναι της μορφής (TP, (CDIa, CDIb, CDIc…)).

Κανόνας Επικύρωσης 3 (Certification Rule 3 – CR3)

Πρέπει να εξασφαλίζεται η αρχή του διαχωρισμού των καθηκόντων

Κανόνας Επικύρωσης 4 (Certification Rule 4 – CR4)

Όλες οι διαδικασίες συναλλαγής θα πρέπει να είναι εξουσιοδοτημένες να γράφουν σε ένα αρχείο (log file) μόνο προσθέτοντας εγγραφές με όλες τις πληροφορίες που απαιτούνται έτσι ώστε να είναι δυνατή η ανακατασκευή της συναλλαγής.

Κανόνας Επικύρωσης 5 (Certification Rule 5 – CR5)

Κάθε διαδικασία συναλλαγής που λαμβάνει ως είσοδο ένα δεδομένο μη περιορισμένου τύπου πρέπει να είναι εξουσιοδοτημένη είτε να πραγματοποιεί μόνο έγκυρους μετασχηματισμούς είτε να μην κάνει κανένα μετασχηματισμό για κάθε πιθανή τιμή του δεδομένου μη περιορισμένου τύπου. Το αποτέλεσμα του μετασχηματισμού θα πρέπει να είναι ένα δεδομένο περιορισμένου τύπου ή αλλιώς η είσοδος να απορρίπτεται.

Κανόνες Υλοποίησης

Κανόνας Υλοποίησης 1 (Enforcement Rule 1 – ER1)

Το σύστημα θα πρέπει να διατηρεί τον κατάλογο των σχέσεων που περιγράφονται στον Κανόνα Υλοποίησης 2 έτσι ώστε να εξασφαλίζεται ότι μόνο διαδικασίες συναλλαγής που είναι εξουσιοδοτημένες να μετασχηματίζουν ένα δεδομένο περιορισμένου τύπου τελικά το επηρεάζουν.

Κανόνας Υλοποίησης 2 (Enforcement Rule 2 – ER2)

Το σύστημα θα πρέπει να διατηρεί κατάλογο για κάθε χρήστη με σχέσεις της μορφής (UserID, (TPi,(CDIa,CDIb,CDIc,…))) όπου συσχετίζεται ένας χρήστης και μία διαδικασία συναλλαγής με τα δεδομένα περιορισμένου τύπου που μπορεί η συναλλαγή αυτή να μετασχηματίσει εκ μέρους του χρήστη. Πρέπει να διασφαλίζεται ότι εκτελούνται μόνο συναλλαγές που αποτυπώνονται σε αυτές τις σχέσεις.

Κανόνας Υλοποίησης 3 (Enforcement Rule 3 – ER3)

Το σύστημα πρέπει να αυθεντικοποιεί την ταυτότητα κάθε χρήστη που επιχειρεί να εκτελέσει μία συναλλαγή.

Κανόνας Υλοποίησης 4 (Enforcement Rule 4 – ER4)

Μόνο η οντότητα που έχει δικαίωμα πιστοποίησης μπορεί να αλλάξει τον κατάλογο των οντοτήτων που συσχετίζονται με άλλες οντότητες, συγκεκριμένα αυτές που σχετίζονται με διαδικασίες συναλλαγής. Η οντότητα πιστοποίησης δε θα πρέπει να έχει δικαίωμα να εκτελέσει αυτές τις διαδικασίες συναλλαγής.

Εν συγκρίσει με τα μοντέλα Bell – La Padula και Biba αυτό που θα πρέπει να σημειωθεί είναι ότι στο μοντέλο Clark – Wilson σε κάθε υποκείμενο/χρήστη ανατίθεται ένα σύνολο διαδικασιών συναλλαγής και όχι ένα επίπεδο ασφάλειας ή ακεραιότητας. Αντίστοιχα, στις διαδικασίες ανατίθεται ένα σύνολο αντικειμένων που μπορούν να μετασχηματίσουν και όχι επίπεδο ασφάλειας/ακεραιότητας. Τέλος, η αρχή που για πρώτη φορά συναντάμε στο μοντέλο αυτό είναι η αρχή του Διαχωρισμού των καθηκόντων [1].

2.5.8. Μοντέλο Domain-Type Enforcement (DTE)

Πρόκειται για ένα βελτιωμένο τύπο του μηχανισμού type enforcement που αναπτύχθηκε τη δεκαετία του ΄80 από τους Robert και Kain για να ενισχύσει το μοντέλο MAC. Ειδικότερα ο μηχανισμός DTE έχει χρησιμοποιηθεί σε firewalls, λειτουργικά συστήματα και έχει αποδειχθεί ότι μπορεί να υποστηρίξει ένα σύνολο από πολιτικές που εκφράζονται μέσω των μοντέλων ελέγχου πρόσβασης βασισμένα σε ρόλους (RBAC) που θα μελετήσουμε παρακάτω.

Στο μοντέλο αυτό συναντάμε τις ενεργές οντότητες, τα υποκείμενα, και τις παθητικές οντότητες, τα αντικείμενα. Κάθε υποκείμενο σχετίζεται με μία ετικέτα τομέα (domain) ανάλογα με τη λειτουργία του και κάθε αντικείμενο με ένα τύπο (type) ανάλογα με τις απαιτήσεις ακεραιότητας του αντικειμένου.

Το μοντέλο υλοποιεί κανόνες υποχρεωτικού ελέγχου πρόσβασης προκειμένου να μεσολαβήσει στην πρόσβαση μεταξύ τομέων και τύπων. Εμφανίζονται δύο τύποι αδειών πρόσβασης: άδειες πρόσβασης από τομέα σε τομέα (domain-domain permissions) και άδειες πρόσβασης από τομέα σε τύπο (domain-type permissions). Για κάθε ένα τύπο άδειας πρόσβασης υπάρχει και ένας αντίστοιχος πίνακας πρόσβασης που τον αναπαριστά. Ο πίνακας ελέγχου πρόσβασης τομέα-τομέα (domain-domain access control table DDAT) είναι ένας δισδιάστατος πίνακας που για κάθε ζευγάρι τομέων παρουσιάζει μια εγγραφή με τα δικαιώματα πρόσβασης μεταξύ αυτών. Ομοίως ο πίνακας ελέγχου πρόσβασης τομέα-τύπου (domain-type access control table DTAT) αποθηκεύει για κάθε ζευγάρι τομέα-τύπου εγγραφή με τα αντίστοιχα δικαιώματα πρόσβασης [1]. Το σύνολο των εγγραφών των δύο αυτών πινάκων αποτελούν τη DTE βάση δεδομένων για ένα υπολογιστικό περιβάλλον.

Υπάρχουν αρκετές ομοιότητες μεταξύ του μοντέλου αυτού και του RBAC με αποτέλεσμα να μπορεί το μοντέλο αυτό να υλοποιεί πολιτικές που εκφράζονται από ένα RBAC μοντέλο.

2.6. Επίλογος

Στις παραπάνω ενότητες παρουσιάσαμε και περιγράψαμε τα βασικότερα μοντέλα ελέγχου πρόσβασης, τις ιδιότητες που ορίζουν αλλά και τους τρόπους με τους οποίους ιεραρχούν τα αντικείμενα, τα υποκείμενα ή και την ίδια την πληροφορία έτσι ώστε να εξασφαλίσουν εμπιστευτικότητα, ακεραιότητα, αυθεντικοποίηση ή και συνδυασμό αυτών.

Είδαμε το Διακριτικό Έλεγχο Πρόσβασης (DAC), πολιτική που υποστηρίζεται ευρέως στα υπάρχοντα υπολογιστικά συστήματα παρόλο που δεν παρέχει υψηλά επίπεδα ασφαλείας. Από

τα σημαντικότερα «τρωτά» της σημεία είναι το ότι είναι ευάλωτη στο Δούρειο Ίππο. Παρουσιάσαμε την πολιτική του Υποχρεωτικού Ελέγχου Πρόσβασης (MAC), πολιτική η οποία ναι μεν παρέχει πιο δυνατούς μηχανισμούς ασφάλειας σε σχέση με το DAC, αλλά που χαρακτηρίζεται από μικρή ευελιξία αφού στηρίζεται στον καθορισμό πολλών στατικών επιπέδων ασφάλειας. Η ιδιότητα αυτή κάνει τη MAC πολιτική ιδιαίτερα δημοφιλή στις στρατιωτικές εφαρμογές. Το μοντέλο Bell – LaPadula βασισμένο σε αυτή την πολιτική κληρονομεί από τον έλεγχο MAC τόσο τα πλεονεκτήματα της εμπιστευτικότητας όσο και τα μειονεκτήματα της εξάρτησης των επιπέδων ασφαλείας από τις εκάστοτε εφαρμογές. Στον αντίποδα του στρατιωτικού κόσμου, παρουσιάζεται το μοντέλο Biba το οποίο βρίσκει μεγάλη απήχηση στις εμπορικές κυρίως εφαρμογές και το οποίο καλύπτει το κενό της προστασίας της ακεραιότητας της πληροφορίας που άφηνε το Bell – LaPadula. Απλό και εύκολο να υλοποιηθεί αποτελείται από ένα σύνολο πολιτικών δίνοντας τη δυνατότητα να επιλεγεί αυτή που κρίνεται κατάλληλη. Το γεγονός ότι δε διαθέτει μηχανισμούς που να εξασφαλίζουν εμπιστευτικότητα, το κάνει να θεωρείται συμπληρωματικό του Bell – LaPadula και όχι εναλλακτικό αυτού. Επίσης, δεν υποστηρίζει την παραχώρηση και την ανάκληση εξουσιοδότησης.

Η περίπλοκη φύση και το μέγεθος του εμπορικού κόσμου, όμως, αποτελούν πρόσφορο έδαφος για τη συνεχή ανάπτυξη μοντέλων ελέγχου πρόσβασης. Τα κενά ασφάλειας που υπάρχουν αλλά και τα όποια κενά δημιουργούνται εξαιτίας του δυναμικά μεταβαλλόμενου επιχειρησιακού περιβάλλοντος απαιτούν λύσεις οι οποίες θα πρέπει να δοθούν μέσα από αυστηρά καθορισμένα πλαίσια ώστε να θεωρηθούν αποτελεσματικές. Ένα μοντέλο αυτού του τύπου, που λειτουργεί υπό σαφώς καθορισμένες αρχές είναι το Clark – Wilson. Ορίζοντας επίπεδα ακεραιότητας, όπως και το Biba, δίνει έμφαση στη συνέπεια της πληροφορίας του συστήματος με τις προσδοκίες των εξωτερικών χρηστών. Παράλληλα εισάγεται για πρώτη φορά η αρχή του διαχωρισμού των καθηκόντων για την εξασφάλιση της συνέπειας αυτής. Εν συγκρίσει με τα μοντέλα Bell – LaPadula και Biba, το μοντέλο των Clark – Wilson περιλαμβάνει μηχανισμούς ταυτοποίησης και αυθεντικοποίησης των υποκειμένων.

Ο καθορισμός ετικετών και επιπέδων ασφάλειας και ακεραιότητας των παραπάνω μοντέλων, περιορίζει τη δυναμικότητα προσαρμογής του ελέγχου που παρέχουν σε νέα δεδομένα. Το Chinese Wall αποτελεί την πρώτη προσπάθεια δυναμικής αλλαγής των δικαιωμάτων πρόσβασης. Βασισμένο κατά κύριο λόγο στη διατήρηση της ιστορικότητας των προσπελάσεων του κάθε υποκειμένου, και έχοντας ως κύριο στόχο την αποφυγή σύγκρουσης συμφερόντων αποτελεί μία νέα προσέγγιση στον έλεγχο της πρόσβασης η οποία δε στηρίζεται στα χαρακτηριστικά της πληροφορίας αυτής καθ' εαυτής.

Σε καμία περίπτωση δεν μπορούμε να δεχτούμε όμως, ότι η απαίτηση για ένα μοντέλο δυναμικό που θα μπορεί εύκολα να προσαρμόζεται στις συνεχείς μεταβολές του εκάστοτε πληροφοριακού συστήματος, και ειδικά αυτών που εντάσσονται στον τομέα των επιχειρήσεων, καλύπτεται από το Chinese Wall. Η βέλτιστη λύση που έχει δοθεί, τουλάχιστον με τα μέχρι τώρα δεδομένα, βασίζεται στην έννοια του ρόλου και περιγράφεται στο επόμενο κεφάλαιο.

3. ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ ΒΑΣΙΣΜΕΝΟΣ ΣΕ ΡΟΛΟΥΣ

3.1. Αντί Εισαγωγής…

Ο άξονας γύρω από τον οποίο αναπτύχθηκαν τα μοντέλα που περιγράφηκαν παραπάνω είναι κυρίως αυτός του τομέα των κυβερνητικών και στρατιωτικών οργανισμών. Άλλωστε ο επίσημος ορισμός τους περιγράφεται στο λεγόμενο «Πορτοκαλί Βιβλίο» (Orange Book) του Υπουργείου Άμυνας των ΗΠΑ. Οι ανάγκες που καλύπτουν αφορούν τον αρκετά περιορισμένο και «αυστηρό» κόσμο των στρατιωτικών εφαρμογών και δεδομένων αλλά και τη λιγότερο απαιτητική ακαδημαϊκή κοινότητα. Οι πολιτικές υποχρεωτικού ελέγχου επικεντρώνονται στην εμπιστευτικότητα των πληροφοριών ενώ οι πολιτικές διακριτικού ελέγχου αποδεικνύονται ανεπαρκείς στη διαχείριση του συνόλου της πληροφορίας.

Η ανάπτυξη των μοντέλων αυτών αποτελούσε ένα πολύ σημαντικό βήμα στη διαχείριση των δικαιωμάτων των χρηστών και στην εξέλιξη του έλεγχου πρόσβασης, και ειδικά ο διακριτικός έλεγχος πρόσβασης ήταν ευρύτατα διαδεδομένος στο επιχειρηματικό περιβάλλον. Παρόλα αυτά δεν καλύπτονταν επαρκώς και με την απαιτούμενη ευελιξία οι ανάγκες του εμπορικού κόσμου. Τη λύση έρχεται να δώσει ένα νέο μοντέλο ελέγχου πρόσβασης βασισμένο σε ρόλους (Role Based Access Control - RBAC).

Όπως φαίνεται και από το όνομά του το νέο αυτό μοντέλο βασίζεται στην έννοια του ρόλου. Ο ρόλος είναι στην ουσία ένα σύνολο δικαιωμάτων που αντιπροσωπεύουν τις δραστηριότητες π.χ. μιας θέσης εργασίας σε μια εταιρεία. Χαρακτηριστικό του ρόλου στα πλαίσια της επιχείρησης είναι ότι αυτός παραμένει σταθερός σε σχέση με τους χρήστες στους οποίους ανατίθεται. Για παράδειγμα η θέση του λογιστή είναι κάτι πάγιο σε μια εταιρεία. Το ποιος χρήστης κατέχει αυτή τη θέση είναι πιο πιθανό να μεταβληθεί ενώ υπάρχει και η δυνατότητα ο ίδιος ρόλος να ανατεθεί σε περισσότερα του ενός άτομα.

Πολλές φορές η έννοια του ρόλου συγχέεται με την έννοια της ομάδας χρηστών. Θα πρέπει να διευκρινιστεί ότι ο ρόλος αποτελεί ένα σύνολο δικαιωμάτων ενώ η ομάδα αποτελεί ένα σύνολο χρηστών, στους οποίους δίνονται κάποια κοινά δικαιώματα.

Το RBAC άλλαξε τα μέχρι τότε δεδομένα στο χώρο της διαχείρισης πρόσβασης προσφέροντας μεγαλύτερη ευελιξία και καλύτερο έλεγχο. Παρακάτω παρουσιάζονται πιο αναλυτικά οι βασικές αρχές καθώς και μερικές από τις σημαντικότερες μετέπειτα επεκτάσεις του.

3.2. Το RBAC στον Άξονα του Χρόνου

Η ιστορία του RBAC ξεκινάει ουσιαστικά το 1992 όταν οι Ferraiolo και Kuhn προτείνουν ένα νέο μοντέλο ελέγχου πρόσβασης [18] που αποτελεί μία διαφορετική άποψη στον τρόπο διαχείρισης των δικαιωμάτων πρόσβασης των χρηστών. Παρακάτω παρουσιάζεται η πορεία του μοντέλου και πώς χρονολογικά αποδίδεται η ανάπτυξή του σύμφωνα με το NIST [17].

- 1992 – Οι David Ferraiolo και D. Richard Kuhn ορίζουν το μοντέλο RBAC το οποίο καθορίζει πρόσβαση μόνο μέσω ρόλων, ιεραρχιών και περιορισμών [18].
- 1994 – Οι Nyanchama και Osborn εισάγουν την έννοια του μοντέλου γραφημάτων ρόλων.
- 1994 – Η IBM παρουσιάζει στην Ευρώπη την πρώτη εφαρμογή που βασίζεται στο RBAC κάνοντας ειδική αναφορά στους Ferraiolo και Kuhn.

- 1995 – Οι Ferraiolo, Cugini, Kuhn επεκτείνουν το αρχικό μοντέλο ορίζοντας τύπους διαχωρισμού καθηκόντων.
- 1996 – Δημοσιεύεται μια νέα μελέτη για την οικογένεια των μοντέλων RBAC από τους Sandhu Coyne, Feinstein και Youman.
- 1996 – Ο Sandhu προτείνει για πρώτη φορά μέθοδο υλοποίησης των αρχών του MAC σε RBAC σύστημα.
- 1997-1998 – Οι εταιρείες Sybase, Secure Computing και Siemens ανακοινώνουν την προώθηση RBAC προϊόντων τα οποία αναφέρεται ότι στηρίζονται άμεσα στο μοντέλο των Ferraiolo-Kuhn.
- 1997 – Η Secure Computing ενσωματώνει το μοντέλο Ferraiolo-Kuhn RBAC model στο καθολικό σύστημα διοίκησης και ελέγχου του Αμερικανικού Υπουργείου Αμύνης (US DoD Global Command and Control System).
- 1997 – Ένα νέο άρθρο του Kuhn επικεντρώνεται στο διαχωρισμό των καθηκόντων ως απαραίτητη και σημαντική συνθήκη για την ασφάλεια.
- 1997 – Μέσα από το άρθρο του Osborn καθορίζεται η σχέση μεταξύ του RBAC και των Πολιτικών Ασφαλείας Πολλών Επιπέδων Υποχρεωτικού Ελέγχου Πρόσβασης (MLS/MAC) [29].
- 1997 – Οι Ferraiolo and Barkley καταγράφουν τα οικονομικά πλεονεκτήματα του RBAC.
- 1998 – Παρουσίαση μεθόδου υλοποίησης RBAC μέσα από MAC συστήματα από τον Kuhn.
- 1999 – Οι Barkley, Ferraiolo, Kuhn, Cincotta αναπτύσσουν πρότυπο ανοικτού κώδικα για την εφαρμογή του RBAC σε εξυπηρετητές ιστού (web servers).
- 2000 – Ορισμός ενοποιημένου RBAC μοντέλου και πρόταση του RBAC προτύπου (standard) από τους Sandhu, Ferraiolo, Kuhn.
- 2004 – Το American National Standards Institute, International Committee for Information Technology Standards (ANSI/INCITS) υιοθετεί την πρόταση των Sandhu, Ferraiolo, Kuhn για το RBAC και το αναγνωρίζει ως ένα κοινά αποδεκτό βιομηχανικό πρότυπο.

Η εξέλιξη του μοντέλου φυσικά δε σταματάει στο 2004. Τα πλεονεκτήματά του το κάνουν ένα ευρέως διαδεδομένο μοντέλο ελέγχου πρόσβασης και δικαιωμάτων ειδικά στον εμπορικό κόσμο. Με την επίσημη καθιέρωσή του ως πρότυπο οριοθετείται μία νέα εποχή όπου πλέον στο μοντέλο αρχίζουν να προστίθενται στοιχεία που διευκολύνουν τις εκάστοτε ανάγκες των οργανισμών και των συστημάτων ανά τον κόσμο. Με αυτόν τον τρόπο δημιουργούνται παραλλαγές του μοντέλου οι οποίες όμως στηρίζονται κατά κύριο λόγο στο πρότυπο όπως αυτό καθιερώθηκε το 2004. Τα μειονεκτήματά του ερευνώνται μέχρι και σήμερα προσφέροντας νέες προκλήσεις για την περαιτέρω εξέλιξή του.

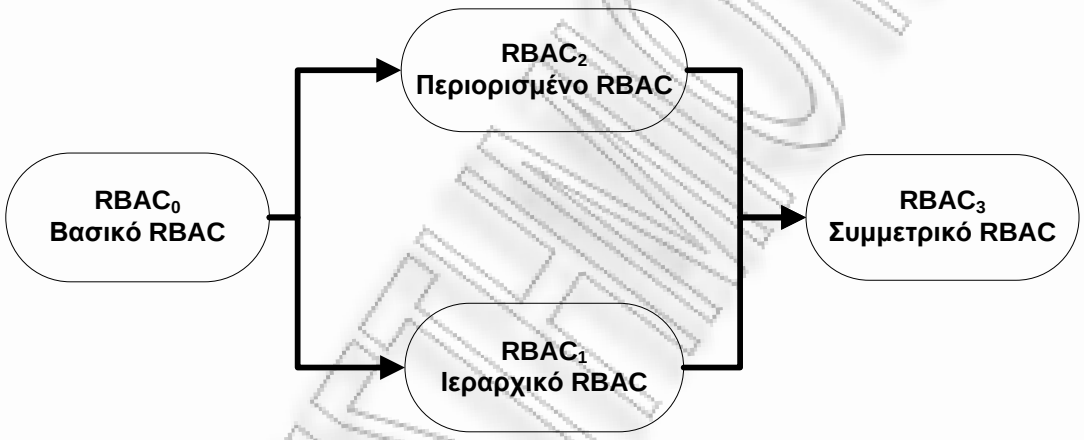
3.3. Μοντέλο Ελέγχου Πρόσβασης Βασισμένο σε Ρόλους (Role Based Access Control – RBAC)

Το μοντέλο ελέγχου πρόσβασης βασισμένο σε ρόλους αποτέλεσε μία καινοτομία στον τρόπο διαχείρισης των δικαιωμάτων πρόσβασης. Εισάγονται για πρώτη φορά έννοιες όπως ο ρόλος και ο δυναμικός διαχωρισμός των καθηκόντων. Η ανάθεση δικαιωμάτων ξεφεύγει πλέον από το χρήστη και γίνεται σε ρόλους. Παράλληλα γίνεται αναφορά σε κληρονομικότητα δικαιωμάτων μέσα από ιεραρχίες ρόλων καθώς και σε δυναμική ενεργοποίηση ρόλων στα πλαίσια

συνεδριών. Όλες αυτές οι έννοιες αναλύονται στη συνέχεια όπου παρουσιάζονται οι τέσσερις βασικές συνιστώσες του μοντέλου RBAC και οι οποίες είναι [23]:

- Βασικό RBAC ($RBAC_0$)
- Ιεραρχικό RBAC ($RBAC_1$)
  - Γενικές Ιεραρχίες
  - Περιορισμένες Ιεραρχίες
- Περιορισμένο RBAC ($RBAC_2$)
  - Στατικός Διαχωρισμός Καθηκόντων
  - Δυναμικός Διαχωρισμός Καθηκόντων
- Συμμετρικό RBAC ($RBAC_3$)

Εικόνα 3.1: Βασικές Συνιστώσες Μοντέλου RBAC



3.3.1. Βασικό RBAC

Το βασικό RBAC ενσωματώνει τα βασικά και απαραίτητα χαρακτηριστικά που συναντάμε σε όλα τα συστήματα RBAC, τα οποία αποτελούν στην ουσία την κύρια αιτία διαφοροποίησής τους από τους υπόλοιπους τύπους ελέγχου πρόσβασης. Προσδιορίζει τον ελάχιστο αριθμό στοιχείων, συνόλων και σχέσεων μεταξύ αυτών που είναι υποχρεωτικά και θεμελιώδη προκειμένου να επιτευχθεί ένα σύστημα ελέγχου πρόσβασης βασισμένο σε ρόλους.

Στο Βασικό RBAC περιλαμβάνονται πέντε βασικά στοιχεία και τα οποία είναι τα εξής: οι χρήστες, οι ρόλοι, τα αντικείμενα, οι επιτρεπτές λειτουργίες επί των αντικειμένων και, τέλος, τα δικαιώματα πρόσβασης. Παρόλο που οι έννοιες αυτές έχουν οριστεί ξανά παραπάνω, θα ήταν σημαντικό να κάνουμε μια σύντομη αναφορά σε αυτές και πάλι. Ο όρος «χρήστης» αναφέρεται σε μια ανθρώπινη οντότητα αν και μπορεί να επεκταθεί και να περιλάβει μηχανήματα, δίκτυα ή έξυπνους αυτόνομους πράκτορες. Ο «ρόλος» αποτελεί μια επαγγελματική θέση ή λειτουργία στα πλαίσια ενός οργανισμού και σχετίζεται με τις εξουσιοδοτήσεις, τα δικαιώματα και τις υποχρεώσεις που παραχωρούνται στο χρήστη στον οποίο ανατίθεται ο ρόλος. Ως «δικαίωμα πρόσβασης» νοείται η εξουσιοδότηση να εκτελεστεί μια λειτουργία σε ένα αντικείμενο του συστήματος και τέλος η «λειτουργία» είναι μια ενεργή διεργασία η οποία όταν προκληθεί, εκτελεί

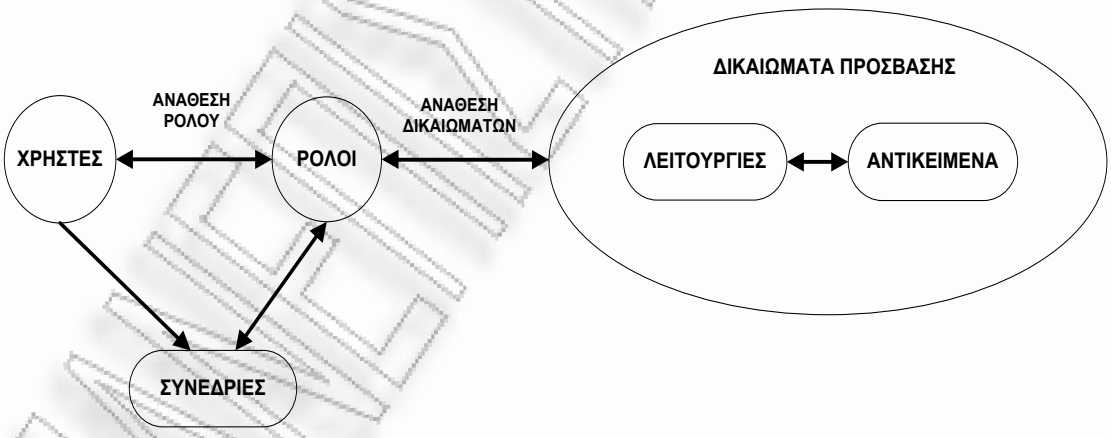
μια λειτουργία για το χρήστη. Οι τύποι των λειτουργιών και των αντικειμένων που περιλαμβάνονται στο RBAC εξαρτώνται από τον τύπο του συστήματος στο οποίο θα υλοποιηθεί ο έλεγχος πρόσβασης βασισμένος σε ρόλους.

Οι διαχειριστές του συστήματος σε έναν οργανισμό, προσδιορίζουν τις απαιτήσεις πρόσβασης στους πόρους με βάση τις τυπικές επιχειρησιακές λειτουργίες που επιτελούνται σε αυτόν και στη συνέχεια δημιουργούν ρόλους για διάφορες θέσεις εργασίας εντός του οργανισμού. Σύμφωνα με το Βασικό Μοντέλο RBAC, στους χρήστες ανατίθενται ρόλοι ανάλογα με τις αρμοδιότητες, τα καθήκοντα, τις εξουσιοδοτήσεις και τις υποχρεώσεις που έχουν στα πλαίσια της εργασίας τους [1]. Επιπλέον, τα δικαιώματα πρόσβασης ανατίθενται στους ρόλους αντανακλώντας τη βασική πολιτική που ακολουθεί ο οργανισμός καθώς και τους κανονισμούς που διέπουν τη λειτουργία του, είτε πρόκειται για εσωτερικούς κανονισμούς είτε για οδηγίες και νόμους του ευρύτερου περιβάλλοντος στο οποίο αυτός λειτουργεί.

Οι σχέσεις μεταξύ των βασικών στοιχείων που περιγράψαμε παραπάνω αποτελούν τον πυρήνα της λειτουργίας του RBAC. Δύο είναι οι βασικές σχέσεις, η ανάθεση ρόλων στους χρήστες (user-role assignment –UA) και η ανάθεση δικαιωμάτων πρόσβασης στους ρόλους (permission-role assignment –PA) [24]. Είναι σημαντικό να τονίσουμε ότι σε ένα RBAC σύστημα τα δικαιώματα πρόσβασης σχετίζονται με ρόλους, οι χρήστες είναι μέλη ρόλων κι επομένως αποκτούν τα δικαιώματα πρόσβασης των ρόλων αυτών [21]. Τα δικαιώματα πρόσβασης δεν ανατίθενται απευθείας και ατομικά στο χρήστη αλλά μέσω του ρόλου του. Το θεμελιώδες αυτό χαρακτηριστικό των συστημάτων RBAC προσφέρει μεγάλη ευελιξία και διαχειριστική ευκολία στα πλαίσια των συνεχώς μεταβαλλόμενων και εξελισσόμενων οργανωτικών λειτουργιών καθώς σε περίπτωση μεταβολών αυτό που χρειάζεται είναι να διαγράφονται τα παλιά δικαιώματα πρόσβασης ενός ρόλου και να του ανατίθενται νέα. Επιπλέον, σε περίπτωση ανάληψης νέων καθηκόντων από ένα χρήστη είναι εύκολη η ανάκληση των υφιστάμενων ρόλων του και η ανάθεση νέων ρόλων βάση των νέων απαιτήσεων εργασίας του.

Το Βασικό Μοντέλο RBAC που ήδη περιγράψαμε παρουσιάζεται συνοπτικά στην παρακάτω Εικόνα 3.2.

Εικόνα 3.2: Βασικό RBAC



Όπως προκύπτει από το παραπάνω σχήμα, το Βασικό Μοντέλο καθορίζει ότι η ανάθεση ρόλων στους χρήστες (user-role assignment –UA) και η ανάθεση δικαιωμάτων πρόσβασης στους ρόλους (permission-role assignment –PA) είναι δύο σχέσεις πολλά-προς πολλά. Αυτό

σημαίνει ότι ένας χρήστης σχετίζεται με έναν ή περισσότερους ρόλους, ένας ρόλος μπορεί να ανατεθεί σε έναν ή περισσότερους χρήστες, ένα δικαίωμα πρόσβασης μπορεί να ανατεθεί σε έναν ή περισσότερους ρόλους και ο κάθε ρόλος σχετίζεται με ένα ή περισσότερα δικαιώματα πρόσβασης.

Οι χρήστες μπορούν να ενεργοποιούν ταυτόχρονα περισσότερους από έναν ρόλους και να εξασκούν ταυτόχρονα τα δικαιώματα πρόσβασης των πολλαπλών αυτών ρόλων. Αυτό απεικονίζεται στην Εικόνα 3.2 μέσω της έννοιας της συνεδρίας (session) ή όπως αλλιώς αποκαλείται μέσω της έννοιας του υποκειμένου (subject). Η συνεδρία είναι μια αντιστοίχιση του χρήστη σε πιθανά πολλαπλούς ρόλους. Για παράδειγμα ο χρήστης εγκαθιδρύει μια συνεδρία στα πλαίσια της οποίας ενεργοποιεί ένα υποσύνολο των ρόλων που του έχουν ανατεθεί [24]. Κάθε συνεδρία σχετίζεται αποκλειστικά με ένα και μόνο χρήστη ενώ ένας χρήστης μπορεί να έχει ανοιχτές ταυτόχρονα παραπάνω από μία συνεδρίες. Τα δικαιώματα πρόσβασης του χρήστη ισούνται με το άθροισμα όλων των δικαιωμάτων πρόσβασης των ενεργών ρόλων του χρήστη σε όλες τις ενεργές συνεδρίες του [24].

Η δυνατότητα που δίνεται στους χρήστες να έχουν ταυτόχρονα ανοιχτές παραπάνω από μία συνεδρίες καθεμία από τις οποίες έχει ενεργοποιημένο ένα διαφορετικό συνδυασμό ρόλων, υποστηρίζει την αρχή του ελαχίστου προνομίου (least privilege) η οποία όπως αναφέραμε σε ένα χρήστη δε θα πρέπει να δίνονται παραπάνω δικαιώματα από αυτά που του είναι απαραίτητα για να επιτελέσει την εργασία του [20]. Ένας χρήστης στον οποίο έχουν ανατεθεί πολλαπλοί ρόλοι, ενεργοποιεί οποιοδήποτε υποσύνολο των ρόλων του χρειάζεται για να ολοκληρώσει την εργασία του στα πλαίσια μιας συγκεκριμένης συνεδρίας. Συνοψίζοντας, το βασικό μοντέλο διέπεται από τους παρακάτω 3 βασικούς κανόνες [18]:

1. Ανάθεση ρόλου (Role assignment): Ένας χρήστης μπορεί να εκτελέσει μια λειτουργία μόνο αν του έχει ανατεθεί κάποιος ρόλος. Επομένως όλοι οι ενεργοί χρήστες απαιτείται να έχουν κάποιο ενεργό ρόλο. Οι διεργασίες της αναγνώρισης και της αυθεντικοποίησης δε νοούνται ως λειτουργίες.
2. Εξουσιοδότηση ρόλου (Role authorization): Ο ενεργός ρόλος ενός χρήστη πρέπει να είναι εξουσιοδοτημένος για το συγκεκριμένο χρήστη από το διαχειριστή ασφαλείας του συστήματος. Σε συνδυασμό με τον κανόνα 1 εξασφαλίζεται ότι οι χρήστες αναλαμβάνουν μόνο ρόλους για τους οποίους είναι εξουσιοδοτημένοι.
3. Εξουσιοδότηση συναλλαγής (Transaction authorization): Ένας χρήστης μπορεί να εκτελέσει μια λειτουργία μόνο αν η λειτουργία αυτή είναι εξουσιοδοτημένη για κάποιον από τους ενεργούς ρόλους του χρήστη. Σε συνδυασμό με τους κανόνες 1 και 2, ο κανόνας αυτός εξασφαλίζει ότι οι χρήστες θα πραγματοποιήσουν μόνο λειτουργίες για τις οποίες είναι εξουσιοδοτημένοι.

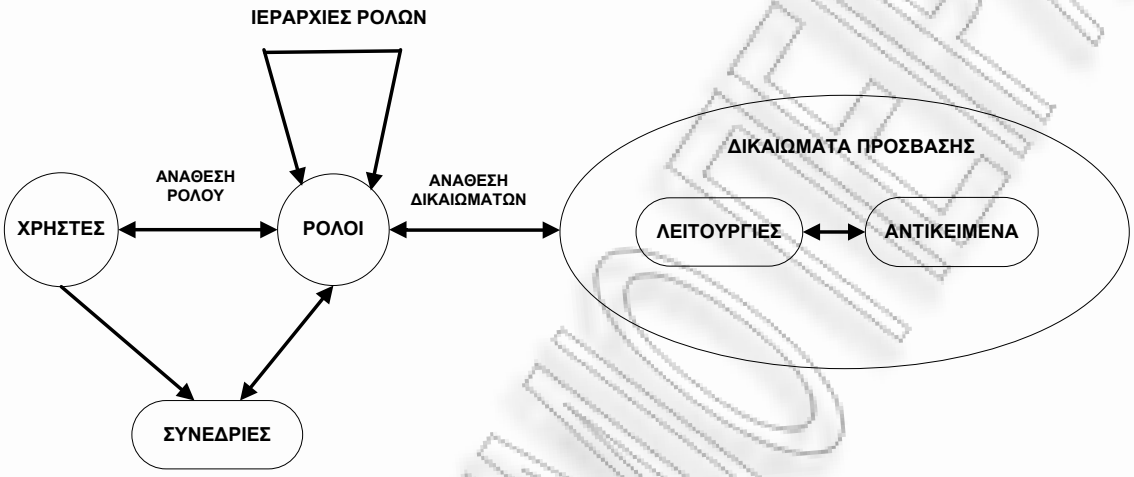
Τέλος στο βασικό RBAC υποστηρίζεται η επανεξέταση ανάθεσης ρόλων σε χρήστες [21]. Είναι σημαντικό να μπορεί να υποστηρίζεται η αλλαγή στους ρόλους που ανατίθενται σε ένα χρήστη. Αυτό γιατί στην πλειονότητα των περιπτώσεων, αυτό που μεταβάλλεται στον άξονα του χρόνου είναι τα καθήκοντά του και κατά συνέπεια αλλάζουν και οι ρόλοι που του ανατίθενται ώστε να αντανακλούν τη νέα δραστηριότητά του (πχ μετακίνηση ενός υπαλλήλου σε άλλο τμήμα της τράπεζας).

3.3.2. Ιεραρχικό RBAC

Στην προσπάθεια να προστεθούν νέες δυνατότητες στον τομέα της διαχείρισης των δικαιωμάτων πρόσβασης των χρηστών, η βάση του core-RBAC άρχισε σιγά-σιγά να εμπλουτίζεται. Έτσι το επόμενο χαρακτηριστικό που βρίσκει εφαρμογή είναι η χρήση των ιεραρχιών και η επέκταση στο $RBAC_1$.

Ετυμολογικά ως ιεραρχία ορίζεται η ταξινόμηση οντοτήτων με βάση κριτήρια αξίας και σπουδαιότητας. Αντίστοιχα η ιεραρχία των ρόλων στο μοντέλο ελέγχου πρόσβασης που βασίζεται σε αυτούς αποτελεί τη μερική διάταξη που καθορίζει σχέσεις υπεροχής μεταξύ των ρόλων.

Εικόνα 3.3: Ιεραρχικό RBAC



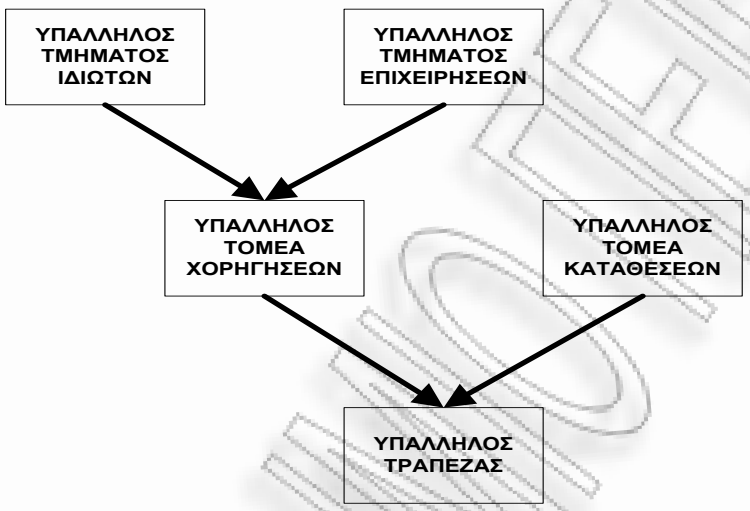
Όπως υποδεικνύει και το όνομά του το ιεραρχικό μοντέλο στηρίζεται στις ιεραρχίες και στα πλεονεκτήματα που αυτές προσδίδουν στη διαχείριση της πρόσβασης. Σε αντίθεση με τις «επίπεδες» δομές ρόλων, οι ιεραρχίες δημιουργούν συσχετίσεις μεταξύ ρόλων που ξεφεύγουν από την απλή ανάθεση ρόλων στους χρήστες και τον καθορισμό των δικαιωμάτων (βλπ core RBAC) [1] (Εικόνα 3.3). Σε αυτό το σημείο θα πρέπει να σημειωθεί ότι ο πιο κοινός τρόπος απεικόνισης των ιεραρχιών είναι με τη χρήση δενδροειδούς δομής. Είναι ίσως ο πιο κατανοητός τρόπος να αναπαρασταθεί η έννοια της διάταξης των ρόλων και της σχέσης μεταξύ τους. Συγκεκριμένα, στη βιβλιογραφία συναντάμε ιεραρχικά σχήματα με τη μορφή δέντρων, ανεστραμμένων δέντρων καθώς και συνδυασμό αυτών που οδηγεί στη δημιουργία πλέγματος.

Το βασικό κίνητρο για τη δημιουργία ιεραρχιών προήλθε μέσα από τον επιχειρηματικό κόσμο και από την ιδέα ότι στα πλαίσια ενός οργανισμού ή μιας επιχείρησης κάποιοι ρόλοι έχουν συχνά επικαλυπτόμενα δικαιώματα [1]. Χαρακτηριστικό παράδειγμα αποτελούν οι εργαζόμενοι σε ένα τμήμα. Ας δεχτούμε ότι στα πλαίσια της οργανωτικής δομής μίας τράπεζας έχουμε τον τομέα των χορηγήσεων ο οποίος χωρίζεται στα εξής δύο τμήματα: Ιδιωτών και Επιχειρήσεων. Τόσο ο υπάλληλος του τμήματος των Ιδιωτών όσο και ο υπάλληλος του τμήματος των Επιχειρήσεων πρέπει να έχουν π.χ. το δικαίωμα να βλέπουν αλλά και να καταχωρούν – ενημερώνουν τα στοιχεία των πελατών στο σύστημα. Το γεγονός αυτό μπορεί να οδηγήσει στη δημιουργία ενός γενικού ρόλου που περικλείει αυτά τα δικαιώματα και που ανατίθεται σε κάθε εργαζόμενο που προσλαμβάνεται στον τομέα των χορηγήσεων ανεξαρτήτως της θέσης του. Σε ό,τι αφορά όμως τα περαιτέρω καθήκοντά τους που διαφοροποιούνται εξαιτίας τις εξειδίκευσης της εργασίας τους αυτά αποτελούν δικαιώματα που ανατίθενται στους ξεχωριστούς ρόλους που αφορούν το κάθε τμήμα. Εάν δεν είχαμε την ιεραρχία τότε αναγκαστικά θα έπρεπε να επαναληφθεί η ανάθεση των κοινών δικαιωμάτων σε κάθε ένα ρόλο που εμφανίζεται στον τομέα. Ο ρόλος αυτός που δημιουργείται με τα κοινά δικαιώματα δύο (ή περισσότερων) άλλων ρόλων που ναι μεν έχουν κοινά δικαιώματα αλλά ο ένας δεν αποτελεί

υποσύνολο του άλλου ονομάζεται ρόλος connector [1]. Το ρόλο connector τον κληρονομούν όσοι έχουν αυτά τα δικαιώματα.

Στο παρακάτω σχήμα, Εικόνα 3.4, απεικονίζεται με τη μορφή ανεστραμμένου δένδρου η ιεραρχία των ρόλων του παραδείγματος που περιγράφηκε παραπάνω.

Εικόνα 3.4: Ιεραρχία Ρόλων με τη Μορφή Ανεστραμμένου Δένδρου

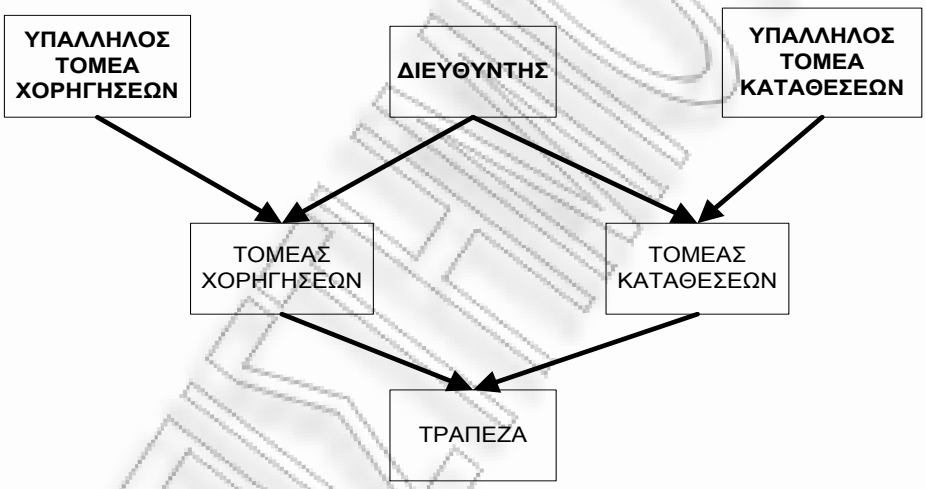


(Ο συνηθέστερος τρόπος απεικόνισης ενός διαγράμματος μερικής διάταξης ρόλων είναι έτσι ώστε να μετακινούμαστε από πάνω προς τα κάτω από τους πιο εξειδικευμένους στους πιο γενικούς ρόλους [21] [24].)

Θα πρέπει να αναφερθεί ότι δεν είναι απαραίτητο σε έναν οργανισμό να είναι όλοι οι ρόλοι μέλη μιας κοινής ιεραρχίας. Ο σκοπός της ιεραρχίας είναι μέσω της κληρονομικότητας να μειωθεί το κόστος που προκύπτει από την επανάληψη της ανάθεσης δικαιωμάτων και όχι να περιορίσει μέσα σε αυστηρά πλαίσια τη δομή του οργανισμού. Η διάταξη των ρόλων οδηγεί στη δημιουργία ρόλων χαμηλών επιπέδων και αντίστοιχα ρόλων υψηλών επιπέδων οι οποίοι συνδέονται με τέτοιο τρόπο ώστε να υποστηρίζεται η μεταβατική ιδιότητα των δικαιωμάτων των ιεραρχιών του μοντέλου [1][21]. Αυτό που γίνεται είναι ότι οι ρόλοι των υψηλότερων επιπέδων κληρονομούν τα δικαιώματα των ρόλων χαμηλότερων επιπέδων με τους οποίους αυτοί σχετίζονται άμεσα ή έμμεσα. Θα πρέπει να σημειωθεί ότι οι ρόλοι των χαμηλότερων επιπέδων είναι πιο γενικοί σε αντίθεση με αυτούς των υψηλότερων επιπέδων οι οποίοι είναι πιο εξειδικευμένοι και πιο «δυνατοί» [21]. Στο πλαίσιο της κληρονομικότητας τη μεταβατική ιδιότητα στα συστήματα που υποστηρίζουν ιεραρχίες ρόλων αντανακλούν τόσο τα δικαιώματα όσο και ο αριθμός των χρηστών – μελών των εκάστοτε ρόλων [1]. Χαρακτηριστικό αποτελεί ότι στις ιεραρχίες των ρόλων το πλήθος των δικαιωμάτων και ο αριθμός των χρηστών στους οποίους αυτοί ανατίθενται ακολουθούν αντίθετες πορείες καθώς κοιτάζουμε μία ιεραρχία ρόλων με τη μορφή δένδρου [1][21][24]. Έτσι στο παράδειγμά μας στο ρόλο του υπαλλήλου του τομέα των χορηγήσεων έχουν ανατεθεί λιγότερα δικαιώματα σε σχέση με αυτά του ρόλου του υπαλλήλου του τμήματος ιδιωτών αλλά ο αριθμός των χρηστών που ανήκουν στο ρόλο αυτό είναι μεγαλύτερος σε σχέση με αυτόν του υπαλλήλου του τμήματος ιδιωτών.

Το πρόβλημα που δημιουργείται με την κληρονομικότητα είναι ότι οι ρόλοι των υψηλών επιπέδων μπορεί τελικά να θεωρούνται και επικίνδυνοι εξαιτίας των πολλών δικαιωμάτων που τελικά έχουν κληρονομώντας και όλα αυτά των προγόνων τους. Προκειμένου να αποφευχθεί κάτι τέτοιο δίνεται η δυνατότητα δημιουργίας ιδιωτικών ρόλων (private) [21]. Για παράδειγμα, στα πλαίσια της τράπεζας, αν θεωρήσουμε την παρακάτω δομή (Εικόνα 3.5), ο διευθυντής κληρονομεί τόσο τα δικαιώματα του τομέα των χορηγήσεων όσο και αυτά του τομέα των καταθέσεων. Αυτό όμως του δίνει πολλές δυνατότητες, πράγμα που μπορεί να θεωρεί και μειονέκτημα καθώς μπορεί εύκολα να προβεί σε κάποια κακόβουλη ενέργεια που μπορεί να πλήξει το σύστημα. Έτσι, δημιουργώντας δύο ιδιωτικούς ρόλους, έναν για κάθε τομέα αντίστοιχα, επιτρέπουμε να κληρονομήσει ο διευθυντής το μεγαλύτερο μέρος των δικαιωμάτων των ρόλων «Υπάλληλος Τομέα Χορηγήσεων» και «Υπάλληλος Τομέα Καταθέσεων» αλλά κάποια δικαιώματα κληρονομούνται μόνο στους αντίστοιχους ιδιωτικούς ρόλους. Με αυτό τον τρόπο περιορίζεται η «δύναμη» του ρόλου του Διευθυντή. Με άλλα λόγια με τη χρήση των ιδιωτικών ρόλων μπορούμε να επιτύχουμε περιορισμό της κληρονομικότητας των δικαιωμάτων [21].

Εικόνα 3.5: Ιεραρχία Ρόλων με Χρήση Ιδιωτικού Ρόλου



Παρόλο που το κόστος για τη σχεδίαση ενός συστήματος είναι πιο υψηλό με τη χρήση ιεραρχιών, τα πλεονεκτήματα που προκύπτουν για τη μετέπειτα χρήση, διαχείριση και ανακατανομή των δικαιωμάτων αντισταθμίζουν το κόστος και οδηγούν στην καλύτερη σχεδίαση πολιτικής διαχείρισης δικαιωμάτων πρόσβασης των χρηστών [1].

Στην πράξη το μοντέλο ορίζει δύο ειδών ιεραρχίες [24]:

- Γενικές Ιεραρχίες Ρόλων (General Role Hierarchies)
- Περιορισμένες Ιεραρχίες Ρόλων (Limited Role Hierarchies)

Γενικές Ιεραρχίες

Πρόκειται για αυθαίρετες διατάξεις ρόλων που επιτρέπουν την πολλαπλή κληρονομικότητα δικαιωμάτων και χρηστών μεταξύ των ρόλων που συμμετέχουν στην ιεραρχία [24]. Με άλλα λόγια ο κάθε ρόλος έχει τη δυνατότητα να κληρονομεί δικαιώματα από περισσότερους του ενός

προγόνους. Με αυτή τη δυνατότητα δημιουργούνται οι λεγόμενοι ρόλοι combiner. Οι ρόλοι αυτοί συνδυάζουν μέρος των δικαιωμάτων δύο περισσοτέρων ρόλων-πηγών [1]. Στην ουσία ο ρόλος combiner αποτελεί το δυικό του ρόλου connector που αναφέρθηκε παραπάνω [1]. Έτσι η απεικόνιση των γενικών ιεραρχιών, εξαιτίας της μεγάλης ευελιξίας και ελευθερίας που παρέχουν, γίνεται κατά κύριο ρόλο μέσα από περίπλοκες δομές διαγραμμάτων που ξεφεύγουν από τα πλαίσια του δένδρου.

Περιορισμένες ιεραρχίες

Οι περιορισμένες ιεραρχίες ρόλων αποτελούν υποσύνολο των γενικών ιεραρχιών. Οι δομές απεικόνισής τους είναι απλούστερα δένδρα τα οποία περιορίζουν τους άμεσους απογόνους σε αυστηρά και μόνο ένα. Παρόλο που μπορεί να μην υποστηρίζουν την πολλαπλή κληρονομικότητα, έχουν σίγουρα συγκριτικό πλεονέκτημα έναντι των «επίπεδων» δομών ρόλων στη διαχείριση αυτών.

Αν και οι γενικές ιεραρχίες αντιπροσωπεύουν πιο ρεαλιστικά τις περίπλοκες δομές των οργανισμών και των επιχειρήσεων, οι περιορισμένες ιεραρχίες είναι αυτές που φαίνεται να έχουν ευρύτερη χρήση [1]. Ο λόγος που συμβαίνει αυτό έγκειται στο ότι παρά τους περιορισμούς που θέτουν είναι πιο απλές στην απεικόνιση αλλά και την κατανόησή τους. Άλλωστε οι δομές δένδρων, μέσα από τις οποίες αναλύονται, χρησιμοποιούνται ήδη σε πάρα πολλά συστήματα διαχείρισης (π.χ. αρχείων, φακέλων κλπ) και είναι αποδεκτές και κατανοητές από το ευρύ κοινό [1].

3.3.3. Περιορισμένο RBAC

Μία ακόμη εκδοχή του RBAC συμπληρώνεται με την έννοια της αρχής του διαχωρισμού των καθηκόντων (separation of duty). Η έννοια αυτή θέτει επιπλέον περιορισμούς στη διαχειριστική δομή του μοντέλου πρόσβασης RBAC και γι' αυτό το λόγο συναντάται στη βιβλιογραφία ως περιορισμένο RBAC (Constrained RBAC).

Σύμφωνα με το ANSI η αρχή του διαχωρισμού των καθηκόντων ορίζεται ως εξής:

Διαίρεση των ευθυνών που αφορούν «ευαίσθητες» πληροφορίες ώστε καμία μονάδα που ενεργεί ατομικά να μην μπορεί να βάλει σε κίνδυνο την ασφάλεια του συστήματος επεξεργασίας δεδομένων [16].

Με άλλα λόγια ο πιο απλός τρόπος για να αντιληφθούμε το τι σημαίνει διαχωρισμός καθηκόντων είναι να σκεφτούμε μία λειτουργία η οποία είναι μεγίστης σημασίας για το σύστημά μας και της οποίας η μη-σωστή εκτέλεση μπορεί να έχει πολύ αρνητικές συνέπειες για τον οργανισμό. Θα πρέπει να σημειωθεί ότι η μη-σωστή εκτέλεση μπορεί να προκύψει είτε από λάθος ενέργεια του χρήστη είτε από κάποια κακόβουλη απόπειρα επέμβασης στο σύστημα. Προκειμένου να αποφευχθεί κάτι τέτοιο γίνεται επιμερισμός της λειτουργίας σε δύο ή περισσότερους ρόλους με τέτοιο τρόπο έτσι ώστε η ολοκλήρωσή της να απαιτεί την υλοποίηση επιμέρους τμημάτων-μερών της λειτουργίας από όλους τους εμπλεκόμενους ρόλους [21]. Το κύριο πλεονέκτημα του διαχωρισμού των καθηκόντων είναι ότι περιορίζεται σε πολύ σημαντικό βαθμό ο κίνδυνος της κακόβουλης ενέργειας στο σύστημα καθότι για να επιτευχθεί κάτι τέτοιο απαιτείται πλέον συντονισμένη ενέργεια όλων των ρόλων στους οποίους έχει επιμεριστεί η ευθύνη. Επιπλέον καθίσταται ευκολότερος ο έλεγχος και ο εντοπισμός τυχόν λαθών αφού εμπλέκονται περισσότεροι από ένας χρήστες [1]. Ο διαχωρισμός των καθηκόντων βρίσκει πολύ συχνά εφαρμογή στον στρατιωτικό τομέα όπου για πολλές κρίσιμες ενέργειες απαιτείται η ταυτόχρονη ενέργεια δύο διαφορετικών ατόμων προκειμένου για παράδειγμα να οπλιστούν συστήματα επίθεσης.

Επιστρέφοντας στο παράδειγμα της τράπεζας η χαρακτηριστικότερη λειτουργία στην οποία βρίσκει υλοποίηση ο διαχωρισμός των καθηκόντων είναι το άνοιγμα του χρηματοκιβωτίου. Στην πλειονότητα των περιπτώσεων απαιτείται η εισαγωγή κατάλληλων συνδυασμών – κωδικών τόσο από το διευθυντή του εκάστοτε καταστήματος όσο και από τον κεντρικό ταμία προκειμένου να επιτευχθεί το άνοιγμα του χρηματοκιβωτίου. Μόνο η συνεργασία των δύο αυτών ρόλων οδηγεί στο επιθυμητό αποτέλεσμα. Κανένας από τους δύο δε θα μπορούσε να ολοκληρώσει τη λειτουργία από μόνος του.

Στο περιορισμένο RBAC διακρίνουμε δύο μεθόδους διαχωρισμού των καθηκόντων:

- Στατικός Διαχωρισμός Καθηκόντων (Static Separation of Duty)
- Δυναμικός Διαχωρισμός Καθηκόντων (Dynamic Separation of Duty)

Η κύρια διαφορά των δύο μεθόδων είναι η χρονική στιγμή εφαρμογής του διαχωρισμού. Ο Στατικός Διαχωρισμός Καθηκόντων θέτει περιορισμούς τη στιγμή της ανάθεσης ενός ρόλου σε ένα χρήστη σε αντίθεση με τον Δυναμικό Διαχωρισμό Καθηκόντων που οι περιορισμοί τίθενται όταν οι χρήστες χρησιμοποιούν ενεργά το σύστημα [18].

Όσο οξύμωρο και αν ακούγεται σε πολλούς οργανισμούς ο διαχωρισμός των καθηκόντων χρησιμοποιείται για την επιβολή πολιτικών σύγκρουσης συμφερόντων. Απώτερος σκοπός είναι ο περιορισμός των χρηστών προκειμένου να μην αποκτήσουν υψηλό επίπεδο εξουσίας ειδικά για θέσεις ισχύος και διοίκησης όπου τα δικαιώματα των χρηστών μπορεί να είναι πολλά και κατά συνέπεια καθίσταται πιο εύκολη και «προκλητική» η επιτέλεση κακόβουλης ενέργειας.

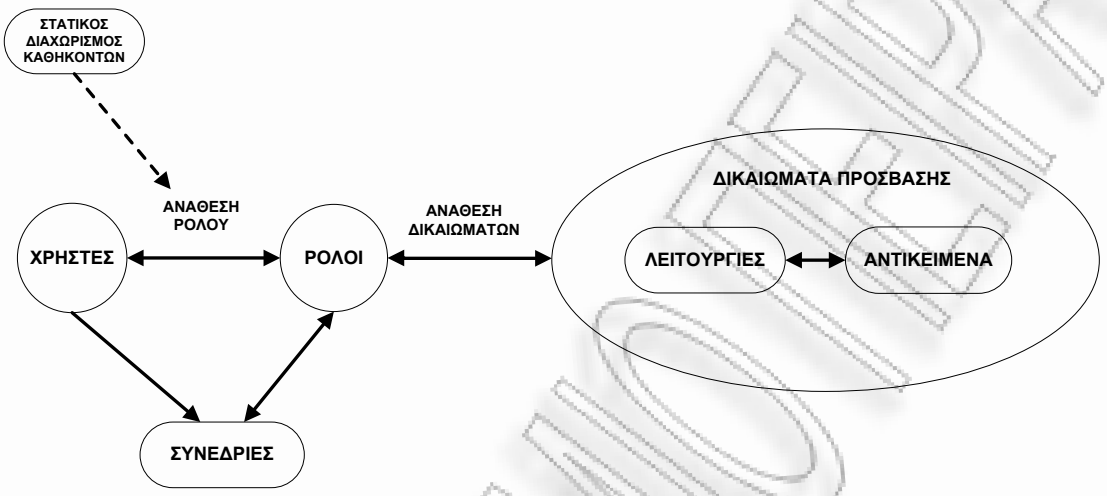
Σύγκρουση συμφερόντων μπορεί να προκύψει όταν ο χρήστης αποκτά εξουσιοδότηση για δικαιώματα πρόσβασης που σχετίζονται με δύο ή περισσότερους αντικρουόμενους ρόλους. Ο Στατικός Διαχωρισμός Καθηκόντων αποτελεί μια λύση στην σύγκρουση συμφερόντων καθώς επιβάλλει περιορισμούς στην ανάθεση ρόλων στους χρήστες. Αυτό στην πράξη σημαίνει ότι αν ένας χρήστης είναι εξουσιοδοτημένος για ένα ρόλο, τότε απαγορεύεται να του ανατεθεί ένας δεύτερος ρόλος ο οποίος έχει συγκρουόμενα με τον πρώτο δικαιώματα πρόσβασης [1]. Οι δύο αυτοί ρόλοι ονομάζονται αμοιβαία αποκλειόμενοι ρόλοι. Επομένως, σύμφωνα με το Στατικό Διαχωρισμό Καθηκόντων σε ένα χρήστη μπορεί να ανατεθεί ένας ρόλος μόνο όταν αυτός ο ρόλος δεν είναι αμοιβαία αποκλειόμενος με οποιονδήποτε από τους ήδη υπάρχοντες ρόλους του χρήστη [24]. Ο έλεγχος αυτός πραγματοποιείται τη στιγμή της ανάθεσης του ρόλου στο χρήστη όπως απεικονίζεται και στην Εικόνα 3.6.

Θα μπορούμε να ορίσουμε το Στατικό Διαχωρισμό Καθηκόντων ως *ένα ζευγάρι (σύνολο ρόλων, ν), όπου σε κανένα χρήστη δε μπορούν να ανατεθούν ταυτόχρονα ν ρόλοι από το σύνολο αυτό* [1]. Στις περισσότερες των περιπτώσεων το ν=2 οπότε και σε κάθε χρήστη μπορεί να ανατεθεί ένας και μόνος ρόλος από το σύνολο αυτό. Όμως από τον ορισμό αυτό προκύπτουν πολλές πολιτικές Στατικού Διαχωρισμού Καθηκόντων ανάλογα με το συνδυασμό των ρόλων για τους οποίους περιορίζεται η ανάθεση στους χρήστες. Για παράδειγμα μπορούν να περιορίσουν ένα χρήστη από το να μπορεί να γίνει μέλος οποιουδήποτε συνδυασμού δύο ή περισσοτέρων ρόλων από το σύνολο ρόλων σε μια περίπτωση ενώ σε μια άλλη να τον περιορίσουν από το να μπορεί να του ανατεθεί κάποιος ρόλος από ένα προκαθορισμένο σύνολο ρόλων.

Επανερχόμενοι στο παράδειγμα της Τράπεζας, μια περίπτωση σύγκρουσης συμφερόντων και διαχωρισμού καθηκόντων εμφανίζεται στη διαδικασία έγκρισης και χορήγησης ενός δανείου. Η αίτηση και η δημιουργία του δανείου πραγματοποιούνται από τον υπάλληλο του τμήματος Ιδιωτών ενώ στη συνέχεια η έγκριση και η τελική εκταμίευση του δανείου γίνονται από τον προϊστάμενο του τμήματος Ιδιωτών. Οι δύο αυτοί ρόλοι είναι αμοιβαία αποκλειόμενοι καθώς αν ο ίδιος υπάλληλος πραγματοποιούσε τόσο τη δημιουργία του δανείου όσο και την έγκριση και την εκταμίευσή του, αυτό σημαίνει μεγάλη συγκέντρωση δύναμης και εξουσίας σε αυτόν και

ελλοχεύει τον κίνδυνο της απάτης. Επομένως, δε μπορεί να πραγματοποιεί όλες τις παραπάνω διαδικασίες ο ίδιος υπάλληλος.

Εικόνα 3.6: Περιορισμένο RBAC με Στατικό Διαχωρισμό Καθηκόντων



Ο Στατικός Διαχωρισμός Καθηκόντων είναι εύκολα υλοποιήσιμος στα πλαίσια ενός RBAC συστήματος όμως είναι αρκετά περιοριστικός και πολλές φορές δύσκολα εφαρμόσιμος σε μικρούς οργανισμούς που απασχολούν μικρό αριθμό ατόμων [1]. Στις περιπτώσεις αυτές καθίσταται δύσκολος ο καθορισμός των αμοιβαία αποκλειόμενων ρόλων καθώς δεν υπάρχει επαρκής αριθμός υπαλλήλων για να πραγματοποιήσουν όλες τις αμοιβαία αποκλειόμενες λειτουργίες.

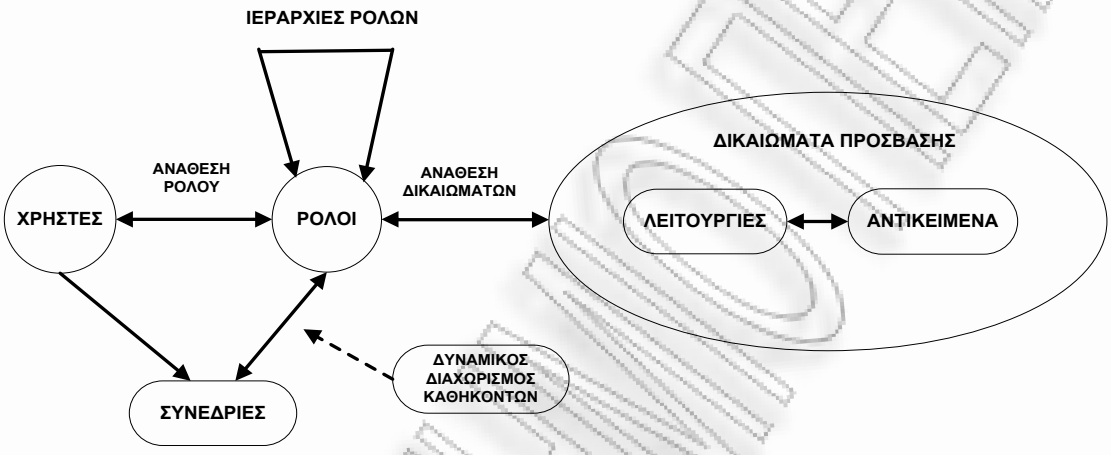
Τη λύση στη δυσκαμψία που εμφανίζει πολλές φορές ο Στατικός Διαχωρισμός Καθηκόντων έρχεται να φέρει ο Δυναμικός Διαχωρισμός Καθηκόντων ο οποίος προσδιορίζει αποκλειστικές σχέσεις όσον αφορά τους ρόλους που ενεργοποιούνται ως μέρος της συνεδρίας ενός χρήστη [24]. Όπως και στο Στατικό Διαχωρισμό, ο σκοπός είναι ο περιορισμός των διαθέσιμων δικαιωμάτων πρόσβασης σε ένα χρήστη. Όπως έχουμε αναφέρει και παραπάνω, ο χρήστης εγκαθιστά μια συνεδρία στα πλαίσια της οποίας μπορεί να ενεργοποιήσει ένα οποιοδήποτε υποσύνολο των εξουσιοδοτημένων γι αυτόν ρόλων. Ο Δυναμικός Διαχωρισμός Καθηκόντων περιορίζει τη διαθεσιμότητα των δικαιωμάτων πρόσβασης θέτοντας περιορισμούς στους ρόλους που μπορούν να ενεργοποιηθούν στα πλαίσια μιας συνεδρίας του χρήστη.

Σε αντίθεση με το Στατικό Διαχωρισμό που παρέχει προστασία από σύγκρουση συμφερόντων πραγματοποιώντας ελέγχους την ώρα της ανάθεσης ενός ρόλου σε ένα χρήστη, ο Δυναμικός Διαχωρισμός πραγματοποιεί ελέγχους και επιβάλλει περιορισμούς την ώρα της ενεργοποίησης ενός ρόλου στα πλαίσια μιας συνεδρίας ενός χρήστη [21] (Εικόνα 3.7). Ο Δυναμικός Διαχωρισμός Καθηκόντων επιτρέπει την εξουσιοδότηση ενός χρήστη σε δύο ρόλους που δεν προκαλούν σύγκρουση συμφερόντων όταν δρουν ανεξάρτητα αλλά θέτουν ζήτημα ασφαλείας όταν ενεργοποιούνται ταυτόχρονα [24]. Εφόσον από την πολιτική του Δυναμικού Διαχωρισμού Καθηκόντων δε θα επιτραπεί ποτέ ταυτόχρονη ενεργοποίηση των δύο ρόλων, δε θα υπάρξει και ποτέ κατάσταση σύγκρουσης συμφερόντων.

Ομοίως με το Στατικό Διαχωρισμό Καθηκόντων, θα μπορούσε να ορίσουμε το Δυναμικό Διαχωρισμό Καθηκόντων ως *ένα ζευγάρι (σύνολο ρόλων, ν), ν≥2, με την ιδιότητα ότι σε καμία*

συνεδρία του χρήστη δε θα ενεργοποιηθούν ταυτόχρονα ν ή περισσότεροι ρόλοι από το σύνολο ρόλων [1]. Ο περιορισμός των ρόλων αντανακλά την πολιτική του οργανισμού κα τους περιορισμούς που διέπουν τη λειτουργία του. Οι ρόλοι που δεν επιτρέπεται να ενεργοποιηθούν ταυτόχρονα ονομάζονται και σε αυτή την περίπτωση αμοιβαία αποκλειόμενοι ρόλοι. Χρησιμοποιώντας τον όρο αυτό ορίζουμε ότι στον Δυναμικό Διαχωρισμό Καθηκόντων ένας χρήστης, στα πλαίσια μιας συνεδρίας του, μπορεί να ενεργοποιήσει ένα ρόλο όταν αυτός δεν είναι αμοιβαία αποκλειόμενος με κάποιον από τους ήδη ενεργούς του ρόλους.

Εικόνα 3.7: Περιορισμένο RBAC με Ιεραρχίες και Δυναμικό Διαχωρισμό Καθηκόντων



Η πολύ σημαντική αρχή του ελαχίστου δικαιώματος ενισχύεται με το Δυναμικό Διαχωρισμό των Δεδομένων αφού κάθε χρήστης έχει διαφορετικά επίπεδα πρόσβασης σε διαφορετικές χρονικές στιγμές ανάλογα με το ρόλο του. Αποφεύγεται με αυτό τον τρόπο η συγκέντρωση παραπάνω δικαιωμάτων πρόσβασης από αυτά που χρειάζεται για να επιτελέσει την εργασία του με όλους τους κινδύνους που αυτό κρύβει. Επιπρόσθετα, ο χρήστης κρατάει τα δικαιώματα πρόσβαση μόνο για το χρονικό διάστημα που τα χρειάζεται για να επιτελέσει την εργασία του. Η ιδιότητα αυτή της Αρχής του Ελαχίστου Δικαιώματος ονομάζεται χρονική ανάκληση της εμπιστοσύνης (timely revocation of trust)[24]. Η δυναμική ανάκληση των δικαιωμάτων πρόσβασης είναι πολύπλοκη διαδικασία ιδιαίτερα χωρίς τη βοήθεια του Δυναμικού Διαχωρισμού Καθηκόντων και γι αυτό η μελέτη της τα τελευταία χρόνια έχει μείνει πίσω.

Ο Δυναμικός Διαχωρισμός Καθηκόντων υποστηρίζει και αυτός με τη σειρά του την ύπαρξη ιεραρχιών και σε αντίθεση με τον Στατικό, οι ρόλοι μπορούν να σχετίζονται ιεραρχικά μεταξύ τους μέσω containment σχέσης [21]. Το γεγονός αυτό είναι απόλυτα συνεπές και δεν παραβιάζει τη βασική ιδιότητα του Δυναμικού Διαχωρισμού που απαγορεύει την ταυτόχρονη ενεργοποίηση ρόλων.

Υπάρχουν πολλές περιπτώσεις στις οποίες θα μπορούσαμε να χρησιμοποιήσουμε Στατικό Διαχωρισμό αντί για Δυναμικό και να πετύχουμε το ίδιο αποτέλεσμα. Η δυσκαμψία που εμφανίζει και το μεγάλο πολλές φορές κόστος που δημιουργεί η χρήση του όμως μας οδηγεί στην επιλογή του Δυναμικού ο οποίος προσφέρει μεγάλη ευελιξία και λειτουργικότητα. Επιστρέφοντας στο παράδειγμα της Τράπεζας, μια τέτοια περίπτωση είναι αυτή της διαδικασίας χορήγησης ενός δανείου. Όπως προείπαμε, απαιτούνται δύο ξεχωριστοί υπάλληλοι καθένας από τους οποίους θα αναλάβει τους αμοιβαία αποκλειόμενους ρόλους του υπαλλήλου που

συμπληρώνει την αίτηση του δανείου και δημιουργεί το δάνειο και του προϊσταμένου που εγκρίνει και εκταμιεύει το δάνειο. Χρησιμοποιώντας Στατικό διαχωρισμό δεδομένων και θέτοντας τους δύο αυτούς ρόλους σαν αμοιβαία αποκλειόμενους προστατεύουμε από συγκέντρωση μεγάλης εξουσίας για την υλοποίηση μιας ιδιαίτερα κρίσιμης διαδικασίας όπως είναι αυτή της χορήγησης ενός δανείου για μια Τράπεζα στα χέρια ενός χρήστη. Δυστυχώς στην πράξη λόγω έλλειψης προσωπικού ή άλλων αιτιών είναι δύσκολο να υπάρχουν δύο διαφορετικά άτομα που θα στελεχώσουν τους ρόλους. Στην περίπτωση αυτή η λύση προσφέρεται από το Δυναμικό Διαχωρισμό Καθηκόντων. Ο κάθε υπάλληλος της Τράπεζας μπορεί να είναι εξουσιοδοτημένος να έχει και το ρόλο αυτού που συμπληρώνει την αίτηση και δημιουργεί το δάνειο (υπάλληλος) και το ρόλο αυτού που εγκρίνει και εκταμιεύει (προϊστάμενος) αλλά απαγορεύεται να ενεργοποιήσει τους δύο αυτούς ρόλους ταυτόχρονα στα πλαίσια της ίδιας συνεδρίας. Συνοψίζοντας, διαπιστώνουμε ότι ο Δυναμικός Διαχωρισμός Καθηκόντων προσφέρει μεγάλη ευελιξία και ευκολία στο σύγχρονο εμπορικό και επιχειρηματικό κόσμο. Αντιπροσωπεύει ίσως πιο ρεαλιστικά τις δομές και τις ανάγκες των οργανισμών.

3.3.4. Συμμετρικό RBAC

Αποτελεί το τέταρτο ουσιαστικά επίπεδο του μοντέλου και συνδυάζει το περιορισμένο καθώς και το ιεραρχικό RBAC που περιγράψαμε παραπάνω.

Πηγαίνοντας ένα βήμα παραπέρα, το μοντέλο του NIST συνδυάζει το Στατικό και Δυναμικό Διαχωρισμό Καθηκόντων με τις Ιεραρχίες που αναφέρθηκαν σε προηγούμενο επίπεδο προσφέροντας με αυτό τον τρόπο ακόμη μεγαλύτερη ευελιξία (Εικόνα 3.8).

Στα πλαίσια μιας ιεραρχίας οι περιορισμοί κληρονομούνται και θα πρέπει να δίνεται μεγάλη προσοχή έτσι ώστε να διασφαλίζεται ότι η κληρονομικότητα δεν υπονομεύει τις πολιτικές του Διαχωρισμού Καθηκόντων [21]. Ο Διαχωρισμός καθηκόντων παρουσία Ιεραρχιών δουλεύει με τον ίδιο ακριβώς τρόπο με τον απλό Διαχωρισμό Καθηκόντων με τη διαφορά ότι όταν επιβάλλονται οι περιορισμοί κατά την ανάθεση ενός ρόλου ελέγχονται για σύγκρουση όχι μόνο οι άμεσα ανατεθειμένοι στο χρήστη ρόλοι αλλά και οι ρόλοι που αυτός έχει κληρονομήσει [21]. Θα ήταν παράλογο να ορίζουμε σχέση αμοιβαία αποκλειόμενων ρόλων μεταξύ δύο ρόλων όπου ουσιαστικά τα δικαιώματα του ενός αποτελούν υποσύνολο των δικαιωμάτων του άλλου.

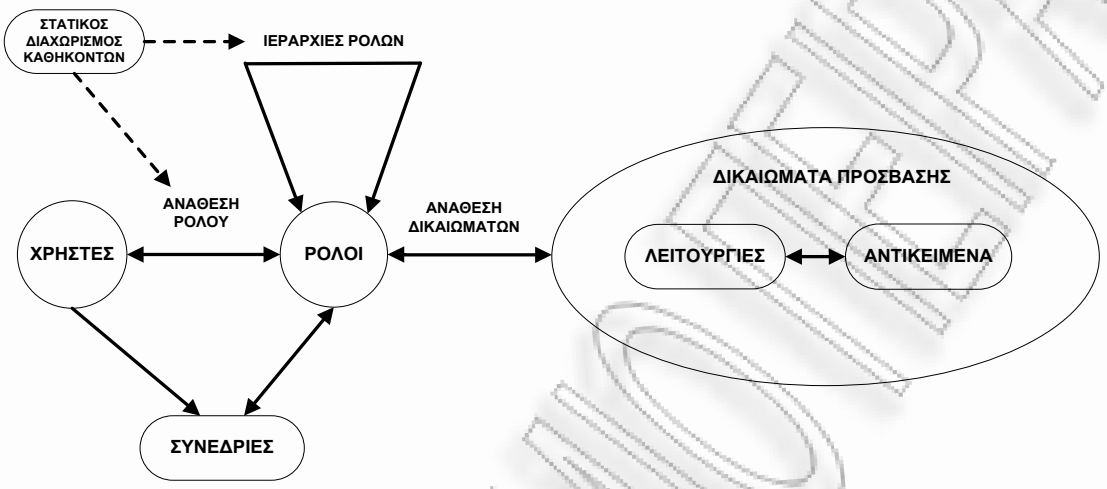
Δεδομένου ότι υποστηρίζονται οι ιεραρχίες και εδώ συναντάμε αυθαίρετες (γενικές ιεραρχίες) αλλά και περιορισμένες διατάξεις ορίζοντας κατ' αυτόν τον τρόπο δύο υποεπίπεδα στο συμμετρικό RBAC.

Η επιπλέον ιδιότητα που προσφέρει αυτό το επίπεδο του μοντέλου είναι η επανεξέταση της ανάθεσης αδειών σε ρόλους [21]. Μπορούμε να το σκεφτούμε σε αντιστοιχία της επανεξέτασης ανάθεσης ρόλων σε χρήστες που υποστηρίζεται στο βασικό RBAC. Η ανάγκη για προσαρμογή των δικαιωμάτων που ανατίθενται στους ρόλους κρίνεται απαραίτητη μέσα σε έναν οργανισμό όπου οι χρήστες και οι ρόλοι τους μπορούν να αλλάζουν δυναμικά. Εάν για παράδειγμα σκεφτούμε την πιθανή προαγωγή ενός υπαλλήλου μιας τράπεζας, τότε θα πρέπει να γίνει πολύ προσεκτική προσαρμογή των δικαιωμάτων του έτσι ώστε ούτε να καταργηθούν δικαιώματα που του είναι χρήσιμα για την εργασία του αλλά ούτε και να του δοθούν περισσότερα από όσα χρειάζονται, τηρώντας την αρχή του ελαχίστου δικαιώματος.

Μία άλλη περίπτωση στην οποία κρίνεται απαραίτητη η επανεξέταση της ανάθεσης δικαιωμάτων σε ρόλους είναι η περίπτωση όπου μέσα στην επιχείρηση γίνεται αλλαγή των εργασιών. Στην περίπτωση της τράπεζας, η απόφαση της διοίκησης για την προώθηση ενός νέου τύπου δανείου δημιουργεί νέες λειτουργίες που θα πρέπει να πραγματοποιούν οι υπάλληλοι που θα τους ανατεθεί η προώθηση αυτού και κατά συνέπεια νέα δικαιώματα στο σύστημα. Έτσι ο διαχειριστής του συστήματος θα πρέπει να διαμορφώσει ανάλογα τους αντίστοιχους ρόλους. Ο λόγος που η ιδιότητα αυτή παρουσιάζεται στο τέταρτο και τελευταίο

επίπεδο του προτύπου είναι εξαιτίας της μεγάλης δυσκολίας που παρουσιάζει η υλοποίησή της ειδικά σε οργανισμούς μεγάλης κλίμακας όπου ο έλεγχος είναι κατανεμημένος [21].

Εικόνα 3.8: Συμμετρικό RBAC



3.4. Αντί Επιλόγου…

Το μοντέλο που περιγράψαμε παραπάνω είναι αυτό που δημοσιεύτηκε από το NIST και αναγνωρίστηκε ως το βασικό πρότυπο. Όπως είδαμε καθορίζει τις βασικές αρχές και κανόνες που πρέπει να διέπουν τη λειτουργία των συστημάτων που βασίζονται στο RBAC.

Ιδιαίτερα σημαντικό είναι να διευκρινιστεί ότι υπάρχουν αρκετά σημεία τα οποία δεν προτυποποιούνται είτε γιατί από τη φύση τους αυτό δεν είναι δυνατό είτε γιατί δε θεωρήθηκε αναγκαία η παρουσία τους στα πλαίσια του προτύπου.

Ένα από αυτά τα στοιχεία είναι η κλιμάκωση του μοντέλου. Στο πρότυπο δε διευκρινίζεται σε κάποιο σημείο το πώς μπορεί να κλιμακωθεί το μοντέλο όσον αφορά των αριθμό των ρόλων, τον αριθμό των δικαιωμάτων πρόσβασης ή και ακόμα το μέγεθος των ιεραρχιών κλπ. Όπως μπορεί κανείς να αντιληφθεί αυτό είναι σημαντικό κριτήριο στην επιλογή διαχειριστικού συστήματος για μεγάλης κλίμακας επιχειρήσεις και οργανισμούς. Επιπλέον, σε ότι αφορά τη φύση των δικαιωμάτων, στο πρότυπο δεν καθορίζεται σαφής προσδιορισμός αυτών. Δε διευκρινίζεται κατά πόσο τα δικαιώματα αφορούν ενέργειες και λειτουργίες του συστήματος σε χαμηλό επίπεδο (πχ δικαιώματα ανάγνωσης και γραφής σε αρχεία) ή σε πιο υψηλό επίπεδο όπου τα δικαιώματα αφορούν τις αρμοδιότητες των χρηστών(πχ δικαίωμα ανάληψης ή κατάθεσης στα πλαίσια ενός τραπεζικού οργανισμού). Εκτός αυτού το μοντέλο δεν αναγνωρίζει τα λεγόμενα αρνητικά δικαιώματα πρόσβασης (negative permissions). Στο μοντέλο καθορίζεται τι μπορεί να κάνει ο χρήστης ενώ δε δίνεται η δυνατότητα στο διαχειριστή του συστήματος να προσδιορίσει τι ΔΕΝ μπορεί να κάνει.

Γενικά, υπάρχουν αρκετά κενά που σχετίζονται με τη διαχείριση του μοντέλου RBAC. Χαρακτηριστικό είναι ότι απουσιάζει η έννοια της εξουσιοδότησης για την επεξεργασία των ρόλων και των δικαιωμάτων. Ποιος τελικά είναι υπεύθυνος για το σχεδιασμό των ρόλων; Πώς γίνεται ο σχεδιασμός των ρόλων και ποια δικαιώματα αυτοί περιλαμβάνουν; Ποιος αναλαμβάνει την ανάθεση αυτών στους χρήστες; Ποιος καθορίζει τον ιεραρχικό συσχετισμό των ρόλων; Όλα

αυτά είναι ερωτήματα που δεν απαντώνται μέσα από το πρότυπο του NIST. Κάθε προϊόν που έχει αναπτυχθεί με βάση το RBAC δίνει τις δικές του απαντήσεις και λύσεις ανάλογα με την αγορά στην οποία απευθύνεται (διαφορετικός ρόλος αναλαμβάνει τη διαχείριση των ρόλων στην περίπτωση ενός τραπεζικού οργανισμού και διαφορετικός σε μια φαρμακευτική εταιρεία).

Έχουμε ήδη αναφέρει ότι στα πλαίσια του βασικού μοντέλου RBAC, δίνεται η δυνατότητα σε κάθε χρήστη να έχει περισσότερους από έναν ρόλους ενεργούς. Δεν περιγράφεται πως γίνεται η ενεργοποίηση των ρόλων και ποιος τελικά επιλέγει ποιοι ρόλοι είναι ενεργοί σε κάθε συνεδρία(είναι προκαθορισμένοι από το σύστημα ή επιλέγει ο χρήστης). Τέλος, ένα σημαντικός παράγοντας είναι η ανάκληση των ρόλων, ο τρόπος χειρισμού της και οι συνέπειες αυτής στο σύστημα. Παρόλα αυτά το μοντέλο δε λαμβάνει υπόψη του αυτή τη συνιστώσα.

Το σύνολο των πλεονεκτημάτων του RBAC, το θέτουν σήμερα στην πρώτη θέση όσον αφορά στην επιλογή μοντέλου για τον έλεγχο πρόσβασης. Η μη εξάρτησή του από πολιτικές, το καθιστούν μοντέλο ιδιαίτερα ευέλικτο, δυναμικό και εύκολα προσαρμόσιμο στις εκάστοτε συνθήκες. Η σημαντική αυτή ιδιότητά του βοήθησε σημαντικά στη γρήγορη εξέλιξη και ανάπτυξή του από θεωρητική προσέγγιση σε πρακτική εφαρμογή.

Το RBAC πέρα από ένα μοντέλου ελέγχου πρόσβασης υπό την έννοια που περιγράφηκε παραπάνω μπορεί να θεωρηθεί και ως μια προσέγγιση της διαχείρισης της συνολικής δραστηριότητας που πραγματοποιείται μέσα σε ένα IT περιβάλλον. Όπως έχουμε ήδη αναφέρει, η αρχή του διαχωρισμού των καθηκόντων, οι ιεραρχίες αλλά και ο συνδυασμός αυτών βοηθούν στην καλύτερη αναπαράσταση των επιχειρηματικών δραστηριοτήτων και κατά συνέπεια στην καλύτερη παρακολούθηση των διεργασιών που λαμβάνουν χώρα και στον καλύτερο έλεγχο της πρόσβασης στην πληροφορία.

Τέλος, ο χαρακτηρισμός του RBAC ως ένα γενικευμένο μοντέλο που παρέχει κεντρικό έλεγχο των πόρων, μπορεί να υποστηριχθεί από το γεγονός ότι τόσο το MAC όσο και το DAC, μπορούν να υλοποιηθούν μέσω του RBAC. Φυσικά αυτό προϋποθέτει τον ορισμό κατάλληλων ρόλων, αναθέσεων και περιορισμών. Εδώ αξίζει να σημειωθεί ότι υλοποίηση του DAC μέσω του RBAC θεωρείται αρκετά πιο περίπλοκη διαδικασία σχετικά με αυτή της υλοποίησης του MAC.

Η άλλη όψη του νομίσματος της γενίκευσης είναι ότι η μη ύπαρξη σαφώς καθορισμένων περιορισμών για παραμέτρους όπως είναι ο χρόνος, το περιβάλλον κλπ δημιουργούν ελλείψεις για την πιο άρτια λειτουργία του μοντέλου. Οι ελλείψεις αυτές ανοίγουν το δρόμο για την εισαγωγή επεκτάσεων του βασικού μοντέλου που περιγράψαμε και προσδίδουν νέες λειτουργικότητες.

4. ΕΠΕΚΤΑΣΕΙΣ RBAC

4.1. Εισαγωγή

Στο προηγούμενο κεφάλαιο, παρουσιάσαμε αναλυτικά το μοντέλο ελέγχου πρόσβασης βασισμένο σε ρόλους. Είδαμε τις τέσσερις βασικές του συνιστώσες: βασικό RBAC, ιεραρχικό RBAC, περιορισμένο RBAC, συμμετρικό RBAC. Κάθε μία από τις συνιστώσες αυτές επέκτεινε το αρχικό μοντέλο (βασικό RBAC), προσδίδοντάς του επιπλέον δυνατότητες και διαχειριστικές ευκολίες.

Παρά τις ομοιότητες που παρουσιάζουν τα διάφορα πληροφοριακά συστήματα του εμπορικού κόσμου, καθένα από αυτά έχει τις δικές του ιδιαιτερότητες. Οι ιδιαιτερότητες αυτές ανοίγουν το δρόμο για την ανάπτυξη νέων επεκτάσεων που βασίζονται στο RBAC και οι οποίες στόχο έχουν να καλύψουν τις εξειδικευμένες ανάγκες του εκάστοτε πληροφοριακού συστήματος.

Στη συνέχεια του κεφαλαίου αυτού περιγράφονται κάποιες από τα βασικότερα μοντέλα – επεκτάσεις του RBAC. Ειδικότερα αναλύονται τα:

- Μοντέλο Ελέγχου Πρόσβασης Βασισμένο σε Ρόλους με Χρονικούς Περιορισμούς - Temporal Role Based Access Control (TRBAC)
- Γενικευμένο Μοντέλο Ελέγχου Πρόσβασης Βασισμένο σε Ρόλους με Χρονικούς Περιορισμούς Generalized – Temporal Role Based Access Control (GTRBAC)
- Γενικευμένο Μοντέλο Ελέγχου Πρόσβασης Βασισμένο σε Ρόλους – Generalized Role-Based Access Control (GRBAC)
- Μοντέλο Ελέγχου Πρόσβασης Βασισμένο σε Ρόλους με Επίκεντρο την Ποιότητα Υπηρεσιών – Quality of Service Role Based Access Control (QRBAC).

4.2. Μοντέλο Ελέγχου Πρόσβασης Βασισμένο Σε Ρόλους με Χρονικούς Περιορισμούς -Temporal Role Based Access Control (TRBAC)

Όπως έχουμε ήδη αναφέρει το RBAC αποτελεί ένα γενικό και σχετικά αφηρημένο μοντέλο. Με αυτό τον τρόπο μπορεί να ενσωματωθεί σε διαφορετικού τύπου πληροφοριακά συστήματα και να προσαρμοστεί στις εκάστοτε απαιτήσεις τους. Το βασικό μοντέλο του RBAC που παρουσιάστηκε και αναλύθηκε παραπάνω ορίζει κληρονόμηση δικαιωμάτων μέσω των δομών ιεραρχιών καθώς και την έννοια του διαχωρισμού των καθηκόντων μέσω της οποίας επιτυγχάνεται διαίρεση των ευθυνών και συνεπώς καλύτερος έλεγχος του συστήματος.

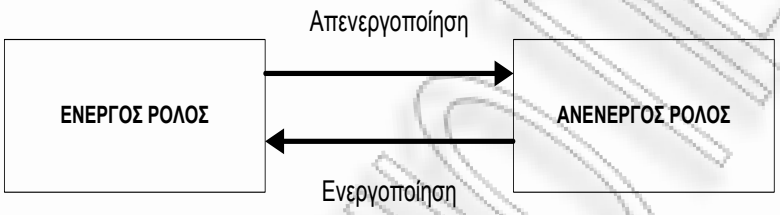
Το 2001 οι Bertino, Bonatti και Ferrari εισάγουν στο βασικό μοντέλο για πρώτη φορά την έννοια του χρόνου. Έτσι προτείνουν το TRBAC (Temporal Role-Based Access Control), μια επέκταση του βασικού μοντέλου που αφορά συστήματα τα οποία απαιτούν χρονικούς περιορισμούς για τον έλεγχο πρόσβασης. Ουσιαστικά περιορίζεται στη διάσταση του χρόνου η ενεργοποίηση των ρόλων και ορίζονται χρονικές εξαρτήσεις μεταξύ των ενεργοποιήσεων αυτών [25].

Η ανάγκη για τη δημιουργία μίας τέτοιας επέκτασης στο RBAC προέκυψε μέσα από συστήματα τα οποία βασίζονται για την εύρυθμη λειτουργία τους στον έλεγχο του χρόνου. Για παράδειγμα, σε πολλά συστήματα κρίνεται απαραίτητος ο περιορισμός χρήσης των πόρων τόσο σε ότι αφορά στο πότε μπορεί αυτός να χρησιμοποιηθεί (συγκεκριμένες ώρες μέσα στην ημέρα) αλλά και στη χρονική διάρκεια που μπορεί τελικά αυτός να χρησιμοποιηθεί. Αυτό μπορεί

να επιτευχθεί με την εισαγωγή της χρονικής διάστασης στους ρόλους. Επιπλέον, σε αρκετά συστήματα απαιτούνται χρονικές εξαρτήσεις μεταξύ των ενεργοποιήσεων των ρόλων, οι οποίες δεν ικανοποιούνται στο βασικό RBAC [25].

Έχουμε ήδη αναφέρει ότι στον κάθε χρήστη μπορούν να ανατεθούν περισσότεροι του ενός ρόλοι και ότι στα πλαίσια μιας συνεδρίας μπορεί να ενεργοποιηθεί ένα υποσύνολο αυτών. Ως ενεργοποίηση ενός ρόλου ορίζουμε τη μετάβαση από την κατάσταση «ανενεργός» στην κατάσταση «ενεργός» που οδηγεί στην απόκτηση των δικαιωμάτων πρόσβασης του ρόλου από το χρήστη. Η ακριβώς αντίστροφη μετάβαση ονομάζεται απενεργοποίηση. Οι καταστάσεις των ρόλων και οι μεταβάσεις μεταξύ αυτών παρουσιάζονται στην Εικόνα 4.1.

Εικόνα 4.1: Καταστάσεις Ρόλων και Μεταβάσεις Μεταξύ Αυτών στο μοντέλο TRBAC



Μία από τις βασικές συνιστώσες του TRBAC είναι η περιοδική ενεργοποίηση και απενεργοποίηση των ρόλων [25]. Περιοδικό είναι ένα γεγονός το οποίο λαμβάνει χώρα ανά τακτούς χρόνους στα όρια ενός καθορισμένου χρονικού διαστήματος. Για την καλύτερη κατανόηση μπορούμε να αναλογιστούμε το ρόλο του ταμία σε ένα κατάστημα τράπεζας. Ο ρόλος αυτός θα πρέπει να ενεργοποιείται μόνο κατά τις ώρες λειτουργίας του καταστήματος, δηλαδή 8:00 με 14:30, και μόνο τις εργάσιμες ημέρες της εβδομάδας.

Η δεύτερη συνιστώσα του TRBAC είναι οι χρονικές εξαρτήσεις μεταξύ των ενεργοποιήσεων και των απενεργοποιήσεων των ρόλων [25]. Για παράδειγμα με την ενεργοποίηση του ρόλου του ταμία θα πρέπει ενεργοποιηθεί και ο ρόλος του προϊσταμένου του (εάν αυτός δεν είναι ήδη ενεργός). Στα πλαίσια του TRBAC αυτοί οι κανόνες που ορίζουν τις χρονικές εξαρτήσεις εκφράζονται μέσω της έννοιας των εναυσμάτων (triggers). Τα εναύσματα είναι ενεργοί κανόνες οι οποίοι εκτελούνται αυτόματα όταν συμβούν συγκεκριμένα γεγονότα [25]. Έτσι η ενεργοποίηση του ρόλου του ταμία αποτελεί έναυσμα για την ενεργοποίηση του ρόλου του προϊσταμένου. Θα πρέπει να σημειωθεί ότι ένα έναυσμα μπορεί να ενεργοποιήσει/απενεργοποιήσει ένα ρόλο είτε άμεσα είτε μετά την πάροδο ενός ρητά προκαθορισμένου χρονικού διαστήματος [25].

Για την εξασφάλιση της ομαλής λειτουργίας του συστήματος πολλές φορές είναι αναγκαία η επέμβαση του διαχειριστή ασφάλειας. Με τις αιτήσεις χρόνου εκτέλεσης (run-time requests) ο διαχειριστής επεμβαίνει δυναμικά αλλάζοντας την κατάσταση των ρόλων και μεταβάλλοντας το σύνολο των χρηστών που μπορούν να ενεργοποιήσουν ένα συγκεκριμένο ρόλο [25]. Οι αιτήσεις χρόνου εκτέλεσης είναι αιτήσεις που δεν προϋποθέτουν την εκτέλεση άλλων γεγονότων και την επαλήθευση συνθηκών. Με αυτό τον τρόπο μπορεί για παράδειγμα να αποφευχθεί η ενεργοποίηση ενός ρόλου από κάποιον κακόβουλο χρήστη προστατεύοντας έτσι το σύστημα. Όπως και τα εναύσματα, έτσι και οι αιτήσεις χρόνου εκτέλεσης μπορούν να εκτελεστούν άμεσα ή μετά από κάποιο διάστημα [25].

Η περιοδικότητα, τα εναύσματα και οι αιτήσεις χρόνου εκτέλεσης μπορεί να οδηγήσουν πολλές φορές το σύστημα σε καταστάσεις συγκρούσεων, αφού υπάρχει πιθανότητα οι

συνθήκες να οδηγούν στην ενεργοποίηση ενός ρόλου και στην ταυτόχρονη απενεργοποίηση του [25]. Προκειμένου να μην οδηγηθούμε σε τέτοιες καταστάσεις ορίζονται προτεραιότητες και φυσικά εκτελείται πρώτο το γεγονός με τη μεγαλύτερη προτεραιότητα. Επιπλέον, εξαιτίας των χρονικών συνθηκών που τίθενται στο μοντέλο πολλές φορές δεν είναι απόλυτα ξεκάθαρο ποιος ρόλος πρέπει να ενεργοποιηθεί. Για την αποφυγή τέτοιων διφορούμενων καταστάσεων ορίζεται κατάλληλος μηχανισμός ασφάλειας που δίνει λύση στις ασάφειες και αντιφάσεις όσον αφορά τις ενεργοποιήσεις/απενεργοποιήσεις των ρόλων [25].

Παρόλο που το TRBAC επεκτείνει το βασικό RBAC προσθέτοντας τη διάσταση του χρόνου, επικεντρώνεται στην προσθήκη χρονικών περιορισμών στην ενεργοποίηση των ρόλων. Αφήνει όμως ανοιχτά ζητήματα που αφορούν τους χρονικούς περιορισμούς που μπορούν να τεθούν στην ανάθεση των ρόλων στους χρήστες και στην ανάθεση των δικαιωμάτων πρόσβασης στους ρόλους.

4.3. Γενικευμένο Μοντέλο Ελέγχου Πρόσβασης Βασισμένο Σε Ρόλους με Χρονικούς Περιορισμούς Generalized – Temporal Role Based Access Control (GTRBAC)

Το μοντέλο TRBAC έθεσε τις βάσεις για την εισαγωγή χρονικών περιορισμών στο βασικό μοντέλο RBAC. Όπως είδαμε θέτει την έννοια του χρόνου στην ενεργοποίηση του ρόλου. Ο χρόνος όμως μπορεί να τεθεί ως περιορισμός και σε άλλα στοιχεία του βασικού μοντέλου. Τις νέες αυτές δυνατότητες έρχεται να καλύψει το GTRBAC των James Joshi, Elisa Bertino, Usman Latif, Arif Ghafoor [28]. Η επέκταση αυτή ορίζει μία νέα κατάσταση στην οντότητα του ρόλου και θέτει χρονικούς περιορισμούς στις αναθέσεις ρόλων, δικαιωμάτων και χρηστών.

Έχουμε ήδη αναφέρει ότι το TRBAC εφαρμόζει περιορισμούς στην ενεργοποίηση και απενεργοποίηση ενός ρόλου, αφήνοντας ανοιχτά ζητήματα τα οποία συνοψίζονται ως εξής:

- Δεν υποστηρίζει τον καθορισμό χρονικών περιορισμών στην ανάθεση ρόλων σε χρήστες και στην ανάθεση δικαιωμάτων σε ρόλους.
- Το TRBAC δε διαχωρίζει τη δυνατότητα ενεργοποίησης ενός ρόλου από το χρήστη (role enabling) από την ενεργοποίησή του (role activation).
- Δε δίνει τη δυνατότητα διαχείρισης των περιορισμών (ενεργοποίησης / απενεργοποίησής τους).

Στη συνέχεια θα αναλύσουμε πως το GTRBAC δίνει απαντήσεις στα θέματα που δεν καλύπτει το TRBAC.

Στα περισσότερα συστήματα στον κάθε χρήστη ανατίθενται περισσότεροι του ενός ρόλοι. Στα πλαίσια μιας συνεδρίας κάθε χρήστης έχει τη δυνατότητα να ενεργοποιήσει ένα υποσύνολο των ρόλων για τους οποίους είναι εξουσιοδοτημένος. Η απόφαση για το ποιος ρόλος τελικά θα ενεργοποιηθεί είναι θέμα του χρήστη ανάλογα με τις αρμοδιότητές του στη συγκεκριμένη συνεδρία καθώς και με τις ενέργειες που θέλει να εκτελέσει. Θα πρέπει, λοιπόν, να γίνει σαφής διαχωρισμός μεταξύ των καταστάσεων στις οποίες μπορεί να βρεθεί ένας ρόλος και οι οποίες είναι πλέον τρεις:

Ρόλος με δυνατότητα ενεργοποίησης (Enabled role)

Ένας ρόλος βρίσκεται στην κατάσταση αυτή όταν υπάρχουν χρήστες οι οποίοι είναι εξουσιοδοτημένοι να αποκτήσουν τα δικαιώματα του ρόλου (εξαιτίας της ανάθεσής του σε αυτούς) αλλά κανένας χρήστης δεν τον έχει ενεργοποιήσει ακόμα.

Ενεργοποιημένος ρόλος (Active role)

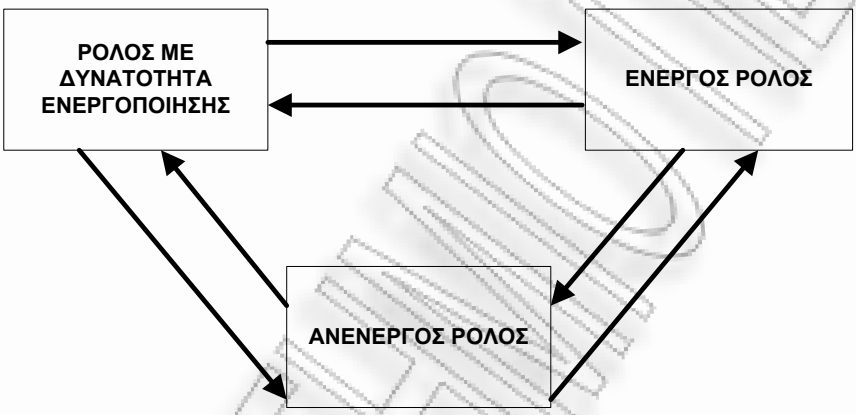
Ένας ρόλος περνά σε αυτή την κατάσταση από τη στιγμή που τουλάχιστον ένας χρήστης τον έχει ενεργοποιήσει. Από την κατάσταση αυτή ο ρόλος μπορεί είτε να περάσει στην κατάσταση enabled είτε να απενεργοποιηθεί εντελώς.

Απενεργοποιημένος ρόλος (Disabled role)

Παρόλο που ο ρόλος μπορεί να έχει ανατεθεί σε έναν ή περισσότερους χρήστες, αυτός δεν μπορεί να χρησιμοποιηθεί σε καμία συνεδρία.

Στο παρακάτω σχήμα (Εικόνα 4.2) παρουσιάζονται οι καταστάσεις στις οποίες μπορεί να βρεθεί ένας ρόλος καθώς και οι μεταβάσεις μεταξύ αυτών.

Εικόνα 4.2: Καταστάσεις Ρόλων και Μεταβάσεις Μεταξύ Αυτών στο GTRBAC



Αναλύοντας σε μεγαλύτερο βαθμό το μοντέλο GTRBAC, οι κύριες κατηγορίες στις οποίες μπορούν να χωριστούν οι χρονικοί περιορισμοί είναι οι περιορισμοί διάρκειας και οι περιορισμοί περιοδικότητας. Και οι δύο αυτές κατηγορίες βρίσκουν εφαρμογή στην ανάθεση ρόλων στους χρήστες, στην ανάθεση δικαιωμάτων πρόσβασης στους ρόλους και στη δυνατότητα ενεργοποίησης ενός ρόλου (role enabling). Επιπλέον, περιορισμοί διάρκειας εφαρμόζονται και στην ενεργοποίηση των ρόλων από τους χρήστες (role activation).

Η περιοδικότητα και οι περιορισμοί διάρκειας όσον αφορά την ανάθεση ρόλου σε χρήστη έγκεινται στον περιορισμό της ανάθεσης σε συγκεκριμένες περιόδους στα πλαίσια ενός χρονικού διαστήματος ή/και σε συγκεκριμένη χρονική διάρκεια. Ως παράδειγμα, μπορεί να αναφερθεί ο ρόλος του ορκωτού ελεγκτή στο τμήμα λογιστηρίου μιας εταιρείας. Ο ρόλος αυτός απαιτείται να ανατεθεί σε χρήστες μόνο στο κλείσιμο του λογιστικού έτους και για χρονικό διάστημα 15 ημερών.

Αντίστοιχα, οι περιορισμοί αυτοί μπορεί να βρουν εφαρμογή στην ανάθεση δικαιωμάτων πρόσβασης σε ένα ρόλο. Ενδεικτικό παράδειγμα είναι το δικαίωμα δήλωσης μαθημάτων που ανατίθενται στο ρόλο του φοιτητή σε ένα Ανώτατο Εκπαιδευτικό Ίδρυμα. Το δικαίωμα αυτό το αποκτούν δύο φορές το χρόνο και για χρονικό διάστημα δύο εβδομάδων.

Ομοίως, περιορισμοί αυτής της μορφής μπορεί να οριστούν και στη διαδικασία αλλαγής της κατάστασης ενός ρόλου από enabled σε disabled και το αντίστροφο. Για παράδειγμα, ο ρόλος του επισκέπτη γιατρού που παρακολουθεί τους νοσηλευόμενους σε ένα νοσοκομείο ασθενείς μπορεί να γίνει enabled από τις 9 το πρωί έως τις 9 το βράδυ. Από τη στιγμή που θα

ενεργοποιηθεί ο ρόλος αυτός, γίνεται αυτόματα enabled για 4 ώρες ο ρόλος του ειδικευόμενου γιατρού.

Χρονικοί περιορισμοί μπορούν να τεθούν και στην ενεργοποίηση ενός ρόλου (role activation). Στην περίπτωση αυτή δε μπορούμε να αναφερθούμε στην έννοια της περιοδικότητας καθώς όπως έχουμε ήδη αναφέρει η ενεργοποίηση ενός ρόλου είναι απόφαση του κάθε χρήστη. Μπορεί όμως εύκολα να τεθούν περιορισμοί χρονικής διάρκειας. Εδώ εντοπίζονται οι παρακάτω κατηγορίες περιορισμών διάρκειας:

- **Συνολική διάρκεια ενεργού ρόλου (Total Active Role Duration)**
  Καθορίζεται η συνολική χρονική διάρκεια που ένας ρόλος μπορεί να παραμείνει ενεργός.
  - Ανά ρόλο
    Περιορίζεται η χρονική διάρκεια που ένας ρόλος μπορεί να παραμείνει ενεργός ανεξάρτητα από το ποιοι και πόσοι χρήστες τον έχουν ενεργοποιήσει. Όταν το άθροισμα της διάρκειας όλων των ενεργοποιήσεων φτάσει τη μέγιστη συνολική διάρκεια, δεν επιτρέπεται περαιτέρω ενεργοποίηση του ρόλου.
  - Ανά ανάθεση χρήστη σε ρόλο
    Περιορίζεται η χρονική διάρκεια που ένας χρήστης μπορεί να ενεργοποιήσει το ρόλο. Όταν ο χρήστης υπερβεί τη διάρκεια αυτή, δεν του επιτρέπεται να τον ενεργοποιήσει ξανά.

  Θα πρέπει να σημειωθεί είναι ότι ο περιορισμός της συνολικής διάρκειας είναι ανεξάρτητος του αριθμού των ενεργοποιήσεων του ρόλου.
- **Μέγιστη διάρκεια ρόλου ανά ενεργοποίηση (Maximum Role Duration per Activation)**
  Εδώ, περιορίζεται η μέγιστη διάρκεια που μπορεί ένας ρόλος να παραμείνει ενεργός ανά ενεργοποίηση.
  - Ανά ρόλο
    Για τον οποιοδήποτε χρήστη έχει τη δυνατότητα να ενεργοποιήσει το ρόλο καθορίζεται μια μέγιστη διάρκεια που μπορεί αυτός ο ρόλος να παραμείνει ενεργός από τη στιγμή που ενεργοποιείται.
  - Ανά ανάθεση χρήστη σε ρόλο
    Καθορίζεται η μέγιστη διάρκεια που ένας χρήστης μπορεί να διατηρήσει ενεργό ένα ρόλο από τη στιγμή που θα τον ενεργοποιήσει.

Επιπλέον στην ενεργοποίηση ενός ρόλου μπορούν να τεθούν χρονικοί περιορισμοί που αφορούν το πλήθος των ενεργοποιήσεων αυτού. Αντίστοιχα όπως με τους περιορισμούς διάρκειας διακρίνουμε δύο κατηγορίες:

- Συνολικός αριθμός ενεργοποιήσεων
- Μέγιστος αριθμός ενεργοποιήσεων

Οι κατηγορίες αυτές μπορούν να αναλυθούν περισσότερο βρίσκοντας εφαρμογή είτε ανά ρόλο είτε ανά ανάθεση χρήστη σε ρόλο.

Στο TRBAC αναφέρθηκαν οι έννοιες των εναυσμάτων και των αιτήσεων χρόνου εκτέλεσης. Οι έννοιες αυτές περιλαμβάνονται και στο μοντέλο του GTRBAC προσαρμοσμένες στα νέα δεδομένα που αυτό εισάγει.

4.4. Γενικευμένο Μοντέλο Ελέγχου Πρόσβασης Βασισμένο Σε Ρόλους – Generalized Role-Based Access Control (GRBAC)

Τόσο το RBAC όσο και οι επεκτάσεις του που έχουμε ως τώρα αναλύσει περιγράφουν τρόπους ελέγχου πρόσβασης και περιορισμού αυτού βασιζόμενα κατά κύριο λόγο στην οντότητα των υποκειμένων. Πώς ο χρήστης δε θα μπορεί να έχει πρόσβαση σε φακέλους, πώς θα περιοριστεί ο χρόνος που έχει δικαίωμα να χρησιμοποιεί πόρους κλπ. Παρ' όλα αυτά ο έλεγχος πρόσβασης μπορεί να εφαρμοστεί δίνοντας δικαιώματα και ορίζοντας ρόλους όχι μόνο για τα υποκείμενα και τους χρήστες αλλά με ανάθεση ρόλων σε αντικείμενα, περιβαλλοντικές παραμέτρους κλπ.

Βασιζόμενοι στο σπίτι του μέλλοντος οι Matthew Moyer,Mustaque Ahamad και Michael Covington προτείνουν το Γενικευμένο Μοντέλο Ελέγχου Πρόσβασης Βασισμένο σε Ρόλους [26]. Η ιδέα ενός σπιτιού με γνώση αποτελεί αντικείμενο έρευνας του Τεχνολογικού Ινστιτούτου της Ατλάντα στη Γεωργία των ΗΠΑ. Το σπίτι αυτό όντας διαμορφωμένο με έμφαση στην εκμετάλλευση όλων των πλεονεκτημάτων της τεχνολογίας και δη της πληροφορικής, αποτελεί ιδανική περίπτωση εφαρμογής του GRBAC. Εδώ ξεφεύγουμε από την κλασική, πλέον, αντιμετώπιση της ανάθεσης ρόλων σε υποκείμενα. Οι κάτοικοι του σπιτιού και χρήστες των χώρων του και των συσκευών μέσα σε αυτούς έχουν το ρόλο που τους ανατίθεται. Μπορούμε να θεωρήσουμε το πιο κλασσικό παράδειγμα των ρόλων γονιός και παιδί. Πέραν αυτών όμως η δυνατότητα χρήσης (δικαίωμα πρόσβασης) αποτελεί συνδυασμό και των ρόλων των αντικειμένων καθώς και των καταστάσεων του περιβάλλοντος.

Σε ό,τι αφορά στους ρόλους αντικειμένων, η ιδέα προέρχεται από την άποψη ότι πολλά αντικείμενα χαρακτηρίζονται από κοινές ιδιότητες και θα μπορούσαμε να τα διαχειριστούμε με μεγαλύτερη ευκολία αν τους αναθέσουμε ένα συγκεκριμένο ρόλο [26]. Έτσι, στα πλαίσια του σπιτιού, μπορούμε να φανταστούμε τις συσκευές της τηλεόρασης, του ραδιοφώνου και του DVD player να τους ανατίθεται ο ρόλος «Συσκευές ψυχαγωγίας». Με αυτόν τον τρόπο οι όποιοι περιορισμοί πρόσβασης μπορεί πλέον να τεθούν στο ρόλο αυτό, ασχέτως με το ποιος ρόλος υποκειμένων αιτείται την πρόσβαση. Ένα απλό τέτοιο παράδειγμα είναι ο περιορισμός ότι οι συσκευές ψυχαγωγίας μπορεί να χρησιμοποιούνται το πολύ τρεις ώρες την ημέρα. Φυσικά οι περιορισμοί μπορούν να οριστούν με συνδυασμό ρόλων αντικειμένων και ρόλων υποκειμένων («Τα παιδιά δεν μπορούν να χρησιμοποιούν τις συσκευές ψυχαγωγίας μετά τις 10 το βράδυ»). Η ταξινόμηση των αντικειμένων και η ανάθεση του κατάλληλου ρόλου σε αυτά μπορεί να βασιστεί τόσο στον τύπο του αντικειμένου, όσο και σε άλλες ιδιότητες όπως η ημερομηνία δημιουργίας-κτήσης, το περιεχόμενο των πληροφοριών που μπορεί να διαθέτουν κλπ [26].

Εκτός από τους ρόλους αντικειμένων, το μοντέλο GRBAC εισάγει την έννοια του ρόλου του περιβάλλοντος [26]. Η έννοια αυτή αντικατοπτρίζει τους ρόλος που αναλαμβάνουν οι παράγοντες του περιβάλλοντος στον έλεγχο της πρόσβασης. Ο χρόνος, η θερμοκρασία, η γεωγραφική περιοχή είναι μόνο μερικά παραδείγματα τέτοιων παραμέτρων. Για παράδειγμα, μπορούμε να ορίσουμε ρόλους ομαδοποιώντας τις ημέρες της εβδομάδος: Δευτέρα με Παρασκευή ορίζουμε το ρόλο «Εργάσιμες Ημέρες» ενώ αντίστοιχα Σάββατο και Κυριακή αντιστοιχούν στο ρόλο «Ημέρες Ξεκούρασης». Σε αυτό το σημείο θα πρέπει να τονίσουμε για μία ακόμη φορά το πλεονέκτημα της έννοιας του ρόλου. Θα μπορούσε κανείς να αναρωτηθεί γιατί δεν ορίζουμε ομάδες (groups) για το διαχωρισμό των ημερών. Η ευελιξία των ομάδων δεν είναι τόσο μεγάλη όσο αυτή των ρόλων. Ίσως σε ότι αφορά τις ημέρες της εβδομάδας αυτό να μην είναι τόσο εμφανές, αλλά η ανάθεση των ρόλων είναι μια πολύ πιο εύκολη διαδικασία σε σχέση με τη διαχείριση των ομάδων και των οντοτήτων χωριστά.

Το πρόβλημα με του ρόλους του περιβάλλοντος είναι ότι το εκάστοτε σύστημα που θέλει να τους ορίσει, για να ληφθούν υπόψη στον έλεγχο της πρόσβασης, πρέπει να είναι σε θέση να συλλέξει με ακρίβεια τα στοιχεία που απαιτούνται για να καθοριστούν έγκυρα οι περιορισμοί [26].

4.5. Μοντέλο Ελέγχου Πρόσβασης Βασισμένο Σε Ρόλους Με Επίκεντρο Την Ποιότητα Υπηρεσιών – Quality of Service Role Based Access Control (QRBAC)

Το βασικό RBAC και οι επεκτάσεις που έχουν έως τώρα παρουσιαστεί αποτελούν έναν από τους πιο σημαντικούς τρόπους ελέγχου πρόσβασης επιτυγχάνοντας την πρόσβαση των εξουσιοδοτημένων και μόνο χρηστών στα δεδομένα και τους λοιπούς πόρους του συστήματος. Δε λαμβάνει όμως υπόψη του έναν ιδιαίτερα σημαντικό παράγοντα που αποτελεί πρόκληση για τα σύγχρονα υπολογιστικά συστήματα, την ποιότητα των υπηρεσιών (Quality of Service-QoS). Τη νέα αυτή διάσταση της ποιότητας των παρεχόμενων υπηρεσιών έρχεται να δώσει στο υπάρχον βασικό RBAC μια νέα επέκταση, το QRBAC.

Προκειμένου να έχουμε ένα επιτυχημένο και αποδοτικό σύστημα RBAC, ταυτόχρονα με την ποιότητα των υπηρεσιών πρέπει να συνυπάρχει και η ασφάλεια του συστήματος [27]. Για παράδειγμα ένα απόλυτα ασφαλές σύστημα μπορεί να μην αποδειχτεί τελικά και τόσο χρήσιμο αν δεν καταφέρει να πετύχει ένα συγκεκριμένο επίπεδο ποιότητας υπηρεσιών. Στον αντίποδα, ένα σύστημα που φτάνει ένα καλό επίπεδο ποιότητας υπηρεσιών χωρίς τους κατάλληλους μηχανισμούς ασφαλείας, μπορεί εύκολα να δεχθεί επίθεση από έναν κακόβουλο χρήστη. Το σύστημα οδηγείται σε άρνηση παροχής υπηρεσιών (Denial of Service-Dos), σε εξάντληση των πόρων του από τον κακόβουλο χρήστη και τελικά σε πτώση της ποιότητας των υπηρεσιών. Κρίνεται λοιπόν απαραίτητος για την επιτυχία ενός συστήματος ο συνδυασμός της ασφάλειας με την ποιότητα των παρεχόμενων υπηρεσιών και αυτό μελετάται μέσα από το QRBAC.

Το QRBAC προτάθηκε από τον Kyoung-Don Kang οποίος μελέτησε την επέκταση αυτή για τις εφαρμογές ηλεκτρονικού εμπορίου (e-commerce). Στις εφαρμογές αυτές τόσο η ποιότητα των παρεχόμενων υπηρεσιών όσο και η ασφάλεια είναι κρίσιμοι παράγοντες για την επιτυχία τους. Το QRBAC εισάγει μια νέα έννοια, αυτή των «ρόλων που έχουν επίγνωση της ποιότητας των υπηρεσιών» (Qos-aware roles), προσφέροντας στο διαχειριστή του συστήματος τη δυνατότητα να προσδιορίζει απευθείας το αναλογούν σε κάθε ρόλο μερίδιο από τους αιτούμενους πόρους του συστήματος προκειμένου να επιτευχθεί η ζητούμενη ποιότητα υπηρεσιών [27]. Για παράδειγμα σε ένα σύστημα ηλεκτρονικού εμπορίου ο διαχειριστής προσδιορίζει για ένα ρόλο το αναλογούν εύρος ζώνης που αυτός χρειάζεται προκειμένου να διαχειριστεί τα αιτήματα για υπηρεσίες με το κατάλληλο επίπεδο ποιότητας, τον μέσο χρόνο απόκρισης στα αιτήματα αυτά κα.

Η δεύτερη καινοτομία του QRBAC είναι ότι εισάγει της έννοιας της «κατάστασης του συστήματος» (system status) ως μέρος του μοντέλου ελέγχου πρόσβασης [27]. Με αυτό τον τρόπο ο μηχανισμός ελέγχου πρόσβασης επιβλέπει άμεσα την κατάσταση του συστήματος και τη χρήση των πόρων αυτού έχοντας τη δυνατότητα να ανιχνεύσει και να αποτρέψει πιθανή υπερφόρτωση του και εξάντληση των πόρων του από κακόβουλους χρήστες [27]. Επανερχόμενοι στο παράδειγμα της εφαρμογής ηλεκτρονικού εμπορίου, η χρήση του QRBAC στοχεύει στο να πετύχει μια καθορισμένη απόδοση πχ ένα μέσο χρόνο απόκρισης ή ένα ανώτατο όριο χρήσης των πόρων για την αποφυγή υπερφορτώσεων. Για να το πετύχει αυτό παρακολουθείται σε τακτά χρονικά διαστήματα η απόδοση του συστήματος και η χρήση των πόρων του και όταν διαπιστωθεί υπερφόρτωση τότε μειώνεται η ποιότητα των υπηρεσιών. Για παράδειγμα παρέχονται στους χρήστες μόνο πληροφορίες κειμένου και όχι εικόνες, χωρίζονται οι χρήστες σε κατηγορίες ανάλογα με τη σημαντικότητα τους κι έτσι εξυπηρετούνται πχ πρώτα οι χρήστες που θέλουν να πραγματοποιήσουν μια πληρωμή και θα αποφέρουν κέρδος στην εφαρμογή.

Όπως έχουμε ήδη αναφέρει, το βασικό RBAC υποστηρίζει δύο ιδιαίτερα σημαντικές αρχές, την αρχή του ελαχίστου προνομίου και την αρχή του διαχωρισμού των καθηκόντων. Τις αρχές αυτές έρχεται να επεκτείνει και να υλοποιήσει με το δικό του τρόπο το QRBAC. Σε ένα σύστημα

QRBAC, όταν ένας ρόλος καταναλώσει πόρους παραπάνω από το μερίδιο που του αναλογεί τότε θεωρείται ότι έχει παραβιαστεί η αρχή του ελαχίστου προνομίου [27]. Αποτέλεσμα της υπερκατανάλωσης πόρων από ένα ρόλο είναι η μείωση της ποιότητας των υπηρεσιών για τους υπόλοιπους πόρους λόγω της έλλειψης πόρων. Ως συνέπεια αυτού παραβιάζεται και η απομόνωση της απόδοσης των ρόλων αφού η απόδοση ενός ρόλου είναι άμεσα συνδεδεμένη με την απόδοση των υπολοίπων [27]. Αυτό θεωρείται πρόβλημα διαχωρισμού των καθηκόντων.

Προκειμένου να υποστηρίξει τις επεκτάσεις των βασικών αυτών αρχών, το QRBAC μπορεί να προσαρμόζει δυναμικά τις άδειες πρόσβασης των ρόλων σε ότι αφορά τη χρήση των πόρων μειώνοντας τους την ποιότητα των υπηρεσιών σε περίπτωση υπερφόρτωσης μέσω πχ μειωμένης ποιότητας εικόνας. Επιπλέον, έχει τη δυνατότητα να προσαρμόζει και να μειώνει δυναμικά το ρυθμό ενεργοποίησης των ρόλων. Για παράδειγμα, μπορεί να μειώσει των αριθμό των ρόλων που μπορούν να έχουν πρόσβαση στους πόρους του συστήματος σε μια δεδομένη χρονική στιγμή ώστε να μπορέσουν να εξυπηρετηθούν οι ρόλοι με τη μεγαλύτερη προτεραιότητα. Τέλος, η επέκταση αυτή δίνει στο διαχειριστή του συστήματος τη δυνατότητα να ανακαλεί όλα τα δικαιώματα πρόσβασης ενός ρόλου ο οποίος προσπαθεί να εξαντλήσει όλους τους διαθέσιμους πόρους.

4.6. Επίλογος

Οι επεκτάσεις του μοντέλου RBAC που παρουσιάστηκαν παραπάνω αποτελούν ενδεικτικά παραδείγματα του συνόλου των επεκτάσεων που έχουν αναπτυχθεί έως τώρα. Φυσικά δεν είναι οι μοναδικές επεκτάσεις αλλά αποτελούν τα μοντέλα που καλύπτουν δύο πολύ σημαντικές παραμέτρους για τα πληροφοριακά συστήματα σήμερα: το χρόνο και την ποιότητα των υπηρεσιών. Δεδομένης της φύσης των σύγχρονων υπολογιστικών συστημάτων, το επίκεντρο του ενδιαφέροντος είναι η παροχή υπηρεσιών. Σημαντικός παράγοντας για την επιτυχία τέτοιων συστημάτων είναι η σωστή επιβολή των χρονικών περιορισμών καθώς και η διασφάλιση της ποιότητας των υπηρεσιών. Είδαμε λοιπόν, πως μπορούν να επιτευχθούν οι δύο αυτοί παράγοντες με την υλοποίηση των μοντέλων TRBAC, GTRBAC, QRBAC. Πέραν αυτών, παρουσιάσαμε και ένα διαφορετικό μοντέλο που ορίζει ρόλους στα αντικείμενα και οι αναθέσεις γίνονται πλέον μεταξύ ρόλων υποκειμένων και ρόλων αντικειμένων.

Λόγω της συνεχούς ανάπτυξης της τεχνολογίας, της συνεχούς μεταβολής των πληροφοριακών συστημάτων και γενικά του περιβάλλοντος στο οποίο αυτά λειτουργούν, προκύπτουν διαρκώς νέες ανάγκες, νέοι περιορισμοί που πρέπει να επιβληθούν. Η κάλυψη αυτών των αναγκών θα φέρνει πάντα στο προσκήνιο νέες βελτιώσεις, νέες επεκτάσεις και πιθανόν νέα μοντέλα που θα ενσωματώνουν τα πλεονεκτήματα του RBAC, θα ξεπεράσουν τα μειονεκτήματα του RBAC και θα προσφέρουν νέες προοπτικές. Προς το παρόν, το RBAC παραμένει ο πρωταγωνιστής στη διαχείριση του ελέγχου πρόσβασης λόγω της ευελιξίας και της διαχειριστικής ευκολίας που αυτό προσφέρει.

5. ΥΛΟΠΟΙΗΣΗ ΕΦΑΡΜΟΓΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ ΒΑΣΙΣΜΕΝΟΥ ΣΕ ΡΟΛΟΥΣ ΓΙΑ ΤΙΣ ΑΝΑΓΚΕΣ ΥΠΟΛΟΓΙΣΤΗ ΣΕ ΣΧΟΛΙΚΟ ΕΡΓΑΣΤΗΡΙΟ

5.1. Εισαγωγή

Στα προηγούμενα κεφάλαιο αναλύσαμε μεθόδους και μηχανισμούς ελέγχου πρόσβασης. Ξεκινήσαμε από την περιγραφή βασικών εννοιών και αρχών ασφάλειας. Παρουσιάσαμε τις βασικότερες δομές ελέγχου πρόσβασης και τις σημαντικότερες πολιτικές, περιγράφοντας μια σειρά μοντέλων που τις υλοποιούν. Είδαμε την εξέλιξη των μοντέλων ελέγχου πρόσβασης και πως από υλοποιήσεις αποκλειστικά και μόνο για το στρατιωτικό κόσμο έφτασαν να προσαρμοστούν και να ενσωματωθούν στις δυναμικά μεταβαλλόμενες ανάγκες του εμπορικού κόσμου. Οι διαφορές μεταξύ των στρατιωτικών εφαρμογών και των επιχειρησιακών πληροφοριακών συστημάτων δημιούργησαν νέες ανάγκες, νέες απαιτήσεις και κατ' επέκταση νέα μοντέλα με κυριότερο εκπρόσωπο το Μοντέλο Ελέγχου Πρόσβασης Βασισμένο σε Ρόλους (RBAC).

Ο μεγάλος αριθμός χρηστών και η ανάγκη για τη δημιουργία ενός μοντέλου με προσαρμοστικότητα στις διαφορετικές συνθήκες που επικρατούν σε κάθε επιχείρηση, καθιστούν το RBAC έναν από τους πιο ελκυστικούς και διαδεδομένους μηχανισμούς ελέγχου πρόσβασης. Από τη μια η ανάγκη για τη συνεχή μεταβολή των δικαιωμάτων πρόσβασης ανά χρήστη και από την άλλη η συνεχής μετακίνηση των χρηστών στα πλαίσια ενός οργανισμού οδήγησαν στην εισαγωγή μιας νέας έννοιας, αυτής του ρόλου. Αποτελώντας μια σταθερή οντότητα που παρεμβάλλεται μεταξύ των χρηστών και των δικαιωμάτων πρόσβασης, ο ρόλος προσέφερε τη διαχειριστική ευελιξία που ήταν απαραίτητη για την αποτελεσματική κατανομή των πόρων και γενικά του ελέγχου ροής της πληροφορίας στο εκάστοτε πληροφοριακό σύστημα.

Σε αυτό το σημεία θα πρέπει να σημειωθεί ότι η έννοια του εμπορικού κόσμου που συνεχώς αναφέρεται, δεν περιορίζεται στη στενή έννοια του όρου της οικονομικής μονάδας. Σε αυτήν περιλαμβάνονται και διαφορετικού τύπου οργανισμοί όπως νοσοκομεία, πανεπιστήμια, σχολεία κλπ.

Η εργασία μας επικεντρώνεται στην ανάπτυξη μιας εφαρμογής που στην ουσία υλοποιεί το βασικό μοντέλο RBAC καθώς και συνιστώσες των επεκτάσεών του που βασίζονται στην παράμετρο του χρόνου και τους περιορισμούς που αυτή θέτει. Στις επόμενες ενότητες παρουσιάζονται αναλυτικά οι απαιτήσεις, η δομή αλλά και η υλοποίηση της εφαρμογής μας. Ειδικότερα το παρόν κεφάλαιο δομείται ως εξής:

- Σκοπός εφαρμογής -Απαιτήσεις
- Εργαλεία Ανάπτυξης – Δομή εφαρμογής
- Εφαρμογή ανάθεσης ρόλων και δικαιωμάτων
- Εφαρμογή υλοποίησης δικαιωμάτων
- Γενική επισκόπηση – Μελλοντική Εργασία

5.2. Σκοπός Εφαρμογής - Απαιτήσεις

Η διαχείριση των δικαιωμάτων πρόσβασης σε τοπικά συστήματα είναι εξίσου σημαντική με τον έλεγχο πρόσβασης που διενεργείται σε δικτυακά και κατανεμημένα πληροφοριακά συστήματα.

Φροντιστήρια, σχολεία αλλά ακόμη και ένας οικιακός ηλεκτρονικός υπολογιστής στον οποίο έχουν πρόσβαση πολλοί χρήστες δε στερούνται της ανάγκης αποτελεσματικής διαχείρισης των δικαιωμάτων πρόσβασης.

Στα πλαίσια της εργασίας μας, υλοποιήσαμε εφαρμογή διαχείρισης δικαιωμάτων πρόσβασης βασισμένης σε ρόλους για τις ανάγκες ενός υπολογιστή σε σχολείο δευτεροβάθμιας εκπαίδευσης (Γυμνάσιο). Σε έναν τέτοιο υπολογιστή έχουν πρόσβαση πολλοί χρήστες όπως μαθητές διαφορετικών τάξεων, καθηγητές διαφόρων ειδικοτήτων, ο διευθυντής κλπ. Καθένας από αυτούς απαιτείται να έχει διαφορετικά επίπεδα πρόσβασης ανάλογα τα καθήκοντα και τις αρμοδιότητές του. Η εναλλαγή των φυσικών προσώπων στις θέσεις αυτές καθώς και η συχνή είσοδος και έξοδος χρηστών από το σχολείο, καθιστά, ίσως ως βέλτιστη λύση, τη χρήση της έννοιας του ρόλου και την εφαρμογή του μοντέλου RBAC στη διαχείριση της πρόσβασης.

Υποθέτοντας ότι βρισκόμαστε στο σχολικό περιβάλλον που περιγράψαμε και για τις ανάγκες τις εργασίας μας ορίσαμε τους εξής ρόλους:

- Υπεύθυνος Εργαστηρίου
  Αναφέρεται στον καθηγητή Πληροφορικής ο οποίος στην ουσία αποτελεί και το διαχειριστή του κοινόχρηστου αυτού υπολογιστή.
- Επισκέπτης
  Πρόκειται για προκαθορισμένο ρόλο του συστήματος ο οποίος διαθέτει τα ελάχιστα δικαιώματα πρόσβασης.
- Καθηγητής
  Ρόλος που ανατίθεται στο διδακτικό προσωπικό
- Μαθητής
  Ρόλος που ανατίθεται σε όλους τους μαθητές του σχολείου
- Καθηγητής Ενισχυτικής Διδασκαλίας
- Μαθητής Ενισχυτικής Διδασκαλίας
- Διευθυντής

Οι παραπάνω ρόλοι είναι ενδεικτικοί και σίγουρα σε ένα πραγματικό σχολικό περιβάλλον μπορεί να διαφέρουν. Οι διαφορετικές ανάγκες που πιθανόν να έχει κάθε σχολείο μπορεί να οδηγήσουν στον καθορισμό διαφορετικών ρόλων. Για παράδειγμα θα μπορούσε να οριστεί ο ρόλος Διδακτικό Προσωπικό αντί των ρόλων Καθηγητής και Καθηγητής Ενισχυτικής Διδασκαλίας. Φυσικά, με τον ορισμό των κατάλληλων ρόλων η εφαρμογή θα μπορούσε να προσαρμοστεί σε οποιοδήποτε σύστημα αντίστοιχων αναγκών και όχι μόνο στο σχολικό περιβάλλον.

Η λογική της εφαρμογής μας στηρίζεται στην αφαίρεση δικαιωμάτων πρόσβασης από τους ρόλους με σκοπό τον περιορισμό τους. Είναι προφανές ότι ο καθένας από τους ρόλους που περιγράψαμε παραπάνω απαιτείται να έχει πρόσβαση σε διαφορετικές εφαρμογές, αρχεία, και φακέλους του τοπικού υπολογιστή. Για παράδειγμα οι χρήστες στους οποίους έχει ανατεθεί ο ρόλος του Μαθητή, δε θα πρέπει να έχουν πρόσβαση στα αρχεία στα οποία είναι καταχωρημένα τα στοιχεία των βαθμών τους. Αντίστοιχα, ο ρόλος του Καθηγητή δε θα πρέπει να έχει πρόσβαση σε φακέλους που ο Διευθυντής αποθηκεύει αρχεία σχετικά με τη διοίκηση της σχολικής μονάδας.

Η ανάθεση των ρόλων και ο τρόπος που θα γίνεται η δήλωση των αρχείων / εφαρμογών και φακέλων για τα οποία ορίζονται δικαιώματα πρόσβασης, θα πρέπει να γίνεται με απλό και εύκολα αντιληπτό τρόπο. Είναι προφανές ότι η διαδικασία ορισμού τόσο των ρόλων του συστήματος όσο και των δικαιωμάτων αυτών είναι μία διαδικασία που θα πρέπει να πραγματοποιείται από το διαχειριστή του Υπολογιστή, ο οποίος στην προκειμένη περίπτωση αποτελεί τον Υπεύθυνο Εργαστηρίου. Πέραν των απαιτήσεων της ορθής εφαρμογής των δικαιωμάτων στους χρήστες, βασική απαίτηση είναι και η φιλική προς το χρήστη διεπαφή ώστε να μπορεί με απλούς χειρισμούς να αναθέτει ρόλους και δικαιώματα στους χρήστες παρέχοντάς

του παράλληλα τη δυνατότητα να διαμορφώνει τις παραμέτρους τους εύκολα και με τέτοιο τρόπο ώστε να καλύπτουν τις ανάγκες του εκάστοτε συστήματος.

Η εφαρμογή μας προσφέρει τη δυνατότητα εισαγωγής της παραμέτρου του χρόνου. Πέραν του βασικού μοντέλου RBAC, οι επεκτάσεις του TRBAC και GTRBAC, και οι οποίες περιγράφηκαν σε προηγούμενο κεφάλαιο, ορίζουν ως μία από τις βασικότερες παραμέτρους το χρόνο για την ενεργοποίηση των ρόλων, την ανάθεση των ρόλων σε χρήστες αλλά και την ανάθεση των δικαιωμάτων σε ρόλους. Σε πολλές περιπτώσεις ο χρονικός περιορισμός αποτελεί βασική απαίτηση για τη σωστή λειτουργία του συστήματος. Τα μοντέλα – επεκτάσεις του RBAC που αφορούν το χρόνο (ειδικά το GTRBAC) παρουσιάζουν διάφορες μεθόδους καθορισμού των περιορισμών αυτών. Ο καθορισμός συγκεκριμένων χρονικών διαστημάτων και ο καθορισμός μέγιστου χρονικού διαστήματος είναι τα βασικότερα παραδείγματα των μεθόδων αυτών. Στην εφαρμογή μας υλοποιήσαμε τη μέθοδο καθορισμού συγκεκριμένων χρονικών διαστημάτων καθώς είναι ο πιο αποτελεσματικός τρόπος ικανοποίησης των απαιτήσεων του σχολικού περιβάλλοντος για τους ρόλους που ενδεικτικά αναφέραμε.

Ο Υπεύθυνος Εργαστηρίου μπορεί να κάνει χρονικό προγραμματισμό των ρόλων, της ανάθεσης ρόλων σε χρήστες αλλά και της ανάθεσης δικαιωμάτων πρόσβασης στους ρόλους. Του δίνεται η δυνατότητα καθορισμού ημερών και ωρών για τις οποίες επιθυμεί ένας ρόλος να είναι ενεργός. Για παράδειγμα, ο Μαθητής Ενισχυτικής Διδασκαλίας θα πρέπει να ενεργοποιείται τις ώρες μετά τη λήξη του κανονικού σχολικού ωραρίου (π.χ ημέρες Δευτέρα με Παρασκευή 14:00 – 17:00 και ίσως Σάββατο 9:00 – 12:00). Επίσης, σε ότι αφορά στον περιορισμό των δικαιωμάτων, θα μπορούσαμε να περιορίσουμε το Μαθητή ώστε να μην έχει πρόσβαση στην εφαρμογή του Internet Explorer κατά τη διάρκεια των ωρών που γίνεται διδασκαλία των μαθημάτων, παρόλο που ένας συγκεκριμένος χρήστης μπορεί να έχει ενεργό το ρόλο αυτό καθ όλη τη διάρκεια της ημέρας. Τέλος, πολλές φορές προκύπτει η ανάγκη εξειδικευμένης ενεργοποίησης ενός ρόλου για συγκεκριμένο χρήστη. Χαρακτηριστικό παράδειγμα είναι η περίπτωση που στο σχολείο εργάζεται για κάποια χρονική περίοδο ένας ωρομίσθιος καθηγητής. Επειδή πρόκειται για μεμονωμένη περίπτωση καθηγητή, ο χρήστης αυτός λαμβάνει το ρόλο του Καθηγητή, αλλά η πρόσβασή τους περιορίζεται ειδικά γι' αυτόν στις ώρες που καθορίζει ο Υπεύθυνος Εργαστηρίου και που λογικά θα είναι υποσύνολο των ωρών που έχουν πρόσβαση οι υπόλοιποι Καθηγητές.

Στο σημείο αυτό θα πρέπει να τονίσουμε ότι η εφαρμογή μας δίνει τη δυνατότητα καθορισμού χρονικών περιορισμών τόσο ημερών της εβδομάδας όσο και ωρών της ημέρας στο κομμάτι που αφορά στην ανάθεση του ρόλου και στην ενεργοποίηση αυτού. Ωστόσο στην προσθήκη χρονικών περιορισμών στην ανάθεση δικαιωμάτων στους ρόλους μπορεί να ορίσει μόνο ώρες που επιθυμεί το δικαίωμα να ενεργοποιείται. Ο λόγος για τον οποίο δε δώσαμε και σε αυτό το σημείο την επιλογή καθορισμού ημερών έχει να κάνει με τον περιορισμό της πολυπλοκότητας της εφαρμογής και όχι με τον περιορισμό των δυνατοτήτων.

Τέλος, θα πρέπει να σημειωθεί ότι η εφαρμογή επιτρέπει την ανάθεση πολλαπλών ρόλων ανά χρήστη όπως ορίζει άλλωστε το βασικό μοντέλο RBAC. Στις περιπτώσεις ενεργοποίησης πολλών ρόλων για ένα χρήστη ταυτόχρονα, για λόγους ορθής εφαρμογής της πολιτικής ασφάλειας, ορίστηκε να ενεργοποιούνται το υπερσύνολο των περιορισμών των ρόλων αυτών. Η αντιμετώπιση περιπτώσεων σύγκρουσης δικαιωμάτων (ορισμού διαφορετικής πρόσβασης για το ίδιο αρχείο από τους διαφορετικούς ρόλους που είναι ενεργοί τη δεδομένη χρονική στιγμή για ένα χρήστη), αντιμετωπίζονται μέσα από την εφαρμογή μας με κατάλληλους ελέγχους και με την επιβολή της άρνησης πρόσβασης στο τελικό αρχείο ή φάκελο.

Είναι αυτονόητο ότι η ορθή λειτουργία της παρούσας εφαρμογής στηρίζεται στη συνεχή λειτουργία της και στην αφαίρεση της δυνατότητας διακοπής της από οποιοδήποτε χρήστη. Και οι δύο αυτές απαιτήσεις ικανοποιούνται μέσω ελέγχων και διαδικασιών που υλοποιούνται από την ίδια την εφαρμογή μας.

Οι λειτουργικότητες αυτές καθώς και ο τρόπος εφαρμογής τους θα παρουσιασθούν αναλυτικότερα στις ενότητες που ακολουθούν.

5.3. Εργαλεία Ανάπτυξης – Δομή Εφαρμογής

Για την ανάπτυξη της εφαρμογής μας έγινε χρήση του Microsoft Visual Studio 2008. Η ευκολία του συγκεκριμένου περιβάλλοντος για την ανάπτυξη εφαρμογών φιλικών προς το χρήστη καθώς και η συμβατότητά του με το λειτουργικό σύστημα των Windows, μας οδήγησε στην επιλογή του ως το βασικό μας εργαλείο. Η εφαρμογή υλοποιήθηκε και λειτουργεί άρτια στο λειτουργικό σύστημα των Windows XP. Η βάση δεδομένων που υποστηρίζει την εφαρμογή μας αναπτύχθηκε σε Microsoft Office Access 2007. Τέλος, για την επεξεργασία των δικαιωμάτων πρόσβασης σε αρχεία, φακέλους και εφαρμογές χρησιμοποιήθηκε το εργαλείο Cacls.exe των Windows. Το εργαλείο αυτό καλείται μέσω της γραμμής εντολών Command Line, και με τη χρήση κατάλληλων παραμέτρων, πραγματοποιεί επεξεργασία της λίστας ελέγχου πρόσβασης (Access Control List - ACL) του εκάστοτε αντικειμένου που δίνεται ως όρισμα.

Η εγκατάσταση της εφαρμογής γίνεται με τη βοήθεια ειδικού προγράμματος εγκατάστασης το οποίο δημιουργήθηκε με το Microsoft Visual Studio 2008.

Η εφαρμογή μας αποτελείται από δύο μέρη – υποεφαρμογές: την Εφαρμογή ανάθεσης ρόλων και δικαιωμάτων (RBACProject) και την Εφαρμογή υλοποίησης δικαιωμάτων (RBACStartUp). Ουσιαστικά, την Εφαρμογή ανάθεσης ρόλων και δικαιωμάτων (RBACProject) τη χειρίζεται αποκλειστικά ο Υπεύθυνος Εργαστηρίου. Μέσω της εφαρμογής αυτής γίνεται η ανάθεση ρόλων στους χρήστες, η ανάθεση δικαιωμάτων πρόσβασης στους ρόλους και ο καθορισμός χρονικών περιορισμών. Τα δεδομένα όλων αυτών των ενεργειών αποθηκεύονται στη βάση δεδομένων. Η πραγματική εφαρμογή των δικαιωμάτων γίνεται μέσω της Εφαρμογής υλοποίησης δικαιωμάτων (RBACStartUp). Η εφαρμογή αυτή έχει σχεδιαστεί ώστε κατά την είσοδο του χρήστη στο σύστημα των Windows (login), να εκκινείται αυτόματα και να τρέχει στο παρασκήνιο. Για να επιτευχθεί αυτό, η εφαρμογή έχει οριστεί ως μέρος του συνόλου των προγραμμάτων εκκίνησης (Start Up Applications). Με τη βοήθεια κλήσης του εργαλείου Cacls και αντλώντας δεδομένα από τη βάση, εφαρμόζει τα δικαιώματα στον τρέχοντα χρήστη. Προκειμένου να εφαρμοστούν οι χρονικοί περιορισμοί απαιτείται σύγκριση της ώρας του συστήματος με τα δεδομένα της βάσης ανά τακτά χρονικά διαστήματα, λειτουργικότητα που επιτυγχάνεται μέσω κλήσης κατάλληλης κλάσης.

Η βάση δεδομένων, η εφαρμογή RBACProject και η εφαρμογή RBACStartUp περιγράφονται αναλυτικά ως προς τη δομή, υλοποίηση και λειτουργικότητά τους στις επόμενες ενότητες.

5.4. Βάση Δεδομένων

Η βάση Δεδομένων που υποστηρίζει την εφαρμογή μας χρησιμοποιείται με το όνομα AdminRDB. Όπως αναφέραμε χρησιμοποιήθηκε η εφαρμογή Microsoft Office Access 2007 για τη δημιουργία της. Αποτελείται από τους εξής πίνακες:

- TUsers
- TRoles
- TMessages
- RUserRole
- TRolePerm
- TRoleSchedule

Παρακάτω παρουσιάζοντα αναλυτικά η περιγραφή των πινάκων αυτών καθώς και τα πεδία από τα οποία δομούνται.

TUsers

Πίνακας που περιέχει όλους τους χρήστες του Τοπικού Συστήματος. Αν δεν έχουν προστεθεί από το διαχειριστή μέσω της εφαρμογής RBACProject, προστίθενται μέσω της RBACStarUp εφαρμογής κατά την είσοδο του χρήστη στα Windows.

Αποτελείται από τα πεδία:

Πεδίο	**Περιγραφή**	**Τύπος**
UserId	Κωδικός Χρήστη	Αριθμός
UserName	Όνομα Χρήστη	Κείμενο

TRoles

Πίνακας που περιέχει όλους τους ρόλους που έχουν οριστεί στην Εφαρμογή RBACProject. Στον πίνακα αυτό οι δύο πρώτες εγγραφές αποτελούν προκαθορισμένους ρόλους (Υπεύθυνος Εργαστηρίου, Επισκέπτης) και η εφαρμογή εξασφαλίζει τη μη διαγραφή τους.

Αποτελείται από τα πεδία:

Πεδίο	**Περιγραφή**	**Τύπος**
RoleId	Κωδικός Ρόλου	Αριθμός
UserName	Όνομα Ρόλου	Κείμενο

TRoleSchedule

Πίνακας που περιέχει τους χρονικούς περιορισμούς των ρόλων. Το κλειδί του πίνακα είναι ο συνδυασμός του ξένου κλειδιού RoleId καθώς και του πεδίου RDay. Στην ουσία αποθηκεύονται όλοι οι περιορισμοί που έχουν ανατεθεί στον κάθε ρόλο με ξεχωριστή εγγραφή για κάθε ημέρα που μπορεί αυτός να ενεργοποιηθεί, καθώς και οι χρονικοί περιορισμοί που πιθανόν έχουν τεθεί (Πλήρης Ώρα Έναρξης, Πλήρης Ώρα Λήξης). Επιπρόσθετα, οι ώρες και τα λεπτά αποθηκεύονται ξεχωριστά τόσο για την ώρα έναρξης του περιορισμού όσο και για την ώρα λήξης, καθότι με αυτό τον τρόπο επιτυγχάνεται η απεικόνισή τους στις αντίστοιχες οθόνες όταν ο Υπεύθυνος θέλει απλά να δει τους χρόνους αυτούς.

Αποτελείται από τα πεδία:

Πεδίο	**Περιγραφή**	**Τύπος**
RoleId	Κωδικός Ρόλου	Αριθμός
RDay	Ημέρα Ισχύος Περιορισμού	Αριθμός
FromTime	Πλήρης Ώρα έναρξης Περιορισμού	Ημερομηνία / Ώρα
ToTime	Πλήρης Ώρα λήξης Περιορισμού	Ημερομηνία / Ώρα
FromHour	Ώρα έναρξης	Κείμενο
FromMinute	Λεπτά έναρξης	Κείμενο
ToHour	Ώρα Λήξης	Κείμενο
ToMinute	Λεπτά Λήξης	Κείμενο

TMessages

Πίνακας που περιέχει όλα τα μηνύματα που προστίθενται στη βάση προς ενημέρωση του Υπευθύνου Εργαστηρίου.

Αποτελείται από τα πεδία:

Πεδίο	**Περιγραφή**	**Τύπος**
MessageId	Κωδικός Μηνύματος	Αριθμός
MsgDate	Ημερομηνία – Ώρα Μηνύματος	Ημερομηνία / Ώρα
MsgTxt	Κείμενο Μηνύματος	Κείμενο
StatusFlg	Ένδειξη αναγνωσμένου μηνύματος (1: Μη Αναγνωσμένο, 0: Αναγνωσμένο)	Αριθμός

RUserRole

Πίνακας που περιέχει τις συσχετίσεις χρηστών και ρόλων. Το κλειδί του πίνακα είναι ο συνδυασμός δύο ξένων κλειδιών (UserId και RoleId) καθώς και του πεδίου RDay. Στην ουσία αποθηκεύονται όλοι οι ρόλοι που έχουν ανατεθεί στον κάθε χρήστη με ξεχωριστή εγγραφή για κάθε ημέρα που μπορεί ο εκάστοτε ρόλος να ενεργοποιηθεί, καθώς και οι χρονικοί περιορισμοί που πιθανόν έχουν τεθεί (Πλήρης Ώρα Έναρξης, Πλήρης Ώρα Λήξης). Επιπρόσθετα, οι ώρες και τα λεπτά αποθηκεύονται ξεχωριστά τόσο για την ώρα έναρξης του περιορισμού όσο και για την ώρα λήξης, καθότι με αυτό τον τρόπο επιτυγχάνεται η απεικόνισή τους στις αντίστοιχες οθόνες όταν ο Υπεύθυνος θέλει απλά να δει τους χρόνους αυτούς.

Αποτελείται από τα πεδία:

Πεδίο	**Περιγραφή**	**Τύπος**
UserId	Κωδικός Χρήστη	Αριθμός
RoleId	Κωδικός Ρόλου	Αριθμός
RDay	Ημέρα Ισχύος Περιορισμού	Αριθμός
FromTime	Πλήρης Ώρα έναρξης Περιορισμού	Ημερομηνία / Ώρα
ToTime	Πλήρης Ώρα λήξης Περιορισμού	Ημερομηνία / Ώρα
FromHour	Ώρα έναρξης	Κείμενο
FromMinute	Λεπτά έναρξης	Κείμενο
ToHour	Ώρα Λήξης	Κείμενο
ToMinute	Λεπτά Λήξης	Κείμενο
RoleStatus	Ένδειξη ενεργού ρόλου (1: Ενεργός, 0: Ανενεργός)	Αριθμός

TRolePerm

Πίνακας που περιέχει όλα τα δικαιώματα πρόσβασης που έχουν οριστεί ανά ρόλο. Το κλειδί του πίνακα είναι ο συνδυασμός του εξωτερικού κλειδιού RoleId καθώς και του πεδίου

PathName. Το πεδίο αυτό διατηρεί την πληροφορία για το πλήρες μονοπάτι του φακέλου ή του αρχείου/εφαρμογής για το οποίο ορίστηκε δικαίωμα πρόσβασης. Με τον ορισμό του ως μέρος του κλειδιού, αλλά και με τους ελέγχους που γίνονται μέσω της εφαρμογής, εξασφαλίζουμε ότι δε θα δοθεί δικαίωμα πρόσβασης δύο φορές για τον ίδιο ρόλο που να αφορά το ίδιο μονοπάτι. Επιπλέον διατηρείται το όνομα του αρχείου ή του φακέλου, καθώς και ένδειξη του τύπου (διαφορετική ένδειξη για φάκελο και αρχείο). Μία άλλη απαραίτητη πληροφορία είναι αυτή του είδους πρόσβασης που καθορίζεται. Το πεδίο στο οποίο διατηρείται είναι το AccessType και παίρνει τις τιμές F και N για την πλήρη πρόσβαση και την απαγόρευση αυτής αντίστοιχα. Τέλος, όπως και στον πίνακα RUserRole, αποθηκεύονται όλοι οι χρονικοί περιορισμοί που πιθανόν έχουν τεθεί στο εκάστοτε δικαίωμα (Πλήρης Ώρα Έναρξης, Πλήρης Ώρα Λήξης). Οι ώρες και τα λεπτά αποθηκεύονται και εδώ ξεχωριστά τόσο για την ώρα έναρξης του περιορισμού όσο και για την ώρα λήξης καθότι με αυτό τον τρόπο επιτυγχάνεται η απεικόνισή τους στις αντίστοιχες οθόνες, όταν ο Υπεύθυνος θέλει απλά να δει τους χρόνους αυτούς.

Αποτελείται από τα πεδία:

Πεδίο	**Περιγραφή**	**Τύπος**
RoleId	Κωδικός Χρήστη	Αριθμός
PathName	Πλήρες Μονοπάτι	Κείμενο
ShortName	Όνομα αρχείου/εφαρμογής, φακέλου	Κείμενο
ItemType	Τύπος Δικαιώματος (1: αρχείο, 2: φάκελος)	Αριθμός
AccessType	Είδος Πρόσβασης (N: Μη Πρόσβαση, F: Πλήρης Πρόσβαση)	Κείμενο
PFromTime	Πλήρης Ώρα έναρξης Περιορισμού	Ημερομηνία / Ώρα
PToTime	Πλήρης Ώρα λήξης Περιορισμού	Ημερομηνία / Ώρα
PFromHour	Ώρα έναρξης	Κείμενο
PFromMinute	Λεπτά έναρξης	Κείμενο
PToHour	Ώρα Λήξης	Κείμενο
PToMinute	Λεπτά Λήξης	Κείμενο
PermStatus	Ένδειξη ενεργού δικαιώματος (1: Ενεργός, 0: Ανενεργός)	Αριθμός

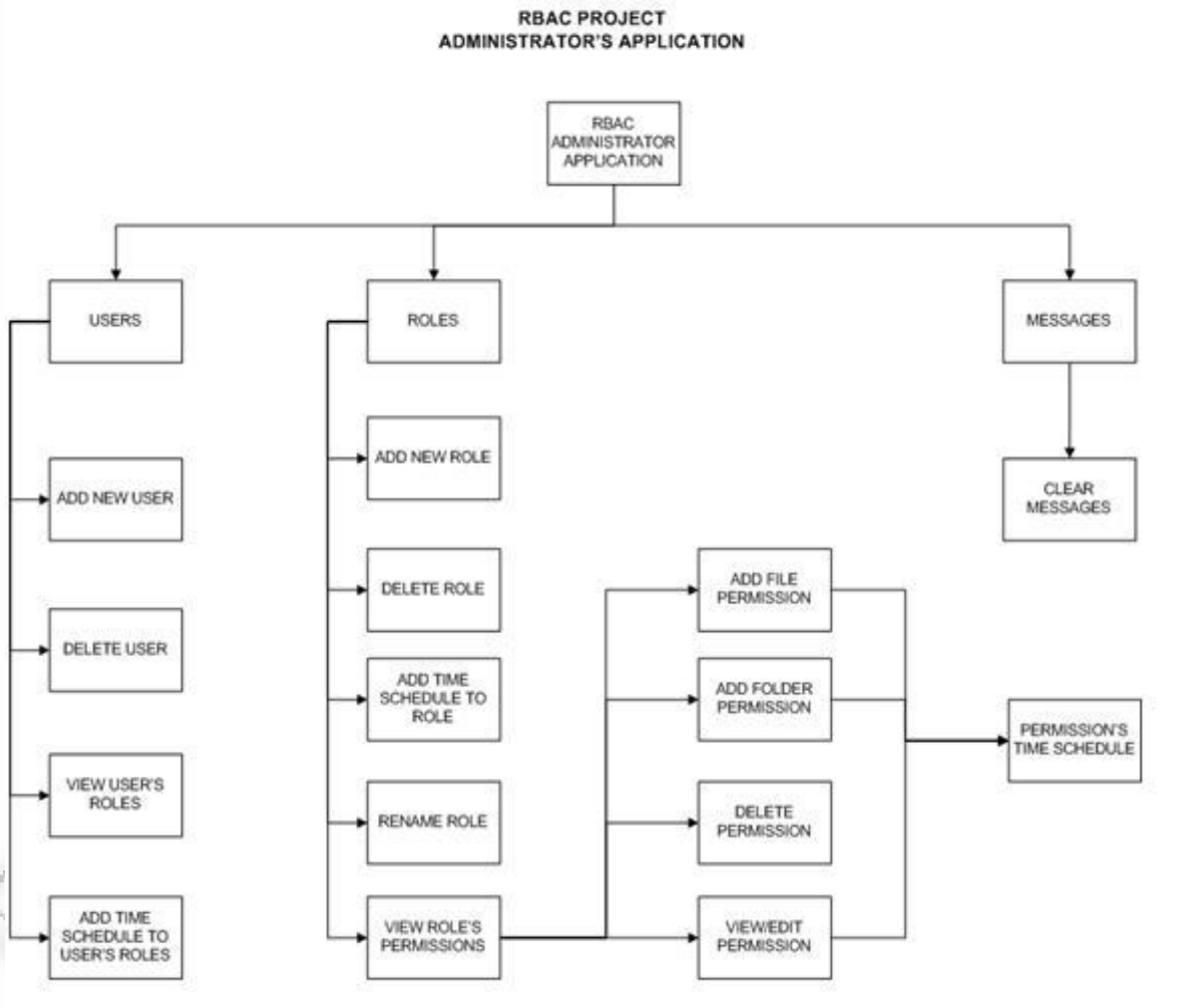
5.5. Εφαρμογή Ανάθεσης Ρόλων και Δικαιωμάτων (RBACProject)

Στην ενότητα αυτή παρουσιάζεται η βασική εφαρμογή που χρησιμοποιεί ο Υπεύθυνος Εργαστηρίου προκειμένου να επιτύχει τη διαμόρφωση της πρόσβαση στο συγκεκριμένο τοπικό υπολογιστή. Αποτελεί την κύρια εφαρμογή μέσω της οποίας στην ουσία υλοποιείται το Βασικό μοντέλο RBAC. Όπως έχουμε ήδη αναφέρει, στο μοντέλο RBAC υπάρχουν δύο βασικές σχέσεις που αποτελούν τον πυρήνα του: η ανάθεση ρόλων σε χρήστες και η ανάθεση δικαιωμάτων πρόσβασης σε ρόλους. Θα δούμε, πως οι δύο αυτές βασικές συνιστώσες του μοντέλου RBAC υλοποιούνται μέσα από την εφαρμογή μας με τη βοήθεια φιλικής προς το χρήστη διεπαφής. Με κύριο γνώμονα την αποφυγή της χωρίς-όρους-πρόσβασης των χρηστών στους φακέλους, αρχεία και εφαρμογές του τοπικού υπολογιστή, ανατίθενται στους χρήστες του ρόλοι ανάλογα με την ιδιότητα τους και το επιθυμητό επίπεδο πρόσβασης. Η εφαρμογή υλοποιεί επιπλέον κάποιες από τις συνιστώσες των μοντέλων TRBAC και GTRBAC, μέσω της προσθήκης χρονικών περιορισμών στην ανάθεση ρόλων στους χρήστες, στην ενεργοποίηση των ρόλων αλλά και στην ανάθεση δικαιωμάτων πρόσβασης στους ρόλους.

Πέραν των λειτουργικοτήτων που αφορούν τη διαμόρφωση της βάσης δεδομένων, βασική απαίτηση αποτελεί η εφαρμογή να είναι προσιτή και φιλική προς το χρήστη, ο οποίος στη συγκεκριμένη περίπτωση είναι ο Υπεύθυνος Εργαστηρίου. Κινούμενες προς αυτό το στόχο, η βασική οθόνη της εφαρμογής RBACProject αποτελείται από τρεις καρτέλες. Οι δύο πρώτες καρτέλες κατευθύνουν τον Υπεύθυνο Εργαστηρίου στο να πραγματοποιήσει: α) την ανάθεση ρόλων σε χρήστες και β) την ανάθεση δικαιωμάτων πρόσβασης σε ρόλους. Τέλος, η τρίτη καρτέλα εμφανίζει μηνύματα προς ενημέρωση του Υπευθύνου Εργαστηρίου. Μία συνοπτική παρουσίαση της δομής της εφαρμογής μας γίνεται μέσω της παρακάτω εικόνας (Εικόνα 5.1).

Για την ορθή λειτουργία της εφαρμογής μας απαιτείται να έχουν πρόσβαση στην εφαρμογή RBACProject μόνο οι χρήστες στους οποίους έχει ανατεθεί και είναι ενεργός ο ρόλος του Υπεύθυνου Εργαστηρίου. Η απαίτηση αυτή διασφαλίζεται μέσω της εφαρμογής RBACStartUp που περιγράφεται σε επόμενη ενότητα και ειδικότερα μέσω της κλήσης της Συνάρτησης SecureMyApplication.

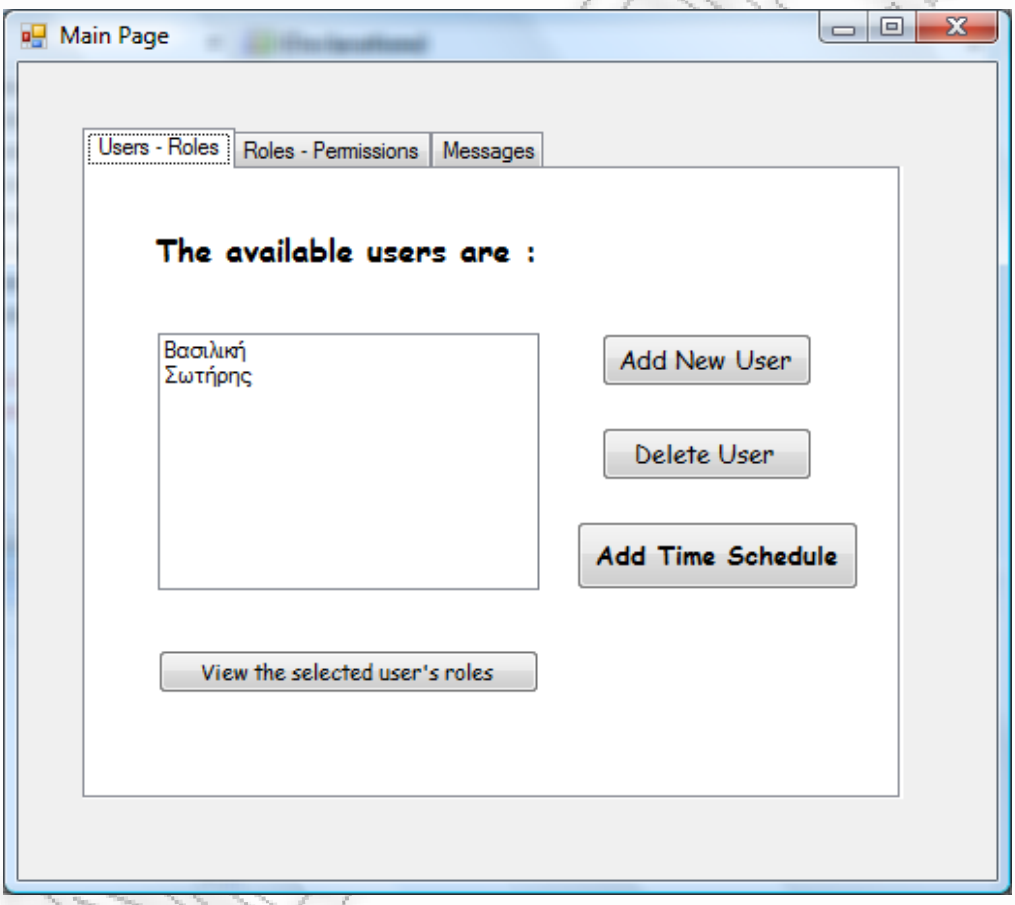
Εικόνα 5.1: Δομή Εφαρμογής Ανάθεσης Ρόλων και Δικαιωμάτων RBACProject



Παρακάτω αναλύονται κάθε μία από τις τρεις καρτέλες που αναφέραμε, καθώς και οι λειτουργικότητες αυτών.

5.5.1. Καρτέλα Διαχείρισης Χρηστών

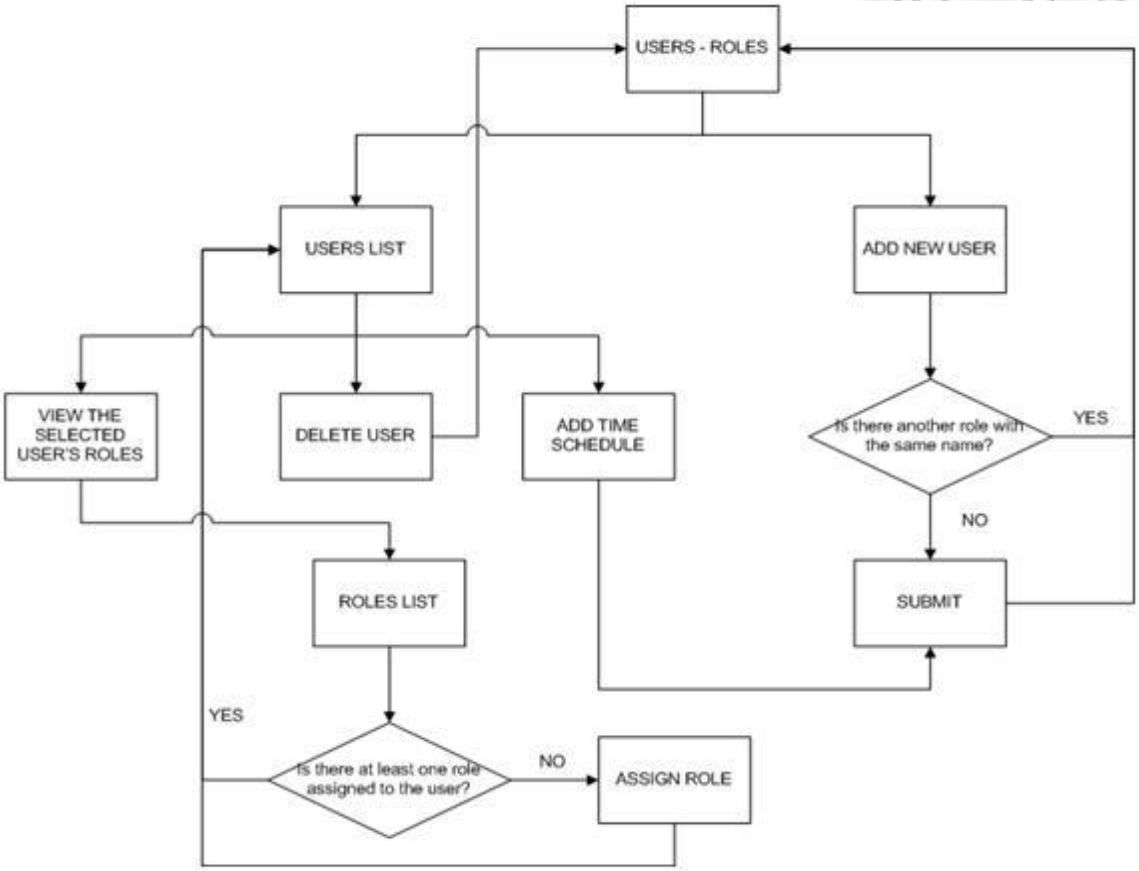
Η καρτέλα Users – Roles, αποτελεί την πρώτη καρτέλα που εμφανίζεται στον Υπεύθυνο Εργαστηρίου με το άνοιγμα της εφαρμογής (Οθόνη 1). Η βασική της λειτουργία επικεντρώνεται στη διαχείριση των χρηστών του συστήματος, στην ανάθεση ρόλων σε αυτούς καθώς και στην προσθήκη χρονικών περιορισμών στην ανάθεση ενός ρόλου σε κάποιο χρήστη.



Οθόνη 1

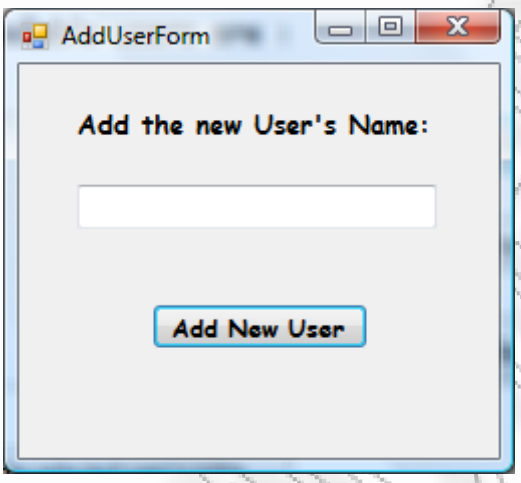
Οι διαφορετικές ενέργειες που μπορεί να εκτελέσει ο Υπεύθυνος Εργαστηρίου γίνονται με τη χρήση κουμπιών που υπάρχουν στη βασική οθόνη. Οι κυριότερες λειτουργίες που μπορούν να πραγματοποιηθούν μέσα από αυτή την καρτέλα παρουσιάζονται στην επόμενη εικόνα (Εικόνα 5.2).

Εικόνα 5.2: Λειτουργίες Καρτέλας Διαχείρισης Χρηστών



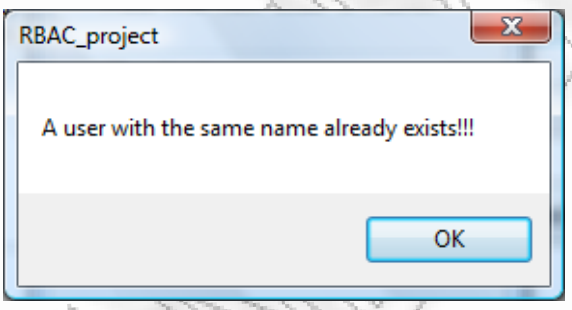
Το μεγαλύτερο μέρος της καρτέλας Users – Roles αποτελείται από τη λίστα όλων των χρηστών του τοπικού υπολογιστή έτσι όπως αυτοί είναι αποθηκευμένοι στη βάση μας. Στην πραγματικότητα πρόκειται για τις εγγραφές του πίνακα TUsers της βάσης δεδομένων της εφαρμογής μας. Οι χρήστες που θα πρέπει να απεικονίζονται σε αυτή τη λίστα είναι οι χρήστες του λειτουργικού συστήματος των Windows. Η εισαγωγή εγγραφών στον πίνακα TUsers μπορεί να γίνει είτε αυτόματα μέσω διαδικασίας της Εφαρμογής υλοποίησης δικαιωμάτων (RBACStartUp), και η οποία περιγράφεται σε επόμενη ενότητα, είτε χειροκίνητα από τον Υπεύθυνο Εργαστηρίου μέσω της καρτέλας Users – Roles. Ο Υπεύθυνος Εργαστηρίου θα πρέπει να προσέξει ώστε τα ονόματα των χρηστών που προσθέτει να αντιστοιχούν σε ονόματα χρηστών έτσι όπως αυτά έχουν δηλωθεί κατά τη διάρκεια δημιουργίας των λογαριασμών τους στα Windows. Παρόλα αυτά η εφαρμογή RBACProject δε διενεργεί κάποιον επιπλέον έλεγχο για να αποτρέψει την εισαγωγή χρήστη που δεν αποτελεί ταυτόχρονα χρήστη των Windows. Στην ουσία αυτή η εγγραφή δε θα χρησιμοποιηθεί ποτέ κατά την εφαρμογή δικαιωμάτων, αφού ο χρήστης αυτός δε θα υφίσταται στο λειτουργικό σύστημα.

Πρώτη λειτουργία, λοιπόν, που μπορεί να κάνει ο Υπεύθυνος Εργαστηρίου είναι η προσθήκη νέων χρηστών. Με ένα κλικ στην επιλογή Add User εμφανίζεται ένα νέο παράθυρο όπου καλείται να δώσει το όνομα που επιθυμεί για το νέο χρήστη (Οθόνη 2).

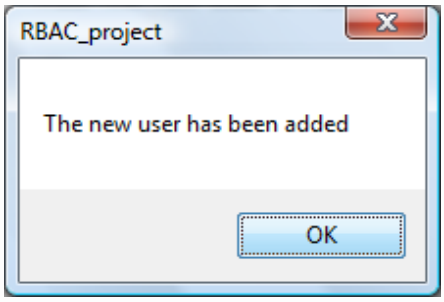


Οθόνη 2

Στο σημείο αυτό τίθεται ο περιορισμός του να μη δοθεί όνομα χρήστη που ήδη υπάρχει. Η εφαρμογή πραγματοποιεί έλεγχο για το αν υπάρχει στη βάση χρήστης με το ίδιο όνομα που πληκτρολογήθηκε. Στην περίπτωση που βρεθεί χρήστης με το ίδιο το όνομα, δεν προχωράει στην προσθήκη νέας εγγραφής εμφανίζοντας παράλληλα κατάλληλο προειδοποιητικό μήνυμα (Οθόνη 3) . Εάν το όνομα του χρήστη που επιθυμεί ο Υπεύθυνος Εργαστηρίου να προσθέσει, δε βρεθεί σε κάποια από τις εγγραφές του πίνακα TUsers, τότε γίνεται αυτόματα εισαγωγή του στη βάση. Ο Υπεύθυνος Εργαστηρίου ενημερώνεται για την επιτυχή εισαγωγή του νέου χρήστη με κατάλληλο μήνυμα . (Οθόνη 4)



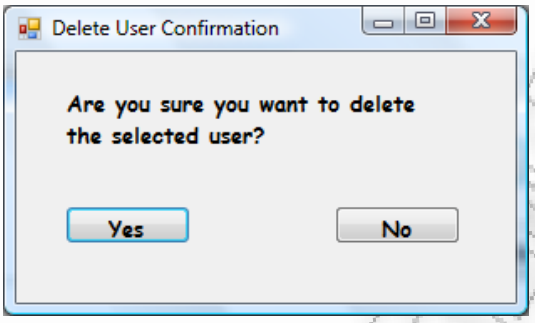
Οθόνη 3



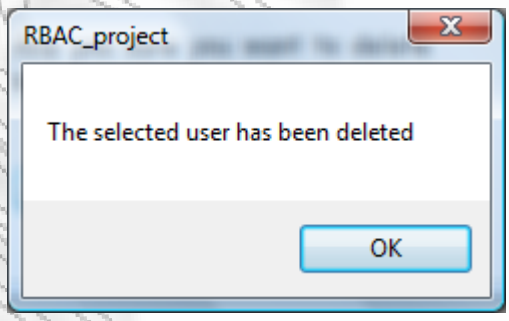
Οθόνη 4

Επόμενη επιλογή που δίνεται στον Υπεύθυνο Εργαστηρίου είναι η διαγραφή ενός χρήστη μέσω της επιλογής του από τη λίστα και στη συνέχεια του πατήματος του αντίστοιχου πλήκτρου (Delete User). Τότε εμφανίζεται στο χρήστη μήνυμα που του ζητάει επιβεβαίωση για την επιθυμία του να διαγράψει τον επιλεγμένο χρήστη (Οθόνη 5), προστατεύοντάς τον από διαγραφή λόγω πατήματος κατά λάθος του πλήκτρου Delete User. Η λειτουργικότητα της

διαγραφής επιτρέπει στον Υπεύθυνο Εργαστηρίου να «καθαρίσει» τη βάση από τους χρήστες που έχουν καταργηθεί από το σύστημα. Στο σημείο αυτό θα πρέπει να τονίσουμε ότι σκοπός της εφαρμογής μας δεν είναι η διαχείριση των χρηστών των Windows, αλλά η διαχείριση των δικαιωμάτων πρόσβασης αυτών σε φακέλους, αρχεία και εφαρμογές, σύμφωνα με τον/τους ρόλους που τους έχουν ανατεθεί και κατ' επέκταση με τα δικαιώματα πρόσβασης που έχουν ανατεθεί στον/στους ρόλους αυτούς. Για το λόγο αυτό, δεν τίθεται κάποιος περιορισμός στη διαγραφή ενός χρήστη μέσω του RBACProject, αφού η διαγραφή αυτή δε συνεπάγεται τη διαγραφή του χρήστη από το σύστημα των Windows. Εφόσον όμως ο χρήστης συνεχίσει να υφίσταται στη λίστα των Windows Users, την επόμενη φορά μετά τη διαγραφή του που θα συνδεθεί στα Windows, θα του δοθεί ένας προκαθορισμένος ρόλος. Ο ρόλος αυτός έχει οριστεί να ανατίθεται στους χρήστες των οποίων τα ονόματα δεν υπάρχουν στον πίνακα TUsers της βάσης μέχρι ότου ο διαχειριστής τους αναθέσει κάποιον άλλο ρόλο. Η λειτουργικότητα αυτή υλοποιείται μέσω της εφαρμογής RBACStartUp και περιγράφεται αναλυτικά σε επόμενη ενότητα. Μετά την διαγραφή του χρήστη, εμφανίζεται και σε αυτή την περίπτωση μήνυμα που ενημερώνει τον Υπεύθυνο Εργαστηρίου για την ολοκλήρωση της διαγραφής (Οθόνη 6).



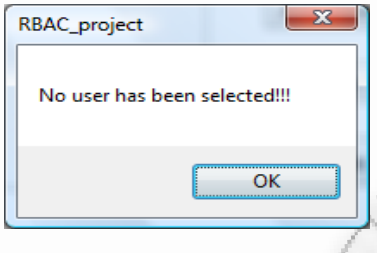
Οθόνη 5



Οθόνη 6

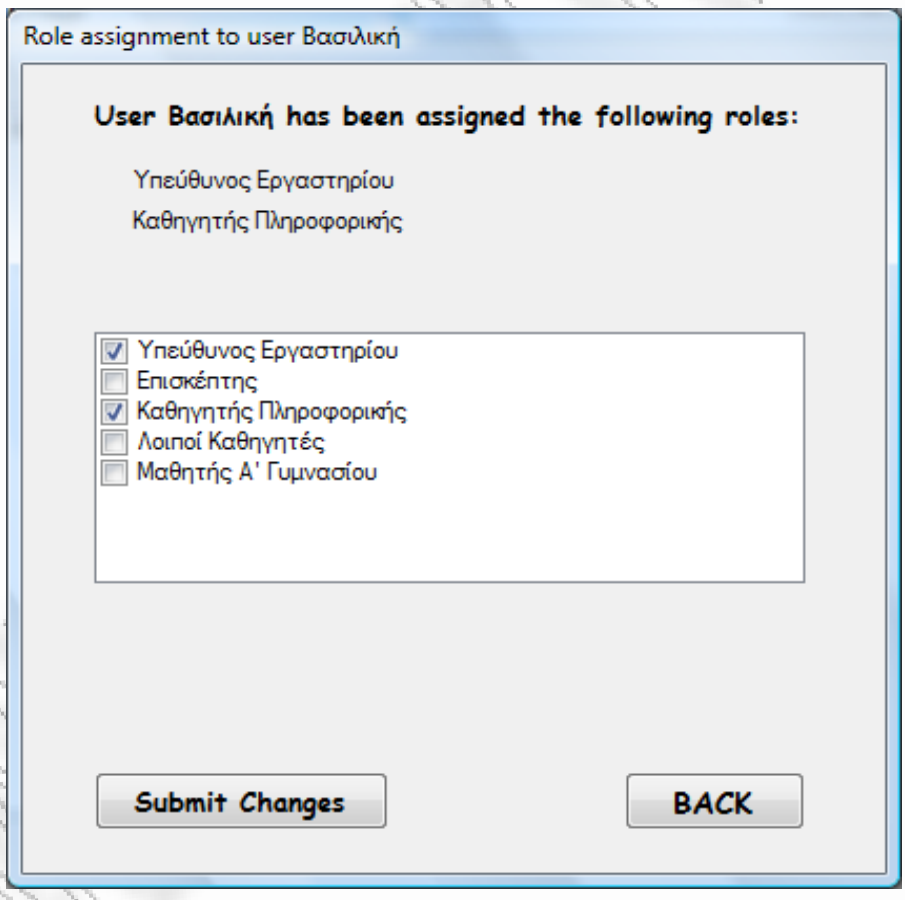
Από προγραμματιστική σκοπιά, η προσθήκη ενός νέου χρήστη μέσω της καρτέλας Users – Roles συνεπάγεται την προσθήκη μιας νέας εγγραφής στον πίνακα TUsers της βάσης με κωδικό χρήστη τον αμέσως επόμενο διαθέσιμο κωδικό και όνομα χρήστη αυτό που πληκτρολογήθηκε από τον Υπεύθυνο Εργαστηρίου. Κατά τη διαγραφή ενός χρήστη, διαγράφεται η αντίστοιχη εγγραφή από τον πίνακα TUsers αλλά και όσες εγγραφές αφορούν το συγκεκριμένο χρήστη από τον πίνακα RUserRole που περιέχει όλες τις αναθέσεις ρόλων στους χρήστες. Με την ενέργεια αυτή επιτυγχάνεται η επικαιροποίηση της βάσης.

Επόμενη ιδιαίτερα σημαντική λειτουργικότητα προσφέρεται στον Υπεύθυνο Εργαστηρίου μέσω του πλήκτρου προβολής των ρόλων του χρήστη (View the selected user's roles) που θα επιλέξει από τη λίστα των χρηστών. Με το πάτημα αυτού του κουμπιού πραγματοποιείται έλεγχος για το αν έχει επιλεχθεί κάποιος χρήστης από τη λίστα των χρηστών προκειμένου να προβληθούν οι ρόλοι του (Οθόνη 7). Αν ο Υπεύθυνος Εργαστηρίου έχει ξεχάσει να επιλέξει χρήστη τότε η εφαρμογή τον ειδοποιεί με κατάλληλο μήνυμα.



Οθόνη 7

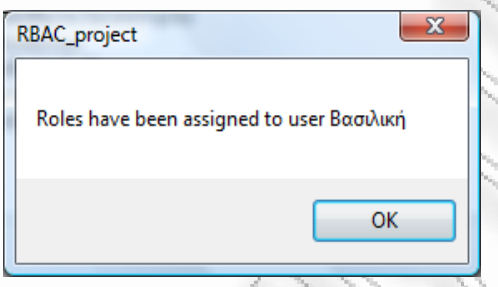
Στη συνέχεια κατευθυνόμαστε σε μία νέα οθόνη (Role Assignment), μέσω της οποίας πραγματοποιείται η ανάθεση ρόλων στους χρήστες (Οθόνη 8). Στο πάνω μέρος της οθόνης εμφανίζεται μήνυμα το οποίο αναφέρει το όνομα του χρήστη και τους ρόλους που είναι ήδη ανατεθειμένοι σε αυτόν. Παράλληλα στην οθόνη εμφανίζεται λίστα, η οποία περιέχει όλους τους ρόλους της εφαρμογής που έχουν οριστεί από τον Υπεύθυνο Εργαστηρίου και οι οποίοι είναι αποθηκευμένοι στον πίνακα TRoles της βάσης δεδομένων.



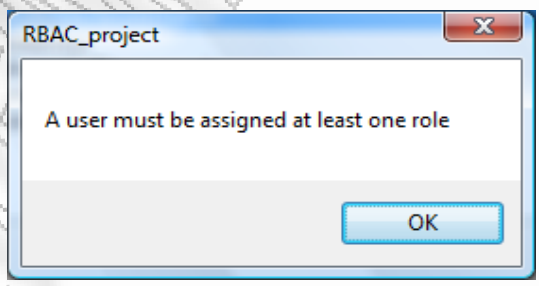
Οθόνη 8

Στο σημείο αυτό θα πρέπει να υπενθυμίσουμε ότι σύμφωνα με το μοντέλο RBAC, σε κάθε χρήστη μπορεί να ανατεθούν περισσότεροι του ενός ρόλοι. Ο κάθε χρήστης μπορεί στα πλαίσια μιας συνεδρίας να ενεργοποιήσει περισσότερους του ενός ρόλους εξασκώντας ταυτόχρονα τα δικαιώματα πρόσβασης των πολλαπλών αυτών ρόλων. Καθώς η εφαρμογή μας έχει σχεδιαστεί για να λειτουργεί στα πλαίσια ενός τοπικού συστήματος, μόνο μία συνεδρία μπορεί να είναι ανοιχτή για το χρήστη. Στα πλαίσια της συνεδρίας αυτής ενεργοποιούνται όλοι οι ρόλοι που του έχουν ανατεθεί και βάσει των χρονικών περιορισμών σε περίπτωση ύπαρξής τους. Επανερχόμενοι τώρα στην οθόνη, οι ανατεθειμένοι στο χρήστη ρόλοι εμφανίζονται στη λίστα ως επιλεγμένοι (μέσω του συμβόλου √ στα αντίστοιχα checkboxes).

Στην οθόνη της ανάθεσης ρόλων στον επιλεγμένο χρήστη (Role Assignment), εκτός από την προβολή των ρόλων του χρήστη, παρέχεται και η δυνατότητα αλλαγής των ρόλων του. Η διαδικασία είναι ιδιαίτερα απλή. Ο Υπεύθυνος Εργαστηρίου προσθέτει και αφαιρεί σε ένα χρήστη ρόλους επιλέγοντας ή αφαιρώντας το σύμβολο √ από το κουτί επιλογής δίπλα στο ρόλο. Για την υποβολή των αλλαγών αυτών χρειάζεται να πατήσει το αντίστοιχο πλήκτρο (Submit Changes) στο κάτω μέρος της οθόνης. Για λόγους προστασίας των φακέλων, των αρχείων και των εφαρμογών του συστήματός μας από μη εξουσιοδοτημένη χρήση, έχουμε ορίσει ότι σε κάθε χρήστη θα πρέπει να ανατεθεί τουλάχιστον ένας ρόλος. Συνεπώς, όταν ο Υπεύθυνος Εργαστηρίου πατάει το κουμπί για την υποβολή των αλλαγών λαμβάνει χώρα έλεγχος που αφορά το κατά πόσο ο χρήστης έχει τουλάχιστον ένα ρόλο. Εάν ο Υπεύθυνος Εργαστηρίου έχει επιλέξει να αφαιρέσει όλους τους ρόλους από το χρήστη, η υποβολή των αλλαγών δεν επιτρέπεται από την εφαρμογή ενώ παράλληλα εμφανίζεται και κατάλληλο ενημερωτικό μήνυμα (Οθόνη 10).



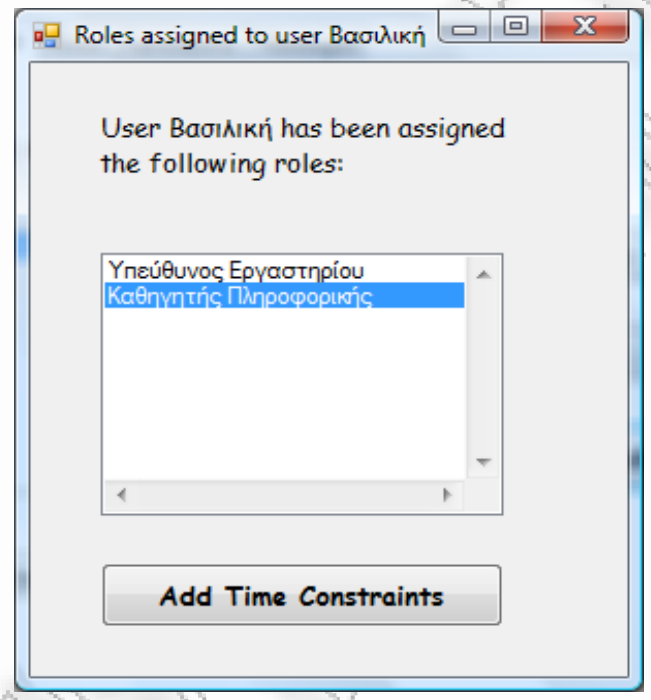
Οθόνη 9



Οθόνη 10

Η υποβολή των αλλαγών, εφόσον ικανοποιείται η συνθήκη της υποχρεωτικής ανάθεσης τουλάχιστον ενός ρόλου στο χρήστη, πραγματοποιείται με διαγραφή από τον πίνακα RUserRole όλων των εγγραφών που αφορούν τον επιλεγμένο χρήστη και προσθέτοντας σε αυτόν νέες εγγραφές με βάση τους νέους ρόλους που έχουν επιλεχθεί γι' αυτόν. Ο αριθμός των εγγραφών που προστίθενται για κάθε ρόλο του χρήστη είναι ίσος με τον αριθμό των εγγραφών που υπάρχουν στον πίνακα TRoleSchedule για το ρόλο αυτό (δηλ όσες ημέρες της εβδομάδας μπορεί να ενεργοποιηθεί ο ρόλος αυτός) . Τα πεδία «Από» (From) και Έως (To) γεμίζουν αντλώντας στοιχεία από τις αντίστοιχες εγγραφές του πίνακα TRoleSchedule. Ο τρόπος με τον οποίο γεμίζει ο πίνακας TRoleSchedule περιγράφεται αναλυτικά παρακάτω. Η διαδικασία ολοκληρώνεται μέσω κατάλληλου μηνύματος που ενημερώνει τον Υπεύθυνο Εργαστηρίου για την πραγματοποίηση των αλλαγών. Σε περίπτωση που ο Υπεύθυνος Εργαστηρίου δεν επιθυμεί να πραγματοποιήσει κάποια μεταβολή μπορεί να επιστρέψει στην προηγούμενη οθόνη μέσω του πλήκτρου της επιστροφής (Back).

Επιστρέφοντας στην οθόνη της καρτέλας Users – Roles, θα περιγράψουμε την τελευταία, ιδιαίτερα σημαντική λειτουργικότητα αυτής, που αφορά στον χρονοπρογραμματισμό του ρόλου για το συγκεκριμένο χρήστη και δίνεται μέσω του κουμπιού υποβολής χρονικών περιορισμών (Time Schedule). Πατώντας το πλήκτρο αυτό γίνεται και πάλι έλεγχος για το αν έχει επιλεχθεί χρήστης για τον οποίο θα καταχωρηθούν χρονικοί περιορισμοί. Αν όχι, τότε εμφανίζεται μήνυμα που ενημερώνει τον Υπεύθυνο Εργαστηρίου. Αφού έχει γίνει επιλογή χρήστη τότε οδηγούμαστε σε μια νέα ενδιάμεση οθόνη (Roles Assigned to User) η οποία εμφανίζει σε λίστα τους ρόλους του χρήστη (Οθόνη 11).

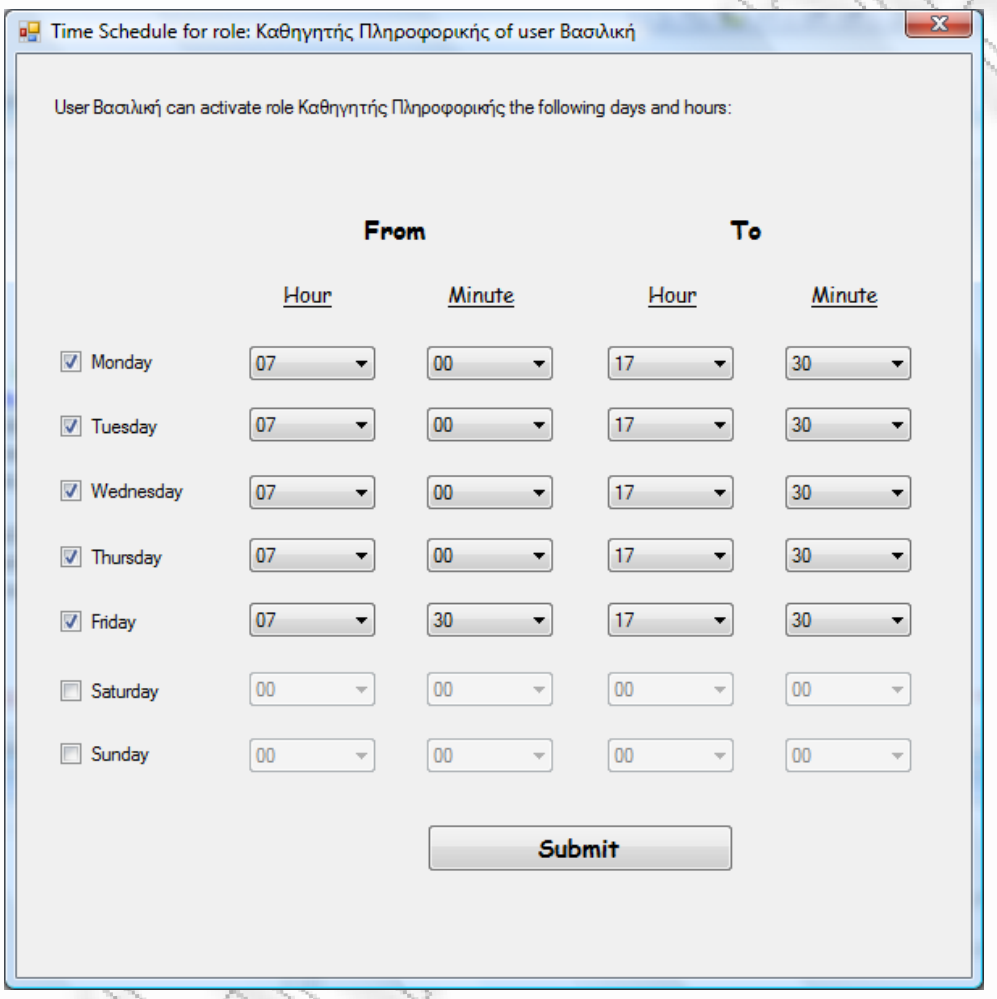


Οθόνη 11

Από τη λίστα αυτή επιλέγεται ο ρόλος του χρήστη για τον οποίο θέλουμε να προσθέσουμε χρονικούς περιορισμούς. Με το πάτημα του πλήκτρου προσθήκης των χρονικών περιορισμών (Add Time Constraints) κατευθυνόμαστε και πάλι σε νέα οθόνη (User Role Schedule) (Οθόνη 12) στην οποία θα προστεθούν οι χρονικοί περιορισμοί.

Η οθόνη User Role Schedule μας παρέχει τη λειτουργικότητα του χρονοπρογραμματισμού του επιλεγμένου ρόλου για το συγκεκριμένου χρήστη. Η οθόνη εμφανίζει με τη μορφή κουμπιών επιλογής (checkboxes) τις ημέρες της εβδομάδας. Δίπλα σε κάθε μέρα της εβδομάδας υπάρχουν 4 πεδία στα οποία αποτυπώνονται τα χρονικά διαστήματα κατά τα οποία μπορεί να είναι ενεργός ο συγκεκριμένος ρόλος του χρήστη τη συγκεκριμένη μέρα της εβδομάδας. Τα πεδία «Από» (From) και Έως (To), ενεργοποιούνται μόνο για τις ημέρες που είναι επιλεγμένες μέσω του συμβόλου √. Σε διαφορετική περίπτωση παραμένουν απενεργοποιημένα. Στο φόρτωμα της οθόνης αυτής, τόσο τα checkboxes που αφορούν τις ημέρες της εβδομάδας όσο και τα πεδία «Από» (From) και Έως (To), είναι συμπληρωμένα με τις ημέρες και με τα χρονικά

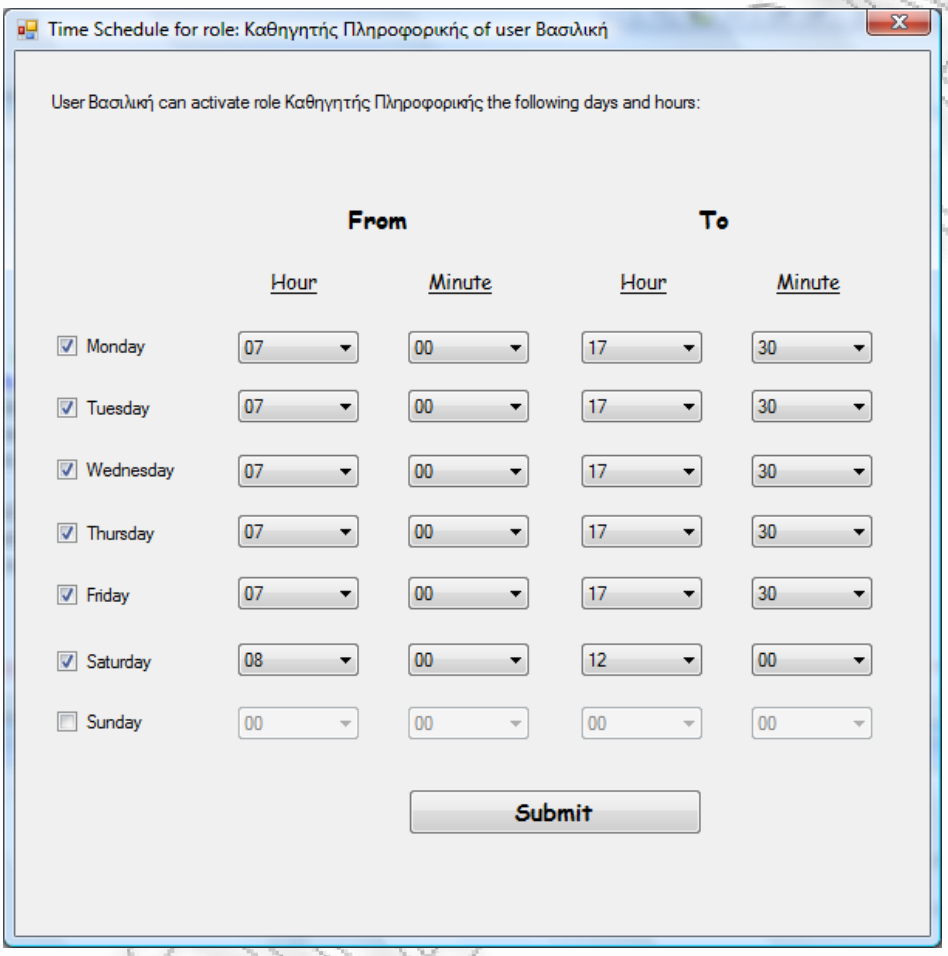
διάστημα ενεργοποίησης του επιλεγμένου ρόλου του χρήστη, αντλώντας τις τιμές από τα αντίστοιχα πεδία του πίνακα RUserRole της βάσης δεδομένων. Δηλαδή, τα πεδία αυτά είναι συμπληρωμένα με τις μέρες και ώρες που μπορεί να ενεργοποιηθεί ο συγκεκριμένος ρόλος όπως τα έχει καθορίσει ο Υπεύθυνος Εργαστηρίου.



Οθόνη 12

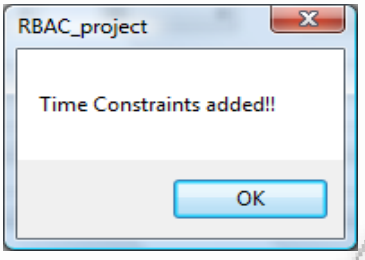
Μέσω της οθόνης που περιγράφηκε παραπάνω (User Role Schedule), η εφαρμογή μας προσφέρει μια επιπλέον λειτουργικότητα, επιτρέποντας στον Υπεύθυνο Εργαστηρίου να ορίζει για το συγκεκριμένο χρήστη και τον επιλεγμένο ρόλο του, διαφορετικούς χρονικούς περιορισμούς από αυτούς που ορίζει ο ρόλος. Οι περιορισμοί που ανατίθενται στο χρήστη είναι και αυτοί οι οποίοι υπερισχύουν. Μπορεί, δηλαδή, να καθορίσει τις μέρες και τα χρονικά διαστήματα κατά τα οποία θα είναι ενεργός για το συγκεκριμένο χρήστη ο ρόλος αυτός. Αυτό πραγματοποιείται επιλέγοντας τις επιθυμητές μέρες μέσω του συμβόλου √ στα αντίστοιχα checkboxes και συμπληρώνοντας τις επιθυμητές ώρες μέσω των πεδίων «Από» (From) και Έως (To) (Οθόνη 13). Εάν θέλουμε ο επιλεγμένος ρόλος του χρήστη να είναι όλη την ημέρα

ενεργός (δηλ να μην υπάρχει χρονικός περιορισμός) τότε είτε φροντίζουμε στα πεδία «Από» (From) και Έως (To) να είναι επιλεγμένη η ίδια ώρα ώστε να καλύπτεται όλο το εικοσιτετράωρο.



Οθόνη 13

Μέσω του πλήκτρου της υποβολής (Submit) γίνεται η καταχώρηση των χρονικών περιορισμών στη βάση και εμφανίζεται ενημερωτικό μήνυμα στον Υπεύθυνο Εργαστηρίου (Οθόνη 14). Ειδικότερα, διαγράφονται από τον πίνακα RUserRoles όλες οι εγγραφές που αφορούν το συγκεκριμένο χρήστη και το συγκεκριμένο ρόλο του και στη συνέχεια προστίθενται νέες εγγραφές με τους νέους χρονικούς περιορισμούς που έχουν οριστεί. Όταν θελήσει, ο Υπεύθυνος Εργαστηρίου μπορεί να δει και να επεξεργαστεί το χρονοπρογραμματισμό ενός ρόλου ακολουθώντας την εξής διαδρομή: επιλέγει από την καρτέλα User Role το όνομα του χρήστη → Add Time Schedule→επιλέγει το ρόλο→Add Time Constraints. Οι μέρες της εβδομάδας και τα πεδία «Από» (From) και Έως (To) είναι συμπληρωμένα με τις τιμές από τα αντίστοιχα πεδία της βάσης δεδομένων. Αφού πραγματοποιήσει τις όποιες αλλαγές επιθυμεί στην ήδη αποθηκευμένη πληροφορία, τις υποβάλλει και επικαιροποιούνται οι αντίστοιχες εγγραφές της βάσης.

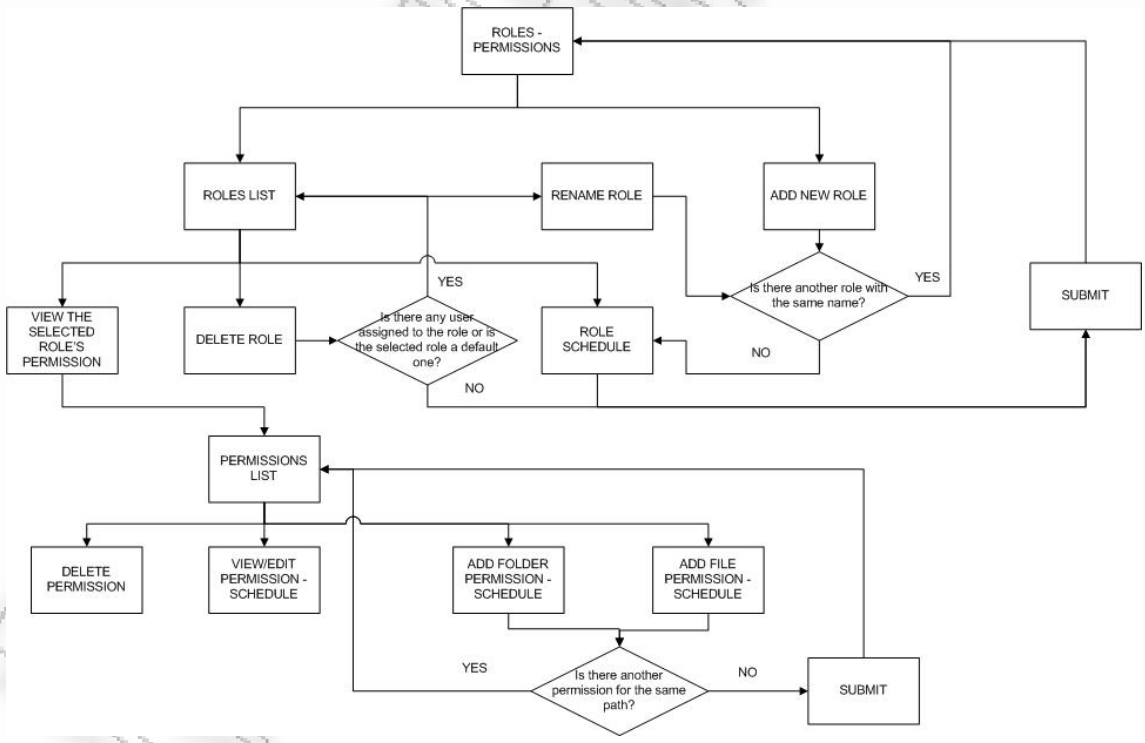


Οθόνη 14

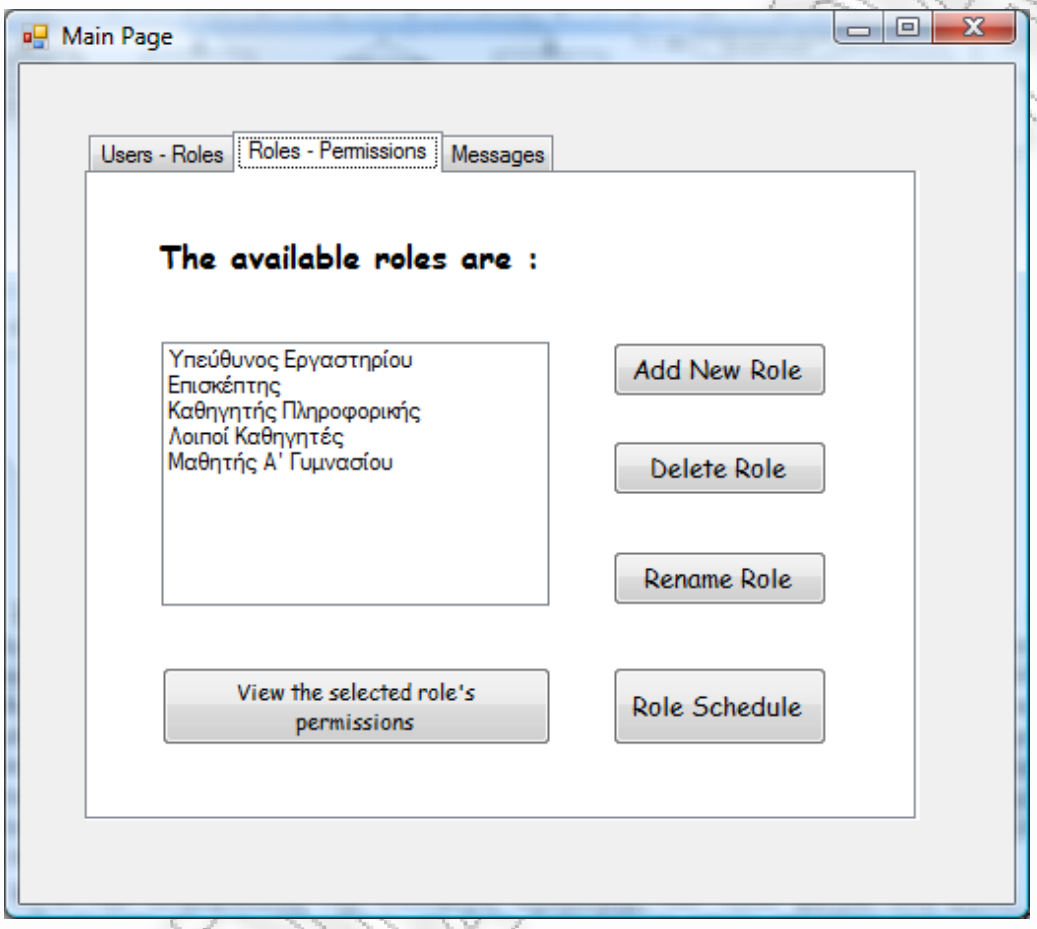
5.5.2. Καρτέλα Διαχείρισης Ρόλων

Το κομμάτι αυτό της εφαρμογής επικεντρώνεται στη διαχείριση των ρόλων που θα εφαρμοστούν τελικά στο σύστημά μας. Υλοποιείται, με λίγα λόγια, η βασική οντότητα του μοντέλου RBAC, που είναι ο ρόλος, αλλά και μία από τις βασικότερες συνιστώσες του, η ανάθεση δικαιωμάτων σε ρόλους. Για να πετύχουμε την ανάθεση αυτή, μέσω της συγκεκριμένης οθόνης μπορούμε να μεταβούμε στην αντίστοιχη καρτέλα για τη διαχείριση των δικαιωμάτων των ρόλων. Οι κυριότερες λειτουργίες που μπορούν να πραγματοποιηθούν μέσα από αυτή την καρτέλα παρουσιάζονται στην επόμενη εικόνα (Εικόνα 5.3).

Εικόνα 5.3: Λειτουργίες Καρτέλας Διαχείρισης Ρόλων



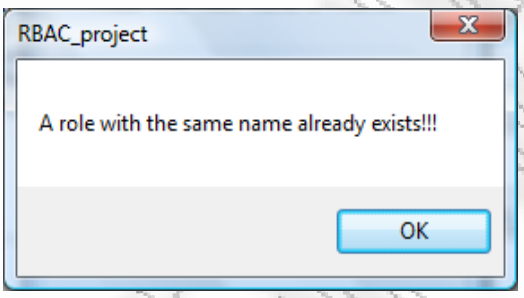
Στην καρτέλα Roles – Permissions εμφανίζεται η λίστα όλων των διαθέσιμων ρόλων (Οθόνη 15). Στην πραγματικότητα πρόκειται για τις εγγραφές του πίνακα TRoles της βάσης δεδομένων της εφαρμογής μας.



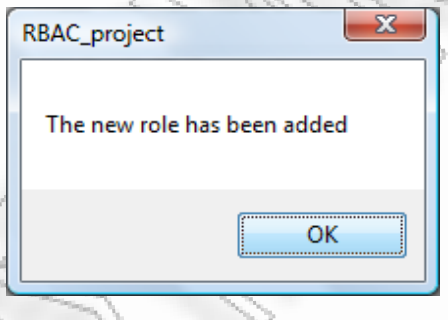
Οθόνη 15

Ο Υπεύθυνος Εργαστηρίου μπορεί να δημιουργήσει όσους και όποιους ρόλους επιθυμεί. Η διαδικασία είναι απλή. Με ένα κλικ στην επιλογή Add New Role εμφανίζεται ένα νέο παράθυρο όπου καλείται να δώσει το όνομα που επιθυμεί για το νέο ρόλο (Οθόνη 16). Ο μόνος περιορισμός που τίθεται σε αυτό το σημείο είναι να μη δοθεί όνομα το οποίο ήδη αντιστοιχεί σε κάποιον άλλο ρόλο. Ακόμη και σε περίπτωση που προσπαθήσει να εισάγει ήδη υπάρχοντα ρόλο, η εφαρμογή πραγματοποιεί έλεγχο ώστε να αποφευχθεί μία τέτοια ενέργεια εμφανίζοντάς του κατάλληλο μήνυμα προειδοποίησης (Οθόνη 17).

Οθόνη 16

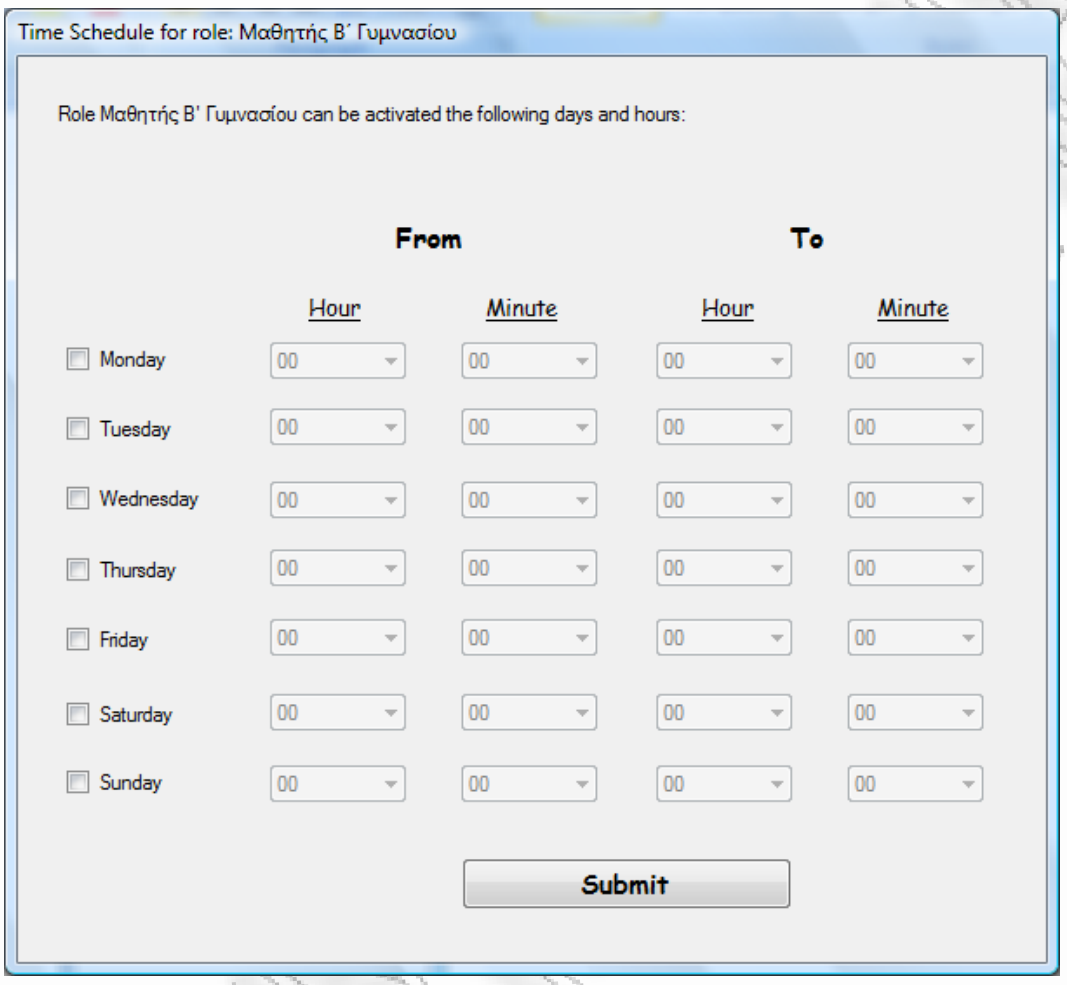


Οθόνη 17



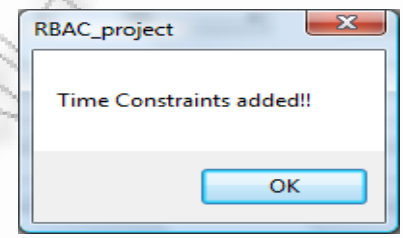
Οθόνη 18

Μετά την επιβεβαίωση της επιτυχούς εισαγωγής του νέου ρόλου στη βάση μας (Οθόνη 18), κατευθυνόμαστε σε μια νέα οθόνη, τη Role Schedule, η οποία επιτρέπει στον Υπεύθυνο Εργαστηρίου να εισάγει χρονικούς περιορισμούς στο νέο αυτό ρόλο. Η οθόνη αυτή λειτουργεί με τον ίδιο τρόπο που περιγράφηκε και προηγούμενα η οθόνη User Role Schedule για τον καθορισμό χρονικών περιορισμών σε συγκεκριμένο ρόλο συγκεκριμένου χρήστη. Εμφανίζει με τη μορφή κουμπιών επιλογής (checkboxes) τις ημέρες της εβδομάδας. Δίπλα σε κάθε ημέρα της εβδομάδας υπάρχουν τέσσερα πεδία στα οποία αποτυπώνονται τα χρονικά διαστήματα κατά τα οποία μπορεί να είναι ενεργός ο συγκεκριμένος ρόλος τη συγκεκριμένη ημέρα. Τα πεδία «Από» (From) και «Έως» (To), ενεργοποιούνται μόνο για τις ημέρες που είναι επιλεγμένες μέσω του συμβόλου √ . Σε διαφορετική περίπτωση παραμένουν απενεργοποιημένα (Οθόνη 19).



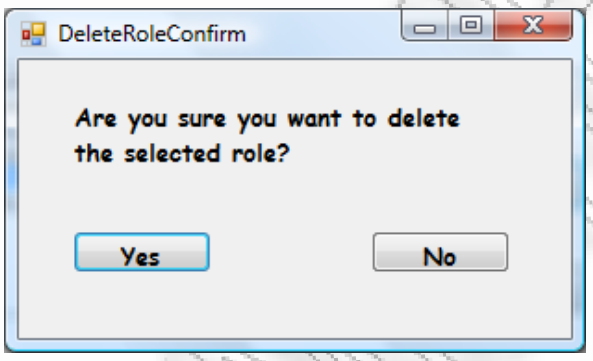
Οθόνη 19

Οι όποιες μεταβολές έχουν επέλθει στους χρονικούς περιορισμούς του ρόλου καταχωρούνται μέσω του πλήκτρου της υποβολής (Submit) οπότε και εμφανίζεται ενημερωτικό μήνυμα στον Υπεύθυνο Εργαστηρίου (Οθόνη 20). Τέλος, επιστρέφουμε στην καρτέλα των ρόλων όπου πλέον στη λίστα των ρόλων εμφανίζεται και ο νέος ρόλος που εισάγαμε.



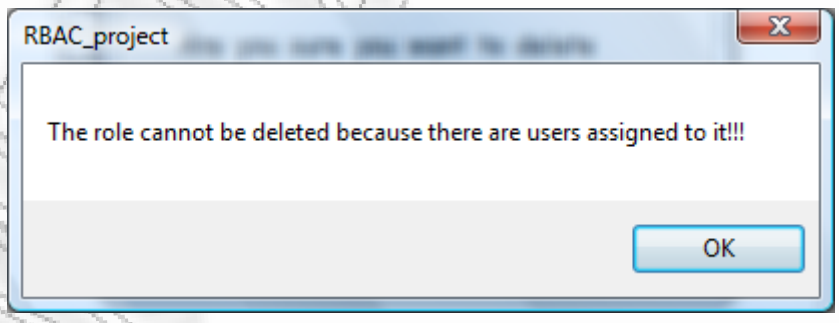
Οθόνη 20

Σε περίπτωση που θελήσει ο Υπεύθυνος Εργαστηρίου να διαγράψει έναν ρόλο, η εφαρμογή του δίνει τη δυνατότητα να το πραγματοποιήσει εύκολα με το αντίστοιχο πλήκτρο (Delete Role). Για να προχωρήσει στη διαγραφή θα πρέπει πρώτα να έχει επιλεγεί ένας ρόλος από τη λίστα. Εάν πατηθεί το πλήκτρο της διαγραφής χωρίς να έχει επιλεγεί κάποιος ρόλος από τη λίστα τότε εμφανίζεται κατάλληλο μήνυμα στον Υπεύθυνο Εργαστηρίου. Για λόγους διασφάλισης της ακεραιότητας και της εγκυρότητας των δεδομένων, που άλλωστε θα χρησιμοποιηθούν σε μετέπειτα βήματα για την εφαρμογή των δικαιωμάτων πρόσβασης, πραγματοποιείται έλεγχος πριν την πλήρη διαγραφή του ρόλου (Οθόνη 21).



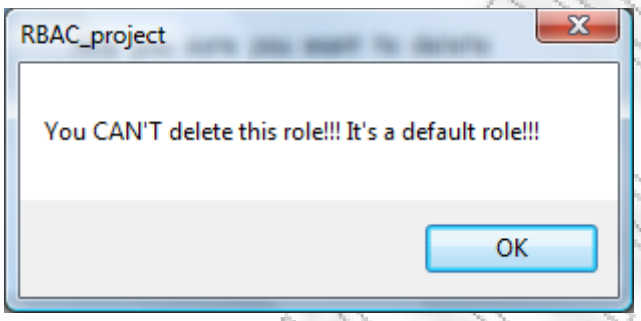
Οθόνη 21

Ο έλεγχος που λαμβάνει χώρα αφορά στο κατά πόσο ο ρόλος που έχει επιλέξει να διαγράψει ο Υπεύθυνος Εργαστηρίου έχει ανατεθεί σε κάποιον χρήστη. Εάν υπάρχει τουλάχιστον ένας χρήστης που έχει αυτό το ρόλο τότε η εφαρμογή δεν επιτρέπει τη διαγραφή του, ενημερώνοντάς τον με κατάλληλο μήνυμα (Οθόνη 22). Θα πρέπει να ανατρέξει στην καρτέλα διαχείρισης χρηστών, να εντοπίσει τους χρήστες που έχουν αυτό το ρόλο και να αναιρέσει την ανάθεσή του σε αυτούς. Τότε θα μπορεί να τον διαγράψει από τη βάση.



Οθόνη 22

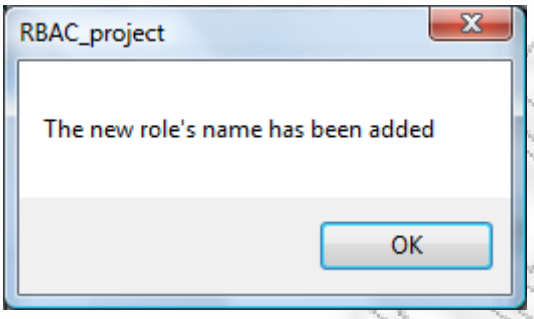
Αξίζει να σημειωθεί ότι η εφαρμογή διαθέτει δύο προκαθορισμένους ρόλους τους οποίους ο Υπεύθυνος Εργαστηρίου δεν μπορεί να διαγράψει, έστω και αν δεν είναι ανατεθειμένοι σε κάποιο χρήστη (Οθόνη 23). Αυτοί είναι οι ρόλοι του Επισκέπτη και του Υπεύθυνου Εργαστηρίου. Θεωρείται ότι τουλάχιστον ένας χρήστης θα έχει το ρόλο του Υπεύθυνου Εργαστηρίου, ενώ ο ρόλος του Επισκέπτη είναι ο ρόλος που ανατίθεται σε οποιονδήποτε άλλο χρήστη χρησιμοποιεί το Σύστημα και ο Υπεύθυνος δεν του έχει καθορίσει διαφορετική ανάθεση.



Οθόνη 23

Μία επιπλέον επιλογή που δίνεται είναι αυτή της μετονομασίας ενός ρόλου. Αφού ο Υπεύθυνος Εργαστηρίου επιλέξει έναν από τους διαθέσιμους στη λίστα, κάνει κλικ στο πλήκτρο Rename Role. Εμφανίζεται ένα παράθυρο παρόμοιο με αυτό της εισαγωγής νέου ρόλου και καλείται να δώσει το όνομα του νέου ρόλου (Οθόνη 24). Πατώντας το πλήκτρο της υποβολής (Submit New Role's Name) εμφανίζεται κατάλληλο μήνυμα που τον ενημερώνει για την ολοκλήρωση της ενέργειάς του (Οθόνη 25). Η δυνατότητα μετονομασίας παρέχεται για όλους τους ρόλους, ασχέτως την ανάθεσής τους σε χρήστες και άσχετα με το αν είναι προκαθορισμένοι ρόλοι. Στη συνέχεια επιστρέφει στην καρτέλα ελέγχου των ρόλων και ο ρόλος εμφανίζεται πλέον με το νέο όνομα που έδωσε.

Οθόνη 24



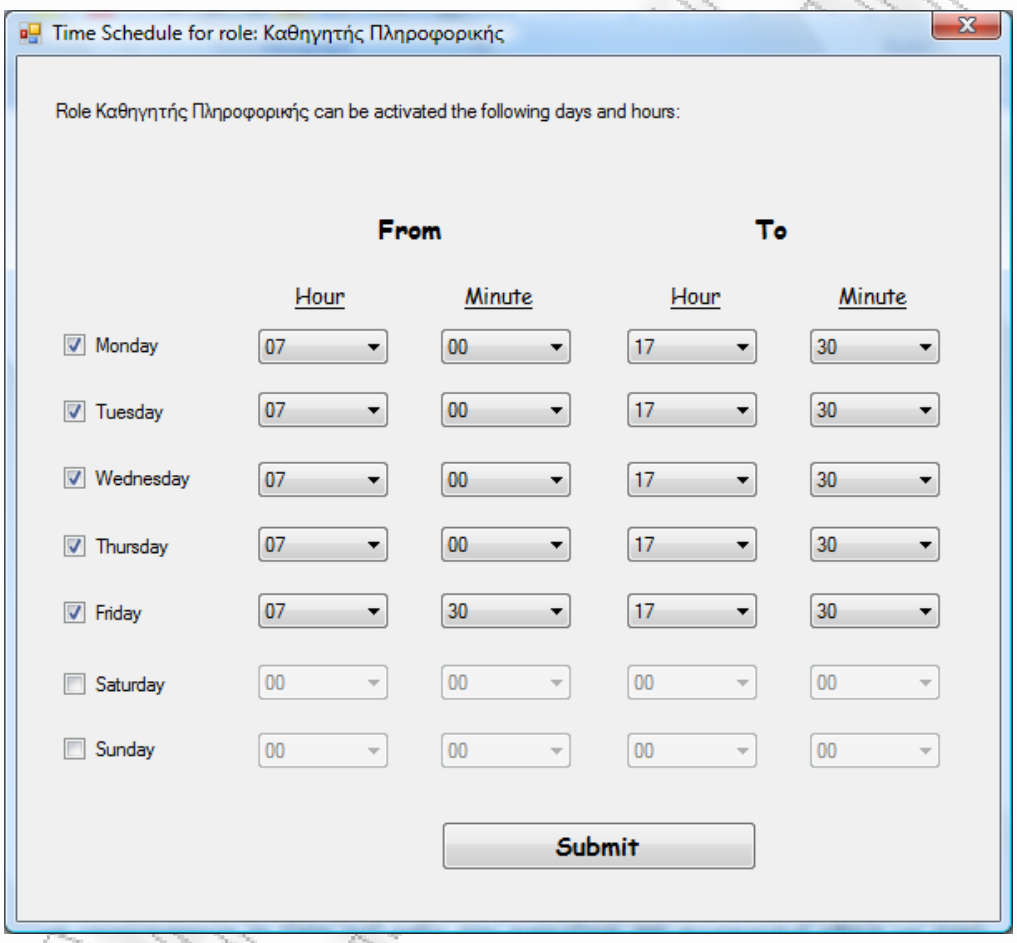
Οθόνη 25

Από τεχνικής άποψης, κατά της εισαγωγή νέου ρόλου δημιουργείται μία νέα εγγραφή στον πίνακα των ρόλων της βάσης μας (TRoles). Ο κωδικός του νέου ρόλου είναι ο επόμενος διαθέσιμος ακέραιος ενώ το όνομα του ρόλου είναι αυτό που πληκτρολόγησε ο Υπεύθυνος Εργαστηρίου. Παράλληλα, προστίθενται στον πίνακα TRoleSchedule νέες εγγραφές με τους χρονικούς περιορισμούς που έχουν οριστεί. Η εισαγωγή των χρονικών περιορισμών γίνεται με το πάτημα του πλήκτρου της υποβολής (submit) στην αντίστοιχη οθόνη, οπότε και προστίθενται στον πίνακα TRoleSchedule τόσες εγγραφές για το ρόλο όσες και οι ημέρες που αυτός ορίστηκε να μπορεί να ενεργοποιηθεί. Αντίστοιχα, στη μετονομασία του ρόλου, εντοπίζεται ο κωδικός του ρόλου που έχει αρχικά επιλέξει ο Υπεύθυνος Εργαστηρίου και στη συνέχεια γίνεται ενημέρωση της αντίστοιχης εγγραφής στο πεδίο που αντιστοιχεί στο όνομα του ρόλου.

Κατά τη διαγραφή του ρόλου, και δεδομένου ότι ικανοποιείται η συνθήκη της μη-ανάθεσής του σε κάποιο χρήστη, διαγράφονται: η εγγραφή που αφορά τον ρόλο από τον πίνακα TRoles, όλες οι εγγραφές που αφορούν το συγκεκριμένο ρόλο από τον πίνακα TRoleSchedule καθώς και όσες εγγραφές αφορούν το συγκεκριμένο κωδικό ρόλου στον πίνακα δικαιωμάτων των ρόλων (TRolePerm). Φροντίζουμε, δηλαδή, να «καθαρίσουμε» τη βάση μας από τα δικαιώματα πρόσβασης και τους χρονικούς περιορισμούς που είχαν ανατεθεί στο ρόλο αυτό.

Όπως αναλυτικά έχουμε αναφέρει, η κυριότερη συνιστώσα του μοντέλο TRBAC αφορά την εισαγωγή χρονικών περιορισμών στην ενεργοποίηση και απενεργοποίηση ενός ρόλου. Η λειτουργικότητα αυτή προσφέρεται στην εφαρμογή μας μέσω του πλήκτρου Role Schedule. Έχοντας ο Υπεύθυνος Εργαστηρίου επιλέξει έναν ρόλο από τη λίστα των ρόλων και πατώντας το πλήκτρο Role Schedule, οδηγείται στην οθόνη Role Schedule μέσω της οποίας γίνεται ο καθορισμός του χρονοπρογραμματισμού για το συγκεκριμένο ρόλο, οθόνη στην οποία οδηγούμαστε και κατά την προσθήκη νέου ρόλου. Η οθόνη αυτή λειτουργεί με τον ίδιο τρόπο που περιγράφηκε στην προσθήκη νέου ρόλου. Στο φόρτωμά της οθόνης αυτής, τόσο τα checkboxes που αφορούν τις μέρες τις εβδομάδας όσο και τα πεδία «Από» (From) και «Έως» (To), είναι συμπληρωμένα με τις ημέρες και με τα χρονικά διάστημα ενεργοποίησης του επιλεγμένου ρόλου, αντλώντας τις τιμές από τα αντίστοιχα πεδία του πίνακα TRoleSchedule της βάσης δεδομένων. Δηλαδή, τα πεδία αυτά είναι συμπληρωμένα με τις ημέρες και ώρες που μπορεί να ενεργοποιηθεί ο συγκεκριμένος ρόλος όπως έχει καθορίσει ο Υπεύθυνος Εργαστηρίου είτε κατά τη δημιουργία του ρόλου είτε σε επόμενη επέμβασή του (Οθόνη 26). Οι όποιες μεταβολές έχουν επέλθει στους χρονικούς περιορισμούς του ρόλου καταχωρούνται μέσω του πλήκτρου της υποβολής (Submit) οπότε και εμφανίζεται ενημερωτικό μήνυμα στον Υπεύθυνο Εργαστηρίου. Ειδικότερα, διαγράφονται από τον πίνακα TRoleSchedule όλες εγγραφές που αφορούν το συγκεκριμένο ρόλο και στη συνέχεια προστίθενται στον ίδιο πίνακα

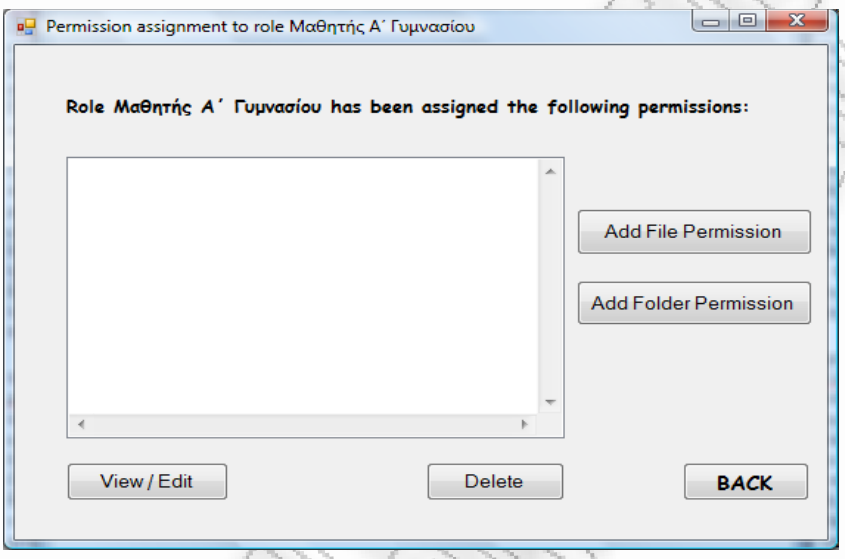
νέες εγγραφές με τους νέους χρονικούς περιορισμούς που έχουν οριστεί. Για τη συνέπεια των δεδομένων μας, οι όποιες αλλαγές γίνουν στους χρονικούς περιορισμούς ενός ρόλου θα πρέπει να πραγματοποιηθούν και στον πίνακα RUserRole ο οποίος κρατάει ξεχωριστή εγγραφή για κάθε τριάδα χρήστη, ρόλου, ημέρα εβδομάδας. Γι' αυτό το λόγο, πραγματοποιείται επιπλέον η διαγραφή από τον πίνακα RUserRole όλων των εγγραφών που αφορούν τον επιλεγμένο ρόλο του συγκεκριμένου χρήστη και τέλος προσθήκη νέων εγγραφών με βάση τους νέους χρονικούς περιορισμούς που ήδη έχουν αποθηκευτεί στον πίνακα TRoleScedule.



Οθόνη 26

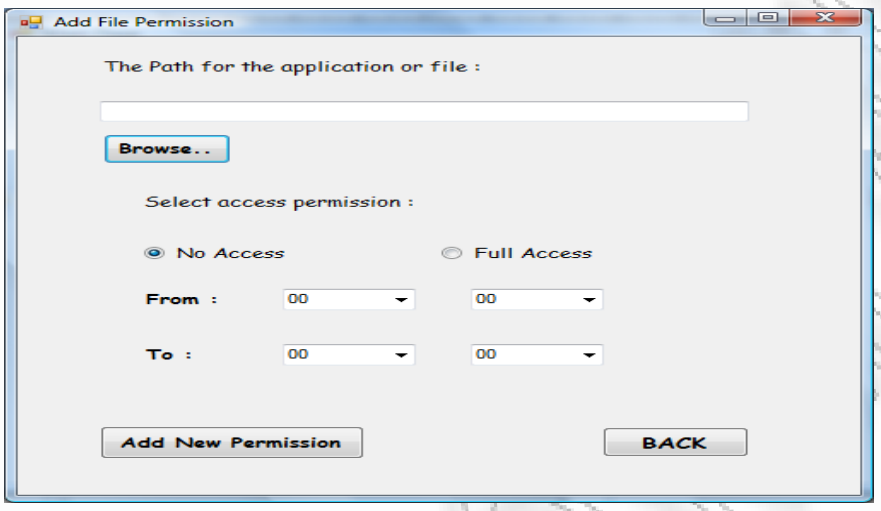
Η τελευταία λειτουργικότητα της καρτέλας αυτής προσφέρεται μέσα από το πλήκτρο προβολής των δικαιωμάτων του επιλεγμένου από τη λίστα ρόλου (View the selected role's permissions). Πατώντας το πλήκτρο αυτό ο Υπεύθυνο Εργαστηρίου οδηγείται σε μία νέα οθόνη που αφορά την ανάθεση δικαιωμάτων (Permission Assignment to role) (Οθόνη 27). Στη νέα λίστα που εμφανίζεται μπορεί να δει όλα τα μονοπάτια (Paths) που αφορούν τους φακέλους και τα αρχεία ή εφαρμογές για τα οποία έχουν οριστεί τα δικαιώματα πρόσβασης για το συγκεκριμένο ρόλο. Θα πρέπει να τονίσουμε στο σημείο αυτό ότι η εφαρμογή μας κατά κύριο

λόγο δίνει τη δυνατότητα καθορισμού μη πρόσβασης σε συγκεκριμένα μονοπάτια. Θα μπορούσαμε, δηλαδή, να χαρακτηρίσουμε τη λίστα των paths που εμφανίζεται στη συγκεκριμένη οθόνη ως λίστα απαγόρευσης (black list). Αυτό όμως δεν αποκλείει το γεγονός ο Υπεύθυνος Εργαστηρίου να μπορεί να καθορίσει πλήρη πρόσβαση για κάποιο αρχείο ή φάκελο της επιλογής του που να αφορά το συγκεκριμένο ρόλο.



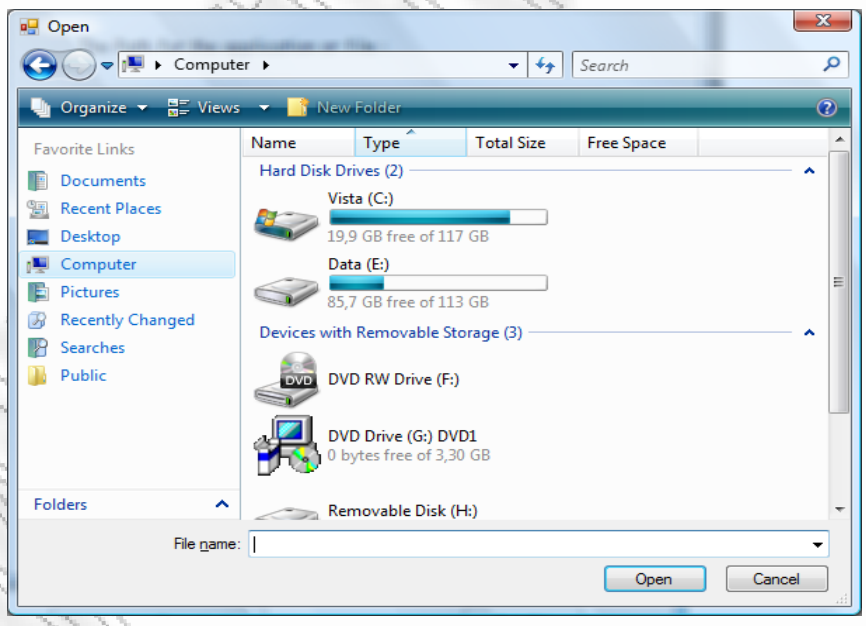
Οθόνη 27

Προκειμένου να προσθέσει ένα νέο περιορισμό στο ρόλο που επέλεξε, ο Υπεύθυνος Εργαστηρίου έχει δύο επιλογές. Μπορεί είτε να επιλέξει την προσθήκη δικαιώματος που αφορά φάκελο είτε να επιλέξει την προσθήκη δικαιώματος που αφορά αρχείο / εφαρμογή. Η εφαρμογή μας διαθέτει δύο διαφορετικά πλήκτρα για κάθε μία από τις επιλογές αυτές : Add File Permission και Add Folder Permission. Και στις δύο περιπτώσεις οδηγούμαστε σε μία νέα οθόνη ίδιων χαρακτηριστικών (Οθόνη 28).



Οθόνη 28

Το νέο παράθυρο που ανοίγεται οδηγεί στο να καθορίσει ο Υπεύθυνος Εργαστηρίου το επιθυμητό μονοπάτι προς το αρχείο ή το φάκελο για τον οποίο θέλει να καθορίσει δικαίωμα πρόσβασης. Μπορεί είτε να πληκτρολογήσει το μονοπάτι είτε να επιλέξει με τη βοήθεια του αντίστοιχου πλήκτρου (Browse) μέσα από παράθυρο αναζήτησης το φάκελο ή το αρχείο που επιθυμεί (Οθόνη 29). Εδώ έγκειται και η διαφορά μεταξύ του Add File Permission και του Add Folder Permission. Ανάλογα με το τι έχει επιλέξει ανοίγει και το αντίστοιχο παράθυρο αναζήτησης.

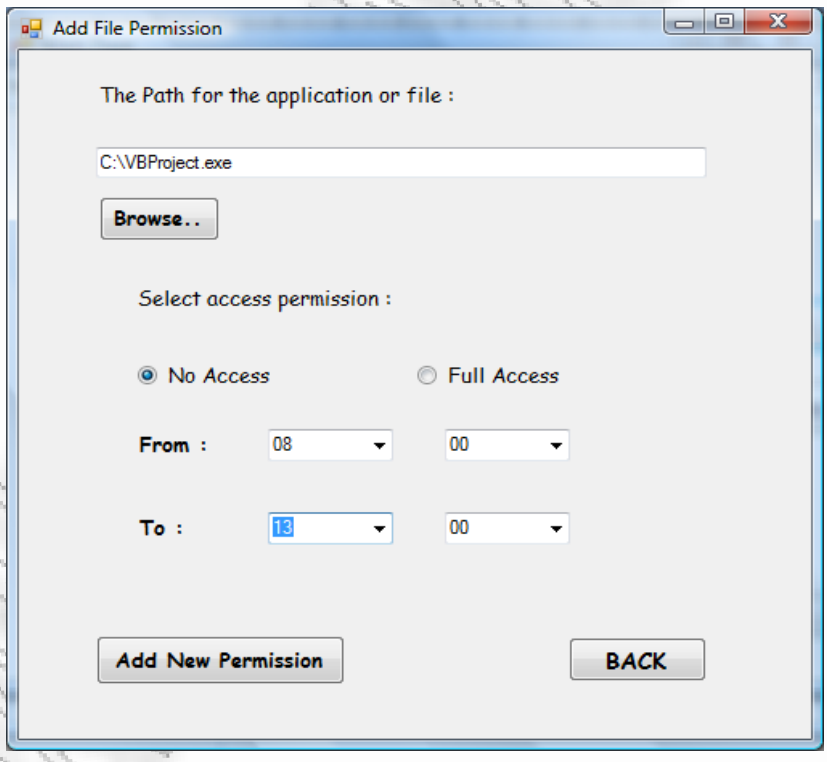


Οθόνη 29

Στη συνέχεια καθορίζει το αν θέλει να έχει πρόσβαση ο ρόλος ή όχι. Υπενθυμίζουμε ότι η λογική είναι να αφαιρούμε δικαιώματα πρόσβασης γι' αυτό και η προκαθορισμένη επιλογή είναι αυτή της μη-πρόσβασης (No Access) (Οθόνη 30). Παρόλα αυτά δίνουμε τη δυνατότητα να προστεθεί δικαίωμα πλήρους πρόσβασης (Full Access) σε περίπτωση που θέλει ο Υπεύθυνος Εργαστηρίου να εξασφαλίσει ότι ο επιλεγμένος ρόλος θα έχει το δικαίωμα αυτό.

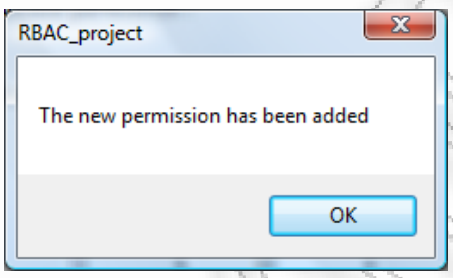
Για την περίπτωση της μη πρόσβασης του δίνεται επιπλέον η επιλογή του χρονοπρογραμματισμού του δικαιώματος. Εάν θέλει το δικαίωμα για το ρόλο αυτό να ισχύει συγκεκριμένες ώρες μπορεί να το ρυθμίσει από τις αντίστοιχες λίστες επιλογής που παρέχονται. Εάν θέλει απλά να δώσει το δικαίωμα χωρίς χρονικό περιορισμό τότε ή αφήνει την προκαθορισμένη επιλογή (00:00 – 00:00) ή θα πρέπει να φροντίσει το «Από» (From) και το «Έως» (To) να είναι η ίδια ώρα ώστε να καλύπτεται όλο το εικοσιτετράωρο.

Θα πρέπει να σημειώσουμε εδώ ότι ο χρονοπρογραμματισμός των δικαιωμάτων πρόσβασης βρίσκεται ένα επίπεδο κάτω από το χρονοπρογραμματισμό των ρόλων. Αυτό σημαίνει ότι προηγείται η ενεργοποίηση του ρόλου και εάν αυτός είναι ενεργός τη δεδομένη χρονική στιγμή τότε ελέγχεται ο χρονικός περιορισμός των δικαιωμάτων του. Με άλλα λόγια αν για έναν ρόλο έχουμε θέσει ως διάστημα ενεργοποίησης τις ώρες 8:00-14:00, ενώ για ένα από τα δικαιώματά του έχει δοθεί μη πρόσβαση 15:00-18:00, είναι προφανές ότι ο περιορισμός αυτός δε θα γίνει ποτέ ορατός στους χρήστες στους οποίους έχει ανατεθεί ο ρόλος αυτός. Τις ώρες αυτές (15:00-18:00) ο ρόλος είναι ανενεργός οπότε δεν εφαρμόζονται τα δικαιώματά του.

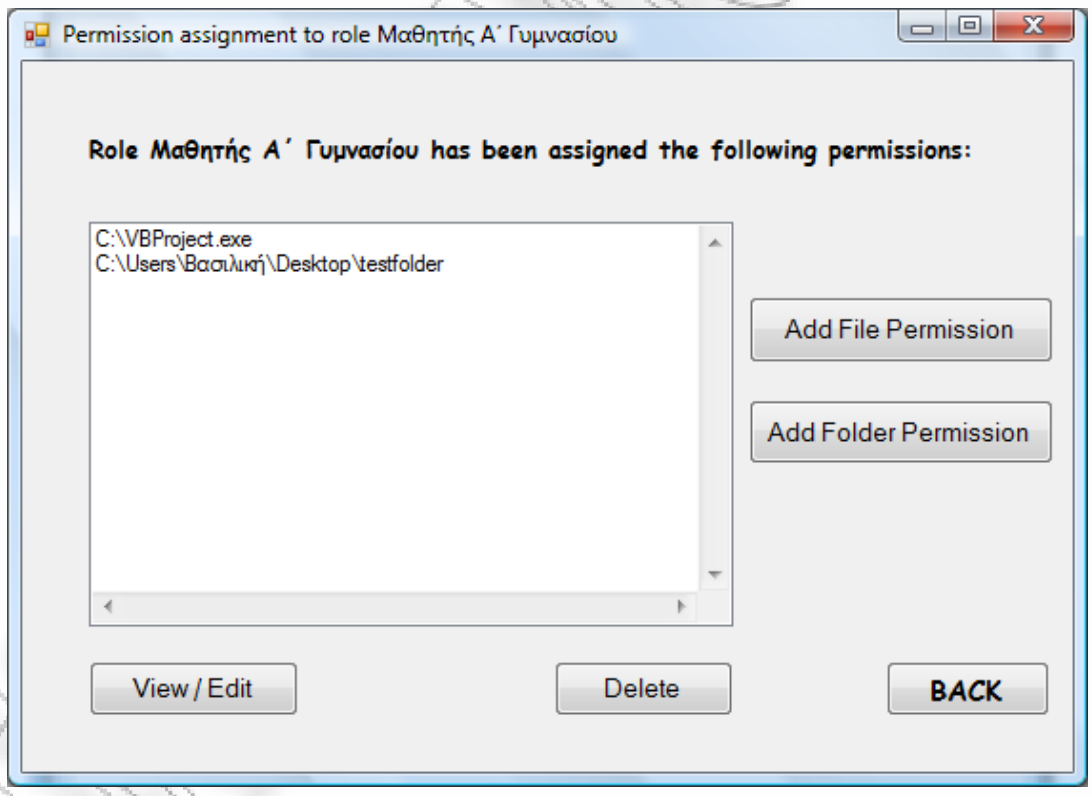


Οθόνη 30

Επιστρέφοντας στην εφαρμογή μας, μετά τον καθορισμό του μονοπατιού και του χρονικού περιορισμού ο Υπεύθυνος Εργαστηρίου μπορεί να ολοκληρώσει την ενέργειά του επιλέγοντας το πλήκτρο Add New Permission (Οθόνη 31) ή αν άλλαξε γνώμη μπορεί να επιστρέψει στην προηγούμενη οθόνη (πλήκτρο Back). Πριν την τελική εισαγωγή του δικαιώματος γίνεται έλεγχος για το αν έχει καθοριστεί για τον επιλεγμένο ρόλο κάποιο άλλο δικαίωμα που να αφορά το ίδιο μονοπάτι. Σε περίπτωση που συμβαίνει κάτι τέτοιο ο Υπεύθυνος Εργαστηρίου ενημερώνεται με το αντίστοιχο μήνυμα και η εισαγωγή δεν πραγματοποιείται.



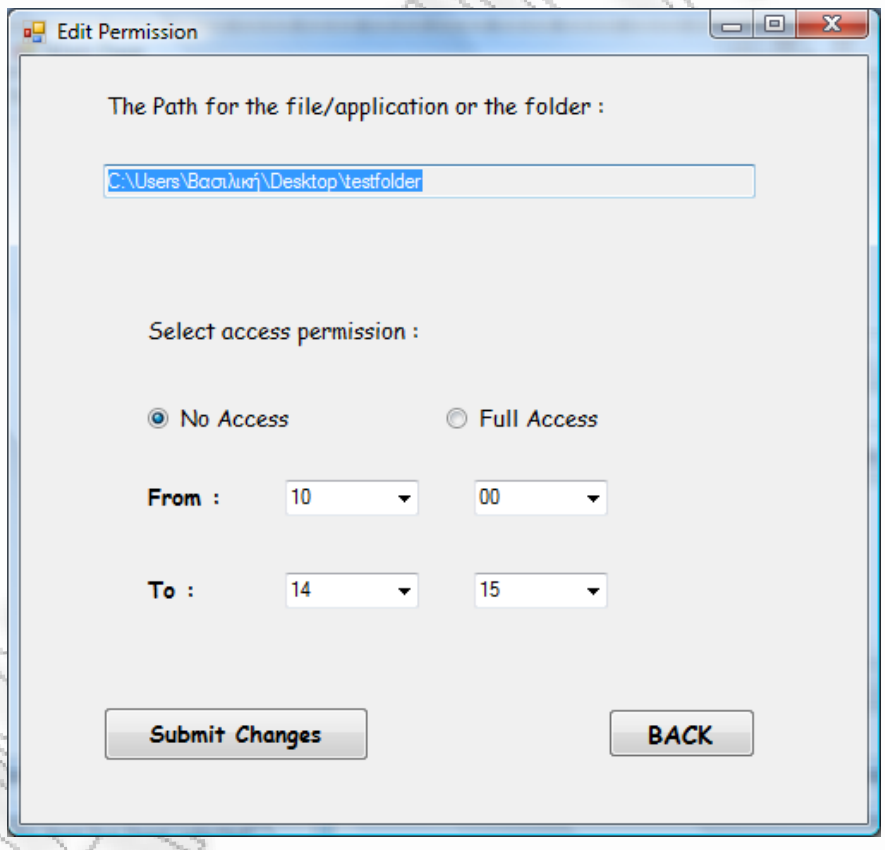
Οθόνη 31



Οθόνη 32

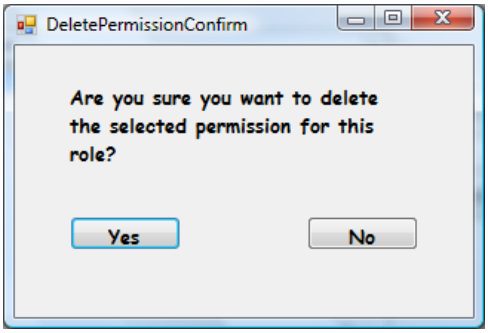
Η καταχώρηση νέου δικαιώματος, από την πλευρά της βάσης μας, σημαίνει την προσθήκη νέας εγγραφής στον πίνακα TRolePerm. Η εγγραφή συμπληρώνεται με τον κωδικό του επιλεγμένου ρόλου ενώ τα υπόλοιπα πεδία γεμίζουν με τις τιμές που συμπληρώθηκαν στο παράθυρο εισαγωγής νέου δικαιώματος (μονοπάτι, τύπος πρόσβασης, χρονικοί περιορισμοί). Τόσο τα δικαιώματα που αφορούν φακέλους όσο και τα δικαιώματα που αφορούν αρχεία και εφαρμογές, αποθηκεύονται στον ίδιο πίνακα. Παρόλα αυτά εισάγεται κατάλληλη ένδειξη για το τι από τα δύο αφορά το εκάστοτε δικαίωμα (1 για αρχεία και 2 για φακέλους).

Εκτός από την προσθήκη νέου δικαιώματος ο Υπεύθυνος Εργαστηρίου μπορεί να δει και να επεξεργαστεί τα ήδη αποθηκευμένα δικαιώματα του ρόλου. Με το πάτημα του πλήκτρου View / Edit, και αφού έχει επιλεγεί κάποιο μονοπάτι από τη λίστα, οδηγείται σε νέο παράθυρο παρόμοιο με αυτό της εισαγωγής νέου δικαιώματος (Οθόνη 33). Η διαφορά είναι ότι το μονοπάτι σε αυτή την οθόνη είναι αυτό που επέλεξε από τη λίστα και τα μόνα πεδία προς επεξεργασία είναι αυτά του τύπου πρόσβασης και των χρονικών περιορισμών. Αφού κάνει τις όποιες αλλαγές επιθυμεί στις ήδη αποθηκευμένες πληροφορίες που εμφανίζονται, τις καταχωρεί και η αντίστοιχη εγγραφή στη βάση επικαιροποιείται. Και σε αυτή την οθόνη υπάρχει η επιλογή επιστροφής στην προηγούμενη χωρίς να αποθηκευτεί η όποια αλλαγή έχει συμβεί.

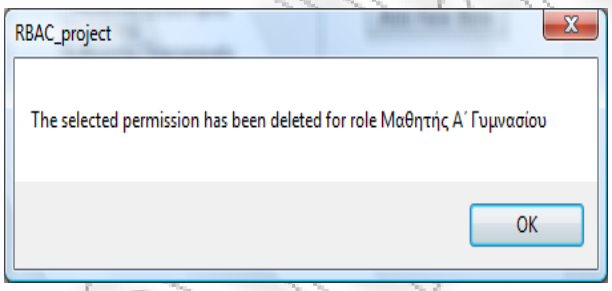


Οθόνη 33

Τέλος, ο Υπεύθυνος Εργαστηρίου μπορεί να διαγράψει όποιο από τα δικαιώματα επιθυμεί. Αφού το επιλέξει από τη λίστα, πατάει το πλήκτρο της διαγραφής (Delete) και αφού επιβεβαιώσει την ενέργειά του (Οθόνη 34) η εγγραφή που αντιστοιχεί στο επιλεγμένο μονοπάτι, για το ρόλο του οποίου τα δικαιώματα επεξεργάζεται, διαγράφεται από τη βάση (από τον πίνακα TRolePerm) (Οθόνη 35).



Οθόνη 34

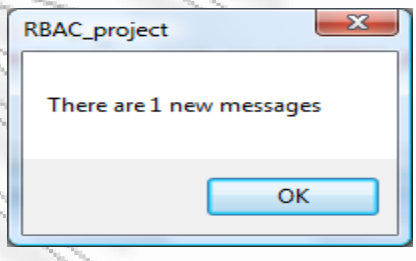


Οθόνη 35

Μόλις τελειώσει με την ανάθεση των δικαιωμάτων μπορεί να επιστρέψει στην καρτέλα Roles – Permissions.

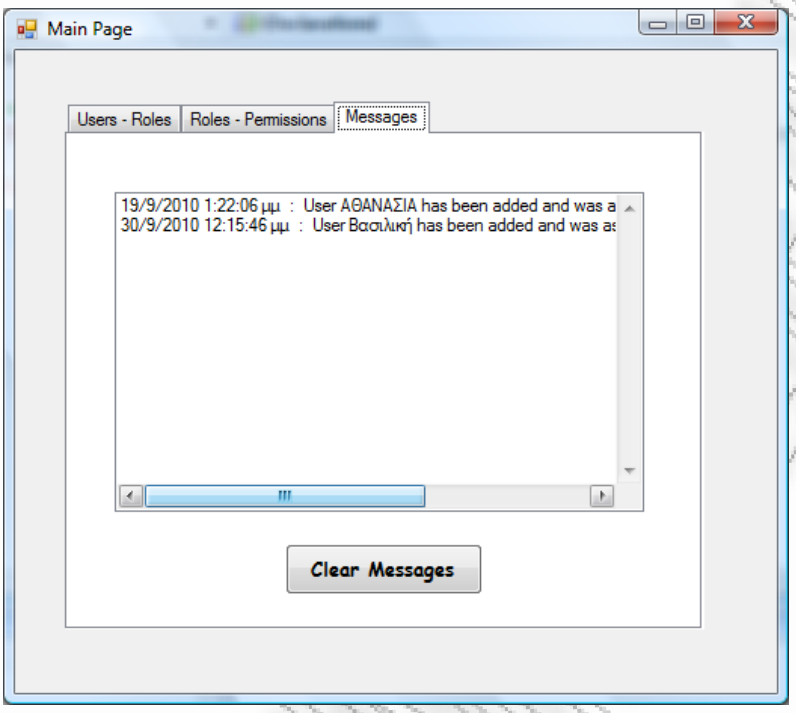
5.5.3. Καρτέλα Μηνυμάτων

Κατά την εκκίνηση της εφαρμογής μας μπορεί να εμφανιστεί ειδοποίηση για την ύπαρξη νέων μηνυμάτων (Οθόνη 36).



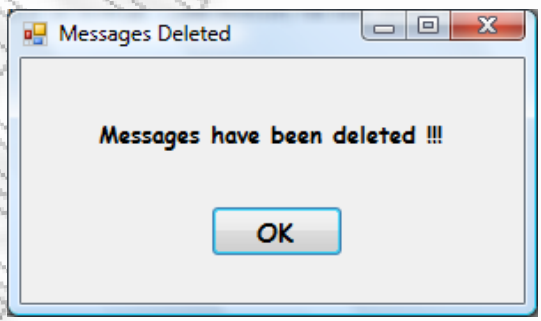
Οθόνη 36

Για να δει ο Υπεύθυνος Εργαστηρίου τα νέα αυτά μηνύματα πρέπει να μεταβεί στην καρτέλα Messages. Στην καρτέλα αυτή εμφανίζονται με χρονολογική σειρά όλα τα μηνύματα που έχουν αποθηκευτεί στη βάση προς ενημέρωσή του (Οθόνη 37). Όταν ο Υπεύθυνος Εργαστηρίου μεταβεί σε αυτή την καρτέλα, όλα τα νέα μηνύματα θεωρούνται πλέον αναγνωσμένα.



Οθόνη 37

Τεχνικά αυτό επιτυγχάνεται με την ύπαρξη κατάλληλης ένδειξης στη βάση δεδομένων η οποία μεταβάλλεται κατά τη μετάβαση στην καρτέλα των μηνυμάτων (πεδίο StatusFlg). Τα μηνύματα είναι ταξινομημένα από το παλαιότερο προς το πιο πρόσφατο, ενώ στην αρχή κάθε μηνύματος αναγράφεται η ημερομηνία και η ώρα που αυτό προστέθηκε στη βάση. Η εισαγωγή νέων μηνυμάτων στον πίνακα γίνεται μέσω της δεύτερου μέρους της εφαρμογής μας, και το οποίο εφαρμόζει τελικά τα δικαιώματα στο σύστημα και περιγράφεται αναλυτικά παρακάτω (RBACStartUp). Παρέχεται επίσης δυνατότητα διαγραφής των μηνυμάτων εφόσον ο Υπεύθυνος Εργαστηρίου το επιθυμεί. Με την επιλογή Clear Messages όλα τα μηνύματα στον πίνακα TMessages της βάσης δεδομένων, και τα οποία έχουν αναγνωσθεί, διαγράφονται (Οθόνη 38).



Οθόνη 38

Με την καρτέλα Μηνυμάτων ολοκληρώνεται η περιγραφή της λειτουργικότητας του RBACProject. Για τη συνολική εικόνα της λειτουργικότητας της Εφαρμογής μας θα πρέπει να αναλυθεί και το κομμάτι της RBACStartUp εφαρμογής, και η οποία ακολουθεί στην επόμενη ενότητα.

5.6. Εφαρμογή Υλοποίησης Δικαιωμάτων (RBACStartUp)

Η εφαρμογή του Υπεύθυνου Εργαστηρίου που περιγράφηκε παραπάνω, διαμορφώνει τη βάση δεδομένων που θα αποτελέσει την πηγή από την οποία θα αντλήσουμε την πληροφορία που χρειάζεται για την εφαρμογή των δικαιωμάτων πρόσβασης. Οι χρήστες, οι ρόλοι που τους έχουν ανατεθεί, τα δικαιώματα πρόσβασης και οι χρονικοί περιορισμοί που τα αφορούν, πρέπει να μετατραπούν από στατικά δεδομένα της βάσης σε δυναμικούς περιορισμούς του συστήματος. Η μετατροπή αυτή θα επιτευχθεί μέσω μιας νέας εφαρμογής που θα προσδώσει τελικά την επιθυμητή λειτουργικότητα (RBACStartUp).

Στόχος είναι να γίνεται εκκίνηση της εφαρμογής αυτής κάθε φορά που κάποιος χρήστης εισέρχεται στο λογαριασμό του στα Windows. Προκειμένου να επιτευχθεί αυτό, το αρχείο εγκατάστασης της εφαρμογής καθορίζει την αντίστοιχη παράμετρο ώστε να ξεκινάει η εφαρμογή τη στιγμή που γίνεται η είσοδος του χρήστη.

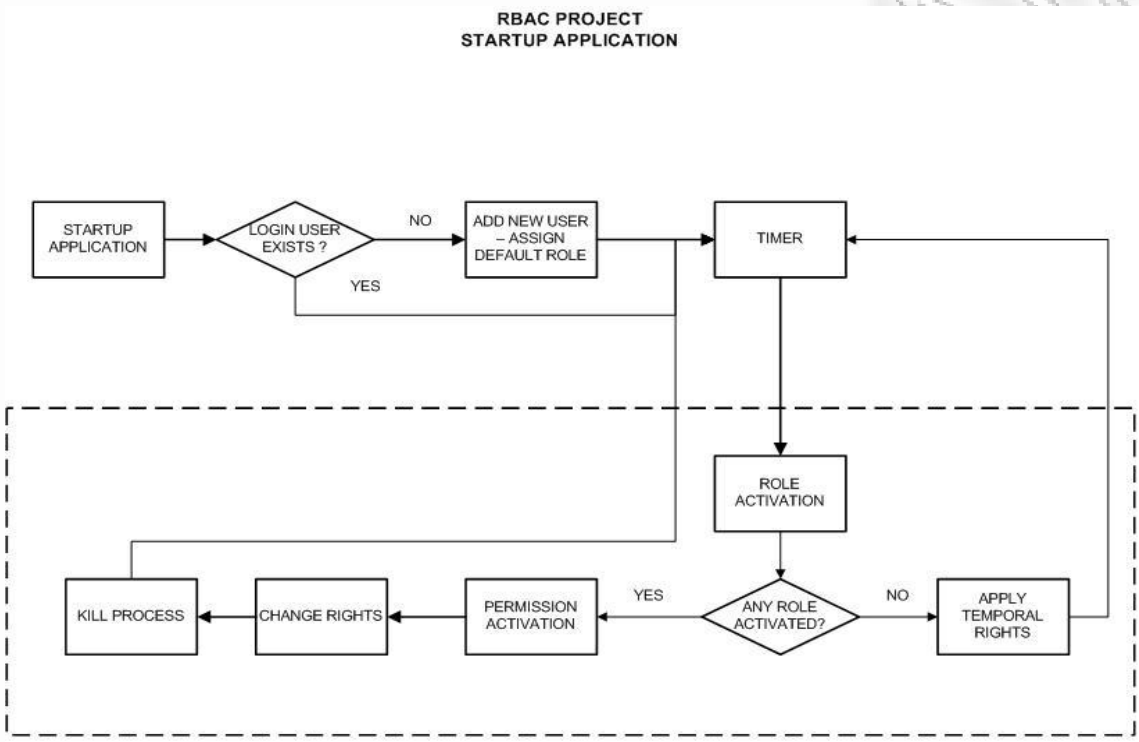
Επόμενη απαίτηση είναι η εφαρμογή να είναι μη εμφανής στο χρήστη έτσι ώστε αυτός να μην μπορεί να παρέμβει στην ορθή λειτουργία της. Κατά ένα μέρος αυτό επιτυγχάνεται με την απόκρυψη της κύριας φόρμας από τη γραμμή εργασιών (καθορισμός της αντίστοιχης ιδιότητας από το Visual Studio), επιτρέποντας της όμως να λειτουργεί στο παρασκήνιο. Προκείμενου να εξασφαλιστεί ότι ο χρήστης δε θα μπορεί να τερματίσει την εφαρμογή RBACStartUp από το Παράθυρο Διαχείρισης Εργασιών των Windows (Task Manager), η δυνατότητα πρόσβασης στο Παράθυρο αυτό απενεργοποιείται για τους χρήστες στους οποίους δεν είναι ενεργός ο ρόλος του Υπεύθυνου Εργαστηρίου την εκάστοτε χρονική στιγμή.

Το σύνολο του κώδικα που αφορά την εφαρμογή αυτή έχει γραφτεί στην κλάση της κεντρικής φόρμας και δομείται ως εξής:

- Υποκλάση Load
- Υποκλάση Timer
- Συνάρτηση CurrentUser
- Συνάρτηση RoleActivation
- Συνάρτηση SecureMyApplication
- Συνάρτηση Permission Activation
- Συνάρτηση ChangeRights
- Συνάρτηση KillProcess
- Συνάρτηση ApplyTemporalRights

Καθεμία από τις παραπάνω ενότητες του κώδικα περιγράφεται αναλυτικά στη συνέχεια, ενώ η γενική δομή της απεικονίζεται στην παρακάτω εικόνα (Εικόνα 5.4).

Εικόνα 5.4: Δομή Εφαρμογής Υλοποίησης Δικαιωμάτων (RBACStartUp)



Υποκλάση Load

Περιέχει τον κώδικα που εκτελείται κατά την εκκίνηση της φόρμας και κατά συνέπεια της εφαρμογής. Η βασική της λειτουργία έγκειται στην ανάκτηση του ονόματος του χρήστη (username), με τη βοήθεια της συνάρτησης CurrentUser, και στον έλεγχο του αν αυτό βρίσκεται ήδη στη βάση δεδομένων (πίνακας TUsers). Εάν το όνομα του χρήστη δεν εντοπιστεί στις εγγραφές του πίνακα χρηστών, τότε συμπεραίνουμε ότι πρόκειται για καινούριο χρήστη των Windows. Σε αυτή την περίπτωση γίνεται αυτόματα εισαγωγή του ονόματός του στη βάση. Συγκεκριμένα, στη νέα εγγραφή ορίζεται ως κωδικός χρήστη (UserId) ο αμέσως επόμενος διαθέσιμος αριθμός, ως UserName το όνομα χρήστη όπως επιστρέφεται από την CurrentUser ενώ τέλος γίνεται και ανάθεση προκαθορισμένου ρόλου. Με τον τρόπο αυτό ικανοποιείται η βασική ιδιότητα του μοντέλου RBAC, σύμφωνα με την οποία σε κάθε χρήστη πρέπει να έχει ανατεθεί τουλάχιστον ένας ρόλος.

Ειδικότερα, εάν ο πίνακας TUsers της βάσης είναι κενός τότε δίνεται στο χρήστη ο προκαθορισμένος ρόλος του Υπεύθυνου Εργαστηρίου. Εάν ο πίνακας TUsers της βάσης είναι κενός, θεωρούμε ότι ο πρώτος χρήστης για τον οποίο θα τρέξει η εφαρμογή StartUp είναι ο Υπεύθυνος Εργαστηρίου και γι αυτό του ανατίθεται ο ρόλος αυτό. Σε αντίθετη περίπτωση, στο νέο χρήστη ανατίθεται ο ρόλος του Επισκέπτη με τα προκαθορισμένα από τον Υπεύθυνο Εργαστηρίου δικαιώματα πρόσβασης. Η ανάθεση του προκαθορισμένου ρόλου στο χρήστη επιτυγχάνεται μέσω της εισαγωγής στον πίνακα RUserRole επτά εγγραφών, μία για κάθε μέρα της εβδομάδας. Κάθε μια από τις εγγραφές αυτές ορίζει ότι ο προκαθορισμένος αυτός ρόλος

του χρήστη μπορεί να ενεργοποιηθεί όλο το εικοσιτετράωρο. Τέλος, εισάγεται μία νέα εγγραφή στον πίνακα των μηνυμάτων (TMessages) και η οποία θα ενημερώσει τον Υπεύθυνο Εργαστηρίου για την εισαγωγή του νέου χρήστη την επόμενη φορά που θα ανοίξει την εφαρμογή RBACProject. Ο κώδικας συνεχίζει με την υποκλάση Timer.

Υποκλάση Timer

Αποτελεί το σημαντικότερο χαρακτηριστικό της εφαρμογής RBACStartUp αφού μέσω αυτής επιτυγχάνεται η εφαρμογή των χρονικών περιορισμών τόσο στην ανάθεση των ρόλων στο συνδεδεμένο χρήστη όσο και στην εφαρμογή των δικαιωμάτων πρόσβασης των εκάστοτε ενεργών ρόλων του χρήστη. Η λειτουργία του Timer είναι να εκτελεί τον κώδικα που περιλαμβάνεται στην υποκλάση του ανά τακτά χρονικά διαστήματα. Το διάστημα που μεσολαβεί μεταξύ των διαδοχικών κλήσεων του Timer έχει οριστεί στα 10 δευτερόλεπτα Θεωρείται ότι το μεσοδιάστημα αυτό είναι αρκετά ικανοποιητικό έτσι ώστε να εξασφαλιστεί ότι ο χρήστης έχει τα σωστά δικαιώματα (όπως τα έχει ορίσει ο Υπεύθυνος Εργαστηρίου) ανά πάσα χρονική στιγμή ακόμα και σε περίπτωση μεταβολής είτε των ενεργών ρόλων είτε των ενεργών δικαιωμάτων εξαιτίας των χρονικών περιορισμών.

Η υποκλάση του Timer καλεί κατά περίπτωση κάποιες συναρτήσεις και υλοποιεί την παρακάτω λογική:

- Βήμα 1

  Ενεργοποίηση εκείνων των ρόλων του χρήστη που καλύπτουν τους χρονικούς περιορισμούς της δεδομένης χρονικής στιγμής.

- Βήμα 2

  Έλεγχος για τον αν τη δεδομένη χρονική στιγμή υπάρχουν ενεργοί ρόλοι για το συγκεκριμένο χρήστη. Ανάλογα με την ύπαρξη ή όχι ενεργών ρόλων διακρίνονται δύο περιπτώσεις:
  - Περίπτωση 1: Αν δεν υπάρχουν ενεργοί ρόλοι για το συγκεκριμένο χρήστη τη δεδομένη χρονική στιγμή τότε γίνεται:
    - Προσωρινή ανάθεση στο χρήστη του ρόλου του Επισκέπτη.
    - Ενεργοποίηση εκείνων των δικαιωμάτων πρόσβασης του ρόλου του Επισκέπτη που ικανοποιούν τους χρονικούς περιορισμούς της δεδομένης χρονικής στιγμής.
  - Περίπτωση 2: Αν υπάρχουν ενεργοί ρόλοι για το συγκεκριμένο χρήστη τη δεδομένη χρονική στιγμή τότε:
    - Ενεργοποίηση εκείνων των δικαιωμάτων πρόσβασης των ενεργών ρόλων του χρήστη που ικανοποιούν τους χρονικούς περιορισμούς της δεδομένης χρονικής στιγμής.

- Βήμα 2

  Εφαρμογή των ενεργών δικαιωμάτων.

- Βήμα 3

  Έλεγχος του πίνακα της Διαχείρισης Εργασιών των Windows (Task Manager) για διακοπή των εφαρμογών που είναι ήδη ανοιχτές (δικαίωμα επιτρεπτό από προηγούμενη κλήση του Timer) και η κλήση της συνάρτησης της εφαρμογής των ενεργών δικαιωμάτων ορίζει πλέον άρνηση πρόσβασης σε αυτές.

Στη συνέχεια παρατίθενται αναλυτικά οι συναρτήσεις που καλούνται στα βήματα 1 έως 3 και υλοποιούν την παραπάνω λογική.

Συνάρτηση RoleActivation

Η συνάρτηση αυτή είναι υπεύθυνη για την ενεργοποίηση των ρόλων που έχουν ανατεθεί στο χρήστη και καλύπτουν τους χρονικούς περιορισμούς τη στιγμή που καλείται. Η ενεργοποίηση των ρόλων του χρήστη γίνεται μέσω της μεταβολής του πεδίου RoleStatus του πίνακα συσχέτισης χρηστών – ρόλων (RUserRole) από την τιμή 0 στην τιμή 1.

Αρχικά, αναζητούνται οι ρόλοι που έχουν ανατεθεί στο συνδεδεμένο χρήστη και για κάθε έναν από αυτούς εξετάζονται οι χρονικοί περιορισμοί. Σε πρώτη φάση επιλέγονται οι ρόλοι που μπορούν να ενεργοποιηθούν τη δεδομένη ημέρα της εβδομάδας και στη συνέχεια εξετάζονται οι χρονικοί περιορισμοί (ώρα - λεπτά) αυτών. Όλες οι παράμετροι του χρόνου που αφορούν την ώρα και χρησιμοποιούνται στη συνάρτηση αυτή έχουν υπολογιστεί σε δευτερόλεπτα, γεγονός που διευκολύνει τους υπολογισμούς και τις συγκρίσεις. Ο αλγόριθμος που χρησιμοποιείται για τη σύγκριση της τρέχουσας ώρας με τις ώρες έναρξης και λήξης των χρονικών περιορισμών που είναι αποθηκευμένες στη βάση δεδομένων παρουσιάζεται αναλυτικά στην Εικόνα 5.5.

Συνάρτηση SecureMyApplication

Η συνάρτηση αυτή εξασφαλίζει τη μη πρόσβαση των χρηστών στους οποίους δεν έχει ανατεθεί ο προκαθορισμένος ρόλος του Υπεύθυνου Εργαστηρίου στην εφαρμογή διαχείρισης χρηστών, ρόλων και δικαιωμάτων,RBACProject. Πιο συγκεκριμένα, εξετάζει αν ο συνδεδεμένος χρήστης την εκάστοτε χρονική στιγμή έχει ενεργό το ρόλο του Υπεύθυνου Εργαστηρίου. Αν όχι τότε του αφαιρεί το δικαίωμα πρόσβασης στην εφαρμογή RBACProject μέσω του εργαλείου cacls. Επίσης, απενεργοποιεί το Παράθυρο Διαχείρισης Εργασιών των Windows (Task Manager) προκειμένου να εξασφαλίσουμε ότι ο εκάστοτε χρήστης δε θα μπορεί μέσω αυτού να τερματίσει την εφαρμογή RBACStartUp, και κατά συνέπεια να μη μπορούν να εφαρμοστούν τα δικαιώματα που του έχει ορίσει ο Υπεύθυνος Εργαστηρίου. Στην αντίθετη περίπτωση που ο χρήστης έχει ενεργό το ρόλο του Υπεύθυνου Εργαστηρίου, εξασφαλίζεται ότι αυτός έχει πλήρη πρόσβαση στην RBACProject καθώς και στον Παράθυρο Διαχείρισης Εργασιών των Windows (Task Manager).

Συνάρτηση PermissionActivation

Ομοίως με τη συνάρτηση RoleActivation, η PermissionActivation ενεργοποιεί τα δικαιώματα εκείνα των ρόλων που η κλήση της συνάρτησης RoleActivation έχει ενεργοποιήσει, και που καλύπτουν τους χρονικούς περιορισμούς τη δεδομένη χρονική στιγμή που καλείται ο Timer. Η ενεργοποίηση των δικαιωμάτων του χρήστη γίνεται και σε αυτή την περίπτωση μέσω της μεταβολής του πεδίου PermStatus του πίνακα TRolePerm από την τιμή 0 στην τιμή 1 ακολουθώντας και πάλι τον αλγόριθμο της Εικόνας 5.5.

Συνάρτηση ChangeRights

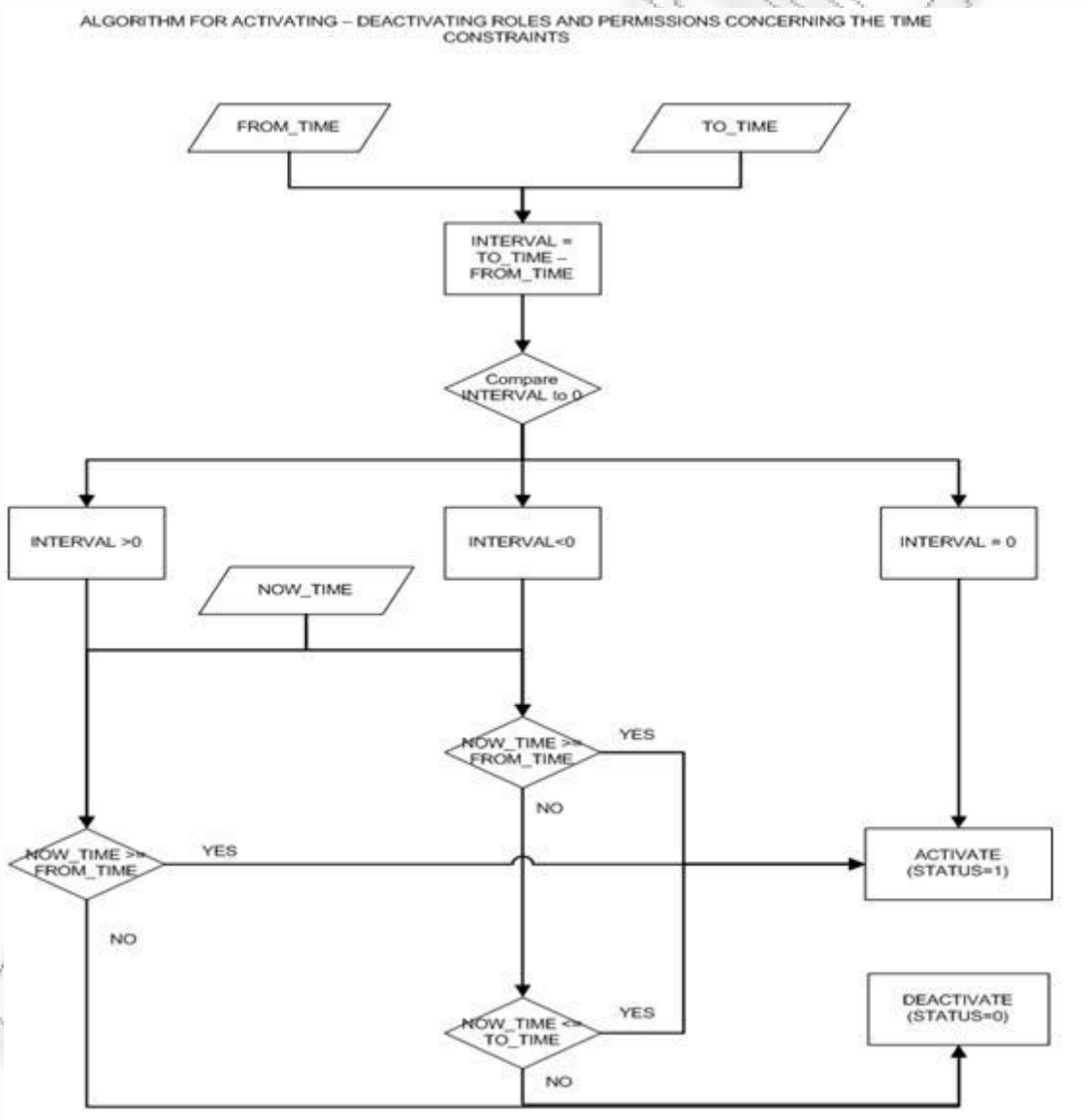
Η κλήση της συνάρτησης αυτής εφαρμόζει τα ενεργά δικαιώματα των ενεργών ρόλων του συνδεδεμένου χρήστη έτσι όπως αυτά έχουν οριστεί από τις δύο προηγούμενες συναρτήσεις. Για την εφαρμογή των δικαιωμάτων χρησιμοποιείται το εργαλείο Cacls δίνοντάς του τις κατάλληλες παραμέτρους.

Πριν γίνει η τελική εφαρμογή των δικαιωμάτων, ορίζουμε πλήρη πρόσβαση για όλα τα μονοπάτια που αντιστοιχούν στους ρόλους που έχουν ανατεθεί στο χρήστη (και όχι μόνο στους ενεργούς του ρόλους). Αυτό καλύπτει την περίπτωση απενεργοποίησης ενός ρόλου στην τρέχουσα κλήση του Timer. Στο σημείο αυτό πρέπει να τονίσουμε ότι η εφαρμογή μας λειτουργεί κυρίως με τη λογική της άρνησης πρόσβασης. Οπότε, η απενεργοποίηση ενός ρόλου θα πρέπει να επαναφέρει την άρνηση πρόσβασης σε ένα αρχείο/εφαρμογή ή φάκελο σε πλήρη

πρόσβαση. Η εφαρμογή της πλήρους πρόσβασης δεν εμποδίζει την μετέπειτα εφαρμογή των ενεργών δικαιωμάτων των ενεργών ρόλων κατά την τρέχουσα κλήση του Timer.

Όπως ορίζει το μοντέλο RBAC, κάθε χρήστης μπορεί να έχει ενεργοποιημένους περισσότερους του ενός ρόλους σε μια χρονική στιγμή. Αυτό όμως μπορεί να οδηγήσει σε σύγκρουση κατά την εφαρμογή αντικρουόμενων δικαιωμάτων που αναφέρονται στο ίδιο αρχείο/εφαρμογή ή φάκελο. Η συνάρτηση αντιμετωπίζει την περίπτωση αυτή θέτοντας το δικαίωμα της μη-πρόσβασης να υπερισχύει αυτού της πλήρους πρόσβασης και εφαρμόζοντας το.

Εικόνα 5.5: Αλγόριθμος Ενεργοποίησης/ Απενεργοποίησης Ρόλων και Δικαιωμάτων Βάσει των Χρονικών Περιορισμών



Συνάρτηση KillProcess

Ένα επιπλέον ζήτημα που πρέπει να καλυφθεί είναι η περίπτωση κατά την οποία το δικαίωμα σε μία εφαρμογή αλλάζει από πλήρη πρόσβαση σε μη πρόσβαση και η εφαρμογή είναι ήδη ανοιχτή. Η συνάρτηση ChangeRigths που έχει κληθεί πριν από την KillProcess, θα εφαρμόσει το δικαίωμα της μη πρόσβασης αλλά δε θα την κλείσει. Για να πετύχουμε την επιπλέον αυτή λειτουργικότητα, πραγματοποιούμε έλεγχο στον πίνακα Διαχείρισης Εργασιών των Windows (Task Manager) και στην καρτέλα των Διεργασιών για την ύπαρξη του εκτελέσιμου αρχείου (.exe) της εφαρμογής. Αν αυτό εντοπιστεί, τότε η συνάρτηση τερματίζει την εφαρμογή. Στην επόμενη κλήση του Timer, δεδομένου ότι θα έχει εφαρμοστεί το δικαίωμα της μη πρόσβασης δε θα είναι εφικτό το άνοιγμα της εφαρμογής από το χρήστη.

Συνάρτηση ApplyTemporalRights

Η συνάρτηση αυτή καλείται στην περίπτωση που τη δεδομένη χρονική στιγμή, κανένας από τους ανατεθειμένους ρόλους του συγκεκριμένου χρήστη δεν είναι ενεργός. Προκειμένου να αποφευχθεί η ανεξέλεγκτη πρόσβαση του χρήστη στο σύστημα, του ανατίθεται προσωρινά ο ρόλος του Επισκέπτη. Είναι σημαντικό να τονίσουμε το «προσωρινά» καθώς δεν εισάγεται εγγραφή για το χρήστη με το ρόλο του Επισκέπτη στον πίνακα RUserRole. Ο ρόλος αυτός χρησιμοποιείται προκειμένου να ενεργοποιηθούν τα δικαιώματα εκείνα του ρόλου του Επισκέπτη που καλύπτουν τους χρονικούς περιορισμούς τη δεδομένη χρονική στιγμή που καλείται ο Timer. Στη συνέχεια εφαρμόζονται τα ενεργά δικαιώματα του ρόλου του Επισκέπτη για το συνδεδεμένο χρήστη μέσω της χρήσης του εργαλείου Cacls. Τέλος, γίνεται και σε αυτή την περίπτωση ο έλεγχος στον πίνακα Διαχείρισης Εργασιών των Windows (Task Manager) και στην καρτέλα των Διεργασιών και ο τερματισμός της εφαρμογής, όπως περιγράφηκε παραπάνω στη συνάρτηση KillProcess.

Στην επόμενη κλήση του Timer θα γίνει και πάλι έλεγχος για τον αν υπάρχει τουλάχιστον ένας ενεργός ρόλος για το χρήστη τη δεδομένη χρονική στιγμή. Στην περίπτωση ύπαρξης ενεργών ρόλων, τότε θα εφαρμόζονται τα ενεργά δικαιώματα πρόσβασης των ρόλων αυτών, διαφορετικά θα ανατίθεται και πάλι στο χρήστη προσωρινά ο ρόλος του Επισκέπτη.

Συνάρτηση CurrentUser

Αποτελεί μια βοηθητική συνάρτηση η οποία παίρνει από το σύστημα το όνομα του συνδεδεμένου χρήστη. Επειδή αυτό επιστρέφεται με τη μορφή μονοπατιού (πχ HOME\USER), αλλά στην εφαρμογή χρησιμοποιούμε μόνο το όνομα του χρήστη (USER), πραγματοποιούμε κατάλληλη επεξεργασία ώστε να απομονώσουμε και να αποθηκεύσουμε το όνομα του χρήστη όπως το χρειαζόμαστε.

Η σειρά με την οποία καλούνται οι παραπάνω συναρτήσεις μέσα στον Timer βασίζεται στη λογική του ότι πρώτα θα πρέπει να ενεργοποιηθούν οι ρόλοι του χρήστη σύμφωνα με τους χρονικούς περιορισμούς και στη συνέχεια να εντοπιστούν τα δικαιώματα αυτών που πρέπει να ενεργοποιηθούν και τέλος να εφαρμοστούν.

Με το πέρας της περιγραφής της εφαρμογής RBACStartUp ολοκληρώνεται η περιγραφή της λειτουργικότητας της συνολικής εφαρμογής μας. Στην επόμενη ενότητα παρουσιάζονται τα γενικά συμπεράσματα για την εφαρμογή μας καθώς και θέματα που μένουν ανοιχτά για περαιτέρω ανάπτυξη αυτής.

5.7. Επίλογος

Στην προσπάθειά μας να αναδείξουμε τα πλεονεκτήματα του μοντέλου RBAC ακόμα και σε μικρού εύρους συστήματα όπως είναι ένας υπολογιστής στο περιβάλλον ενός σχολείου, αναπτύξαμε την εφαρμογή που περιγράψαμε στις προηγούμενες ενότητες. Ουσιαστικά, η υλοποίηση του μοντέλου γίνεται μέσω της εφαρμογής RBACProject, αφού μέσω αυτής γίνεται η ανάθεση ρόλων στους χρήστες και η ανάθεση δικαιωμάτων πρόσβασης στους ρόλους, συνιστώσες οι οποίες είδαμε ότι αποτελούν τα βασικά συστατικά του RBAC. Η τελική εφαρμογή των δικαιωμάτων σύμφωνα με τους περιορισμούς που έχει ορίσει ο διαχειριστής του συστήματος γίνεται με τη βοήθεια μίας άλλης εφαρμογής που λειτουργεί στο παρασκήνιο (RBACStartUp).

Οι απαιτήσεις του περιβάλλοντος στο οποίο επιλέξαμε να ενσωματώσουμε την εφαρμογή μας, επιβάλουν την ικανοποίηση χρονικών περιορισμών. Οι περιορισμοί αυτοί αποτελούν σημαντικό παράγοντα στον έλεγχο της χωρίς όρια πρόσβασης στον τοπικό υπολογιστή. Η προσέγγιση που επιλέξαμε να ακολουθήσουμε είναι αυτή της επιβολής περιορισμών σε επίπεδο ημέρας και ώρας, χρονικοί περιορισμοί που θεωρούμε ότι πλησιάζουν περισσότερο στα δεδομένα του σχολικού περιβάλλοντος. Μια πιθανή βελτίωση της εφαρμογής θα ήταν η δυνατότητα καθορισμού χρονικών περιορισμών σε επίπεδο μήνα και έτους.

Σε ότι αφορά στα δικαιώματα πρόσβασης που δίνονται μέσω της εφαρμογής μας, περιοριστήκαμε στην επιβολή δικαιώματος μη – πρόσβασης και δικαιώματος πλήρους πρόσβασης. Επιπλέον, εξασφαλίζεται ότι εάν μία εφαρμογή είναι ανοιχτή και «τρέχει» κατά τη χρονική στιγμή επιβολής δικαιώματος μη – πρόσβασης, τότε αυτή τερματίζεται. Στόχος της παρούσας διπλωματικής είναι η ανάπτυξη εφαρμογής που θα αναδεικνύει τα πλεονεκτήματα χρήσης του μοντέλου RBAC και όχι η εστίαση στη διαχείριση των δικαιωμάτων πρόσβασης στο περιβάλλον των Windows. Μία περαιτέρω εξέλιξη στη διαχειριστική ευκολία που προσφέρεται μέσω της εφαρμογής θα ήταν η προσθήκη περισσότερων επιλογών όσον αφορά στους τύπους των δικαιωμάτων πρόσβασης (π.χ. δικαίωμα εγγραφής, δικαίωμα ανάγνωσης κλπ).

Ο τρόπος που έχει αναπτυχθεί η εφαρμογή προσφέρει δυνατότητα προσαρμογής της και σε άλλα περιβάλλοντα εκτός του σχολικού. Η δυνατότητα μετονομασίας των ρόλων και μεταβολής των δικαιωμάτων πρόσβασης που έχουν ανατεθεί σε αυτούς, με απλό και εύκολα αντιληπτό από το χρήστη τρόπο, την καθιστά αρκετά ευέλικτη για την ενσωμάτωσή της σε διαφορετικό σύστημα. Τέλος, το γεγονός ότι δε μπορεί να παρέμβει ο οποιοσδήποτε χρήστης πλην του Υπεύθυνου Εργαστηρίου στη λειτουργία της εφαρμογής, αποτελεί ένα ακόμα σημαντικό πλεονέκτημά της ικανοποιώντας μία ακόμα από τις αρχικές απαιτήσεις που τέθηκαν κατά το σχεδιασμό της.

Είναι γνωστό ότι τα περισσότερα πληροφοριακά συστήματα βασίζονται πλέον στις υποδομές δικτύου και τη συγκέντρωση του ελέγχου σε μία κεντρική μονάδα η οποία ελέγχει και διαχειρίζεται όλες τις περιφερειακές μονάδες. Θέλοντας όμως να δείξουμε πόσο σημαντική είναι η συνεισφορά του μοντέλου RBAC στη διαχείριση της πρόσβασης ακόμα και σε ένα μικρό αυτόνομο σύστημα τοπικού υπολογιστή, αναπτύξαμε την εφαρμογή μας στα πλαίσια ενός τοπικού υπολογιστή. Με τις κατάλληλες προσθήκες και επεκτάσεις, η εφαρμογή μπορεί να λειτουργήσει στα ευρύτερα πλαίσια ενός τομέα (εφαρμογή που θα καλύπτει τις ανάγκες του δικτύου ενός σχολικού εργαστηρίου).

6. ΣΥΝΟΛΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

Το μέγεθος των πληροφοριακών συστημάτων σήμερα, το οποίο συνεχώς αυξάνεται, το πλήθος των πληροφοριών που διακινούνται μέσω αυτών καθώς και ο μεγάλος αριθμός χρηστών που έχουν πρόσβαση στις πληροφορίες αυτές φέρνουν στο επίκεντρο την Ασφάλεια. Η εξουσιοδότηση των χρηστών προκειμένου να αποκτήσουν πρόσβαση, η εμπιστευτικότητα και η ακεραιότητα των δεδομένων είναι καίριες απαιτήσεις που θα πρέπει να εξασφαλιστούν σε κάθε σύγχρονο πληροφοριακό σύστημα ανεξαρτήτως μεγέθους. Η παρούσα μεταπτυχιακή διατριβή επικεντρώθηκε στη μελέτη του ελέγχου πρόσβασης και στον τρόπο που μπορεί αυτή να εφαρμοστεί ώστε να ικανοποιηθούν οι παραπάνω απαιτήσεις.

Αρχικά παρουσιάσαμε και περιγράψαμε τα βασικότερα μοντέλα ελέγχου πρόσβασης. Από τα πρώτα πληροφοριακά συστήματα για τα οποία προέκυψε η ανάγκη διαχείρισης των χρηστών και προστασίας της πληροφορίας, και τα οποία αφορούσαν στρατιωτικές εφαρμογές, μέχρι και τα πιο σύγχρονα που συναντώνται πλέον σε κάθε επιχειρησιακό περιβάλλον, η ανάγκη για τον έλεγχο της πρόσβασης σε αυτά αποτελεί βασικό μέλημα των διαχειριστών. Η εξέλιξη των αναγκών και των απαιτήσεων οδήγησε στη δημιουργία διαφόρων μοντέλων για την κάλυψη αυτών. Ο Διακριτικός Έλεγχος Πρόσβασης (DAC), ο Υποχρεωτικός Έλεχος Πρόσβασης (MAC), το μοντέλο Clark Wilson και η πολιτική του Κινέζικου Τείχους (Chinese Wall) είναι μόνο μερικά από τα μοντέλα και τις πολιτικές που δημιουργήθηκαν για το έλεγχο πρόσβασης.

Στη συνέχεια εστιάσαμε στο πλέον διαδεδομένο και ευρέως χρησιμοποιούμενο Μοντέλο Ελέγχου Πρόσβασης Βασισμένο σε Ρόλους (RBAC). Δημοσιευμένο ως πρότυπο από το NIST το 2004 εισάγει του έννοια του ρόλου στη διαχείριση δικαιωμάτων πρόσβασης και καθιερώνεται ως ένα κοινά αποδεκτό βιομηχανικό πρότυπο. Η ανάθεση των δικαιωμάτων πρόσβασης φεύγει πλέον από τον άξονα των χρηστών και μεταφέρεται στον άξονα των ρόλων καθιστώντας το μοντέλο ευέλικτο και εύκολα προσαρμόσιμο σε οποιοδήποτε πληροφοριακό σύστημα. Η δυνατότητα καθορισμού ιεραρχιών, ο στατικός και δυναμικός διαχωρισμός των καθηκόντων καθώς και ο συνδυασμός αυτών αποτελούν πρόσθετες συνιστώσες του βασικού RBAC προσφέροντας επιπλέον λειτουργικότητες σε αυτό και διαχειριστικές ευκολίες.

Το σύνολο των πλεονεκτημάτων του RBAC, η μη εξάρτησή του από πολιτικές και κατά συνέπεια η αναγνώρισή του ως ένα γενικευμένο μοντέλο, το θέτουν σήμερα στην πρώτη θέση σε ότι αφορά στην επιλογή μοντέλου για τον έλεγχο πρόσβασης. Παρόλα αυτά η έλλειψη σαφώς καθορισμένων περιορισμών για παραμέτρους όπως είναι ο χρόνος, το περιβάλλον κλπ δημιούργησαν την ανάγκη για την εισαγωγή επεκτάσεων του βασικού μοντέλου RBAC. Ενδεικτικές επεκτάσεις όπως το TRBAC, το GTRBAC, το GRBAC και το QRBAC παρουσιάστηκαν στο Κεφάλαιο 4 της παρούσας διατριβής.

Στη συνέχεια, παρουσιάσαμε τον τρόπο υλοποίησης εφαρμογής η οποία στηρίζεται στο RBAC με σκοπό τη διαχείριση δικαιωμάτων πρόσβασης σε σύστημα τοπικού υπολογιστή με εγκατεστημένο το λειτουργικό σύστημα των Windows. Σκοπός μας ήταν η μελέτη των πλεονεκτημάτων του βασικού μοντέλου RBAC, αλλά και επεκτάσεών του όπως το TRBAC και το GTRBAC, ακόμη και σε συστήματα μικρού μεγέθους όπως αυτό ενός αυτόνομου υπολογιστή πολλών χρηστών. Για την περιγραφή της λειτουργικότητας της εφαρμογής, την «τοποθετήσαμε» σε υπολογιστή σχολικού περιβάλλοντος καθορίζοντας παραμέτρους που αντιπροσωπεύουν ένα τέτοιο σύστημα.

Η υλοποίηση των βασικών συνιστωσών του μοντέλου ελέγχου πρόσβασης βασισμένο σε ρόλους όπως η ανάθεση των ρόλων που ο Υπεύθυνος Εργαστηρίου έχει ορίσει στους χρήστες του τοπικού υπολογιστή, η ανάθεση δικαιωμάτων στους ρόλους γίνεται μέσω απλών και φιλικών προς το χρήστη οθονών. Η εφαρμογή προσφέρει τη δυνατότητα ανάθεσης περισσοτέρων του ενός ρόλου στον εκάστοτε χρήστη καθώς και δυνατότητα προσθήκης χρονικών περιορισμών στην ενεργοποίηση των ρόλων, στην ανάθεση των ρόλων στο χρήστη

και στην ανάθεση δικαιωμάτων πρόσβασης στο ρόλο, δυνατότητες που την κάνουν να υπερτερεί συγκριτικά με τις ομάδες διαχείρισης των χρηστών (groups) που ήδη διαθέτουν τα Windows.

Στόχος της παρούσας διπλωματικής είναι η ανάπτυξη εφαρμογής που θα αναδεικνύει τα πλεονεκτήματα χρήσης του μοντέλου RBAC και όχι η εστίαση στη διαχείριση των δικαιωμάτων πρόσβασης στο περιβάλλον των Windows. Γι' αυτό το λόγο ορίζονται μόνο δύο είδη δικαιωμάτων: μη πρόσβαση και πλήρης πρόσβαση. Η προσθήκη περισσότερων επιλογών όσον αφορά στους τύπους των δικαιωμάτων πρόσβασης (π.χ. δικαίωμα εγγραφής, δικαίωμα ανάγνωσης κλπ) θα μπορούσε να αποτελέσει μια περαιτέρω εξέλιξη της εφαρμογής η οποία όμως είναι εκτός των ορίων μελέτης της παρούσας διατριβής. Επίσης, προκειμένου η εφαρμογή μας να ενσωματωθεί στα σύγχρονα πληροφοριακά συστήματα, θα πρέπει να γίνει κατάλληλη προσαρμογή της ώστε να μπορεί να λειτουργήσει στα πλαίσια ενός τομέα (domain) και κατά συνέπεια δικτυακά.

Παρά τον «τοπικό» χαρακτήρα της εφαρμογής μας, αυτή μπορεί να βρει χρήση με ικανοποιητικά αποτελέσματα σε πολλά συστήματα που χρησιμοποιούνται και όπου ο έλεγχος πρόσβασης κρίνεται αναγκαίος για την εύρυθμη λειτουργία τους. Πέραν του σχολικού περιβάλλοντος που παρουσιάσαμε ως παράδειγμα για την περιγραφή της υλοποίησής της, η εφαρμογή με την κατάλληλη διαμόρφωση ρόλων και καθορισμού αντίστοιχων δικαιωμάτων μπορεί να χρησιμοποιηθεί στα πλαίσια οικιακού υπολογιστή ώστε οι γονείς να ελέγχουν την πρόσβαση των παιδιών σε αρχεία και φακέλους, στα πλαίσια υπολογιστή που λειτουργεί στο γραφείο καθηγητή πανεπιστημίου και στον οποίο έχουν πρόσβαση οι φοιτητές που συνεργάζονται μαζί του κλπ. Γενικότερα η εφαρμογή μπορεί να χρησιμοποιηθεί σε συστήματα που το μέγεθος του είναι τέτοιο που δε δικαιολογεί την εγκατάσταση δικτύου αλλά που είναι αναγκαίος ο έλεγχος της πρόσβασης σε αυτά.

7. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] D.F.Ferraiolo, D.R.Kuhn, R.Chandramouli, “Role-Based Access Control”, Artech House (Second Edition)

[2] M.Bishop, “Computer Security: Art and Science”, Addison Wesley (Copyright 2003)

[3] R.Sandhu, P.Samarati, “Access Control: Principles and Practice”, IEEE Communications Magazine, Volume 32, Number 9, September 1994.

[4] C.Hu, D.F. Ferraiolo, D.R.Kuhn, “ Assessment of Access Control Systems”, National Institute of Standards and Technology (NIST), September 2006

[5] J.H.Saltzer, M.D.Schroeder, “The protection of information in computer systems”, Proceedings of the IEEE, Volume 63, Number 9, September 1975, p.1278-1308

[6] Department of Defence (DOD), “Trusted Computer System Evaluation Criteria”, 5200.28-STD, December 1985

[7] National Computer Security Center (NCSC), “A guide to understanding discretionary access control in trusted systems”, Version1, September 1987

[8] Σ.Κάτσικας, Δ.Γκρίτζαλης, “Ασφάλεια Πληροφοριακών Συστημάτων”, Εκδόσεις Νέων Τεχνολογιών, 2004

[9] Z.Mao, N.Li, H.Chen, X.Jiang, “Trojan Horse Resistant Discretionary Access Control”, Proceedings of the 14th ACM symposium on Access control models and technologies, 2009

[10] D.E.Bell, “Looking Back at the Bell – La Padula Model”, Reston VA, 20191, December 2005

[11] D.E.Bell, L.J.La Padula, “Secure Computer System: Unifies Exposition and Multics Interpretation”, March 1976

[12] D.F.C. Brewer, M.J. Nash, “The Chinese Wall Security Policy”,,Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, May1989, p 206-214

[13] M.V.Tripunitara, N.Li, “ The Foundational work of Harrison-Ruzzo-Ullman Revisited “

[14] M.A.Harrison, W.L.Ruzzo, J.D.Ullman, “Protection in Operating Systems”

[15] D.D.Clark, D.R.Wilson, “A Comparison of Commercial and Military computer Security Policies”, IEEE Symposium of Security and Privacy, 1987, http://csrc.nist.gov/groups/SNS/rbac/

[16] American National Standard for Telecommunications, “Telecom Glossary 2000”, American National Standards Institute

[17] http://csrc.nist.gov/groups/SNS/rbac/faq.html

[18] D.F.Ferraiolo, D.R.Kuhn, “Role Based Access Controls”, 15th National Computer Security Conference, October 1992, p 554-563

[19] D.F.Ferraiolo, D.J.Cugini, D.R.Kuhn, “Role-Based Access Control: Features and Motivations”, Proceedings of the Annual Computer Security Applications Conference, 1995

[20] R.S.Sandhu, E.J.Coyne, H.L.Feinstein, C.E.Youman, “Role-Based Access Control Models", IEEE Computer, Volume 29, Number 2, 1996, p. 38 - 47

[21] R.Sandhu, D.F.Ferraiolo, D.R.Kuhn, "The NIST Model for Role Based Access Control: Towards a Unified Standard", Proceedings of the 5th ACM Workshop on Role Based Access Control, July 2000

[22] D.F.Ferraiolo, R.Kuhn, R.Sandhu, "RBAC Standard Rationale: comments on a Critique of the ANSI Standard on Role Based Access Control", IEEE Security & Privacy, Volume 5, Number 6, November/December 2007

[23] H.A.Weber, "Role-Based Access Control: The NIST Solution", SANS Institute InfoSec Reading Room, October 2003

[24] American National Standard Institution (ANSI), "Role Based Access Control", ANSI INCITS 359-2004

[25] Bertino, E.A.Bonatti, E.Ferrari, "TRBAC: A Temporal Role-Based Access Control Model", ACM Transactions on Information and System Security, Volume 4, Number 3, September 2001

[26] M.J.Covington, M.J.Moyer, M.Ahamad, "Generalized Role-Based Access Control for Securing Future Applications", College of Computing, Georgia Institute of Technology, Atlanta,Georgia

[27] K.D.Kang, "Integrated Security and Quality of Service Support in E-Commerce", Department of Computer Science University of Virginia

[28] James Joshi, Elisa Bertino, Usman Latif, Arif Ghafoor, "Generalized Temporal Role Based Access Control Model – Specification and Modelling", Part 1

[29] Osborn, "Mandatory Access Control and Role-Based Access Control Revisited", Proceedings of Second ACM Workshop on Role-Based Access Control, November 1997

[30] K.J.Biba, "Integrity Considerations for Secure Computer Systems", MTR-3153, The Mitre Corporation, April 1977