ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΑΤΡΙΒΗ
για την απόκτηση Διδακτορικού Διπλώματος
του Τμήματος Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

Πέτρου Μπέλση

ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΣΕ ΚΑΤΑΝΕΜΗΜΕΝΑ ΠΕΡΙΒΑΛΛΟΝΤΑ ΣΥΝΑΣΠΙΖΟΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Συμβουλευτική Επιτροπή:

Πρόεδρος:

Στέφανος Γκρίτζαλης
Αναπληρωτής Καθηγητής
Πανεπιστημίου Αιγαίου

Μέλη:

Σωκράτης Κάτσικας
Καθηγητής
Πανεπιστημίου Αιγαίου

Σπυρίδων Κοκολάκης
Επίκουρος Καθηγητής
Πανεπιστημίου Αιγαίου

Εξεταστική Επιτροπή:

Πρόεδρος:

Στέφανος Γκρίτζαλης
Αναπληρωτής Καθηγητής
Πανεπιστημίου Αιγαίου

Μέλη:

Σωκράτης Κάτσικας
Καθηγητής
Πανεπιστημίου Αιγαίου

Βασίλειος Χρυσικόπουλος
Καθηγητής
Ιονίου Πανεπιστημίου

Σπυρίδων Λυκοθανάσης
Καθηγητής
Πανεπιστημίου Πατρών

Σπυρίδων Κοκολάκης
Επίκουρος Καθηγητής
Πανεπιστημίου Αιγαίου

Κωνσταντίνος Λαμπρινουδάκης
Επίκουρος Καθηγητής
Πανεπιστημίου Αιγαίου

Ελισάβετ Κωνσταντίνου
Λέκτορας
Πανεπιστημίου Αιγαίου

Πρόλογος και Ευχαριστίες

Η παρούσα διατριβή είναι το αποτέλεσμα ερευνητικής προσπάθειας ετών που πραγματοποιήθηκε στο Πανεπιστήμιο Αιγαίου. Η ολοκλήρωση της δεν θα ήταν εφικτή χωρίς την υποστήριξη και δημιουργική καθοδήγηση ενός από τους πιο εργατικούς ανθρώπους που έχω γνωρίσει, του εποπτεύοντα καθηγητή μου Στέφανου Γκρίτζαλη. Για το ότι με εμπιστεύτηκε για όλα αυτά τα χρόνια, μου μετέδωσε σημαντικό κομμάτι της ερευνητικής του εμπειρίας, αλλά και για το ότι με στήριξε αντιμετωπίζοντας με το ήρεμο ύφος του όλες τις καταστάσεις, τον ευχαριστώ ειλικρινά.

Ευχαριστώ επίσης τα μέλη της τριμελούς επιτροπής, τον καθηγητή Σωκράτη Κάτσικα και τον Επίκουρο καθηγητή Σπυρίδωνα Κοκολάκη. Από τη συνεργασία μαζί τους κέρδισα πολλά, ειδικά σε σχέση με τη συγγραφή ερευνητικών εργασιών, τα εξαιρετικά χρήσιμα σχόλιά τους και η συνεισφορά τους στην κοινή μας έρευνα με βοήθησαν να αποκομίσω τα μέγιστα.

Ευχαριστώ επίσης τους καθηγητές του ΤΕΙ Αθήνας Γραμματή Πάντζιου, Χρήστο Σκουρλά και Ιωάννη Χάλαρη για το ότι μου παρείχαν σε όλα τα χρόνια των σπουδών μου ένα αρμονικό επαγγελματικό περιβάλλον, δίνοντας μου την ευκαιρία να συμμετέχω στα ερευνητικά έργα που διηύθυναν, καθώς επίσης για την εμπιστοσύνη και τη φιλία τους. Ένα ξεχωριστό ευχαριστώ οφείλω στον καθηγητή Χρήστο Σκουρλά που με στήριξε επιστημονικά, αλλά ακόμη και με τις συμβουλές του σε κρίσιμες προσωπικές αποφάσεις.

Θα ήθελα ακόμη να ευχαριστήσω τους φίλους από τα πρώτα χρόνια των μεταπτυχιακών μας σπουδών, Απόστολο Μαλατρά, Βασίλειο Ζαφείρη και Χρήστο Δουλκερίδη για τις συζητήσεις και τις απόψεις που ανταλλάξαμε σε πολλά ερευνητικής φύσεως ζητήματα. Επίσης θα ήθελα να ευχαριστήσω τον Βασίλειο Τσουκαλά για τις συμβουλές του σε τεχνικής φύσεως θέματα.

Ευχαριστώ τέλος, την οικογένεια μου για τη στήριξη που μου παρείχε σε όλα τα χρόνια των σπουδών, συμμεριζόμενη την αγωνία αλλά και τις χαρές σε αυτή τη μακρόχρονη και δύσκολη πορεία.

Περίληψη

Η διείσδυση των Τ.Π.Ε. και η διαδικτύωση των συστημάτων, έδωσαν την δυνατότητα δημιουργίας νέων μορφών οργάνωσης και ανάπτυξης Π.Σ. Οι συνασπισμοί Πληροφοριακών Συστημάτων ανήκουν σε αυτή την κατηγορία σύγχρονων συστημάτων, προκύπτουν δε από τη συνεργασία διαφορετικών Π.Σ. με στόχο το διαμοιρασμό πόρων και προκειμένου για την επίτευξη ενός κοινού στόχου, όπως για παράδειγμα η συνεργασία σε ερευνητικά θέματα, η αντιμετώπιση εκτάκτων καταστάσεων (όπως φυσικές καταστροφές), η εθνική ασφάλεια κοκ. Μεταξύ των κυρίων χαρακτηριστικών των συνασπισμών είναι ο δυναμικός τους χαρακτήρας, που καθιστά τη διαχείρισή τους -και κυρίως τη διαχείριση της ασφάλειας- μία ιδιαίτερα απαιτητική διαδικασία. Ανάμεσα στα κύρια ερευνητικά και τεχνολογικά προβλήματα που σχετίζονται με τη διαχείριση των συνασπισμών, μπορούμε να διακρίνουμε:

α) την αντιμετώπιση του προβλήματος της αποτελεσματικής αναζήτησης πόρων στα διαφορετικά συστήματα,

β) την αντιμετώπιση των προβλημάτων ετερογένειας και τη δυνατότητα υποβολής ερωτημάτων στα διαφορετικά συστήματα με ελαχιστοποίηση της κατανάλωσης υπολογιστικών και δικτυακών πόρων,

γ) τη διαχείριση της ασφάλειας του συνασπισμού.

Στα πλαίσια της παρούσας διατριβής, προτείνεται:

α) Η αντιμετώπιση του προβλήματος της διήθησης πληροφορίας εισάγοντας μία προσέγγιση που βασίζεται στην χρήση αποδοτικών ταξινομητών σε συνδυασμό με αλγορίθμους επιλογής βέλτιστων χαρακτηριστικών από ένα στατιστικό δείγμα. Η συγκεκριμένη τεχνική που αναπτύχθηκε, συγκρίνεται πειραματικά προκειμένου να αποδειχθεί η υπεροχή της έναντι άλλων καταγεγραμμένων στη διεθνή βιβλιογραφία.

β) Στα πλαίσια του δεύτερου επιστημονικού προβλήματος προτείνεται η δημιουργία των εικονικών δικτύων οντολογιών προκειμένου για τη θεματική κατηγοριοποίηση των πόρων ενός δικτύου, επιτυγχάνοντας την αντιμετώπιση των προβλημάτων ετερογένειας καθώς και την αποφυγή υποβολής ερωτημάτων σε τμήματα του συστήματος που δεν περιέχουν πόρους θεματολογικά συναφείς προς το ερώτημα.

γ) Προκειμένου για τη διαχείριση της ασφάλειας του συνασπισμού προτείνεται η λύση της αντιστοίχησης ρόλων και της δημιουργίας ενός μηχανισμού με αυξημένα χαρακτηριστικά διαλειτουργικότητας, βασισμένου σε μία πρότυπη γλώσσα περιγραφής πολιτικών ασφάλειας. Παράλληλα προτείνεται ένα πλαίσιο ελαχιστοποίησης του διαχειριστικού φόρτου, καθώς επίσης και ένα πλαίσιο επίλυσης συγκρούσεων μεταξύ των διαφορετικών πολιτικών βασισμένο στη συνδυασμένη χρήση προγραμματισμού με περιορισμούς και ασαφούς λογικής. Προκειμένου για την υποστήριξη του προτεινόμενου πλαισίου, αναπτύχθηκε στα πλαίσια της διατριβής ένα πιλοτικό πρωτότυπο που επιτυγχάνει την αντιστοίχηση πολιτικών, ενώ διαθέτει ενσωματωμένο ένα μηχανισμό επίλυσης συγκρούσεων βασισμένο στη χρήση μετρικών ασαφούς λογικής όπως αυτός αναπτύχθηκε στα πλαίσια της διατριβής.

Executive Summary

The emergence of networked infrastructures has led to the development of new forms of organization and structuring of Information Systems. Coalitions of Information Systems fall in this category; they are often formed from different collaborating autonomous systems in order to achieve a common target (such as cooperation for research purposes, national security prevention, handling emergency response situations like physical disasters, etc). Among the main characteristics of coalitions is their dynamic character, which makes their management – with emphasis on their security management- a challenging task.

As research issues of prime importance relevant to the management of coalitions, we can distinguish:

a) Handling with the problem of effective identification of knowledge assets among the participating systems,
b) Handling with heterogeneity issues and with the ability to direct queries to the different participating systems, while eliminating computing and networking resources consumption,
c) Dealing with the Security Management of the coalition.

In order to deal with the above research issues, this dissertation focuses on:

a) Managing the problem of efficient information filtering, by introducing an approach, which utilizes effective classifiers combined with feature selection algorithms. These feature selection algorithms allow the determination of the most appropriate features using a statistical sample. The technique developed within the framework of this dissertation, is evaluated subject to carefully designed experiments and compared to relevant approaches as recorded in relevant literature.
b) Dealing with heterogeneity issues, introducing the concept of Virtual Ontology Networks (VON's), which allow the classification of a domain's assets to predefined categories. By doing so, we enable bandwidth consumption minimization, since we can determine without querying explicitly the network nodes, if the user's query is relevant to the content of the domain's assets.
c) Managing the coalition system's security, by introducing a flexible technique, which enables to map different policies. The proposed framework, based on the concept of policy mappings allows interoperation between different systems by determining corresponding roles among different policies. In order to achieve interoperability characteristics for the proposed solution, we have extended an existing (standardized) policy language. We have also introduced a framework that allows security management optimization by reducing administrative overhead, which utilizes constraint programming techniques and fuzzy logic in order to resolve conflicts emerging due to ambiguities in the independent policies. We have also provided a concept of proof implementation through a prototype developed for the purposes of this dissertation, the modules of which implement - the described throughout the chapters of this thesis - functions of the proposed access control framework.

ΚΕΦΑΛΑΙΟ 1 - Εισαγωγή

1.1 Οριοθέτηση του προβλήματος

Τα τελευταία χρόνια η ραγδαία ανάπτυξη της τεχνολογίας και η αξιοποίηση στην καθημερινή ζωή των Τεχνολογιών Επικοινωνιών και Πληροφορικής (Τ.Π.Ε.), δημιούργησαν νέα δεδομένα και μία νέα πραγματικότητα, χαρακτηριζόμενη τόσο από προκλήσεις όσο και από μία σειρά προβλήματα που σχετίζονται κυρίως με θέματα ασφάλειας και κινδύνους από τη μη εξουσιοδοτημένη επεξεργασία δεδομένων.
Μεταξύ των σημαντικότερων προκλήσεων που εισάγει η δικτύωση των συστημάτων, είναι και αυτή της δυνατότητας διασύνδεσης Πληροφοριακών Συστημάτων (Π.Σ.) μεταξύ τους, γεγονός που πολλαπλασιάζει τα οφέλη από την πρόσβαση σε μεγαλύτερο όγκο πληροφοριών. Ταυτόχρονα, προκύπτει η ανάγκη δημιουργίας νέων μοντέλων ασφάλειας, ικανών να αποτυπώσουν και ανταποκριθούν στις ιδιαίτερες ανάγκες της διασύνδεσης συστημάτων.
Ειδικής μνείας χρήζουν τα συστήματα διαχείρισης γνώσης, που αποτελούν συστήματα με προηγμένες δυνατότητες αποθήκευσης, ανάκτησης και επεξεργασίας ετερογενών πόρων. Η επιτυχημένη σχεδίαση και ανάπτυξη συστημάτων διαχείρισης γνώσης, συνιστά από μόνη της παράγοντα ικανό να προσδώσει ανταγωνιστικό πλεονέκτημα στους σύγχρονους οργανισμούς. Υψηλής χρησιμότητας είναι οι μελέτες που τεκμηριώνουν την αύξηση της ανταγωνιστικότητας μεγάλων οργανισμών λόγω της επιτυχημένης εγκατάστασης συστημάτων διαχείρισης γνώσης,τα οποία πλέον αποτελούν αναπόσπαστο τμήμα του πληροφοριακού συστήματος που υποστηρίζει τη λειτουργία τους σε καθημερινή βάση. Παράλληλα, τα τελευταία χρόνια η ανάπτυξη κατανεμημένων συστημάτων διαχείρισης γνώσης παρουσιάζει σημαντική πρόοδο (Belsis et al, 2005e) (Belsis et al, 2004b) (εικ. 1.1). Η διασύνδεση διαφορετικών βάσεων γνώσης και ο διαμοιρασμός δεδομένων και πόρων από διαφορετικούς οργανισμούς στα πλαίσια της συνεργασίας διαφορετικών Π.Σ. για την επίτευξη ενός κοινού στόχου προβάλλει ως μία εξόχως ενδιαφέρουσα προοπτική, εισάγοντας ωστόσο και μία σειρά από τεχνολογικές - και όχι μόνο - προκλήσεις. Μεταξύ άλλων, οι προκλήσεις αυτές αφορούν στην αναζήτηση πόρων στα κατανεμημένα αυτά περιβάλλοντα, τη δημιουργία μεθόδων και ανάπτυξη τεχνικών ικανών να επιτρέψουν την ασφαλή διαχείριση πόρων στο κατανεμημένο σύστημα.

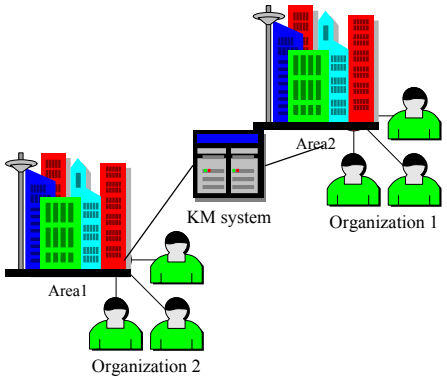
1.2 Κίνητρα της παρούσας έρευνας

Η επίδραση των Τ.Π.Ε. έχει - μεταξύ άλλων - επιφέρει τη σε καθημερινή βάση επικοινωνία με ποικίλα Π.Σ. Προκειμένου για την ολοκλήρωση μιας διαδικασίας, απαιτείται συχνά μία σειρά από ενέργειες που αφορούν στην αναζήτηση και ανάκτηση πληροφοριών σε περισσότερα του ενός Π.Σ. Η επικοινωνία με καθένα από αυτά απαιτεί χρόνο και κόπο, αν δεν υπάρχει μία τεχνική διασύνδεσης αυτών των συστημάτων. Για παράδειγμα, προκειμένου να αποκτήσει κάποιος άδεια άσκησης επαγγέλματος, απαιτείται μία σειρά από πιστοποιητικά από διαφορετικούς φορείς: ποινικό μητρώο, βεβαιώσεις ασφαλιστικού φορέα, κλπ. Η συναλλαγή των πολιτών με καθένα από τα διαφορετικά συστήματα των αρμοδίων φορέων, είναι μία χρονοβόρα διαδικασία και συχνά πολύπλοκη. Στην περίπτωση των διασυνδεδεμένων συστημάτων, είναι εφικτό από έναν από τους διασυνδεδεμένους οργανισμούς να ολοκληρωθούν οι αναγκαίες διαδικασίες.
Ωστόσο, το εγχείρημα αντιμετωπίζει μία σειρά από εμπόδια:

- Τα προβλήματα διαχείρισης ασφάλειας γίνονται εξαιρετικά πολύπλοκα, αφού απαιτείται η διαχείριση πολύ μεγάλου αριθμού χρηστών, με διαφορετικές απαιτήσεις ασφάλειας σε κάθε οργανισμό, ενώ υπάρχει και ένας σημαντικός αριθμός πόρων που μπορούν να θεωρηθούν ως ευαίσθητα και θα μπορούσαν να αποτελέσουν στόχο κακόβουλων επιθέσεων, ειδικά στην περίπτωση που υπάρχει δυνατότητα πρόσβασης και από τρίτους ρόλους, εκτός οργανισμού. Υπό μία οπτική, δηλαδή, οι στόχοι της διασύνδεσης συστημάτων είναι αντιφατικοί: αφενός είναι επιθυμητός ο διαμοιρασμός δεδομένων όπου αυτό είναι αναγκαίο, αφετέρου είναι σκόπιμο να περιορίζονται στο ελάχιστο τα δικαιώματα πρόσβασης.
- Ένα άλλο πρόβλημα αφορά στον τρόπο με τον οποίο θα καταστεί εφικτή η ανάκτηση πόρων σε περιβάλλοντα συνασπιζόμενων Π.Σ. (Information Systems coalition environments). Κάθε σύστημα χρησιμοποιεί δικό του τρόπο αρχειοθέτησης, διαφορετικές κωδικοποιήσεις, συνεπώς είναι αναγκαίο να υπάρχει ένας μηχανισμός ικανός να αναζητήσει με το ελάχιστο δυνατό κόστος για το χρήστη, τους αναγκαίους πόρους στο κατανεμημένο περιβάλλον.

1.3 Εφαρμογές των αποτελεσμάτων της έρευνας στην καθημερινή ζωή

Η αξιοποίηση των αποτελεσμάτων της διατριβής σε διαφορετικούς τομείς της ανθρώπινης δραστηριότητας μπορεί να συνεισφέρει στην αύξηση της αποδοτικότητας και σε καλύτερη ποιότητα παροχής υπηρεσιών των οργανισμών. Το κυριότερο όφελος είναι η δυνατότητα πρόσβασης στο σύνολο του όγκου των πληροφοριών που χαρακτηρίζουν ένα κλιμακούμενο αριθμό οργανισμών, μέσα σε μικρό χρονικό διάστημα και με διαφανή στο χρήστη τρόπο (transparently). Αναλυτικότερα, μία σειρά από τομείς στους οποίους η συνεισφορά της διατριβής μπορεί να επιφέρει σημαντική βελτίωση, είναι οι ακόλουθοι:



Εικόνα 1.1 Κατανεμημένα συστήματα διαχείρισης γνώσης – γενική θεώρηση.

1.3.1 Περιβάλλοντα ηλεκτρονικής διακυβέρνησης (e-Government)

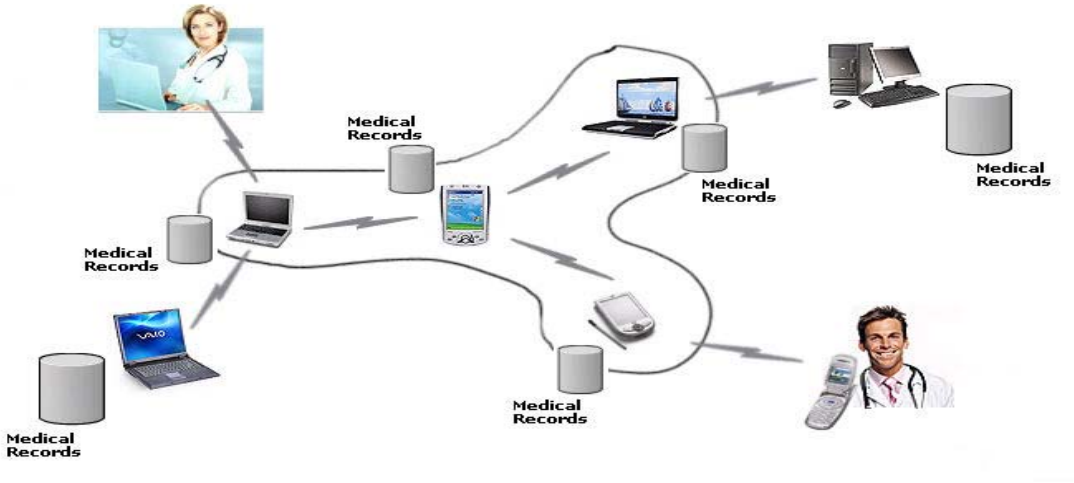
Η διασύνδεση των οργανισμών του δημόσιου τομέα μεταξύ τους (Government-to-Government), καθώς και η διασύνδεση με οργανισμούς και επιχειρήσεις του ιδιωτικού τομέα (Government-to-Business and Business-to-Government), μπορεί να αυξήσει σημαντικά την αποδοτικότητα των συμμετεχόντων οργανισμών, των παρεχόμενων υπηρεσιών προς τον πολίτη, αλλά και τους χρόνους απόκρισης των οργανισμών. Στη μέχρι σήμερα επικρατούσα κατάσταση, η ολοκλήρωση μίας συναλλαγής πολλές φορές περιλαμβάνει αναζήτηση πληροφοριών από διαφορετικούς οργανισμούς. Συνήθως ο μηχανισμός αναζήτησης, ακόμη και αν υποβοηθάται ηλεκτρονικά, δεν λειτουργεί αυτοματοποιημένα, δηλαδή απαιτεί την επικοινωνία των εμπλεκομένων μερών σε κάθε οργανισμό, την επιβεβαίωση της ταυτότητας του

καθενός και κατόπιν την ολοκλήρωση της διαδικασίας που αφορά τα εμπλεκόμενα μέρη. Στην περίπτωση της ολοκληρωμένης διασύνδεσης μεταξύ συστημάτων ηλεκτρονικής διακυβέρνησης, θα υπάρχει η δυνατότητα ακόμη και αν κάποιος λειτουργός δεν ανήκει σε κάποιον οργανισμό να μπορεί υπό προϋποθέσεις να εκτελεί συγκεκριμένα καθήκοντα σε άλλον οργανισμό, υπό την αίρεση βεβαίως αντίστοιχης εξουσιοδότησης και μόνον αυτά που απαιτούνται για την ολοκλήρωση της διαδικασίας. Για παράδειγμα, ένας υπάλληλος στην υπηρεσία έκδοσης αδειών εργασίας θα μπορεί να έχει πρόσβαση στα στοιχεία ποινικού μητρώου και με διαβάθμιση τέτοια ώστε να επιτρέπεται η ταχύτερη και με ασφαλή τρόπο εκτέλεση της διαδικασίας προς όφελος του πολίτη.

1.3.2 Διασυνδεδεμένα Ιατρικά Πληροφοριακά Συστήματα

Η μετακίνηση των ασθενών σε διαφορετικά νοσοκομεία, ειδικά αυτών που πάσχουν από χρόνιες παθήσεις, οδηγεί στη δημιουργία ενός κατακερματισμένου ιατρικού φακέλου που περιέχει το ιστορικό κάθε ασθενούς. Η αναζήτηση και ανάκτηση των δεδομένων που αφορούν στον ίδιο ασθενή από διαφορετικά συστήματα είναι μία πολύ σημαντική δυνατότητα (Gritzalis et al, 1999). Για παράδειγμα, στα πλαίσια των καθηκόντων του, ένας γιατρός ενδέχεται να διαθέτει διαφορετικούς ρόλους σε διαφορετικές μονάδες. Ένας χειρουργός μπορεί να εργάζεται στα εξωτερικά ιατρεία ενός νοσοκομείου και κάποια απογεύματα ως υπεύθυνος της μονάδας άμεσης βοήθειας. Στα πλαίσια της εκτέλεσης των διαφορετικών καθηκόντων του θα ήταν εξαιρετικά σημαντικό να έχει αναπτυχθεί και να αξιοποιείται ένας μηχανισμός ώστε στην περίπτωση της υπηρεσίας του σε μία από τις δύο θέσεις να μπορέσει να έχει εύκολη και άμεση πρόσβαση στα αρχεία της άλλης μονάδας που υπηρετεί, ώστε να είναι σε θέση να παρέχει υψηλότερου επιπέδου υπηρεσίες. Συχνά στη μονάδα εκτάκτων περιστατικών καταφθάνουν ασθενείς σε κατάσταση σύγχυσης ή με μερική απώλεια αισθήσεων. Στις περιπτώσεις αυτές καθίσταται εξαιρετικά κρίσιμο να μπορέσει ο γιατρός να έχει πρόσβαση σε πολύ σύντομο χρονικό διάστημα στο ιατρικό ιστορικό του ασθενούς. Λόγω ωστόσο του ευαίσθητου χαρακτήρα των προσωπικών δεδομένων ιατρικού χαρακτήρα καθίσταται προφανές πως η πραγμάτωση μίας τέτοιας διαδικασίας υπόκειται σε πολλούς προορισμούς ασφάλειας, που βεβαίως επιβάλλονται και από το υφιστάμενο νομοθετικό πλαίσιο. Προκειμένου να ληφθούν υπόψη τα ιδιαίτερα χαρακτηριστικά ενός συστήματος αποτελούμενου από συνεργαζόμενα ιατρικά αυτόνομα συστήματα, απαιτούνται ειδικές τεχνικές διαχείρισης ασφάλειας, τόσο σε επίπεδο επιβολής ελέγχων πρόσβασης όσο και χρήσης ειδικών κρυπτογραφικών τεχνικών (Gritzalis et al, 2006).

1.3.3 Ασύρματα διασυνδεδεμένα περιβάλλοντα ειδικού σκοπού



Εικόνα 1.2 Ασύρματα διασυνδεδεμένα ιατρικά περιβάλλοντα

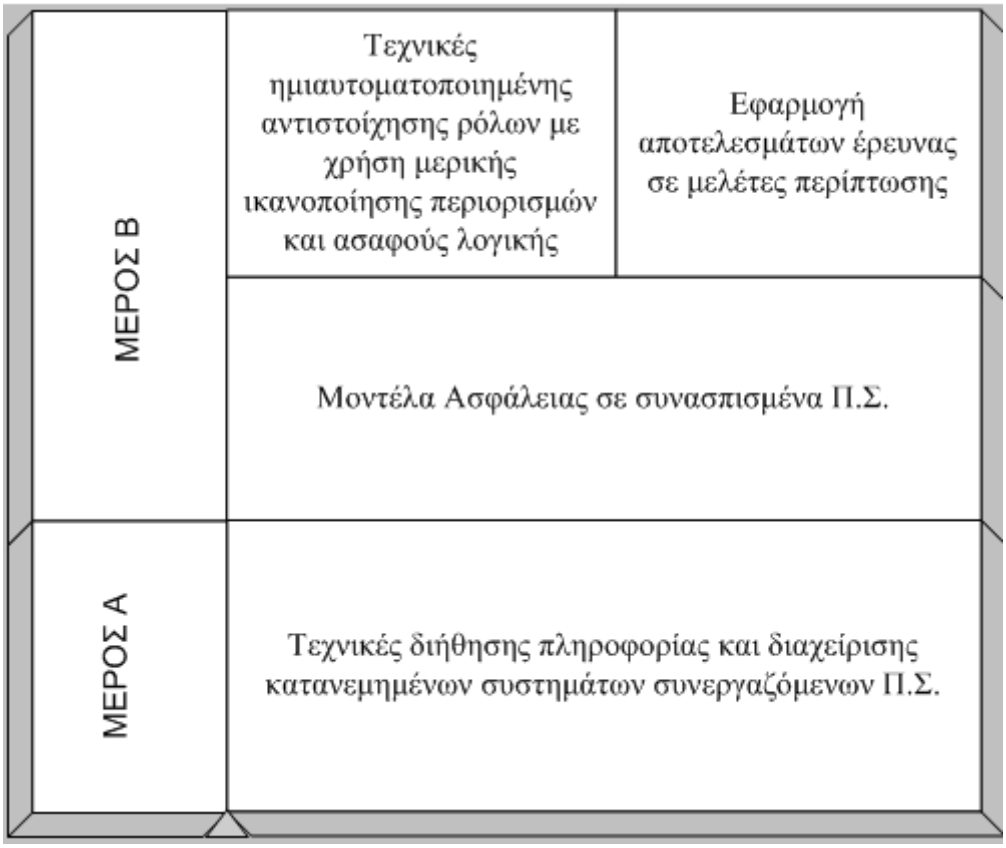
Η διείσδυση νέων τεχνολογιών στην καθημερινή ζωή δημιούργησε πρόσθετες δυνατότητες για επεξεργασία και ανταλλαγή πληροφοριών. Χαρακτηριστικό παράδειγμα αποτελεί η ανάπτυξη ασύρματων τεχνολογιών και η δημιουργία νέου τύπου περιβαλλόντων, όπως δικτύων ειδικού σκοπού (ad-hoc networks) και περιβαλλόντων διεισδυτικού υπολογίζειν (pervasive computing environments). Τα τελευταία χρόνια τα παραπάνω παραδείγματα κερδίζουν διαρκώς έδαφος, καθώς ολοένα αυξάνεται ο αριθμός φορητών συσκευών και γίνεται διαρκώς πιο δημοφιλής η χρήση τους. Στα κυριότερα χαρακτηριστικά των παραπάνω περιβαλλόντων μπορούμε να διακρίνουμε το χαμηλό τους κόστος και τη σχετικά εύκολη χρήση τους, καθώς και την έλλειψη κεντρικής διαχείρισης που επιτρέπει μεγάλο βαθμό αυτονομίας στους χρήστες (Malatras et al, 2005a, 2005b). Η δημιουργία ασύρματων διασυνδεδεμένων περιβαλλόντων εισάγει νέες δυνατότητες για την ανταλλαγή και επεξεργασία δεδομένων με πολλαπλές εφαρμογές: για παράδειγμα, η δημιουργία ασύρματα διασυνδεδεμένων ιατρικών περιβαλλόντων (Εικ. 1.2) δίνει τη δυνατότητα της παροχής υπηρεσιών υγείας σε πολύ συντομότερο χρόνο και απευθείας στο περιβάλλον νοσηλείας καθώς το εξουσιοδοτημένο νοσηλευτικό προσωπικό μπορεί να έχει πρόσβαση στην αναγκαία πληροφορία από οποιοδήποτε σημείο και αν βρίσκεται σε μία κλινική. Τα προβλήματα που σχετίζονται με την ομαλή και ασφαλή λειτουργία τέτοιων περιβαλλόντων αναπτύσσονται στο κεφάλαιο 5, με βάση και τα συμπεράσματα που καταγράφονται στις εργασίες (Belsis et al, 2005d) (Belsis et al, 2005g) (Malatras et al, 2005a) (Malatras et al, 2005b).

1.4 Συνεισφορά της παρούσας έρευνας

Η παρούσα διατριβή επιχειρεί να δημιουργήσει ένα πλαίσιο διαχείρισης σε κατανεμημένα περιβάλλοντα συνασπιζόμενων αυτόνομων Π.Σ. (Distributed environments of coalitions of autonomous Information Systems) εστιάζοντας κατά κύριο λόγο στη διαχείριση της ασφάλειας.
Στο πλαίσιο αυτό, δύο βασικά επιστημονικά ερωτήματα ανακύπτουν:
α) Πώς μπορεί να ενισχυθεί το υπάρχον πλαίσιο διαχείρισης και αξιοποίησης πληροφορίας από κατανεμημένα συνασπισμένα Π.Σ.
β) Ποια προβλήματα ασφάλειας ανακύπτουν σε ένα τέτοιο περιβάλλον διαφορετικών πολιτικών και πώς μπορούν να ενοποιηθούν οι συγκεκριμένες πληροφοριακές υποδομές, δημιουργώντας ταυτόχρονα ένα πλαίσιο ασφαλούς ανάκτησης και

ανταλλαγής πληροφοριών, επιβαρύνοντας στο ελάχιστο δυνατό την πολυπλοκότητα της διαχείρισης της ασφάλειας.
Στα πλαίσια αυτά, η συνεισφορά της διατριβής μπορεί κατ' αρχάς να χωριστεί σε δύο κύριους άξονες, με διαφορετική βαρύτητα:

- ο ελάσσονος σημασίας άξονας, στον οποίο μελετώνται οι τεχνικές που θα μπορέσουν να αυξήσουν την αποδοτικότητα ενός πλαισίου ενοποιημένων βάσεων γνώσης σε περιβάλλον διαφορετικών Π.Σ.
- ο μείζονος σημασίας άξονας, στον οποίο εστιάζει η διατριβή στα προβλήματα ασφάλειας που ανακύπτουν από τη συνύπαρξη και ταυτόχρονη ανταλλαγή πληροφοριών μεταξύ ενός κλιμακούμενου αριθμού Π.Σ. με διαφορετικές πολιτικές ασφάλειας



Εικόνα 1.3 Σχηματική αναπαράσταση τομέων συνεισφοράς διατριβής

Πιο συγκεκριμένα, η συνεισφορά της διατριβής μπορεί να καταγραφεί στα εξής:

Στα πλαίσια του πρώτου ερωτήματος, σε σχέση με την αποτελεσματικότερη αξιοποίηση των δυνατοτήτων ενός κατανεμημένου περιβάλλοντος συνεργαζόμενων Π.Σ. προτείνονται τεχνικές και τεχνολογίες που συνεισφέρουν στην αποτελεσματικότερη διαχείριση των πόρων του συστήματος. Παράλληλα, αντιμετωπίζεται ο ρόλος κατανεμημένων εφαρμογών και προηγμένων διεπαφών στην ανάπτυξη συστημάτων διαχείρισης γνώσης (Belsis et al, 2004a) (Belsis et al, 2005e), μελετώνται οι ερευνητικής και τεχνικής φύσεως προκλήσεις για ενοποίηση βάσεων γνώσης και προκειμένου για την υλοποίηση κατανεμημένων συστημάτων διαχείρισης γνώσης (Belsis et al, 2004b), (Belsis et al, 2005e), μελετάται το πρόβλημα της ταξινόμησης της πληροφορίας με συγκεκριμένα κριτήρια, κάτι που επιτρέπει ως δυνατότητα τη διήθηση ανεπιθύμητης πληροφορίας, που συχνά εντοπίζεται με τη μορφή θορύβου στις προσπάθειες ανάκτησης πληροφορίας. Στα υπάρχοντα πλαίσια

έχει ήδη καταγραφεί στη διεθνή βιβλιογραφία ο ρόλος των τεχνικών μηχανικής μάθησης (machine learning) με αποδοτικότερες έως τώρα τις Bayesian τεχνικές. Στις εργασίες (Belsis et al, 2006a) (Belsis et al, 2006d) προτείνεται μία εναλλακτική τεχνική και τεκμηριώνονται πειραματικά τα σημεία υπεροχής της προτεινόμενης τεχνικής έναντι των ήδη υπαρχουσών.

Στα πλαίσια της ενασχόλησης με το δεύτερο επιστημονικό ερώτημα, και αφού καταγραφεί το εννοιολογικό πλαίσιο διασύνδεσης των γνωστικών περιοχών Διαχείρισης Γνώσης και Ασφάλειας Πληροφοριακών Συστημάτων (Belsis et al, 2005a), η κύρια συνεισφορά της διατριβής μπορεί να συνοψιστεί στα εξής:

- Υιοθετούνται λύσεις που αφορούν στον έλεγχο πρόσβασης σε κατανεμημένα συστήματα συνεργαζόμενων Π.Σ και στη διαχείριση κατανεμημένων βάσεων γνώσης (Belsis et al, 2005b), (Belsis et al, 2005c).
- Προτείνεται μία αποτελεσματική λύση για την αντιστοίχηση ρόλων ανάμεσα σε διαφορετικά Π.Σ. ενώ το πρόβλημα της αντιστοίχησης και διασύνδεσης πολιτικών ασφάλειας ανάγεται σε πρόβλημα αντιστοίχησης-απεικόνισης οντολογιών (Belsis et al, 2005f) (Belsis et al, 2005g) (Belsis et al, 2005h) (Malatras et al, 2005b). Προκειμένου για την επίτευξη διαλειτουργικού (interoperable) τρόπου διασύνδεσης διαφορετικών πολιτικών ασφάλειας, εισάγεται η έννοια του κατανεμημένου μητρώου διαχείρισης συνασπισμού Π.Σ. (Distributed Coalition Management Registry) (Belsis, 2006e), (Belsis et al, 2006c) (Malatras et al, 2005b) (Malatras et al, 2005a). Στις εργασίες (Malatras et al, 2005b) και (Malatras et al, 2005a) η συνεισφορά της παρούσας διατριβής έγκειται στην επίλυση των προβλημάτων ασφάλειας σε ad-hoc δίκτυα με την εισαγωγή των αντιστοιχήσεων ρόλων (role mappings) καθώς και της περιγραφής του κατανεμημένου μηχανισμού επιβολής ελέγχων πρόσβασης που καθιστά εφικτή τη διασύνδεση των περιοχών διαφορετικών πολιτικών.
- Στα πλαίσια μιας ευέλικτης αναπαράστασης ρόλων και δικαιωμάτων προτείνεται η υιοθέτηση μιας πρότυπης γλώσσας εφαρμογής ελέγχων πρόσβασης, ενώ προκειμένου να αναπαρασταθούν πιο ευέλικτα οι συσχετίσεις μεταξύ ρόλων σε διαφορετικά επίπεδα της ιεραρχίας προτείνεται μια αναπαράσταση ρόλων γλώσσα περιγραφής πολιτικής ανώτερου επιπέδου, με χρήση τεχνολογιών σημασιολογικής αναπαράστασης (Belsis et al, 2005h).
- Προτείνονται μικρής κλίμακας τροποποιήσεις - επεκτάσεις στο βασισμένο σε ρόλους μοντέλο ελέγχου πρόσβασης (Role Based Access Control Model – RBAC) που επιτρέπουν την απεικόνιση χρονικής περιοδικότητας στην περιγραφή των ρόλων και στον καθορισμό παραμέτρων σχετιζόμενων με το περιβάλλον δραστηριοποίησης των ρόλων (Belsis et al, 2005h) (Belsis et al, 2005g).
- Επεκτείνεται το πλαίσιο διαπραγμάτευσης πολιτικών και προτείνεται ένα μοντέλο και ένα αντίστοιχο μαθηματικό πλαίσιο που επιτρέπει την εφαρμογή τεχνικών ημι-αυτοματοποιημένης διαχείρισης του περιβάλλοντος πολλαπλών πολιτικών (Belsis et al, 2006b) (Belsis, 2006e).
- Εισάγεται ένα μοντέλο επίλυσης συγκρούσεων (conflicts resolution model) χαμηλής κρισιμότητας σε περιβάλλοντα πολλαπλών πολιτικών, καθώς και ένας αντίστοιχος μαθηματικός φορμαλισμός βασισμένος στη χρήση ασαφούς λογικής (fuzzy logic) (Belsis et al, 2006c).
- Στην περίπτωση που είναι επιθυμητή η απόκρυψη κρίσιμων πληροφοριών της πολιτικής ασφάλειας υιοθετείται η πρακτική της μετατροπής της XML

αναπαράστασης πολιτικής σε σχεσιακή μορφή με αυτοματοποιημένο τρόπο, ώστε να είναι δυνατή η κλιμάκωση (Belsis et al, 2005f).

- Επιχειρείται η υλοποίηση των παραπάνω σε συγκεκριμένες μελέτες περίπτωσης: σε περιβάλλοντα πανταχού και διεισδυτικού υπολογίζειν (Ubiquitous and Pervasive computing) (Malatras et al, 2005a) (Malatras et al, 2005b) και σε ιατρικά ασύρματα συνδεδεμένα συνεργαζόμενα περιβάλλοντα πολλαπλών πολιτικών (Belsis et al, 2005d) (Belsis et al, 2005g) όπου περιγράφεται η έννοια των απεικονίσεων πολιτικών και των εικονικών οντολογικά αναπαριστώμενων δικτύων (Virtual Ontology Networks – VONs). Παράλληλα, επεκτείνεται η εφαρμογή των συμπερασμάτων των παραπάνω εργασιών σε συνδυασμό με τη χρήση κρυπτογράφησης για τη διαφύλαξη της αρχής της εμπιστευτικότητας σε ευαίσθητα ιατρικά περιβάλλοντα όπως περιγράφεται στην εργασία (Gritzalis et al, 2006).

1.5 Δομή της διατριβής

1.5.1 Περιγραφή των περιεχόμενων της διατριβής

Η παρούσα διατριβή αποτελείται από δύο μέρη και οκτώ κεφάλαια. Στο πρώτο μέρος εισάγεται η προβληματική και τα κίνητρα που οδήγησαν στην εκπόνηση της συγκεκριμένης έρευνας. Στη συνέχεια γίνεται μία συγκριτική επισκόπηση υπαρχουσών ερευνητικών προσεγγίσεων και ταξινομούνται ανά κατηγορία οι συναφείς ερευνητικές εργασίες της διεθνούς βιβλιογραφίας. Ακολούθως περιγράφονται οι λύσεις που προτείνονται στα πλαίσια της εργασίας σχετικά με τη δυνατότητα δημιουργίας ενός αποδοτικού συστήματος ταξινόμησης εγγράφων και διήθησης της πληροφορίας.

Στο δεύτερο μέρος αναπτύσσεται το πρόβλημα της ασφάλειας σε δυναμικά σχηματιζόμενους συνασπισμούς αυτόνομων Π.Σ. Αναπτύσσονται οι λύσεις που προτείνονται στα πλαίσια της διατριβής και που αφορούν στην αντιστοίχηση ρόλων μεταξύ διαφορετικών μοντέλων ασφάλειας κάθε οργανισμού (Belsis et al, 2005h) (Belsis et al, 2005d) (Belsis et al, 2005g) (Malatras et al, 2005a) (Malatras et al, 2005b). Παράλληλα περιγράφονται οι προτεινόμενες τεχνικές για τη δυνατότητα σημασιολογικής αναπαράστασης ρόλων καθώς και οι προτεινόμενες τεχνικές για το πρόβλημα της απόκρυψης του συνόλου της πολιτικής των συμμετεχόντων μερών σε περιβάλλοντα που χαρακτηρίζονται από έλλειψη εμπιστοσύνης (Belsis et al, 2005f).

Περιγράφονται εφαρμογές των προτεινόμενων λύσεων σε συγκεκριμένες μελέτες περίπτωσης (Belsis et al, 2005d) (Belsis et al, 2005e) (Belsis et al, 2005g) (Malatras et al, 2005a) (Malatras et al, 2005b) (Gritzalis et al, 2006). Στη συνέχεια αναπτύσσεται το μαθηματικό υπόβαθρο που αναπτύσσεται στα πλαίσια της παρούσας διατριβής και αφορά στην δημιουργία ενός ημι-αυτοματοποιημένου πλαισίου διαχείρισης προκειμένου για την ελάττωση της επέμβασης των διαχειριστών του συστήματος. Παράλληλα δημιουργείται ένα πλαίσιο επίλυσης πολιτικών συγκρούσεων με βάση τη χρήση ασαφούς λογικής. Στο τέλος του δευτέρου μέρους παρουσιάζεται μία υλοποίηση που ενσωματώνει τις προτεινόμενες λύσης στο θέμα της επιβολής ελέγχων πρόσβασης σε περιβάλλοντα πολλαπλών πολιτικών (Belsis et al, 2006b) (Belsis et al, 2006c).

1.5.2 Συνοπτική περιγραφή περιεχομένων και συνεισφοράς ανά κεφάλαιο

Στο κεφάλαιο 1 περιγράφεται το αντικείμενο, οι στόχοι, η συνεισφορά και η δομή της διατριβής.
Στο κεφάλαιο 2 επισκοπούνται συναφείς ερευνητικές εργασίες και περιγράφονται συγκριτικά οι διαφορές με την προσέγγιση που ακολουθείται στην παρούσα διατριβή.
Στο κεφάλαιο 3 παρουσιάζεται η προτεινόμενη λύση προκειμένου για την αποτελεσματική κατηγοριοποίηση των γνωσιακών πόρων των συμμετεχόντων οργανισμών σε διαφορετικές θεματικές κατηγορίες-κλάσεις και παρουσιάζονται συγκριτικά με άλλες προσεγγίσεις τα πειραματικά αποτελέσματα που αποδεικνύουν την ανωτερότητά της.
Στο κεφάλαιο 4 αναλύονται οι τεχνικές που επιτρέπουν τη σημασιολογική απεικόνιση των πολιτικών καθώς και την αναπαράσταση συσχετίσεων μεταξύ ρόλων με χρήση τεχνολογιών σημασιολογικού ιστού, αναλύεται η τεχνική της αντιστοίχησης ρόλων και η υλοποίησή της με χρήση διαλειτουργικών τεχνολογιών, ενώ παρουσιάζεται μία λύση που επιτρέπει τη διαπραγμάτευση πολιτικών με απόκρυψη κρίσιμων πληροφοριών προκειμένου για την εφαρμογή της σε περιβάλλοντα που υπάρχει έλλειψη εμπιστοσύνης μεταξύ των μερών.
Στο κεφάλαιο 5 περιγράφονται, στο πρώτο μέρος μία σειρά από μελέτες περίπτωσης στις οποίες εφαρμόζονται οι προτεινόμενες τεχνικές ελέγχου πρόσβασης σε συνασπισμούς αυτόνομων Π.Σ. ενώ στο δεύτερο μέρος του κεφαλαίου αναπτύσσεται το πλαίσιο ημι-αυτοματοποιημένης διαχείρισης και ο αντίστοιχος φορμαλισμός που χρησιμοποιείται, βασισμένος στη χρήση χαλαρών περιορισμών (soft constraints).
Στο κεφάλαιο 6 αναπτύσσεται το πλαίσιο επίλυσης συγκρούσεων μεταξύ πολιτικών σε περιβάλλοντα συνασπισμών Π.Σ. με χρήση τεχνικών μερικής ικανοποίησης περιορισμών και με χρήση ασαφούς λογικής (fuzzy logic). Παράλληλα αναπτύσσεται η αρχιτεκτονική που επιτρέπει την ενσωμάτωση του μηχανισμού λήψης αποφάσεων στο σύστημα διαχείρισης πολιτικής ασφάλειας.
Στο κεφάλαιο 7 περιγράφονται τα τεχνικά χαρακτηριστικά του συστήματος που υλοποιήθηκε προκειμένου για τη διαχείριση και επιβολή πολιτικών ασφάλειας και την εφαρμογή ελέγχου πρόσβασης, ενώ περιγράφεται η λειτουργία του πιλοτικού συστήματος που ενσωματώνει τις αρχές που περιγράφηκαν σε προηγούμενα κεφάλαια.
Στο κεφάλαιο 8 αναπτύσσονται τα συμπεράσματα και προτείνονται κατευθύνσεις μελλοντικής έρευνας.

ΜΕΡΟΣ	Κεφάλαια	Συμβολή
ΜΕΡΟΣ Α	Κεφάλαιο 1	Αντικείμενο, οι στόχοι, η συνεισφορά και η δομή της διατριβής.
	Κεφάλαιο 2	Κριτική επισκόπηση συναφών ερευνητικών εργασιών από τη διεθνή βιβλιογραφία
	Κεφάλαιο 3	Τεχνικές αυτοματοποιημένης κατηγοριοποίησης γνωσιακών πόρων
ΜΕΡΟΣ Β	Κεφάλαιο 4	Σημασιολογική απεικόνιση ρόλων σε πολιτικές ασφάλειας Δημιουργία πλαισίου αντιστοίχησης ρόλων Απόκρυψη πολιτικών ασφάλειας σε περιβάλλοντα με έλλειψη εμπιστοσύνης
	Κεφάλαιο 5	Εφαρμογή σε μελέτες περίπτωσης Ανάπτυξη πλαισίου ημι-αυτοματοποιημένης διαχείρισης ασφάλειας
	Κεφάλαιο 6	Μοντέλο επίλυσης συγκρούσεων με χρήση μερικής ικανοποίησης περιορισμών και ασαφούς λογικής
	Κεφάλαιο 7	Περιγραφή λειτουργιών πρωτοτύπου
	Κεφάλαιο 8	Συμπεράσματα – προτάσεις για μελλοντική έρευνα

Πίνακας 1.1 Περιεχόμενα της διατριβής ανά κεφάλαιο

ΚΕΦΑΛΑΙΟ 2 - Επισκόπηση ερευνητικού πεδίου

Αφετηρία κάθε αναφοράς σε θέματα ασφάλειας αποτελούν οι τρεις θεμελιώδεις έννοιες της *εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας* (ISO 17799). Προκειμένου να επιτευχθεί η διαφύλαξη των βασικών αυτών ιδιοτήτων, κύρια χρησιμοποιούμενες τεχνικές είναι αυτές του ελέγχου πρόσβασης και της αυθεντικοποίησης. Τις τελευταίες δεκαετίες, έχουν αναπτυχθεί μια σειρά από μοντέλα, άλλα με έμφαση στο φορμαλισμό και άλλα με περισσότερο πρακτική διάσταση, με στόχο την εξυπηρέτηση των βασικών απαιτήσεων ασφάλειας.
Στο παρόν κεφάλαιο περιγράφονται μια σειρά από ερευνητικές προσπάθειες, χωρισμένες σε θεματικές ενότητες ανάλογα και με τους διαφορετικούς τομείς συνεισφοράς της διατριβής. Στην πρώτη ενότητα του παρόντος κεφαλαίου γίνεται αναφορά σε παλαιότερα μοντέλα ασφάλειας, τα οποία αν και δεν χρησιμοποιούνται ευρέως διατηρούν μια εξέχουσα θέση στη σχετική βιβλιογραφία (κυρίως λόγω του ότι δεν έχει υπάρξει ένα καθολικά αποδεκτό πρότυπο που να καλύπτει όλες τις θεμελιώδεις απαιτήσεις ασφάλειας), αλλά και λόγω του ότι κάθε μοντέλο αποσκοπεί στην εξυπηρέτηση ενός στόχου κατά προτεραιότητα (άλλα μοντέλα δίνουν κυρίως έμφαση στη διαφύλαξη της εμπιστευτικότητας, ενώ άλλα στη διαφύλαξη της ακεραιότητας).
Στα πλαίσια της διατριβής μας ενδιαφέρει και η συσχέτιση των παραπάνω μοντέλων με τη θεωρία δικτυωμάτων (lattice theory), στοιχεία της οποίας αξιοποιούνται και στο φορμαλισμό που εισάγεται στα κεφάλαια 5 και 6 και που αφορά στο κομμάτι της βελτιστοποίησης του συστήματος διαχείρισης πολλαπλών πολιτικών με χρήση χαλαρών περιορισμών (soft constraints), όσο και στο κομμάτι του μοντέλου επίλυσης συγκρούσεων (conflict resolution model) με χρήση ασαφούς λογικής (fuzzy logic).

2.1 Μοντέλα ελέγχου πρόσβασης

2.1.1 Μοντέλα ελέγχου πρόσβασης υποχρεωτικής διαβάθμισης - Mandatory Access Control (MAC) models

Το μοντέλο των Bell και LaPadula είναι από τα πρώτα μοντέλα που εμφανίστηκαν χρονολογικά και που αφορούν στον έλεγχο πρόσβασης. Από την πρώτη θεμελίωση του μοντέλου έχουν εμφανιστεί μια σειρά από παραλλαγές του, με αποτέλεσμα να υπάρχει μία σύγχυση γύρω από το σύνολο των αρχών που διέπουν το μοντέλο, ωστόσο σε όλες τις παραλλαγές του οι γενικές αρχές παραμένουν οι ίδιες.
Στο ιεραρχικό μοντέλο τύπου Bell LaPadula (καθώς επίσης και στις παραλλαγές του) εισάγονται μια σειρά από διαφορετικά επίπεδα διαβάθμισης (εμπιστευτικό, απόρρητο, άκρως απόρρητο). Στο μοντέλο αυτό εισάγεται μια κατηγοριοποίηση κατά επίπεδα χρηστών και αντικειμένων. Στην εργασία του Shandhu (Shandhu 93) εισάγεται ένα μοντέλο που ενθυλακώνει τις βασικές έννοιες της αρχικής έκδοσης, καλύπτοντας παράλληλα ορισμένες αδυναμίες του. Σύμφωνα με το μοντέλο αυτό, για κάθε υποκείμενο s και για κάθε αντικείμενο ο εισάγεται μια κατηγοριοποίηση λ(s) και λ(ο) αντίστοιχα. Έτσι σχηματίζεται με μια σχέση ολικής διάταξης ‘‘≤’’, ένα δικτύωμα. Το κύριο μέλημα των τύπου MAC μοντέλων είναι η διαφύλαξη της εμπιστευτικότητας, κυρίως λόγω του πεδίου εφαρμογής τους, που είχε ως αφετηρία στρατιωτικά και κυβερνητικά περιβάλλοντα. Δύο είναι οι βασικές αρχές που το χαρακτηρίζουν:

- η ιδιότητα no-read-up: ένα υποκείμενο s μπορεί να διαβάσει ένα αντικείμενο ο όταν $\lambda(o) \leq \lambda(s)$
- η ιδιότητα no-write-down (ή *-ιδιότητα): ένα υποκείμενο μπορεί να έχει δικαίωμα εγγραφής γράψει σε ένα αντικείμενο μόνο όταν ισχύει $\lambda(s) \leq \lambda(o)$.

Τυπικά δηλαδή δεν επιτρέπεται βάσει της πρώτης ιδιότητας σε χρήστες να διαβάσουν αντικείμενα υψηλότερης διαβάθμισης, ενώ βάσει της δεύτερης ιδιότητας δεν επιτρέπεται σε προγράμματα να γράφουν σε αντικείμενα με χαμηλότερο βαθμό διαβάθμισης, για να αποτραπεί η πιθανότητα από κακόβουλο λογισμικό (ενεργώντας εν γνώσει ή εν αγνοία του χρήστη) να επιδράσει στο σύστημα. Πολλές φορές σε παραλλαγές του μοντέλου η * ιδιότητα ισχύει και προς τα πάνω, επιτρέποντας τη ροή πληροφορίας μόνο όταν λ(s) = λ(o).

2.1.2 Πολιτικές ελέγχου ροής πληροφοριών (Information flow policies)

Οι πολιτικές ελέγχου ροής πληροφοριών αφορούν στη δυνατότητα μεταφοράς πληροφοριών από μια κλάση ασφάλειας σε άλλη. Θεωρούμε ότι σε κάθε σύστημα, η πληροφορία μεταφέρεται μεταξύ αντικειμένων. Ως αντικείμενο μπορούμε να ορίσουμε οτιδήποτε περιέχει πληροφορία. Τυπικά παραδείγματα αντικειμένων αποτελούν τα αρχεία, οι κατάλογοι αρχείων και οι σχέσεις ή οι πλειάδες σε μια βάση δεδομένων.
Η ροή πληροφορίας ελέγχεται αντιστοιχώντας σε κάθε αντικείμενο μια κλάση. Οποτεδήποτε υπάρχει ροή πληροφορίας από ένα αντικείμενο χ σε ένα αντικείμενο y υπάρχει και μια ροή πληροφορίας από την κλάση στην οποία ανήκει το χ στην κλάση στην οποία ανήκει το y.
Σύμφωνα με τη Denning (Denning 1976) η έννοια της πολιτικής ροής πληροφοριών ορίζεται ως εξής:
Μια τριάδα <SC,→,⊕>, όπου SC είναι ένα σύνολο κλάσεων ασφάλειας, η → όπου $\rightarrow \subseteq SC \times SC$ είναι μια δυαδική σχέση στο SC και η ⊕ (με $\oplus \subseteq SC \times SC$) είναι μια δυαδική σχέση με βάση την πράξη συνδυασμού ή τομής στην SC.
Τα τρία μέλη της παραπάνω σχέσης δεν μπορούν να αλλάξουν. Με βάση τους παραπάνω ορισμούς μπορούν να δημιουργούνται και να καταστρέφονται αντικείμενα δυναμικά, χωρίς ωστόσο να ισχύει κάτι τέτοιο και για τις κλάσεις ασφάλειας.
Συνήθως για λόγους ευκολίας χρησιμοποιούμε ενδοδιατεταγμένο (infix) συμβολισμό: A→B σημαίνει ότι είναι επιτρεπτή η ροή πληροφορίας από το A στο B. Επίσης $(A,B) \notin \rightarrow$ σημαίνει ότι απαγορεύεται η μεταφορά πληροφορίας από το A στο B.
Παράλληλα, ορίζουμε τη σχέση A⊕B=C για τον τελεστή σύνδεσης (join). Ο τελεστής αυτός μας επιτρέπει να ορίζουμε την ροή πληροφορίας από την κλάση A στην κλάση B. Συγκεκριμένα, η σχέση A⊕B=C ορίζει ότι αντικείμενα που περιέχουν πληροφορία από τις κλάσεις A, B θα πρέπει να σημανθούν ως μέλη της κλάσης C.
Στη συνέχεια θα αναφερθούμε εν συντομία στις βασικές αρχές του μοντέλου:
Ορισμοί (αξιώματα):
1. Το σύνολο των SC των κλάσεων ασφάλειας είναι πεπερασμένο
2. Η επιτρεπτή ροή πληροφορίας είναι μια σχέση μερικής διάταξης στο SC
3. Το SC είναι άνω φραγμένο ως προς τη σχέση →
4. Ο τελεστής σύνδεσης είναι ένας ολικά καθορισμένος τελεστής ελάχιστου άνω φράγματος.

Το πρώτο αξίωμα επιτρέπει τη δημιουργία και καταστροφή αντικειμένων δυναμικά, χωρίς περιορισμούς στον αριθμό των δημιουργούμενων αντικειμένων. Το δεύτερο αξίωμα ορίζει ότι η σχέση → είναι σχέση μερικής διάταξης στο SC. Μια μερική διάταξη είναι αντισυμμετρική, μεταβατική και ανακλαστική δυαδική συσχέτιση. Η έννοια της ανακλαστικότητας βασίζεται στην προϋπόθεση ότι μεταξύ της ίδιας κλάσης είναι επιτρεπτή η ροή πληροφορίας. Προκειμένου για τη μεταβατικότητα, είναι προφανές ότι αν A→B και B→C, τότε A→C, δηλαδή θα πρέπει να επιτρέπεται και απευθείας η ροή πληροφορίας ανάμεσα σε δύο κλάσεις, εφόσον επιτρέπεται και

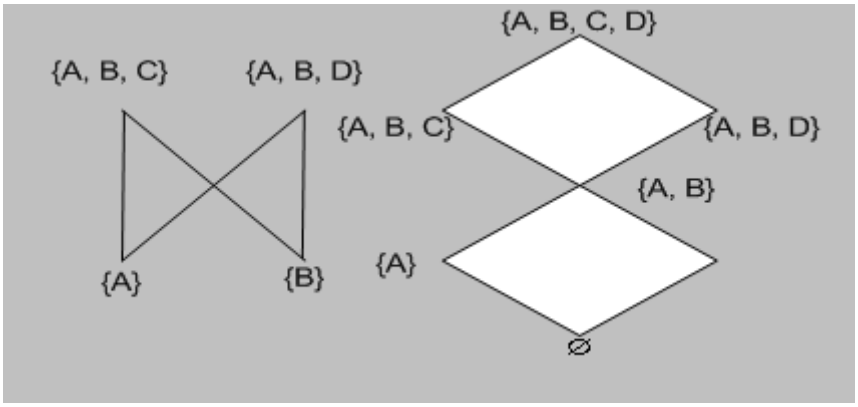
έμμεσα. Η αντισυμμετρικότητα υποδεικνύει ότι αν A→B και B→A τότε A=B. Το τρίτο αξίωμα υποδεικνύει ότι το SC έχει ένα κάτω όριο L, δηλαδή L→A $\forall A \in$ SC. Το αξίωμα αυτό, υποδεικνύει την ύπαρξη ενός επιπέδου αδιαβάθμητης πληροφορίας σε κάθε σύστημα. Το τέταρτο αξίωμα δηλώνει ότι ο τελεστής τομής έχει ένα ελάχιστο άνω φράγμα. Αυτό σημαίνει ότι για όλα τα A, B, C αν ισχύει μια ιδιότητα 1, η οποία ορίζει A→A⊕B και B→A⊕B και μια ιδιότητα 2 που ορίζει ότι A→C και B→C, τότε ισχύει A⊕B→C. Η ιδιότητα 1 εξάγεται από τη βασική λειτουργία του τελεστή τομής. Δηλαδή A⊕B είναι η διαβάθμιση που εξάγεται από τις δύο κλάσεις A και B σαν σύνολο. Επομένως, στην κλάση A⊕B θα πρέπει να επιτρέπεται η μεταφορά πληροφορίας από τις A και B. Αντίστοιχα, προκειμένου για την ιδιότητα 2, αν η πληροφορία επιτρέπεται να μεταφέρεται από την A στη C ή από τη B στη C μεμονωμένα, τότε θα πρέπει να επιτρέπεται να μεταφέρεται και από τις A και B στη C. Σημαντικό επακόλουθο του τέταρτου αξιώματος είναι ότι ο τελεστής τομής μπορεί να εφαρμοστεί σε οποιοδήποτε αριθμό κλάσεων. Επομένως μπορούμε να υπολογίσουμε το $A_1 \oplus A_2 \oplus .. \oplus A_n$ ως το ελάχιστο άνω φράγμα των $\{A_{1..} A_2....A_n\}$.

2.1.3 Μοντέλα προσανατολισμένα σε στρατιωτικά περιβάλλοντα

Το πιο απλό παράδειγμα πολιτικής ροής πληροφορίας εφαρμόζεται όταν η σχέση → είναι σχέση μερικής ή ολικής διάταξης ανάμεσα στις κλάσεις ασφάλειας. Το πιο χαρακτηριστικό παράδειγμα ολικής διάταξης είναι οι κλάσεις TS (top secret) S (secret) C (confidential) U (unclassified), κατηγορίες που συναντώνται σε στρατιωτικού τύπου μοντέλα.

Στην περίπτωση αυτή μπορούμε να θεωρήσουμε τη σχέση υποτέλειας (dominance) ‘‘≤’’ που είναι σχέση ολικής διάταξης αν και μόνο αν η αντίστροφή της → είναι σχέση ολικής διάταξης. Επίσης, δεν υπάρχουν μη συγκρινόμενες κλάσεις, ενώ A⊕B είναι απλά το μέγιστο από τα A και B σε σχέση με τη σχέση ≤. Δηλαδή από δύο κλάσεις A και B επιλέγεται αυτή που ανήκει στην υψηλότερη κλίμακα. Στην πράξη, μπορούμε να εφαρμόσουμε βασικές σχέσεις της θεωρίας δικτυωμάτων προκείμενου για ιεραρχικά μοντέλα. Από δύο ή περισσότερες κλάσεις μπορούμε να σχηματίσουμε ένα δικτύωμα ή ένα υποδικτύωμα (sub-lattice). Έτσι θεωρώντας τρεις κλάσεις A, B και C μπορούμε να συνδυάσουμε τις τρεις με σχέσεις μερικής ή ολικής διάταξης και να προκύψουν επιμέρους δομές που είναι πλήρη ή όχι πλήρη δικτυώματα.

Η επιλογή ενός αυθαίρετου τμήματος δικτυώματος δεν συνιστά απαραίτητα και δικτύωμα από μόνη της. Για παράδειγμα στο σχήμα 2.1α το αναπαριστώμενο υποδικτύωμα δεν συνιστά πλήρες δικτύωμα. Τα άνω φράγματα των A και B είναι μη συγκρίσιμα, για δύο λόγους: α) δεν υπάρχει κατώτερη και ανώτερη κλάση για το σύστημα και β) τα άνω φράγματα των {A} και {B} είναι μη συγκρίσιμα, δηλαδή δεν υπάρχει ελάχιστο άνω φράγμα για τα {A} και {B}. Συμπληρώνοντας ωστόσο με την κατώτερη και την ανώτερη κλάση, μπορούμε να επεκτείνουμε τη μερική διάταξη του σχήματος 2.1α ώστε να προκύψει η διάταξη του σχήματος 2.1β.



Εικόνα 2.1α (αριστερά) Υποδικτύωμα χωρίς μέγιστο και ελάχιστο στοιχείο. 2.1β(δεξιά) Εισαγωγή σχέσης μερικής διάταξης σε δικτύωμα (από Sandhu 93)

Μια τέτοια κατασκευή είναι πάντα εφικτή για οποιαδήποτε μερική διάταξη. Οι παραπάνω διατάξεις συχνά συνδυάζονται, όπως ισχύει στην περίπτωση του στρατιωτικού ή του κυβερνητικού τομέα (όπου η ιεραρχία μπορεί να καθορίζεται από διάφορους περιορισμούς, όπως για παράδειγμα από νομικούς περιορισμούς).
Τα δύο δικτυώματα που αναφέρθηκαν παραπάνω (πλήρη και μη πλήρη) μπορούν συχνά να συνδυαστούν σε ένα. Για παράδειγμα το {TS, A} κυριαρχεί στο {S, A} αλλά δεν μπορεί να συγκριθεί με το {S, B}. Η τομή των δύο επίσης προκύπτει από την τομή των μεμονωμένων συνιστωσών. Π.χ. <TS, A>⊕<S, B>=<TS,{A,B}>. Με χρήση του συνδυασμού μπορούμε να παράγουμε ένα πολύ μεγάλο αριθμό δικτυωμάτων. Στην πράξη μόνο ένα μικρό σύνολο αυτών θα ήταν χρήσιμο. Κυρίως εφαρμογές των παραπάνω δομών εμφανίζονται σε στρατιωτικά και περιβάλλοντα διακυβέρνησης πολλαπλών επιπέδων (MultiLevel – MLS).

2.1.3.1 Το μοντέλο Biba

Κατά πολλούς θεωρείται το δυαδικό του Bell LaPadula. Η βασική του ιδέα είναι ότι η ροή της πληροφορίας δεν θα πρέπει να γίνεται προς τα πάνω στην ιεραρχία. Η βασική μέριμνα του παραπάνω μοντέλου είναι η διαφύλαξη της ακεραιότητας. Αν στο BLP μοντέλο το κύριο ενδιαφέρον έγκειται στη διαφύλαξη της εμπιστευτικότητας, στο Biba κύριο ρόλο αποκτά η ακεραιότητα. Έτσι, η υψηλή ακεραιότητα τοποθετείται στο υψηλότερο σημείο της ιεραρχίας ενώ η χαμηλή στο κατώτερο. Έτσι, η επιτρεπτή κατεύθυνση της πληροφορίας είναι από πάνω προς τα κάτω.
Δύο είναι οι βασικοί έλεγχοι που γίνονται στο Biba:

- Η απλή ακεραιότητα: Το υποκείμενο s έχει δικαίωμα ανάγνωσης στο ω μόνο αν $\omega(s) \leq v(o)$.
- Η ιδιότητα *-ακεραιότητας. Το υποκείμενο έχει δικαίωμα εγγραφής σε ένα αντικείμενο αν $\omega(s) \geq \omega(o)$.

Εάν θελήσουμε να διατηρήσουμε κάποια αντιστοιχία με το BLP μοντέλο, θα πρέπει να τοποθετήσουμε στην κορυφή της ιεραρχίας την χαμηλή ακεραιότητα και στη βάση την υψηλή ακεραιότητα. Η τοποθέτηση μίας κατάστασης στην κορυφή ή στη βάση μπορεί να γίνει κατά σύμβαση. Αυτό που έχει σημασία είναι να οριστεί σωστά η κατεύθυνση επιτρεπτής ανταλλαγής πληροφοριών. Στην περίπτωση που στο κατώτερο σημείο τοποθετηθεί η υψηλή ακεραιότητα, η επιτρεπτή ροή θα πρέπει να γίνει κατά αντίστροφο τρόπο από ότι στο BLP, δηλαδή από πάνω προς τα κάτω. Τυπικά δεν υπάρχει θεμελιώδης διαφορά από το ένα μοντέλο στο άλλο. Το BLP μοντέλο επιτρέπει την ροή πληροφοριών προς τα πάνω, ενώ το Biba προς τα κάτω.

Ένα πρόβλημα προκύπτει στην περίπτωση που είναι επιθυμητή η ταυτόχρονη διαφύλαξη των δύο ιδιοτήτων της ακεραιότητας και της εμπιστευτικότητας, όπου η μόνη επιτρεπτή κατάσταση ροής πληροφορίας θα ήταν ανάμεσα στην ίδια κλάση, απαγορεύοντας οποιαδήποτε ανταλλαγή πληροφορίας μεταξύ διαφορετικών κλάσεων, κυρίως λόγω της αντίθετης φοράς που επιβάλλει το κάθε μοντέλο. Μια προτεινόμενη λύση στο πρόβλημα αυτό, είναι ο χαρακτηρισμός της κάθε κλάσης με βάση την αντιστοίχηση δύο μεταβλητών, μία που θα χαρακτηρίζει την εμπιστευτικότητα και μία για την ακεραιότητα. Έστω $\Lambda=\{\lambda_1,\lambda_2,..,\lambda_v\}$ ένα δικτύωμα που αντιστοιχεί στην εμπιστευτικότητα και $\Omega=\{\omega_1,\omega_2,..,\omega_\kappa\}$ ένα δικτύωμα που αντιστοιχεί στην ακεραιότητα. Υποθέτοντας ότι σε κάθε δικτύωμα η υψηλή εμπιστευτικότητα και η υψηλή ακεραιότητα βρίσκονται στην κορυφή, τότε οι αντίστοιχοι κανόνες ελέγχου πρόσβασης είναι:

- Το υποκείμενο s μπορεί να διαβάσει το αντικείμενο ο μόνο αν $\lambda(s) \geq \lambda(o)$ και $\omega(s) \leq \omega(o)$.
- Το υποκείμενο s μπορεί να γράψει στο αντικείμενο ο, αν $\lambda(s) \leq \lambda(o)$ και $\omega(s) \geq \omega(o)$. Υλοποιήσεις του μοντέλου αυτού έχουν εφαρμοστεί σε λειτουργικά συστήματα, συστήματα βάσεων δεδομένων και δικτύων, προκειμένου να καλύψουν κυρίως τις ανάγκες στρατιωτικών συστημάτων.

2.1.3.2 Πολιτικές σινικού τείχους (Chinese Wall policy)

Προκειμένου να καλυφθούν οι ανάγκες για εμπιστευτικότητα σε περιπτώσεις συνεργασίας, οι Brewer-Nash (1989) εισήγαγαν την πολιτική σινικού τείχους. Χαρακτηριστικό παράδειγμα εφαρμογής του παραπάνω τύπου πολιτικής είναι η περίπτωση εταιρίας παροχής συμβουλευτικών υπηρεσιών σε επιχειρήσεις. Σκοπός της πολιτικής είναι να αποτρέψει την πρόσβαση σε πληροφορίες αντικρουόμενων συμφερόντων. Για παράδειγμα ένας σύμβουλος μπορεί να έχει πρόσβαση στα στοιχεία που αφορούν σε μια εταιρία. Από τη στιγμή που αποκτά το δικαίωμα πρόσβασης, δεν μπορεί να έχει πρόσβαση σε καμία εταιρία αντίστοιχης δραστηριότητας, αφού κάτι τέτοιο θα διακύβευε τα συμφέροντα της μιας από της δύο ή και των δύο. Στο συγκεκριμένο μοντέλο, οι πληροφορίες κατατάσσονται σε διαφορετικές κλάσεις αντικρουόμενων συμφερόντων, μία για κάθε εταιρία. Η πολιτική σινικού τείχους ορίζει ένας σύμβουλος να μην μπορεί να αποκτήσει πρόσβαση σε πληροφορίες που αφορούν μία εταιρία και για περισσότερες από μία εταιρίες σε οποιαδήποτε από τις κλάσεις στις οποίες δυνητικά θα μπορούσε να συμμετέχει.
Παρά την ικανότητα των πολιτικών υποχρεωτικού τύπου που εξετάστηκαν στις προηγούμενες παραγράφους να απεικονίσουν και να ικανοποιήσουν τις απαιτήσεις στρατιωτικών περιβαλλόντων, ωστόσο υπάρχει μια εγγενής αδυναμία να ικανοποιήσουν τις απαιτήσεις ασφάλειας των περισσότερων εμπορικών εφαρμογών και συστημάτων.

2.1.4 Μοντέλα διακριτικού ελέγχου πρόσβασης - Discretionary access control (DAC) models

Τα μοντέλα διακριτικού ελέγχου πρόσβασης (ή τύπου DAC μοντέλα) προέρχονται από τον ακαδημαϊκό χώρο, κυρίως από υλοποιήσεις λειτουργικών συστημάτων. Σε ένα στατικό κόσμο, τα τύπου DAC μοντέλα αντιπροσωπεύουν τα δικαιώματα πρόσβασης ανά πόρο και χρήστη, καταγεγραμμένα με τη μορφή ενός πίνακα πρόσβασης. Η βασική αρχή των μοντέλων αυτών είναι ότι οι χρήστες διατηρούν το δικαίωμα να ορίζουν δικαιώματα σε αντικείμενα των οποίων έχουν την κυριότητα.

Κλασσικό παράδειγμα είναι οι λίστες ελέγχου πρόσβασης, στις οποίες τα αντικείμενα συνδέονται με ένα σύνολο χρηστών ή ομάδων στις οποίες επιτρέπεται η πρόσβαση. Ένα σημαντικό ζήτημα αφορά στην αποθήκευση αυτών των πινάκων που σχηματίζονται, οι οποίοι λόγω του πολύ μεγάλου πλήθους των αντικειμένων και του πολύ μεγάλου αριθμού χρηστών, μπορεί να γίνουν πολύ μεγάλοι ακόμη και αν είναι σχετικά αραιοί (Sandhu and Samarati 1994). Μεταξύ άλλων οι πίνακες:

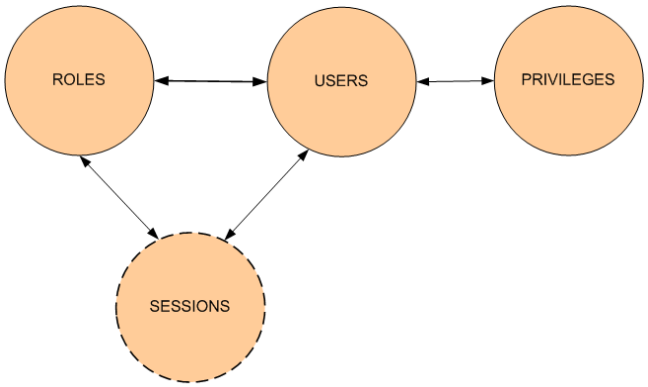
- Μπορεί να φυλάσσονται κατά στήλες, θεωρώντας κάθε στήλη σαν μια λίστα.
- Μπορεί να φυλάσσονται κατά γραμμές. Κάθε γραμμή αντιπροσωπεύει με τη μορφή λίστας τα επιτρεπτά δικαιώματα για κάθε αντικείμενο.
- Μπορεί να φυλάσσονται μόνο τα συμπληρωμένα κελιά μαζί με τη θέση τους στον πίνακα.

Η περιορισμένη δυνατότητα εφαρμογής των παραπάνω μοντέλων, οφείλεται όχι μόνο στα προβλήματα που σχετίζονται με την αποθήκευση της πληροφορίας που αφορά στην έλεγχο πρόσβασης, αλλά κυρίως με την αδυναμία να διαχειριστούν δυναμικά μεταβαλλόμενες καταστάσεις, όπου νέοι χρήστες εισέρχονται στο σύστημα, παλιοί διαγράφονται ενώ στην δεύτερη αυτή περίπτωση, θα πρέπει να αποφασιστεί ποια από τα δικαιώματα που αυτοί οι χρήστες είχαν δημιουργήσει θα παραμείνουν μετά τη διαγραφή τους και ποια όχι. Για το πρόβλημα αυτό του αν η αφαίρεση των δικαιωμάτων που είχε παραχωρήσει ένας χρήστης που διαγράφηκε θα πυροδοτήσει μια αλυσιδωτή ανάκληση δικαιωμάτων από άλλους χρήστες (cascading revocation of rights), έχουν προταθεί διάφορες λύσεις (Bertino et al, 1995) είναι ωστόσο προφανές ότι οι δυνατότητες του μοντέλου να διαχειριστούν μεγάλο αριθμό χρηστών και σε δυναμικά μεταβαλλόμενες συνθήκες είναι εξαιρετικά περιορισμένες.

2.1.5 Μοντέλα ελέγχου βασισμένα σε ρόλους – (Role Based Access Control - RBAC) Models.

Η ιδέα της αντιστοίχησης προνομίων βάσει ρόλων είναι αρκετά παλιά, ωστόσο ολοκληρωμένα εμφανίστηκε για πρώτη φορά στις εργασίες των (Gligor, 1995) και (Sandhu et al, 1996). Τα μοντέλα ελέγχου πρόσβασης που βασίζονται σε ρόλους, καθορίζουν την πρόσβαση που έχουν οι χρήστες σε ένα σύστημα βάσει των υποχρεώσεων και δραστηριοτήτων που τους έχουν ανατεθεί στα πλαίσια του συστήματος. Στο RBAC ένας ρόλος δηλώνεται σαν ένα σύνολο δικαιωμάτων πρόσβασης που συσχετίζεται με μια θέση σε ένα οργανισμό, ή με μία συγκεκριμένη δραστηριότητα που πρέπει να επιτελείται. Το RBAC απλοποιεί τη διαχείριση της ασφάλειας συμπεριλαμβάνοντας μηχανισμούς για την αντιστοίχηση δικαιωμάτων πρόσβασης και χρηστών σε ρόλους. Η διαχείριση των προνομίων πρόσβασης για κάθε χρήστη μεμονωμένα είναι μια επιρρεπής σε λάθη τακτική και ταυτόχρονα μη διαχειρίσιμη στην περίπτωση μεγάλων οργανισμών με μεγάλο αριθμό χρηστών (Schaad et al, 2002). Τα βασισμένα σε ρόλους μοντέλα καθορίζουν την πρόσβαση αντιστοιχίζοντας δικαιώματα σε ρόλους, και κατόπιν αντιστοιχώντας τους χρήστες (με βάση τα καθήκοντα που τους ανατίθενται στα πλαίσια του οργανισμού) σε κάποιον (ή κάποιους) από τους ρόλους που έχουν ήδη δημιουργηθεί στο σύστημα.
Η έννοια των ρόλων είναι γενικότερη αυτής των ομάδων χρηστών, μια και οι ρόλοι απαρτίζονται από μια συλλογή χρηστών, δικαιωμάτων πρόσβασης καθώς και άλλους ρόλους (Sandhu 1995). Επίσης σε αντίθεση με την περίπτωση των ομάδων, οι χρήστες μπορούν να πάρουν μέρος σε ρόλους κατόπιν συγκεκριμένης απαίτησης, για παράδειγμα ένας χρήστης μπορεί να ενεργοποιήσει ένα ρόλο μόνο όταν χρειαστεί τα δικαιώματα που σχετίζονται με το συγκεκριμένο ρόλο.

Χάρη σε αυτή την ικανότητα, το RBAC υποστηρίζει την αρχή του ελαχίστου προνομίου, που αντιστοιχεί σε κάθε χρήστη τα ελάχιστα προνόμια που απαιτούνται για την εκτέλεση κάποιας δραστηριότητας (Schroeder et al, 1975).
Το RBAC είναι ένα γενικό μοντέλο που μπορεί να καλύψει τα κενά των μοντέλων τύπου MAC και τύπου DAC αλλά και υπό προϋποθέσεις να εκφράσει πολιτικές τύπου DAC ή MAC (Sandhu et al, 1998).
Υπάρχουν τέσσερις διαφορετικές εκδοχές του RBAC: το $RBAC_0$ γνωστό και ως επίπεδο RBAC, είναι η απλούστερη εκδοχή και αποτελεί τον πυρήνα για τις επόμενες μορφές του μοντέλου. Το $RBAC_1$ αποτελεί το ιεραρχικό RBAC, που υποστηρίζει την κληρονομικότητα ανάμεσα στα προνόμια, το $RBAC_2$ κάνει χρήση περιορισμών ενώ το $RBAC_3$ είναι γνωστό και ως συμμετρικό RBAC και επεκτείνει τις δυνατότητες των προηγούμενων υποστηρίζοντας κληρονομικότητα και ιεραρχίες. Αν και πιο ενημερωμένες εκδοχές του μοντέλου υποστηρίζουν συσχετίσεις μεταξύ ρόλων ή ομάδες χρηστών, η χρησιμότητά τους είναι περιορισμένη.
Οι βασικές έννοιες του $RBAC_0$ είναι οι χρήστες, τα δικαιώματα και οι συνεδρίες (sessions) (εικ. 2.2). Στο RBAC η σχέση μεταξύ ρόλων-χρηστών όπως και αυτή μεταξύ δικαιωμάτων-ρόλων είναι πολλά-προς-πολλά. Η έννοια των συνεδριών εισάγεται προκειμένου να υποστηριχτεί η αρχή της απόδοσης των ελάχιστων προνομίων, που ορίζει ότι σε κάθε ρόλο θα πρέπει να αντιστοιχιστούν τα ελάχιστα δυνατά προνόμια προκειμένου για την εκτέλεση των καθηκόντων που του έχουν αντιστοιχιστεί. Τυπικά μια συνεδρία είναι μια ενεργοποίηση του ρόλου για όσο διάστημα είναι αναγκαίο για την ολοκλήρωση των λειτουργιών που έχουν ανατεθεί στο χρήστη στα πλαίσια του συστήματος. Ένας χρήστης στα πλαίσια μιας συνεδρίας μπορεί να ενεργοποιήσει διαφορετικούς ρόλους. Έτσι οι συνεδρίες μπορούν να θεωρηθούν ως μια έμμεση διασύνδεση μεταξύ ρόλων και χρηστών. Μετά τον τερματισμό μιας συνεδρίας, όλοι οι ρόλοι που ενεργοποιήθηκαν στη διάρκειά της ανακαλούνται.

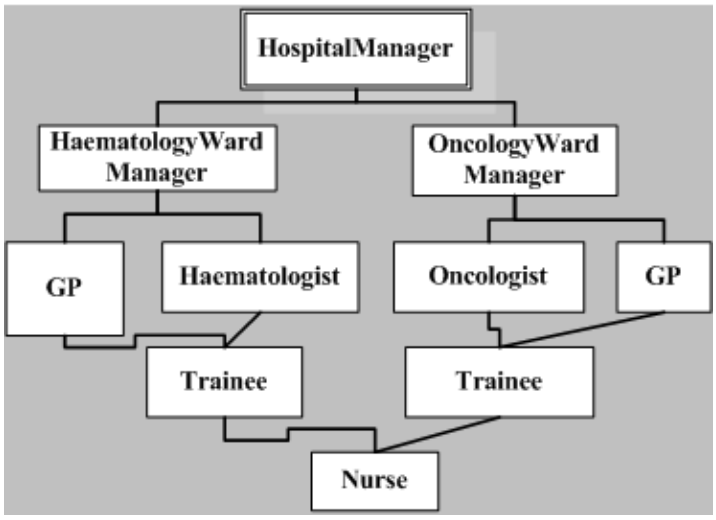


Εικόνα 2.2 Βασικές έννοιες στο RBAC μοντέλο

2.1.5.1 Ιεραρχίες ρόλων

Στο $RBAC_1$ εισάγεται η έννοια της κληρονομικότητας κατά τη μετάβαση των δικαιωμάτων. Τυπικά σε ένα οργανισμό, οι ρόλοι που βρίσκονται υψηλότερα στην ιεραρχία είθισται να έχουν και τα περισσότερα προνόμια. Οι ιεραρχίες ρόλων θεωρούνται μια φυσική απεικόνιση της δομής των σύγχρονων οργανισμών (Εικ. 2.3). Η κληρονομικότητα στη μετάδοση των δικαιωμάτων αντιπροσωπεύει τη μετάβαση των δικαιωμάτων από τις χαμηλότερες προς τις υψηλότερες θέσεις της ιεραρχίας. Πιο συγκεκριμένα, κάθε ρόλος κληρονομεί τα δικαιώματα των αμέσως κατώτερων.

Οι ιεραρχίες ρόλων έχουν το πλεονέκτημα ότι απλοποιούν τη διαχείριση της ασφάλειας· ωστόσο, πολλές φορές υπάρχει μια αναντιστοιχία της παραπάνω παραδοχής με τις πραγματικές συνθήκες που αφορούν στην πολιτική ενός οργανισμού.



Εικόνα 2.3 Ιεραρχία ρόλων

2.1.5.2 Περιορισμοί

Το $RBAC_2$ εισάγει την έννοια των περιορισμών (Chen and Sandhu, 1995). Σχετικά πρόσφατα, η αναπαράσταση του μοντέλου RBAC καθώς και καταστάσεων πρόσβασης με χρήση περιορισμών έχει αποκτήσει ιδιαίτερο ενδιαφέρον. Οι (Ahn και Shandhu 2000), ορίζουν μια καινούργια γλώσσα για τον καθορισμό περιορισμών που σχετίζονται με ρόλους βασισμένοι σε ένα συντακτικό κατηγορηματικής λογικής α' τάξης. Στις εργασίες τους οι Ahn και Shandhu υποστηρίζουν την αναπαράσταση περιορισμών που αφορούν σε ρόλους, όπως για παράδειγμα περιορισμούς που αφορούν στο διαχωρισμό καθηκόντων. Παράλληλα, νεότερες εργασίες (Barker et al 2003) επεκτείνουν τις δυνατότητες του RBAC και τη χρήση των περιορισμών σε προβλήματα ασφάλειας.

Μοντέλα	*Χαρακτηριστικά*
Bell La Padula	Διαφύλαξη Εμπιστευτικότητας Εφαρμογή σε στρατιωτικού τύπου Π.Σ.
Πολιτικές ροής πληροφορίας	Διαφύλαξη Εμπιστευτικότητας Εφαρμογή κυρίως σε στρατιωτικά και κυβερνητικά περιβάλλοντα με αρχιτεκτονική πολλαπλών επιπέδων (multilevel)
Biba	Διαφύλαξη ακεραιότητας Εφαρμογή σε στρατιωτικού τύπου Π.Σ.
Πολιτικές σινικού τείχους	Διαφύλαξη Εμπιστευτικότητας Εφαρμογή σε εταιρίες συμβούλων και χρηματοοικονομικά περιβάλλοντα
Μοντέλα διακριτικού ελέγχου πρόσβασης	Εφαρμογή σε λειτουργικά συστήματα Αδυναμία χειρισμού δυναμικά μεταβαλλόμενων συστημάτων
RBAC$_0$	Υποστήριξη μεγάλου εύρους συστημάτων Ευελιξία διαχείρισης
RBAC$_1$	*RBAC$_0$ + υποστήριξη ιεραρχιών*
RBAC$_2$	*RBAC$_1$ + υποστήριξη περιορισμών*
RBAC$_3$	*RBAC$_2$ + κληρονομικότητα και ιεραρχίες*

Πίνακας 2.1 Μοντέλα ασφάλειας – κύρια χαρακτηριστικά

Προϋποθέσεις

Συχνά τίθενται μια σειρά από περιορισμοί που αφορούν στις συνθήκες που πρέπει να πληροί ένας ρόλος προκειμένου να επιτραπεί η ενεργοποίησή του. Για παράδειγμα η ενεργοποίηση ενός ρόλου μπορεί να επιτρέπεται κατόπιν μόνο της ενεργοποίησης κάποιου άλλου ρόλου προηγουμένως. Άλλες προϋποθέσεις μπορεί να αφορούν στην ικανοποίηση συγκεκριμένων κριτηρίων που σχετίζονται με τα χρονικά διαστήματα ενεργοποίησης, την περιοχή (domain) από την οποία προέρχεται ένα αίτημα (Bertino et al, 2001). Στις επεκταμένες μορφές του μοντέλου RBAC μπορούμε να χρησιμοποιήσουμε μία σειρά από παραμέτρους, ικανές να αξιοποιηθούν προκειμένου για την εξουσιοδότηση χρηστών, βάσει του πλαισίου (context) και των μεταβλητών περιβάλλοντος που χαρακτηρίζουν την περιοχή στην οποία ανήκουν.

Διαχωρισμός καθηκόντων (Separation of Duty –SoD)

Ένας άλλος τύπος περιορισμών είναι ο διαχωρισμός καθηκόντων (Separation of Duty SoD). Είναι ένας από τους πιο σημαντικούς περιορισμούς, και αποτελεί ένα σημαντικό μηχανισμό για την πρόληψη απάτης, μέσω του διαμοιρασμού των καθηκόντων για την ολοκλήρωση ενός στόχου σε διαφορετικά μέρη. Για παράδειγμα, το πρόσωπο που εγκρίνει την έκδοση μιας οικονομικής εντολής δεν θα πρέπει να ταυτίζεται με το πρόσωπο που την εγκρίνει και το πρόσωπο που την εκδίδει. Υπάρχουν διαφορετικές εκδοχές των περιορισμών διαμοιρασμού καθηκόντων:

- **Στατικός διαχωρισμός καθηκόντων (Static Separation of Duty)**, αφορά στις περιπτώσεις που δύο ή περισσότεροι ρόλοι δεν μπορούν να ενεργοποιηθούν ταυτόχρονα.
- **Δυναμικός διαχωρισμός καθηκόντων (Dynamic Separation of Duty)**, επιτρέπει την ταυτόχρονη ενεργοποίηση ρόλων που υπόκεινται σε περιορισμούς διαχωρισμού καθηκόντων, ωστόσο οι όποιοι έλεγχοι γίνονται κατά τη στιγμή εφαρμογής της πολιτικής ελέγχου πρόσβασης.

Κλιμάκωση

Η δυνατότητα κλιμάκωσης αποτελεί βασική προϋπόθεση για όλα τα κατανεμημένα συστήματα. Ταυτόχρονα με την αύξηση του μεγέθους των συστημάτων η επιβολή ελέγχων πρόσβασης δυσχεραίνεται, καθώς η παρουσία πολλαπλών ιεραρχιών αυξάνει την πολυπλοκότητα. Προκειμένου γα την υποστήριξη της κλιμάκωσης και την ικανότητα επιβολής ελέγχου πρόσβασης από διαφορετικά Π.Σ. το σύνολο των γενικών κανόνων που αφορούν στη διαχείριση ασφάλειας, κωδικοποιείται σε μια σειρά από κανόνες, που αποτελούν την πολιτική ασφάλειας.
Σύγχρονες ερευνητικές προσπάθειες, υποστηριζόμενες ενίοτε και από εταιρίες λογισμικού στοχεύουν στην υλοποίηση ενός ενιαίου μηχανισμού ικανού να διαχειριστεί πολιτικές ασφάλειας. Ο μηχανισμός αυτός μπορεί να αποσκοπεί είτε στη διαχείριση ασφάλειας ενός μεμονωμένου Π.Σ. είτε στην επίτευξη ενός ενιαίου μηχανισμού διαχείρισης μιας σειράς από αυτόνομα, ανεξάρτητα Π.Σ.
Στις επόμενες παραγράφους περιγράφονται μια σειρά από διαφορετικές γλώσσες περιγραφής πολιτικής ασφάλειας και παρατίθενται συγκριτικά τα κυριότερα χαρακτηριστικά τους, καθώς και οι τεχνικές δυνατότητες που παρέχει η χρήση αυτών.

2.2 Πολιτικές Ασφάλειας – γλώσσες περιγραφής πολιτικών

Στη βιβλιογραφία υπάρχουν αρκετοί ορισμοί για την πολιτική ασφάλειας. Ένας ορισμός για την πολιτική ασφάλειας αναφέρει ότι σχετίζεται με τους κανόνες σε υψηλό επίπεδο, βάσει των οποίων καθορίζεται ο έλεγχος πρόσβασης (Samarati et al, 2001). Στα πλαίσια της παρούσας διατριβής υιοθετούμε την προσέγγιση που περιγράφεται στην εργασία (Kokolakis and Kiountouzis, 2000), σύμφωνα με την οποία η πολιτική είναι ένα σύνολο από δηλώσεις, που καθορίζουν το σύνολο των δυνατών επιλογών σε σχέση με μελλοντικές διαδικασίες. Η πολιτική ασφαλείας μπορεί να εκφράζεται με μια ποικιλία αναπαραστάσεων, από μια αυστηρή μαθηματική αναπαράσταση δικαιωμάτων πρόσβασης, έως την έκφραση σε πολύ γενική μορφή κάποιων αρχών και πεποιθήσεων (Kokolakis et al, 1998). Σχετικά με τις δυνατότητες αναπαράστασης έχουν αναπτυχθεί διάφορες γλώσσες, άλλες με έμφαση στη γραφική αναπαράσταση και άλλες που κατά κύριο λόγο εστιάζουν στη χρήση συγκεκριμένου συντακτικού καθώς επίσης και στη δυνατότητα καταγραφής σε ημιδομημένο κείμενο. Θα επιχειρηθεί μια σύντομη αναφορά στις κυριότερες από αυτές, αναφέροντας τα υπέρ και τα κατά κάθε γλώσσας.

Η Lasco (Hoagland et al, 1998), είναι μια γλώσσα γραφικά αναπαριστώμενη και συνεπώς γίνεται εύκολα κατανοητή από τους ανθρώπους, αλλά δεν μπορεί να υποστηρίξει πολιτικές βασισμένες στις υποχρεώσεις του υποκειμένου (obligation policies), ενώ δεν μπορεί να υποστηρίξει τη σύνθεση πολιτικών (Damianou 2002).
Η Trust Policy Language (IBM) (Herzberg et al, 2000) παρέχει τη δυνατότητα διαχωρισμού των υποκειμένων, μέσω αυθεντικοποίησης βασισμένης σε πιστοποιητικά. Στόχος της γλώσσας είναι να μπορούν να αντιστοιχηθούν άγνωστοι χρήστες σε συγκεκριμένους ρόλους. Ωστόσο η αντιστοίχηση προνομίων πρόσβασης σε συγκεκριμένους ρόλους είναι εκτός του πεδίου εφαρμογής της TPL, γεγονός που καθιστά δύσκολη τη χρήση της σε προβλήματα ελέγχου πρόσβασης.
Η RSL (Ahn et al, 1999) είναι μια τυπική γλώσσα που μπορεί να χρησιμοποιηθεί για το διαχωρισμό αρμοδιοτήτων σε συστήματα βασισμένα σε ρόλους. Ωστόσο δεν υποστηρίζεται η δυνατότητα αναπαράστασης χρονικών περιορισμών.
Η Tower (Hitchens et al, 2001) βασίζεται στην έννοια της ιδιοκτησίας: κάθε αντικείμενο έχει δομή και ένα ιδιοκτήτη. Είναι αδικαιολόγητα πολύπλοκη γλώσσα. Επίσης, ο καθορισμός των ρόλων στην Tower καθίσταται προβληματικός (Damianou 2002).
Η PDL (Lobo et al, 1999) είναι μια γλώσσα με απλό συντακτικό, στην οποία οι πολιτικές περιγράφονται από μια συλλογή εκφράσεων δύο τύπων: κανόνες πολιτικής (policy rules) και προτάσεις πολιτικής βασισμένες σε γεγονότα (policy defined event propositions). Ωστόσο δεν υποστηρίζει πολιτικές ελέγχου προσπέλασης, δεν υποστηρίζει τη μετατροπή κανόνων σε ρόλους ή άλλες αντίστοιχες οργανωτικές δομές. Παρά τις προηγούμενες διαπιστώσεις, έχουν προταθεί αρχιτεκτονικές που υποστηρίζουν την PDL.
Η Ponder (Damianou, 2002) (Lupu et al, 2000) είναι μια ισχυρή γλώσσα που υποστηρίζει εκτός από πολιτικές τύπου RBAC, πολιτικές τύπου MAC αλλά και τύπου DAC ενώ μπορεί να εφαρμοστεί για τη διαχείριση δικτυακών πόρων. Υποστηρίζει τον καθορισμό ρόλων, ενώ σε αντίθεση με άλλες γλώσσες, μπορεί να υποστηρίξει πολιτικές εκχώρησης εξουσιοδοτήσεων (delegation policies). Ωστόσο δεν υπάρχει πλέον υποστήριξη από εργαλεία λογισμικού (ο μεταγλωττιστής και το γραφικό περιβάλλον ανάπτυξης πολιτικών σε PONDER δεν υποστηρίζονται αλλά και δεν διατίθενται πλέον).
Για λόγους διαλειτουργικότητας, τελευταία έχουν προταθεί γλώσσες πολιτικής ασφάλειας βασισμένες στην XML (Extensible Markup Language) γλώσσα (XML, 2004). Η γλώσσα XACML (OASIS 2004) βασίζεται στην XML για την έκφραση πολιτικών και για τον καθορισμό προνομίων πρόσβασης σε πόρους σε διαδικτυωμένα περιβάλλοντα, υποστηρίζεται δε από τον οργανισμό OASIS (Organisation for the Advancement of Structured Information Standards). Η γλώσσα αυτή, της οποίας τις βασικές αρχές χρησιμοποιήσαμε στην προτεινόμενη αρχιτεκτονική διαχείρισης ασφάλειας σε περιβάλλοντα πολλαπλών πολιτικών, επιτρέπει τον καθορισμό τριάδων αποτελούμενων από το υποκείμενο, το αιτούμενο προς προσπέλαση αντικείμενο και την ενέργεια που το υποκείμενο αιτείται επί του αντικειμένου. Τόσο το αίτημα όσο και η απάντηση, διαμορφώνεται με μορφή μηνύματος κωδικοποιημένου σε γλώσσα XML. Στα αρνητικά της γλώσσας μπορεί να αναφερθεί ότι λόγω της ανάγκης τήρησης του συντακτικού της XML δεν γίνεται άμεσα κατανοητό το περιεχόμενο των μηνυμάτων, καθώς και λόγω του ότι δεν υπάρχουν μέχρι στιγμής εργαλεία ανάπτυξης συμβατών με την XACML πολιτικών, αυτό απαιτείται να γίνεται είτε χειρονακτικά, είτε με κατά περίπτωση αναπτυσσόμενα εργαλεία λογισμικού. Στα πλαίσια της διατριβής αναπτύχθηκε περιβάλλον με

γραφικές δυνατότητες διαχείρισης πολλαπλών πολιτικών, το οποίο περιγράφεται στο κεφάλαιο 7.
Οι (Bhatti et al, 2004) προτείνουν μια γλώσσα βασισμένη στο μοντέλο RBAC που χρησιμοποιεί τη γλώσσα XML για την αναπαράσταση των ρόλων και των πεδίων (attributes) που σχετίζονται με τους ρόλους, την αντιστοίχηση χρηστών σε ρόλους καθώς και την αντιστοίχηση δικαιωμάτων σε ρόλους. Το πρόβλημα με την XRBAC είναι κατ' αρχάς ότι δεν είναι ευρέως διαδεδομένη καθώς δεν είναι διαθέσιμα ακόμη εργαλεία που να την υποστηρίζουν.

	Θετικά	***Αρνητικά***
Authorization Specification Language	Υποστηρίζει RBAC	Δεν υποστηρίζει κλιμάκωση
RSL	Υποστηρίζει RBAC – Υποστηρίζει διακριτά καθήκοντα	Δεν υποστηρίζει χρονικά κυμαινόμενους περιορισμούς
Tower	Υποστηρίζει ατομικά δικαιώματα πρόσβασης	Πολύπλοκη - Προβληματικός ορισμός ρόλων
XACML	Υποστηρίζει RBAC – Βασισμένη σε XML	Δύσκολη στην κατανόηση
TPL	Υποστήριξη RBAC – επεκτείνει το μοντέλο RBAC αντιστοιχώντας άγνωστους χρήστες σε καθορισμένους ρόλους – Υποστήριξη XML	Απαιτεί μακροσκελή αρχεία περιγραφής (XML) – όχι ευανάγνωστη
Policy Description Language	Απλό συντακτικό	Δεν υποστηρίζει ελέγχους πρόσβασης – δεν υποστηρίζει την αντιστοίχηση κανόνων πολιτικής σε ρόλους
PONDER	Ισχυρή, υποστηρίζει πολλαπλά μοντέλα εξουσιοδότησης, υποστήριξη διαχείρισης πόρων	Απαιτεί δικά της εργαλεία ελέγχου και δεν αποτυπώνεται σε XML αρχεία
XRBAC	Υποστήριξη RBAC, υποστηρίζει χρονικούς περιορισμούς, αποτυπώνεται σε XML	Απουσία εργαλείων – δεν αποτελεί πρότυπο και δεν είναι και ευρέως διαθέσιμη

Πίνακας 2.2 Συγκριτική επισκόπηση γλωσσών περιγραφής πολιτικών ασφάλειας

2.3 Περιβάλλοντα πολλαπλών πολιτικών

Τελευταία, ιδιαίτερο ενδιαφέρον τόσο από ερευνητικής απόψεως όσο και λόγω των τεχνολογικών προκλήσεων που ανακύπτουν, αποκτά η διαχείριση της ασφάλειας για ένα περιβάλλον συνεργασίας πολλαπλών, δυναμικά μεταβαλλόμενων σε αριθμό Π.Σ. Τα κίνητρα για τη δημιουργία αντίστοιχων περιβαλλόντων είναι πολλαπλά: συχνά

ανακύπτει η ανάγκη συνεργασίας μεταξύ οργανισμών, στα πλαίσια της λειτουργίας τους σε ένα κοινό πλαίσιο. Για παράδειγμα πληροφοριακά συστήματα υπουργείων που συναλλάσσονται μεταξύ τους στα πλαίσια του δημόσιου τομέα, ή οργανισμοί ερευνητικοί που διαμοιράζονται πόρους με στόχο την συνεργασία σε ερευνητικά προγράμματα κλπ. Οι μέχρι τώρα προσεγγίσεις καθώς και οι μηχανισμοί διαχείρισης πολιτικών ασφάλειας, έχουν σχεδιαστεί με γνώμονα την εφαρμογή τους στο μοντέλο ασφάλειας του ενός οργανισμού. Οι τεχνολογικές εξελίξεις, η διείσδυση του διαδικτύου και η ανάγκη για συνεργασία μεταξύ συστημάτων και οργανισμών, δημιουργούν την ανάγκη για ένα νέο πλαίσιο διαχείρισης αυτόνομων συστημάτων και επικοινωνίας μεταξύ τους.

Οι λύσεις που έχουν κατά καιρούς προταθεί από την ερευνητική κοινότητα στο χώρο της ασφάλειας θα μπορούσαν ανάλογα και με το μοντέλο που υιοθετούν, να κατηγοριοποιηθούν σε δύο ευρύτερες κατηγορίες (Belsis et al, 2005f):

1. Συστήματα βασισμένα στην εμπιστοσύνη: Η έννοια της εμπιστοσύνης, έχοντας ως αφετηρία την ερμηνεία που δίνεται και στις ανθρώπινες συναλλαγές, βρίσκει εφαρμογή κατά κανόνα σε πολύπλοκα, μη ιεραρχικά συστήματα -όπως το διαδίκτυο- όπου συχνά εντελώς άγνωστοι μέχρι πρότινος ρόλοι χρειάζεται να έρθουν σε επαφή και να συνάψουν συναλλαγές μεταξύ τους. Τυπικό παράδειγμα αποτελούν οι συναλλαγές ηλεκτρονικού εμπορίου. Η εξουσιοδότηση μιας συναλλαγής, συχνά βασίζεται σε μια εκτίμηση του κόστους και της ενδεχόμενης επικινδυνότητας που συνεπάγεται η αποδοχή της συναλλαγής από τα δύο μέρη, εκτιμώντας και την προηγούμενη φήμη που μπορεί να εκτιμηθεί από προηγούμενες συναλλαγές των δύο μερών με άλλους χρήστες.
2. Αυτόνομα συστήματα, τα οποία χαρακτηρίζει μια σαφώς διατυπωμένη πολιτική και στα οποία απαιτείται ένας μηχανισμός ικανός να επιτύχει τη διαλειτουργικότητα μεταξύ των συμμετεχόντων συστημάτων, προτείνοντας ταυτόχρονα ένα αποδοτικό αλλά και ασφαλή μηχανισμό διαχείρισης των διαμοιραζόμενων πόρων. Το μοντέλο ασφάλειας που περιγράφεται στα πλαίσια της διατριβής ανήκει στη δεύτερη κατηγορία. Όπως διαφαίνεται και από τις περισσότερες προσεγγίσεις στο χώρο της διαλειτουργικότητας σε περιβάλλοντα πολλαπλών πολιτικών, υπάρχουν δύο κατευθύνσεις στις ακολουθούμενες τακτικές, οι οποίες αποσκοπούν στην επίτευξη (Bidan et al, 1998):

- *Διαλειτουργικότητας μεταξύ πολιτικών,* που αναφέρεται σε μια σύνθετη πολιτική που βασίζεται στις ιδιότητες των επιμέρους πολιτικών και
- *Συνδυασμού πολιτικών,* που καθορίζει τη δημιουργία μιας νέας πολιτικής, με βάση τις προδιαγραφές που ορίζονται στις συνιστώσες πολιτικές.

Για λόγους πληρότητας θα γίνει μια σύντομη αναφορά σε συστήματα που ακολουθούν το μοντέλο ασφάλειας που βασίζεται στην εμπιστοσύνη και κατόπιν θα αναφερθούν προσεγγίσεις πιο άμεσα συνδεδεμένες με την ακολουθούμενη προσέγγιση στα πλαίσια της διατριβής.

2.4 Διαχείριση ασφάλειας συνασπισμών αυτόνομων συστημάτων

Στην ενότητα αυτή επισκοπούνται κυρίως τεχνικές που αποσκοπούν στη διαχείριση της ασφάλειας για συνεργαζόμενα συστήματα, ή αλλιώς συνασπισμούς πληροφοριακών συστημάτων. Χαρακτηριστικό των συνασπισμών είναι η δυναμική τους συμπεριφορά, δηλαδή ότι ο αριθμός των συμμετεχόντων μερών μπορεί να αυξάνεται ή να ελαττώνεται δυναμικά.

Αν θεωρήσουμε το πρόβλημα της από μηδενικής βάσης (χωρίς περιορισμούς) διαπραγμάτευσης των συμμετεχόντων μερών, τότε στην πράξη αποδεικνύεται ότι για δύο πολιτικές είναι δυσεπίλυτο πρόβλημα (NP-hard), ενώ για περισσότερες από δύο πολικές, αποδεικνύεται ότι το πρόβλημα γίνεται NP-πλήρες (McDaniel et al, 2002). Στην ουσία για περισσότερες από δύο πολιτικές, δεδομένου ότι κάθε πολιτική μπορεί να θεωρηθεί σαν ένα σύνολο από δυαδικούς περιορισμούς (όπου το 1 αντιστοιχεί στο ότι μια πρόσβαση είναι επιτρεπτή και το 0 στο να είναι μη επιτρεπτή), τότε το πρόβλημα της διαπραγμάτευσης πολλαπλών πολιτικών είναι μια μορφή του προβλήματος της ικανοποιησιμότητας (satisfiability problem) που είναι γνωστό ότι είναι NP-πλήρες (Bharadwaj et al, 2003). Έτσι στις διαφορετικές προσεγγίσεις, τίθενται διαφορετικοί περιορισμοί προκειμένου να καθίσταται εφικτή η εξεύρεση λύσης.

Στις περισσότερες περιπτώσεις, η πολιτική που προκύπτει είτε από το συνδυασμό των επιμέρους πολιτικών είτε μέσω ενός μηχανισμού διαλειτουργικότητας μεταξύ των συμμετεχόντων μερών, υπόκειται σε μια σειρά από συμβάσεις ή συμφωνίες. Μία τέτοια σύμβαση μπορεί να είναι η ύπαρξη ενός εποπτεύοντος πλαισίου όπως για παράδειγμα ένα κυβερνητικό ή άλλο αντίστοιχο ρυθμιστικό πλαίσιο (Ao et al, 2003). Η ύπαρξη ενός ρυθμιστικού μηχανισμού που εποπτεύει το σχηματισμό των αντιστοιχήσεων ρόλων όπως παρουσιάζεται στα πλαίσια της διατριβής είναι αναγκαία προϋπόθεση προκειμένου για την εύρεση ικανοποιητικής λύσης.

Ο Gibson (Gibson 2001), μελέτησε την ανάγκη για σχηματισμό συνασπισμών σε στρατιωτικά περιβάλλοντα και πρότεινε μια αρχιτεκτονική που καθιστά εφικτό το σχηματισμό συνασπισμών. Η εργασία του θέτει μια σειρά από προϋποθέσεις για την ανάγκη διαμοιρασμού πόρων σε στρατιωτικά περιβάλλοντα, αλλά δεν παραθέτει λύση στο πρόβλημα της διαχείρισης των διαμοιραζόμενων πόρων.

Οι (Joshi et al, 2004) χρησιμοποιώντας την γλώσσα X-RBAC επιχειρούν να εφαρμόσουν μια σύνθεση διαφορετικών τοπικών πολιτικών με στόχο τη δημιουργία μιας καθολικής πολιτικής, με βάση την τεχνική της αντιστοίχησης ρόλων. Η διαφορά από τη δική μας προσέγγιση είναι ότι προκειμένου για την ελάττωση της πολυπλοκότητας διαχείρισης της πληροφορίας που αφορά στις αντιστοιχίσεις ρόλων, προτείνεται στα πλαίσια της παρούσας διατριβής η τεχνική της εισαγωγής μιας γενικής ιεραρχίας με την οποία υποχρεούνται οι επιμέρους πολιτικές να εναρμονιστούν. Συγκεκριμένα ορισμένοι ρόλοι από τον ένα οργανισμό αντιστοιχίζονται σε ρόλους μιας γενικής ιεραρχίας και μέσω αυτής σε ρόλους του άλλου οργανισμού. Το πρόβλημα της προσέγγισης των (Joshi et al, 2004) έγκειται στην περιορισμένη δυνατότητα κλιμάκωσης καθώς και στην πολυπλοκότητα της. Σε επόμενη εργασία της ίδιας ερευνητικής ομάδας (Shafiq et al, 2005) προτείνεται η χρήση ενός αλγορίθμου που συνθέτει μια καθολική πολιτική από τις συνιστώσες πολιτικές. Ο προτεινόμενος αλγόριθμος συνένωσης των μεμονωμένων πολιτικών, απαιτεί πολυωνυμικό χρόνο εκτέλεσης, κάτι που καθιστά δύσκολη την ενημέρωση της καθολικής πολιτικής σε πραγματικό χρόνο. Αποτέλεσμα είναι οι αλλαγές που υφίστανται οι πολιτικές σε τοπικό επίπεδο να ανακλώνται μετά από σημαντική καθυστέρηση στη γενική πολιτική, κάτι που συνιστά βασικό περιορισμό για ένα δυναμικό, κατανεμημένο σύστημα. Προκειμένου τέλος για την επίλυση καταστάσεων σύγκρουσης, επιλέγεται η μερική απώλεια αυτονομίας των επιμέρους οργανισμών. Στη δική μας προσέγγιση αντίθετα, η ενημέρωση των αλλαγών στην πολιτική γίνεται με πολύ πιο γρήγορο - και ταυτόχρονα αποτελεσματικό – τρόπο, ενώ παράλληλα προτείνεται ένα πλαίσιο βελτιστοποίησης και ελαχιστοποίησης του διαχειριστικού φόρτου με χρήση τεχνικών βασισμένων στο μαθηματικό φορμαλισμό των χαλαρών

περιορισμών, σε συνδυασμό με ένα μηχανισμό αυτοματοποιημένης επίλυσης μη κρίσιμων συγκρούσεων, βασισμένου στη χρήση ασαφούς λογικής.

Στην εργασία του Khurana (Khurana 2002), εισάγεται το πρόβλημα της δημιουργίας με δυναμικό τρόπο συνασπισμών Π.Σ. μεταξύ αυτόνομων περιοχών και συζητούνται τρόποι με τους οποίους μπορούν να σχηματιστούν συνασπισμοί ως αποτέλεσμα της επίτευξης μιας κοινά αποδεκτής λύσης από το σύνολο των συμμετεχόντων μερών, όπου μια σειρά από πόρους είναι κοινά διαμοιραζόμενοι από όλα τα μέλη του συνασπισμού. Στη συγκεκριμένη ερευνητική προσέγγιση, αν και υιοθετείται το μοντέλο RBAC, δεν λαμβάνονται υπόψη οι συνεδρίες (sessions) ενώ επίσης δεν παρέχεται υποστήριξη για ιεραρχίες ρόλων. Επιπρόσθετα, όλοι οι ρόλοι που συμμετέχουν στο συνασπισμό, θεωρείται εξαρχής ότι έχουν πρόσβαση σε όλους τους κοινά διαμοιραζόμενους πόρους. Προκειμένου για την επίτευξη του συνασπισμού, τα συμμετέχοντα μέρη παίρνουν σειρά σε μια κυκλικά εναλλασσόμενη (round robin) διαδικασία και αποδέχονται ή όχι τις προτάσεις των υπολοίπων μέχρι να επιτευχθεί η συμφωνία για τους αναγκαίους πόρους. Στη συνέχεια αφού επιτευχθεί συμφωνία σχετικά με το ποιοι είναι οι πόροι που θα διαμοιραστούν, σχηματίζεται ένας πίνακας πρόσβασης που διατηρεί όλους τους ρόλους και όλους τους διαμοιραζόμενους πόρους. Ένα μειονέκτημα της παραπάνω προσέγγισης είναι ότι το μέγεθος των πινάκων που χρειάζεται να διατηρηθούν (που περιέχουν τους ρόλους ανά περιοχή που συμμετέχουν, τους νέους ρόλους που σχηματίζονται στα πλαίσια του συνασπισμού, τους πόρους και τα δικαιώματα των καθολικών ρόλων έναντι των πόρων), ενδέχεται να αυξηθεί κατά πολύ, κάνοντας δύσκολη τη διαχείριση του συνασπισμού. Παράλληλα, ο φορμαλισμός που χρησιμοποιείται είναι βασισμένος σε μια παραλλαγή της RCL2000, που αποτελεί μία τύπου RBAC γλώσσα. Για τον προσδιορισμό της γλώσσας διαπραγμάτευσης χρησιμοποιείται περιορισμένη κατηγορηματική λογική α΄ τάξης (Restricted First Order Predicate Language- RFOPL), που δημιουργεί δυσκολίες στην υλοποίηση ενός ενιαίου μηχανισμού διαπραγμάτευσης, ερμηνείας και εφαρμογής της πολιτικής.

Ο Belokosztolszki (Belokosztolszki 2004) (Belokosztolszki et al, 2003), εισάγει την έννοια των πολιτικών διεπαφών και κάνει χρήση της έννοιας του συναφούς πλαισίου (context). Στις εργασίες αυτές, εισάγεται η έννοια των αντιστοιχήσεων ρόλων με τρόπο παρόμοιο με αυτό της δική μας προσέγγισης. Ωστόσο υιοθετείται η πρακτική του ελέγχου της ροής πληροφοριών (information flow) όπου ορίζονται επιτρεπτές ροές και μη επιτρεπτές ροές σε συγκεκριμένες περιοχές. Μεταξύ των διαφορετικών περιοχών συνάπτονται συμφωνίες επιπέδου υπηρεσιών (Service Level Agreements-SLA's), οι οποίες δεν έχουν περιορισμό σε αριθμό. Στη δική μας προσέγγιση προτείνονται πιο ευέλικτοι τρόποι αναπαράστασης της σχετικής με ρόλους πληροφορίας, ενώ εισάγεται ένας φορμαλισμός που βοηθά στην βελτιστοποίηση της λειτουργίας του συστήματος πολλαπλών πολιτικών, σε συνδυασμό με ένα πλαίσιο επίλυσης συγκρούσεων βασισμένο στη χρήση ασαφούς λογικής.

Οι (Shands et al, 2000) προτείνουν τη δημιουργία των ασφαλών ιδεατών κλωβών (Secure Virtual Enclaves). Στη συγκεκριμένη ερευνητική προσπάθεια, σε κάθε Π.Σ. δημιουργείται μια περιοχή από διαφορετικούς πόρους που τίθενται προς διαμοιρασμό. Οι ρόλοι πρέπει να συμφωνηθούν εξαρχής για όλους τους οργανισμούς, χωρίς να γίνεται χρήση τεχνολογικών μέσων. Αυτό συνιστά ένα βασικό περιορισμό στο πόσοι και ποιας μορφής οργανισμοί μπορούν να απεικονιστούν στο συγκεκριμένο σύστημα. Η κλιμάκωση επίσης - τόσο από άποψη αρχιτεκτονικής όσο και από την άποψη των υιοθετούμενων τεχνολογικών λύσεων - λόγω της αυξημένης

κατανάλωσης υπολογιστικών πόρων της συγκεκριμένης προσέγγισης, τίθεται υπό αμφισβήτηση.

Στην εργασία των (Seamons et al, 1997) προτείνεται η αντιστοίχηση χρηστών σε ρόλους βάσει πιστοποιητικών, χρησιμοποιώντας τη γλώσσα προγραμματισμού Prolog. Το μειονέκτημα της παραπάνω λύσης είναι ότι δεν υπάρχει μια συγκεκριμένη γλώσσα πολιτικής, αλλά αντίθετα ένα ξεχωριστό πρόγραμμα θα πρέπει να γραφεί για κάθε εφαρμογή, γεγονός που θέτει ένα ανυπέρβατο περιορισμό στην κλιμάκωση του συστήματος. Επιπλέον, η συγκεκριμένη προσέγγιση βασίζεται ση χρήση αλυσιδωτών πιστοποιητικών που οδηγούν σε μια κεντρική αρχή πιστοποίησης, γεγονός που προσθέτει επιπλέον την ανάγκη εισαγωγής υποδομών δημόσιου κλειδιού. Στη συγκεκριμένη εργασία όπως και στην εργασία των (Winsborough et al, 2000) εισάγεται η έννοια των διαπραγματεύσεων στη λογική του έλεγχου εξουσιοδότησης σε περιπτώσεις διαπραγμάτευσης εξυπηρέτη-εξυπηρετούμενου, χωρίς ωστόσο να συζητάται η περίπτωση διαπραγματεύσεων στην περίπτωση που ο αριθμός των συμμετεχόντων μερών αυξάνει σημαντικά.

Οι (Ao and Minsky, 2003) παρουσιάζουν ένα μοντέλο διαχείρισης συνασπισμών, στο οποίο λειτουργούν αντίθετα με άλλες προσεγγίσεις, υιοθετώντας μία από πάνω προς τα κάτω προσέγγιση (top-down approach). Αρχικά δημιουργείται η πολιτική του συνασπισμού και στη συνέχεια επιτρέπεται στα συμμετέχοντα μέρη να δημιουργήσουν τις επιμέρους πολιτικές τους, πάντοτε έχοντας υπόψη τις αρχές που πρεσβεύει η καθολική πολιτική. Το γεγονός αυτό καθώς και η μη υποστήριξη του μοντέλου RBAC, καθιστούν την δυνατότητα εφαρμογής της παραπάνω προσέγγισης περιορισμένη.

Οι (Gligor et al, 2001) προτείνουν μια τεχνική διαπραγμάτευσης βασισμένη στη θεωρία παιγνίων. Κάθε Π.Σ. προτείνει μια σειρά από πόρους προς διαμοιρασμό και αναζητείται λύση που θα είναι βέλτιστη με βάση τις αρχές της θεωρίας παιγνίων, δηλαδή δεν θα δίνει σε κάποιο από τα συμμετέχοντα μέρη κυριαρχικό δικαίωμα και επίσης δεν θα υπάρχει κατάσταση που να παρέχει καλύτερες συνθήκες για οποιαδήποτε από τα συμμετέχοντα μέρη (pareto efficient). Ωστόσο στην παραπάνω εργασία γίνεται απλά μια πρώτη συζήτηση για ένα τρόπο αντιστοίχησης πολιτικών, αφήνοντας σαν ανοικτό πρόβλημα τις λεπτομέρειες ενός πρωτοκόλλου.

Τέλος, στην εργασία (Mukkamala et al,2005) προτείνεται μια κλιμακούμενη λύση στο πρόβλημα του σχηματισμού συνασπισμών, κυρίως με έμφαση σε δυναμικά μεταβαλλόμενα συστήματα και κατά περίπτωση (ad-hoc) περιβάλλοντα. Προτείνεται η χρήση ενός κατανεμημένου μητρώου (distributed coalition registry) μεταξύ ασύρματα διασυνδεδεμένων περιοχών. Στην προσέγγιση αυτή, το κατανεμημένο μητρώο έχει αντίστοιχο ρόλο με το μητρώο διαχείρισης του συνασπισμού που περιγράφηκε στις εργασίες (Malatras et al, 2005a) (Malatras et al, 2005b) (Belsis et al, 2006c)(Gritzalis et al, 2006). Ωστόσο η εφαρμογή των αρχών που προτείνονται στις δύο τελευταίες αυτές εργασίες ως επέκταση και της εργασίας (Belsis et al, 2005h) καθιστά την εφαρμοσιμότητά τους πολύ μεγαλύτερη σε διαφορετικών απαιτήσεων περιβάλλοντα.

2.5 Περιβάλλοντα πολλαπλών πολιτικών και μαθηματικά μοντέλα

Στην εργασία των (Bharadwaj et al, 2003), περιγράφεται η γενική αρχιτεκτονική ενός πράκτορα διαμεσολάβησης επιφορτισμένου με το έργο της υποστήριξης του δυναμικού σχηματισμού συνασπισμών. Εισάγεται ένας φορμαλισμός βασισμένος στη

χρήση χαλαρών περιορισμών (soft constraints), ενώ το πρόβλημα του σχηματισμού του συνασπισμού και της επίτευξης μιας σταθερής κατάστασης περιγράφεται μαθηματικά ως ένα πρόγραμμα λογικού προγραμματισμού με χρήση χαλαρών περιορισμών. Το μαθηματικό πλαίσιο αυτό επεκτείνεται στα πλαίσια της παρούσας διατριβής ώστε να περιλάβει και την έννοια των αντιστοιχήσεων ρόλων, καθώς και τη δημιουργία ενός πλαισίου αυτοματοποιημένης διαχείρισης των μηχανισμών ελέγχου πρόσβασης του συνασπισμού.

Οι (Barker and Stuckey, 2003) χρησιμοποιούν τον προγραμματισμό με χρήση περιορισμών για να εκφράσουν πολιτικές σε περιβάλλοντα μιας ή και πολλαπλών πολιτικών. Στην εργασία τους δεν υποστηρίζεται ωστόσο η δυνατότητα χειρισμού αιτήσεων για πρόσβαση σε αντικείμενα από διαφορετικές περιοχές. Παράλληλα, δε συζητώνται τίθενται ζητήματα επίλυσης συγκρούσεων σε περιπτώσεις ύπαρξης πολλαπλών περιορισμών, ενώ επίσης δεν υποστηρίζεται η δυνατότητα έκφρασης προτιμήσεων για τις διαφορετικές περιοχές.

Στα πλαίσια της διατριβής, επεκτείνεται η χρήση των περιορισμών για την αναπαράσταση καταστάσεων πρόσβασης σε περιβάλλοντα πολλαπλών πολιτικών. Παράλληλα, με τη χρήση σημειολογίας από το χώρο της ασαφούς λογικής και τεχνικών μερικής ικανοποίησης περιορισμών, επιχειρείται η επίλυση αντικρουόμενων καταστάσεων σε περιβάλλοντα πολλαπλών πολιτικών.

Οι (Bonatti et al, 2000), (Bonatti et al, 2002), προτείνουν μια άλγεβρα για τη δημιουργία σύνθετης πολιτικής ασφάλειας από απλούστερες πολιτικές. Στη δουλειά των Bonatti et al, αποδεικνύεται ότι η σημειολογία της προτεινόμενης γλώσσας είναι ισοδύναμη με εκφράσεις λογικής α΄ τάξεως. Ωστόσο δε συζητώνται θέματα αρχιτεκτονικής σχετικά με το σχηματισμό του συνασπισμού, ενώ δεν υπάρχει επίσης δυνατότητα υποστήριξης προτιμήσεων για τα συμμετέχοντα μέρη. Παράλληλα πρέπει να αναφέρουμε και τη δυσκολία στην υλοποίηση μηχανισμών πρόσβασης που βασίζονται στη χρήση λογικής α΄ τάξεως.

2.6 Συστήματα διαχείρισης ασφάλειας βασισμένα στην εμπιστοσύνη - Trust Management Systems

Στην ενότητα αυτή επισκοπείται η έρευνα που έχει επιτελεσθεί στον τομέα του ελέγχου πρόσβασης με βάση το μοντέλο διαχείρισης εμπιστοσύνης (trust based model). Το μοντέλο αυτό, όπως αναφέρθηκε, επιτρέπει τη σύναψη συναλλαγών και τη διαχείριση ασφάλειας με βάση την έννοια της εμπιστοσύνης όπως αυτή εκφράζεται και στις ανθρώπινες συναλλαγές. Τυπικά ο χρήστης παρέχει στο σύστημα κάποια πιστοποιητικά που βοηθούν στο να επιβεβαιωθεί η ταυτότητα του και στη συνέχεια αντιστοιχούνται κάποια προνόμια σε αυτόν/αυτήν ανάλογα με την πολιτική που έχει διατυπωθεί και τον ρόλο που του αντιστοιχείται. Υπάρχει ακόμη και η δυνατότητα να συλλέγεται κάποια πληροφορία στην περίπτωση που ο χρήστης είναι άγνωστος στο σύστημα, με βάση τη φήμη που έχει συλλέξει συναλλασσόμενος με τρίτα έμπιστα μέρη. Το πλεονέκτημα του μηχανισμού αυτού είναι ότι μπορεί να βρει εφαρμογή ακόμη και σε εντελώς ανοικτά περιβάλλοντα, όπως το διαδίκτυο. Για παράδειγμα, στις εφαρμογές ηλεκτρονικού εμπορίου συχνά εμφανίζεται το ενδεχόμενο συναλλαγής με κάποιον χρήστη εντελώς άγνωστο, του οποίου η ταυτότητα και η συμπεριφορά είναι εντελώς καινούργια για το σύστημα. Αντίστοιχα και ο/η συναλλασσόμενος/η δεν γνωρίζει τη φερεγγυότητα του συστήματος το οποίο του πραγματοποιεί την πώληση. Σε αυτές τις περιπτώσεις ο μηχανισμός εμπιστοσύνης μπορεί να λειτουργήσει ικανοποιητικά και να δώσει και στα δύο μέρη να συνεκτιμήσουν την επικινδυνότητα αξιολογώντας πληροφορίες που προκύπτουν

από τη σχετική εμπειρία τρίτων μερών αλλά και το ύψος της συναλλαγής και το σχετικό κόστος που θα είχε η τυχόν κακοπιστία ενός από τα μέρη.
Στην εργασία των (Herzberg et al, 1998) επιχειρείται η αντιστοίχηση ρόλων σε χρήστες ξένους προς τον οργανισμό, χτίζοντας μια ιεραρχία δικτύου εμπιστοσύνης (web of trust). Προκειμένου για την αυθεντικοποίηση χρησιμοποιούνται τύπου X.509 πιστοποιητικά. Το πλεονέκτημα της παραπάνω αρχιτεκτονικής σε αντίθεση με άλλες όπως το Keynote (Blaze et al, 1998), Policy Maker, REFEREE (Chu et al, 1997) είναι ότι στις τελευταίες παρέχεται ένας ενιαίος μηχανισμός για την αξιολόγηση της εμπιστοσύνης και την επιβολή ελέγχου πρόσβασης, κάτι που κάνει δύσκολη την ολοκλήρωσή τους με υπάρχοντα λειτουργικά συστήματα. Ωστόσο όπως και στην προσέγγιση των (Shands et al, 2000) που αναφέρθηκε στην προηγούμενη παράγραφο, υπάρχει δυσκολία όταν δεν υπάρχει μια ακριβής απεικόνιση ρόλων από τον ένα οργανισμό στον άλλο.
Προκειμένου για τη διαχείριση των διαμοιραζόμενων πόρων, χρησιμοποιούνται κατά βάση τεχνικές βασισμένες στην υποδομή δημόσιου κλειδιού (PKI- public key infrastructure) όπως για παράδειγμα X.509 (X.509, 1997) πιστοποιητικά, ή εφαρμογές όπως το SPKI (Elisson et al, 1999) και άλλες τύπου PKI εφαρμογές.
Οι (Abadi *et al,* 1991) παρουσιάζουν μια λογική ελέγχου πρόσβασης βασισμένη στη χρήση πιστοποιητικών. Ωστόσο στην προσέγγισή τους χρησιμοποιούν πιστοποιητικά τα οποία δεν μπορούν να υποστηρίξουν την ανάκληση των δικαιωμάτων, προϋποθέτοντας ότι αυτά έχουν πολύ μικρή διάρκεια ζωής. Στα συστήματα SPKI (Ellison et al, 1998) και (Aura, 1998) χρησιμοποιούνται πιστοποιητικά εξουσιοδότησης (authorization certificates) τα οποία αντιστοιχούν προνόμια απευθείας σε συγκεκριμένα δημόσια κλειδιά. Ωστόσο δεν υποστηρίζουν τη δυνατότητα για ταυτόχρονη απόδοση προνομίων σε περισσότερους από ένα ρόλους μέσω κατανεμημένων κλειδιών (Khurana, 2002).
Το PolicyMaker (Blaze et al, 1996) και Keynote (Blaze et al, 1998) είναι συστήματα διαχείρισης εμπιστοσύνης που μπορούν να αποδίδουν προνόμια σε συγκεκριμένα δημόσια κλειδιά. Ωστόσο, ο μηχανισμός διαχείρισης των κλειδιών όπως και αυτός της ανάκλησης πιστοποιητικών λειτουργεί εξωτερικά του συστήματος, περιορίζοντας την ικανότητα αυτόνομης λειτουργίας των παραπάνω συστημάτων.
Τα βασισμένα στην εμπιστοσύνη συστήματα χαρακτηρίζονται από τη δυνατότητα ενιαίας διαχείρισης των διαδικασιών αυθεντικοποίησης και εξουσιοδότησης. Οι (Keromytis et al, 2001) επικρίνουν τη χρήση μιας καθολικής γλώσσας υψηλού επιπέδου για το σκοπό αυτό, χαρακτηρίζοντάς την ως τακτική πολύπλοκη και επιρρεπή σε λάθη. Επιπλέον θεωρούν μια τέτοια προσέγγιση ως ακατάλληλη λόγω του ότι υποθέτει την ύπαρξη ομοιογένειας σε διαφορετικά τμήματα ενός δικτύου. Έτσι αντιπροτείνουν τη χρήση πολλαπλών γλωσσών πολιτικής προσανατολισμένων στο επίπεδο εφαρμογής. Οι γλώσσες αυτές αντιστοιχούν (με χρήση κατάλληλων μεταγλωττιστών) σε ένα κοινό διαλειτουργικό στρώμα υλοποιούμενο με το σύστημα Keynote (Blaze et al, 1998). Το μειονέκτημα της παραπάνω προσέγγισης είναι ότι συγκεκριμένα χαρακτηριστικά της πολιτικής ελέγχου πρόσβασης (όπως για παράδειγμα η εκχώρηση δικαιωμάτων (delegation of rights) πρέπει να καθοριστούν σε χαμηλό επίπεδο, δυσκολεύοντας πολύ τον προσδιορισμό των προδιαγραφών του συστήματος. Ωστόσο, η διαλειτουργικότητα μπορεί να επιτευχθεί σε μεγαλύτερο βαθμό αν χρησιμοποιηθεί μια ενιαία γλώσσα, αντί των πολλαπλών γλωσσών επιπέδου εφαρμογής.

2.7 Διαχείριση Γνώσης – κατανεμημένα συστήματα διαχείρισης γνώσης

Αρχικός στόχος της παρούσας διατριβής δεν είναι απλά η μελέτη μοντέλων ελέγχου πρόσβασης, αλλά και η συνδυασμένη εφαρμογή τους σε κατανεμημένα συστήματα καθώς και σε συνεργαζόμενα Π.Σ. που σχηματίζουν δυναμικά μεταβαλλόμενους συνασπισμούς. Σε πολλές από τις προσεγγίσεις που αναφέρθηκαν, το πρόβλημα της ετερογένειας και της αναζήτησης πόρων αναφέρεται ακροθιγώς. Για παράδειγμα στην εργασία (Shafiq et al, 2005), αναφέρεται ότι τα προβλήματα ετερογένειας μπορούν να αντιμετωπιστούν με τεχνικές που εμπίπτουν στο γνωστικό χώρο των βάσεων δεδομένων. Ανάλογη είναι και η αντιμετώπιση από τον (Belokosztolszki, 2004), στη διατριβή του. Για λόγους συνέχειας, καθώς και προκειμένου να αντιμετωπιστεί κατά το δυνατόν πληρέστερα το αρχικό ερευνητικό πρόβλημα της παρούσας διατριβής, προτείνονται στα πλαίσια των παραγράφων 3.4 και 5.6 ενδεικτικές λύσεις στο πρόβλημα τόσο της δυνατότητας αποτελεσματικής αξιοποίησης της γνώσης (η οποία συχνά είναι σε αδόμητη μορφή), όσο και στο πρόβλημα της αναζήτησης γνωσιακών αγαθών στο συνασπισμό με ελαχιστοποιημένη κατανάλωση δικτυακών πόρων. Στα πλαίσια αυτά, θα παρουσιάσουμε συνοπτικά και συγκριτικά με την προτεινόμενη αρχιτεκτονική στα πλαίσια της παρούσας διατριβής, συστήματα κατανεμημένης διαχείρισης γνώσης, καθώς και τα μοντέλα ασφάλειας που αυτά υιοθετούν.

2.7.1 Κατανεμημένα συστήματα διαχείρισης γνώσης - υλοποιήσεις

Το σύστημα ADAM (Seleznyov et al, 2004) είναι ένα κατανεμημένο σύστημα, που χρησιμοποιεί το βασισμένο στην εμπιστοσύνη μοντέλο προκειμένου να διαπραγματευτεί την εξουσιοδότηση μιας συναλλαγής μεταξύ διαφορετικών χρηστών του συστήματος. Η αρχιτεκτονική του είναι βασισμένη στη χρήση πρακτόρων, όπου σε κάθε περιοχή που συμμετέχει στο σύστημα αντιστοιχείται ένας πράκτορας υπεύθυνος για την αναζήτηση (Search-Agent) και ένας πράκτορας υπεύθυνος για την εξουσιοδότηση του χρήστη (Security-Agent). Ο χρήστης από την πλευρά του απλά παρέχει κάποιο αναγνωριστικό κωδικό (PIN) και στη συνέχεια ο Security-Agent αναζητά το αναγνωριστικό κλειδί του χρήστη και επιχειρεί την έναρξη συναλλαγής διπραγματευόμενος για λογαριασμό του/της. Το σύστημα ADAM είναι μόνο με την γενικευμένη έννοια ένα σύστημα κατανεμημένης διαχείρισης γνώσης και όχι με την ειδικότερη, λόγω του ότι η γνώση που διαχειρίζεται είναι απλά γνώση που αφορά στην πρότερη συμπεριφορά των χρηστών, δηλαδή συνίσταται στην αναζήτηση πληροφοριών σχετικών με την προηγούμενη δραστηριότητα ενός χρήστη. Παράλληλα, το μοντέλο ασφάλειας που υιοθετεί, επιτρέπει σε ένα χρήστη με κακόβουλη συμπεριφορά να αλλάξει ταυτότητα και να ξεκινήσει από μηδενικής βάσης τη σύναψη συναλλαγών. Το γεγονός αυτό το καθιστά εφαρμόσιμο σε περιβάλλοντα που δεν διαθέτουν σαφώς διατυπωμένη πολιτική, ωστόσο καθίσταται ακατάλληλο για συστήματα με ευαίσθητο περιεχόμενο, περιορισμός που δεν ισχύει για τη δική μας προσέγγιση.

Το Edutella (Nejdl et al, 2002) είναι ένα πολύ ενδιαφέρον σύστημα πολλαπλών δυνατοτήτων, υλοποιημένο με χρήση της βασισμένης στη Java τεχνολογίας JXTA, που ακολουθεί την αρχιτεκτονική των ομότιμων (peer to peer) δικτύων. Το Edutella χρησιμοποιεί την τεχνολογία RDF (Resource Description Framework) για τη διαχείριση των μεταδεδομένων, ενώ χρησιμοποιεί μια ειδική γλώσσα για την υποβολή ερωτημάτων που αφορούν σε πόρους που βρίσκονται διασκορπισμένοι σε διαφορετικά μέρη του συστήματος. Το σύστημα Edutella έχει την ικανότητα να ελέγχει τη ροή της πληροφορίας προκειμένου για την αποφυγή ανάσχεσης της ροής πληροφορίας (bottleneck). Το μοντέλο ασφάλειας που χρησιμοποιεί, βασίζεται στην

ιδέα ότι οι κόμβοι που συμμετέχουν δανείζουν στους υπόλοιπους πιστοποιητικά ώστε ο κάθε κόμβος να χτίζει μια δική του κοινότητα εμπιστοσύνης. Η υλοποίηση του παραπάνω μοντέλου ασφάλειας βασίζεται σε μια ειδικά κατασκευασμένη γλώσσα βασισμένη στη γλώσσα Datalog. Στη δική μας προσέγγιση αντίθετα, βασιζόμαστε σε μια λύση που υιοθετεί το μοντέλο RBAC, κάτι που την καθιστά εφαρμόσιμη σε πολύ μεγαλύτερο εύρος συστημάτων και σε περιβάλλοντα συνασπιζόμενων Π.Σ. με χαρακτηριστικότερα παραδείγματα τα περιβάλλοντα ηλεκτρονικής διακυβέρνησης, ιατρικά διασυνδεδεμένα περιβάλλοντα κοκ.

Το σύστημα XAROP (Tempich et al, 2004) βασίζεται και αυτό στην τεχνολογία ομότιμων δικτύων και μπορεί να διαχειρίζεται ετερογενείς πόρους γνώσης με χρήση οντολογιών. Η αυθεντικοποίηση γίνεται με χρήση πιστοποιητικών στα πλαίσια μιας αρχής έκδοσης πιστοποιητικών που λειτουργεί στα πλαίσια του συστήματος. Ο καθορισμός των προνομίων πρόσβασης σε πόρους γίνεται με μια μηχανική αντιστοίχηση προνομίων σε ομάδες χρηστών, από τον ίδιο το χρήστη στον οποίο ανήκουν οι πόροι. Κάτι τέτοιο δυσχεραίνει αφενός μεν τους χρήστες, αφού πρέπει να καθορίζουν από μόνοι τους μια σειρά από κανόνες για τη διαχείριση κάθε πόρου ξεχωριστά, αφετέρου δυσχεραίνει τη δυνατότητα κλιμάκωσης του συστήματος καθώς για μεγάλο αριθμό πόρων και χρηστών η πληροφορία η σχετική με το ποια πρόσβαση είναι επιτρεπτή, καθίσταται δύσκολα διαχειρίσιμη.

Το SemanticLIFE (Weippl et al, 2004) είναι μια πλατφόρμα που αποσκοπεί στο να αποθηκεύει όλα τα ηλεκτρονικά αρχεία ενός χρήστη. Το μοντέλο ασφάλειας του στηρίζεται κυρίως στην υλοποίηση RBAC ελέγχων μέσα από τη χρήση συστήματος διαχείρισης βάσης δεδομένων - ΣΔΒΔ. Ωστόσο δεν παρέχει δυνατότητες για συνεργασία με άλλα συστήματα παρόμοιου ή διαφορετικού τύπου, ενώ σε αντίθεση με τον περιοριστικό ρόλο της εισαγωγής ενός προσαρμοσμένου σε ΣΔΒΔ μοντέλου ασφάλειας, η δική μας προσέγγιση είναι πολύ πιο γενική και μπορεί να εφαρμοστεί σε επίπεδο εφαρμογής, χωρίς να είναι δεσμευτική η εισαγωγή βάσης δεδομένων.

2.8 Συμπεράσματα – συγκριτική επισκόπηση

Με βάση την παραπάνω ανάλυση καθίσταται προφανές, πως παρά την ύπαρξη διαφορετικών μοντέλων ασφάλειας, την ύπαρξη διαφορετικών γλωσσών καταγραφής πολιτικών ασφάλειας και την ύπαρξη διαφορετικών προσεγγίσεων στο θέμα της αντιμετώπισης ταυτόχρονα πολλαπλών πολιτικών, υπάρχει ανάγκη για μια ενιαία, ολιστική αντιμετώπιση του προβλήματος. Συγκεκριμένα, υπάρχει ανάγκη για μία προσέγγιση που θα δίνει απαντήσεις στα ακόλουθα προβλήματα:

- Θα προτείνει μια κλιμακούμενη λύση στο πρόβλημα της διαχείρισης πολλαπλών αυτόνομων συστημάτων, όπου το καθένα διατηρεί την αυτονομία του αλληλεπιδρώντας με τα υπόλοιπα με ασφαλή τρόπο.
- Θα διακρίνεται από απλότητα στην εφαρμογή, και θα ελαχιστοποιεί το διαχειριστικό φόρτο.
- Θα αξιοποιεί πρότυπες τεχνολογίες σε μεγάλο βαθμό, ώστε να υποστηρίζει τη διαλειτουργικότητα σε επίπεδο εφαρμογής καθώς και την ανεξαρτησία από συγκεκριμένες πλατφόρμες.
- Θα αντιπροτείνει ένα λειτουργικό και υλοποιήσιμο - με σχετικά χαμηλή πολυπλοκότητα - τρόπο επίλυσης χαμηλής κρισιμότητας συγκρούσεων.

Στα πλαίσια της παρούσας διατριβής όπως αναφέρθηκε, κατά κανόνα οι προτεινόμενες λύσεις χρησιμοποιούν το πλέον διαδεδομένο και καθιερωμένο μοντέλο

ασφάλειας, το βασισμένο σε ρόλους (RBAC) και μάλιστα στην τελευταία του μορφή που υποστηρίζει περιορισμούς όσο και ιεραρχίες. Προκειμένου για την αυτοματοποιημένη διαχείριση και την κωδικοποίηση των κανόνων σε γλώσσες πολιτικής επιλέχτηκε ο βασικός πυρήνας της XACML γλώσσας, με τις κατάλληλες προσαρμογές όπως αυτές περιγράφονται στις εργασίες: (Belsis et al, 2005g)(Malatras et al, 2005a) (Belsis et al, 2005b)(Belsis 2006e) προκειμένου για την εφαρμογή των προτεινόμενων λύσεων σε περιβάλλοντα πολλαπλών πολιτικών. Η υποστήριξη κληρονομικοτήτων και η κωδικοποίησή τους σε γλώσσα πολιτικής υψηλού επιπέδου γίνεται με χρήση της βασισμένης στην XML γλώσσα RDF.

Η προτεινόμενη λύση στο πρόβλημα της διαχείρισης πολλαπλών αυτόνομων οργανισμών, τυγχάνει εφαρμογής σε διαφορετικού τύπου συστήματα, είναι δε χαμηλής σχετικά πολυπλοκότητας. Η προτεινόμενη αρχιτεκτονική που την υλοποιεί περιγράφεται στο κεφάλαιο 7 της παρούσας διατριβής. Παράλληλα, προκειμένου για τη δημιουργία ενός πλαισίου αυτοματοποιημένης διαχείρισης και ελάττωσης του διαχειριστικού φόρτου, προτείνεται η χρήση ενός μηχανισμού που αξιοποιεί τεχνικές προγραμματισμού με χρήση περιορισμών. Σε αντίθεση με τις προσεγγίσεις τις βασισμένες στο μοντέλο εμπιστοσύνης, διακρίνουμε το πρόβλημα της αυθεντικοποίησης από αυτό της εξουσιοδότησης σε πόρους, δίνοντας έμφαση στην αυτοματοποιημένη διαχείριση ασφάλειας. Έτσι η κωδικοποίηση των κανόνων ασφάλειας γίνεται από μια γλώσσα υψηλού επιπέδου, αφήνοντας τη διασύνδεση με τα κατώτερα επίπεδα να γίνεται σε επίπεδο εφαρμογής. Παράλληλα, το πρόβλημα της ταυτόχρονης διαχείρισης πόρων και χρηστών προερχόμενων από διαφορετικά επίπεδα είναι αρκετά πολύπλοκο και με πολλές και διαφορετικές παραμέτρους, καθιστώντας το πρόβλημα της αυθεντικοποίησης δευτερεύον που μπορεί να αντιμετωπιστεί εφαρμόζοντας μία από τις καλά εδραιωμένες λύσεις (πχ χρήση ψηφιακών πιστοποιητικών κλπ).

Στα χαρακτηριστικά της προτεινόμενης λύσης στα πλαίσια της παρούσας διατριβής είναι η δυνατότητα κλιμάκωσης, ενώ με την εισαγωγή του μοντέλου που κάνει συνδυασμένη χρήση περιορισμών και ασαφούς λογικής εισάγεται μία καινοτομική λύση στο θέμα της επίλυσης συγκρούσεων μεταξύ πολιτικών.

ΚΕΦΑΛΑΙΟ 3 - Διαχείριση Διαμοιραζόμενων Γνωσιακών πόρων σε κατανεμημένα περιβάλλοντα

Σε κατανεμημένα περιβάλλοντα συνεργαζόμενων Π.Σ. όπου ο αριθμός των συμμετεχόντων μερών μεταβάλλεται δυναμικά (όπως επίσης και ο αριθμός διαμοιραζόμενων πόρων), ένα από τα σημαντικά προβλήματα που ανακύπτουν έχει να κάνει με την χρήση τεχνικών αποδοτικής ανάκτησης, κατηγοριοποίησης και διάχυσης των γνωσιακών πόρων. Στα παραπάνω πλαίσια, δύο είναι τα σημαντικότερα προβλήματα τα οποία αποτέλεσαν αντικείμενο μελέτης:

- Η χρήση τεχνικών αναζήτησης και διήθησης της πληροφορίας μέσα από το σύνολο των πόρων που διαθέτει το κάθε υποσύστημα.
- Η υποβολή ερωτημάτων και αντίστοιχα η λήψη απαντήσεων, ελαχιστοποιώντας την κατανάλωση δικτυακών και άλλων πόρων του συστήματος.

Στα πλαίσια της αναζήτησης λύσεων στα δύο παραπάνω προβλήματα, στο παρόν κεφάλαιο θα περιγραφούν οι τεχνικές που αναπτύχθηκαν προκειμένου για την κατηγοριοποίηση ημιδομημένων κειμένων σε κατηγορίες με κριτήρια που καθορίζονται δυναμικά από τους ίδιους τους χρήστες, ενώ στη συνέχεια θα περιγραφούν οι τεχνικές για την υποβολή ερωτήσεων σε δικτυακά περιβάλλοντα με ελαχιστοποιημένη κατανάλωση των δικτυακών πόρων.

3.1 Αποδοτική κατηγοριοποίηση εγγράφων

Στην πρώτη ενότητα του κεφαλαίου θα περιγράψουμε εν συντομία μια λύση που επιτρέπει την κατηγοριοποίηση εγγράφων σε δύο (ή και περισσότερες) κατηγορίες-κλάσεις. Οι κλάσεις μπορούν να προσδιοριστούν από τα κριτήρια που θέτει ο χρήστης, ο οποίος δημιουργεί μηχανικά ένα μικρό δείγμα με βάση το οποίο θα ταξινομηθούν τα υπόλοιπα κείμενα. Η κύρια ιδέα πίσω από τη συγκεκριμένη προσέγγιση είναι ότι ένα κείμενο μπορεί ή όχι να περιέχει ορισμένα από τα συγκεκριμένα χαρακτηριστικά που έχουν οριστεί στο δείγμα. Για κάθε κείμενο σχηματίζεται ένας πίνακας που καταγράφει την ύπαρξη ή όχι ενός χαρακτηριστικού στο συγκεκριμένο κείμενο και κατόπιν με βάση τις εγγραφές του πίνακα κατατάσσεται το κείμενο σε μία από τις παραπάνω κατηγορίες. Στα συγκεκριμένα πειράματα που έγιναν στα πλαίσια της διατριβής χρησιμοποιήθηκαν δύο κλάσεις, στις οποίες κατατάσσονταν τα κείμενα, ως ενδιαφέροντα ή μη ενδιαφέροντα, ανάλογα με την ύπαρξη ή όχι μιας σειράς από χαρακτηριστικά στο περιεχόμενο των κειμένων.

Οι τεχνικές κατηγοριοποίησης κειμένων έχουν αποκτήσει ιδιαίτερο ενδιαφέρον κυρίως λόγων της πληθώρας των εφαρμογών τους αλλά και του χαμηλού κόστους ανάπτυξης τους. Οι περισσότερες από αυτές λειτουργούν στη βάση της κατηγοριοποίησης κειμένων σε ενδιαφέροντα και μη (Cohen 1996) (Brutlag et al, 2000) (Sahami et al, 1998) (Gee, 2003). Προκειμένου για την μέτρηση της απόδοσης μιας τεχνικής χρησιμοποιούνται οι ακόλουθες παράμετροι (Drucker et al, 1999):

$\text{Recall} = \frac{Categories\_Found\_correct}{Total\_Categories\_Correct}$, $\text{Precision} = \frac{Categories\_Found\_Correct}{Total\_categories\_Found}$ Για παράδειγμα αν ένα έγγραφο δεν είναι ενδιαφέρον και $N_{S\to S}$ είναι ο αριθμός των εγγράφων που σωστά έχουν κατηγοριοποιηθεί ως μη ενδιαφέροντα και $N_{S\to L}$ είναι ο

αριθμός μη ενδιαφερόντων εγγράφων που έχουν κατηγοριοποιηθεί εσφαλμένα ως ενδιαφέροντα και $N_{L\to S}$ είναι ο αριθμός ενδιαφερόντων εγγράφων που έχουν κατηγοριοποιηθεί ως μη ενδιαφέροντα, τότε έχουμε: Precision=$\frac{N_{S\to S}}{N_{S\to S}+N_{L\to S}}$ Recall=$\frac{N_{S\to S}}{N_{S\to S}+N_{S\to L}}$. Οι αντίστοιχες τιμές για τις μετρικές Recall και Precision ξεκινώντας με αντίστροφη αφετηρία, δηλαδή αν θεωρήσουμε ότι ο στόχος μας είναι να εντοπίσουμε τα έγκυρα έγγραφα, ορίζονται τελείως συμμετρικά. Αν και οι προαναφερθείσες συναφείς ερευνητικές προσεγγίσεις χαρακτηρίζονται από υψηλό βαθμό ακρίβειας, εμφανίζουν χαμηλά ποσοστά ανάκλησης (recall). Σκοπός της προσέγγισής μας είναι να επιτύχουμε όχι μόνο υψηλά ποσοστά ακρίβειας, αλλά και χαμηλούς χρόνους εκπαίδευσης του συστήματος. Προκειμένου για την κατηγοριοποίηση του δείγματος, επιλέξαμε τον αλγόριθμο Ιεραρχικής Μίξης Εμπειρογνώμονα (Hierarchical Mixtures of Experts -HME) που έχει εφαρμοστεί στο παρελθόν επιτυχώς σε αντίστοιχα προβλήματα (Jordan et al, 1994) (Waterhouse et al, 1994).

Προκειμένου να βελτιώσουμε την ακρίβεια του αλγορίθμου εφαρμόστηκαν στρατηγικές επιλογής χαρακτηριστικών (feature selection strategies) βασισμένες στην επιλογή περιθωρίου (margin) στα δεδομένα εκπαίδευσης του συστήματος. Στις επόμενες παραγράφους περιγράφουμε τις επιλογές μας, ξεκινώντας από την ερμηνεία της κρισιμότητας της επιλογής των σημαντικότερων χαρακτηριστικών.

Μία από τις πιο σημαντικές δραστηριότητες στην διαδικασία κατάταξης είναι η επιλογή κατάλληλων χαρακτηριστικών ικανών να αναπαραστήσουν με επιτυχία τις επιθυμητές κλάσεις. (Kira et al, 1992). Η επιλογή των υποψήφιων χαρακτηριστικών μπορεί να είναι ένα πραγματικό μειονέκτημα για ένα αλγόριθμο, τόσο σε δυσκολία όσο και στους απαιτούμενους χρόνους (Jacobs et al, 1991), (Jordan et al, 1994).

Θεωρούμε όλα τα έγγραφα (τόσο αυτά του δείγματος που θα χρησιμοποιηθεί για την εκπαίδευση του συστήματος, όσο και τα υπόλοιπα μη κατηγοριοποιημένα έγγραφα) ότι μπορούν να αναπαρασταθούν από διανύσματα με δυαδικά χαρακτηριστικά: $e=(f_1, f_2,.. f_N)$, όπου N είναι ο αριθμός των χαρακτηριστικών.

Χρησιμοποιούμε την εξής απλή πρακτική: για κάθε έγγραφο αντιστοιχείται η τιμή 1 στο χαρακτηριστικό f_j εάν το έγγραφο περιέχει το χαρακτηριστικό f_j και 0 στην αντίθετη περίπτωση. Στην περίπτωση εγγράφων που ανήκουν στο δείγμα που θα χρησιμοποιηθεί προς εκπαίδευση, κάθε διάνυσμα περιέχει μια επιπλέον συνιστώσα (Label): ($f_1, f_2,.. f_N,$ *Label)*. Σύμφωνα με τα χαρακτηριστικά του δείγματος αυτού, ενδιαφερόμαστε να αντιστοιχίσουμε σε κάθε ένα από τα έγγραφα μια ένδειξη (label) ενδεικτική της κατηγοριοποίησης. Επομένως η συνάφεια κάθε νεοεισερχόμενου εγγράφου καθορίζεται από τις χαρακτηριστικές ενδείξεις που αντιστοιχούνται σε αυτό. Ο πίνακας 3.1 παρουσιάζει ένα τρόπο αναπαράστασης μιας απλοποιημένης συλλογής εγγράφων χρησιμοποιώντας τις συχνότητες ως χαρακτηριστικά. Επομένως, αντί να χρησιμοποιούμε τις τιμές 0 ή 1 για κάθε χαρακτηριστικό χρησιμοποιούμε τις συχνότητες εμφάνισης των χαρακτηριστικών. Στην πρώτη στήλη έχουμε ενδεικτικά 15 χαρακτηριστικά να έχουν εξαχθεί από το χρησιμοποιούμενο προς εκπαίδευση δείγμα (ο αριθμός των χαρακτηριστικών συνήθως είναι πολύ μεγαλύτερος). Στη δεύτερη στήλη έχουμε τη συλλογή συχνοτήτων χαρακτηριστικών (collection feature frequency - cff) (πόσες φορές ένα χαρακτηριστικό εμφανίζεται στο δείγμα) ενώ οι υπόλοιπες στήλες καταγράφουν την συχνότητα χαρακτηριστικών (feature frequency - ff) (πόσες φορές ένα χαρακτηριστικό εμφανίζεται σε συγκεκριμένο έγγραφο).

Εξαχθέντα χαρακτηριστικά	Συχνότητα cff	#αριθμός στα κείμενα	Κείμενο1	Κείμενο2	Κείμενο3	Κείμενο4
Feature1	$cff_1=3$	2	$ff_{1\ 1}=0$	$ff_{2\ 1}=1$	$ff_{3\ 1}=0$	$ff_{4\ 1}=2$
Feature2	$cff_2=3$	2	$ff_{1\ 2}=0$	$ff_{2\ 2}=2$	$ff_{3\ 2}=1$	$ff_{4\ 2}=0$
Feature3	$cff_3=3$	3	$ff_{1\ 3}=0$	$ff_{2\ 3}=1$	$ff_{3\ 3}=1$	$ff_{4\ 3}=1$
Feature4	$cff_4=4$	2	$ff_{1\ 4}=0$	$ff_{2\ 4}=1$	$ff_{3\ 4}=0$	$ff_{4\ 4}=3$
Feature5	$cff_5=4$	2	$ff_{1\ 5}=3$	$ff_{2\ 5}=0$	$ff_{3\ 5}=1$	$ff_{4\ 5}=0$
Feature6	$cff_6=4$	3	$ff_{1\ 6}=2$	$ff_{2\ 6}=1$	$ff_{3\ 6}=0$	$ff_{4\ 6}=1$
Feature7	$cff_7=5$	3	$ff_{1\ 7}=1$	$ff_{2\ 7}=3$	$ff_{3\ 7}=0$	$ff_{4\ 7}=1$
Feature8	$cff_8=5$	3	$ff_{1\ 8}=3$	$ff_{2\ 8}=1$	$ff_{3\ 8}=0$	$ff_{4\ 8}=1$
Feature9	$cff_9=5$	3	$ff_{1\ 9}=2$	$ff_{2\ 9}=0$	$ff_{3\ 9}=2$	$ff_{4\ 9}=1$
Feature10	$cff_{10}=5$	3	$ff_{1\ 10}=1$	$ff_{2\ 10}=2$	$ff_{3\ 10}=2$	$ff_{4\ 10}=0$
Feature11	$cff_{11}=6$	3	$ff_{1\ 11}=1$	$ff_{2\ 11}=0$	$ff_{3\ 11}=2$	$ff_{4\ 11}=3$
Feature12	$cff_{12}=7$	2	$ff_{1\ 12}=0$	$ff_{2\ 12}=6$	$ff_{3\ 12}=0$	$ff_{4\ 12}=1$
Feature13	$cff_{13}=8$	4	$ff_{1\ 13}=2$	$ff_{2\ 13}=2$	$ff_{3\ 13}=1$	$ff_{4\ 13}=3$
Feature14	$cff_{14}=8$	4	$ff_{1\ 14}=3$	$ff_{2\ 14}=2$	$ff_{3\ 14}=1$	$ff_{4\ 14}=2$
Feature15	$cff_{15}=9$	3	$ff_{1\ 15}=1$	$ff_{2\ 15}=4$	$ff_{3\ 15}=0$	$ff_{4\ 15}=4$
Label			1	1	1	0

Πίνακας 3.1. Παράδειγμα κατηγοριοποίησης εγγράφων μετρώντας τη συχνότητα ενός χαρακτηριστικού σε ένα έγγραφο. Η τελευταία γραμμή αντιστοιχεί στην ένδειξη που αντιστοιχείται στο έγγραφο. Label ←0 σημαίνει ενδιαφέρον έγγραφο. Οι τελευταίες τέσσερις στήλες αποτελούν ενδεικτική αναπαράσταση εγγράφων με διανύσματα.

Στο παράδειγμα του πίνακα 3.1 υποθέτουμε (βλ. την ετικέτα στην πρώτη στήλη του πίνακα) ότι η διαδικασία επιλογής χαρακτηριστικών έχει ολοκληρωθεί πριν από το σχηματισμό του πίνακα και μόνο 15 χαρακτηριστικά έχουν τελικά χρησιμοποιηθεί για να αναπαραστήσουν το σύνολο των εγγράφων. Σε μια εναλλακτική προσέγγιση (υποθέτοντας πάλι ότι το σύνολο των χαρακτηριστικών είναι 15 όπως στην προηγούμενη περίπτωση) μπορούμε να χρησιμοποιήσουμε ένα αλγόριθμο επιλογής χαρακτηριστικών ώστε να ελαχιστοποιήσουμε τον αριθμό των χρησιμοποιούμενων χαρακτηριστικών και να παραμείνουν μόνο τα σημαντικότερα από αυτά στη διαδικασία κατηγοριοποίησης. Άλλες ενδιαφέρουσες αναπαραστάσεις κειμένων μπορούν να συμπεριλάβουν βάρη στον υπολογισμό των αντίστοιχων χαρακτηριστικών. Επομένως, μπορούμε να απλοποιήσουμε τον απαιτούμενο χώρο για την αναπαράσταση χαρακτηριστικών χρησιμοποιώντας δύο στήλες για κάθε έγγραφο: μία που θα δηλώνει την ύπαρξη ή όχι ενός χαρακτηριστικού (αντιστοιχώντας τις τιμές 0 ή 1) και μια άλλη στήλη να απεικονίζει βάρη με την τυπική τους μορφή (για παράδειγμα ένα αριθμό που να δηλώνει πόσες φορές ένα χαρακτηριστικό εμφανίζεται σε ένα έγγραφο, διαιρεμένο με τη συχνότητα εμφάνισης στη συλλογή). Ο πίνακας 3.2 που ακολουθεί αποτελεί μια παραλλαγή του πίνακα 3.1, που υλοποιεί τις παραπάνω αρχές).

Σύνολο χαρακτηριστικών	Συχνότητα cff	#αριθμός σε έγγραφα	…	Δυαδικά χαρακτηριστικά	Σχετικά βάρη στο έγγραφο	…..
Feature1	$cff_1=3$	2		1(εμφανίζεται)	$ff_{2\,1}=1/3$	
Feature2	$cff_2=3$	2		1	$ff_{2\,2}=2/3$	
Feature3	$cff_3=3$	3		1	$ff_{2\,3}=1/3$	
Feature4	$cff_4=4$	2		1	$ff_{2\,4}=1/4$	
Feature5	$cff_5=4$	2		0 (δεν εμφανίζεται)	$ff_{2\,5}=0/4$	
Feature6	$cff_6=4$	3		1	$ff_{2\,6}=1/4$	
….				…	…	
Label					1	

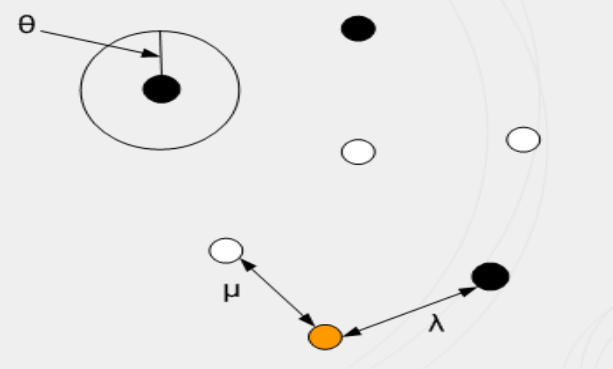
Πίνακας 3.2 Ελάττωση του αριθμού των αναγκαίων χαρακτηριστικών για την αναπαράσταση εγγράφων. Η τελευταία στήλη καταγράφει τα βάρη που αντιστοιχούνται σε συγκεκριμένα χαρακτηριστικά.

Στα επόμενα θα θεωρήσουμε ότι τα έγγραφα αναπαριστώνται χρησιμοποιώντας μόνο δυαδικά χαρακτηριστικά (1 αν το χαρακτηριστικό υπάρχει στο έγγραφο και 0 αν δεν υπάρχει). Επίσης χρησιμοποιήθηκαν όλα τα διαθέσιμα χαρακτηριστικά ενός εγγράφου. Απαιτείται μια καλή επιλογή των καταλληλότερων χαρακτηριστικών ώστε να ελαττωθεί ο αριθμός χρησιμοποιούμενων χαρακτηριστικών στην τελική διαδικασία μια και συνήθως η διαδικασία επιλογής απαιτεί σημαντικούς χρόνους, λόγω του ότι για μεγάλο αριθμό εγγράφων ο αριθμός διαθέσιμων χαρακτηριστικών μπορεί να μεγαλώσει υπερβολικά. Ο χρόνος που απαιτείται για την αναζήτηση των καλύτερων χαρακτηριστικών αποτελεί και ένα από τα κύρια χαρακτηριστικά της παραπάνω προσέγγισης. Το βέλτιστο σύνολο χαρακτηριστικών εξαρτάται τόσο από το είδος των δεδομένων που χρησιμοποιούνται για έλεγχο καθώς και από το χρησιμοποιούμενο αλγόριθμο. Από ένα πολύ μεγάλο σύνολο δεδομένων ο τελικός αριθμός χαρακτηριστικών μπορεί να μειωθεί στο 1-3% κάτι που υποδεικνύεται και από διαφορετικές έρευνες και πειράματα (Lewis 1992)(Koller et Sahami, 1997) (Mladenic 1998), που έδειξαν ότι συστήματα που έκαναν χρήση του 1-3% των χαρακτηριστικών τελικά δεν είχαν σημαντική μείωση στην απόδοση.

3.1.1 Επιλογή χαρακτηριστικών - εκτίμηση της ποιότητας των χαρακτηριστικών

Προκειμένου για την επιλογή χαρακτηριστικών σε ένα πρόβλημα ταξινόμησης μπορούν να υιοθετηθούν διαφορετικοί αλγόριθμοι. Είναι όμως σημαντικό να μπορούν να καθοριστούν όχι μόνο τα καλύτερα χαρακτηριστικά αλλά και η ποιότητα της λύσης. Τα περιθώρια (margins) είναι μια χρήσιμη έννοια προκειμένου να μετρήσουμε την ποιότητα του συνόλου των χαρακτηριστικών (Schapire et al, 1997). Ένα περιθώριο είναι η γεωμετρική απόσταση που βοηθά να εκτιμήσουμε την ποιότητα ενός ταξινομητή (classifier) σε σχέση με το αποτέλεσμά του (Shapire et al 1999). Οι (Bachrach et al, 2004) παρουσιάζουν δυο αλγορίθμους επιλογής χαρακτηριστικών τον άπληστο αλγόριθμο ανάκρουσης (Greedy Feature Flip, G-Flip algorithm) και τον επαναληπτικό αλγόριθμο αναζήτησης με βάση το περιθώριο (Iterative Search Margin Based Algorithm) ή εν συντομία το Simba αλγόριθμο. Αυτοί οι δύο αλγόριθμοι χρησιμοποιούν περιθώρια με βάση γειτονικά σημεία $1^{ης}$ τάξεως (Crammer et al, 2002). Η χρήση περιθωρίων για γείτονες $1^{ης}$ τάξεως εγγυάται καλή απόδοση για κάθε επιλογή χαρακτηριστικών, καθώς επιλέγει ένα μικρό υποσύνολο χαρακτηριστικών διατηρώντας παράλληλα μεγάλα περιθώρια.

Υπάρχουν δύο τρόποι να οριστεί ως μετρική το περιθώριο σε σχέση με ένα κανόνα κατάταξης: το απλό περιθώριο (simple margin) και το βασισμένο στην υπόθεση περιθώριο (hypothesis margin measure). Το πρώτο μετρά απλά την απόσταση από το όριο λήψης της απόφασης. Σαν μετρική είναι όμως ασταθής και δύσκολη στον υπολογισμό της αφού για μεγάλο αριθμό στιγμιότυπων και θεωρώντας μικρές μεταβολές στις θέσεις των στιγμιότυπων, θα απαιτούσε δύσκολους υπολογισμούς και θα προκαλούσε μεγάλες αποκλίσεις στα αποτελέσματα. Το βασισμένο στην υπόθεση περιθώριο αντίθετα, υπολογίζει πόσο μπορούν να μετακινηθούν τα όρια χωρίς να αλλάξουν οι κατηγοριοποιήσεις στα στιγμιότυπα (εικ. 3.1). Αποδεικνύεται ότι ο υπολογισμός του περιθωρίου αυτού γίνεται με βάση τη σχέση: $\theta_P^W(x) = \frac{1}{2}(\| x-\mu \|_W - \| x-\lambda \|_W)$ (1), όπου μ και λ είναι τα πλησιέστερα σημεία στο χ με την ίδια και διαφορετική κατηγοριοποίηση αντίστοιχα ενώ το z δίνεται από τη σχέση $\| z \|_W = \sqrt{\sum_i w_i^2 z_i^2}$ (2). Θα πρέπει να σημειωθεί ότι η δοσμένη επιλογή χαρακτηριστικών επηρεάζει το περιθώριο μέσω του υπολογισμού της απόστασης.



Εικόνα 3.1Υπολογισμός του περιθωρίου (margin) βάσει των παραμέτρων μ και λ

3.1.2 Επιλογή χαρακτηριστικών με χρήση του Επαναληπτικού Αλγόριθμου Αναζήτησης Βάσει περιθωρίου - Feature selection using the Iterative Search Margin Based Algorithm (Simba)

Προκειμένου για την επιλογή των πιο σχετικών χαρακτηριστικών εφαρμόστηκε ο αλγόριθμος Simba. Ο λόγος για την επιλογή του αλγορίθμου Simba είναι ότι εμφανίζεται να υπερτερεί άλλων στατιστικών προσεγγίσεων όπως ο αλγόριθμος αμοιβαίας ανταλλαγής πληροφορίας (mutual information criterion) κλπ (Bachrach et al, 2004). Ο αλγόριθμος παρέχει ένα διάνυσμα με βάρη $w=(w_1, w_2, .. w_N)$, όπου N είναι ο αριθμός των υποψήφιων χαρακτηριστικών και κάθε w_j καταγράφει τη σημαντικότητα ενός χαρακτηριστικού στη διαδικασία κατηγοριοποίησης.

Για ένα σύνολο P από στιγμιότυπα στην περίπτωσή μας έγγραφα, υπολογίζουμε το περιθώριο υπόθεσης για κάθε στιγμιότυπο $x \in P$ χρησιμοποιώντας τη σχέση (1). Ο αλγόριθμος στο ξεκίνημα αρχικοποιεί το διάνυσμα ως $w = (1, 1, ...,1)$ και μετά από ένα αριθμό επαναλήψεων T χρησιμοποιώντας μία αύξουσα στοχαστική κλίση (stochastic gradient ascent) επί του αθροίσματος $\sum_i \theta_p(x_i)$ για όλα τα στιγμιότυπα x_i, ενημερώνει το διάνυσμα w: $w=w+\Delta$, όπου το διάνυσμα Δ δίνεται από την ακόλουθη εξίσωση:

$$\Delta i = \sum_{x \in P} \frac{\partial \theta(x_i)}{\partial w_i} = \frac{1}{2} \sum_{x \in P} \left(\frac{(x_i - \mu)^2}{\| x-\mu \|_w} - \frac{(x_i - \lambda)^2}{\| x-\lambda \|_w} \right) \quad (3)$$

Ο αλγόριθμος τελικά μετά από ένα αριθμό επαναλήψεων παρέχει ένα διάνυσμα w που περιέχει τις σχετικές βαρύτητες του κάθε χαρακτηριστικού.

3.1.3 Επιλογή χαρακτηριστικών με χρήση του άπληστου αλγόριθμου ανάκρουσης (Greedy Feature Flip Algorithm - G-flip)

Ένας εναλλακτικός αλγόριθμος που χρησιμοποιήθηκε στις εργασίες (Belsis et al, 2006a) και (Belsis et al, 2006d) είναι ο άπληστος αλγόριθμος ανάκρουσης (Greedy Feature Flip Algorithm (G-flip) (Crammer et al, 2002), ο οποίος δεν εξαρτάται από παραμέτρους, με την έννοια ότι δεν χρειάζεται να παραμετροποιούμε τον αριθμό των χαρακτηριστικών. Ο αλγόριθμος G-flip είναι άπληστος αλγόριθμος που επιχειρεί να μεγιστοποιήσει μία συνάρτηση *e(F)*, όπου F είναι το σύνολο των χαρακτηριστικών. Ενώ εκτελεί την ίδια διαδικασία ενημερώνει διαρκώς το σύνολο των χαρακτηριστικών. Σε κάθε επανάληψη ο αλγόριθμος επιλέγει να αφαιρέσει ή να προσθέσει το τρέχον χαρακτηριστικό υπολογίζοντας την συνάρτηση εκτίμησης $e(w) = \sum_{x \in S} \theta^{W}_{S \setminus x}(x)$ (4) υπολογίζοντας και εξαιρώντας το συγκεκριμένο χαρακτηριστικό.

Ο ακόλουθος ψευδοκώδικας από το (Crammer et al, 2002), περιγράφει τα βασικά βήματα που περιλαμβάνονται στην επιλογή του συνόλου των χαρακτηριστικών.

Αρχή

1. *Αρχικοποίησε το σύνολο των επιλεγμένων χαρακτηριστικών με το κενό σύνολο: F=∅ ;*
2. *Για όλα τα στιγμιότυπα στο δείγμα προς εκπαίδευση 1,2,..*
    a. *Αρχικοποίησε ένα τυχαίο συνδυασμό s από N χαρακτηριστικά*
    b. *Για i=1 μέχρι N*
        Υπολόγισε $e_1=e(F \cup s(i))$ // περιέλαβε το i-οστό χαρακτηριστικό
        υπολόγισε $e_2=e(F\setminus\{s(i)\})$ // απέκλεισε το i-οστό χαρακτηριστικό
        εάν e1>e2 τότε περιέλαβε στο F το i-οστό χαρακτηριστικό F= {F ∪ s(i)}
        αλλιώς απέκλεισε το i-οστό χαρακτηριστικό F=F\{s(i)}
    c. *εάν δεν έγινε καμία αλλαγή στο βήμα (b) σταμάτησε*

Τέλος

Ο αλγόριθμος επιχειρεί να μεγιστοποιήσει τη συνάρτηση εκτίμησης, καθώς σε κάθε βήμα αυξάνεται η τιμή της.

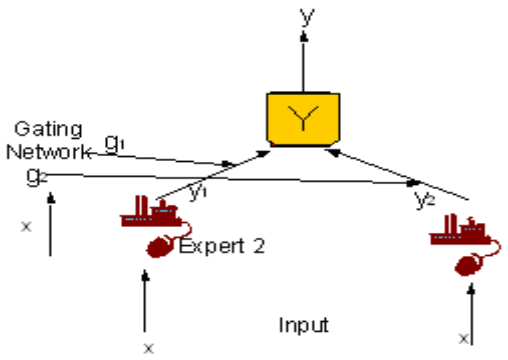
Αυτοί οι δύο αλγόριθμοι μπορούν να χρησιμοποιηθούν αποδοτικά για την εξαγωγή χαρακτηριστικών σε εποπτευόμενα συστήματα κατηγοριοποίησης σε πολλαπλές κλάσεις. Ο Simba επιστρέφει ένα διάνυσμα με βάρη που μας επιτρέπει να επιλέξουμε τα χαρακτηριστικά με το υψηλότερο βάρος, ενώ ο G-flip επιστρέφει ένα βέλτιστο σύνολο χαρακτηριστικών.

3.2 Ο αλγόριθμος ιεραρχικής μίξης εμπειρογνωμόνων (Hierarchical Mixtures of Experts Algorithm)

Το εξαγόμενο της διαδικασίας επιλογής βέλτιστων χαρακτηριστικών μπορεί να αξιοποιηθεί από ένα αλγόριθμο κατάταξης σε κλάσεις, βάσει προδιαγεγραμμένων κριτηρίων και με βάση μια σειρά από παρατηρήσεις. Μπορούμε να ορίσουμε μια παρατήρηση επί ενός συνόλου σαν μια συλλογή από αριθμητικές μετρήσεις που δηλώνονται από ένα διάνυσμα $x=(x_1, x_2, \ldots, x_k)$, όπου $x \in R^k$. Σε εφαρμογές κατηγοριοποίησης συνήθως δηλώνεται μια αντιστοίχηση $f: R^k \rightarrow \{0, 1\}$. Αυτή η

αντιστοίχηση συνήθως αναφέρεται ως ταξινομητής. Τα νέα δεδομένα άγνωστης μέχρι πρότινος συμπεριφοράς χαρακτηρίζονται από μία τιμή $y=f(x)\in\{0, 1\}$.
Ένας ταξινομητής μπορεί να οριστεί με ένα γενικό τρόπο θεωρώντας τα χαρακτηριστικά κάθε υπό εξέταση οντότητας. Επομένως ένας ταξινομητής είναι μια αντιστοίχηση $f : R^k \rightarrow CC$ από το χώρο των χαρακτηριστικών R^k, στο σύνολο των κλάσεων $CC = \{cc_1, cc_2, \ldots, cc_n\}$. Η επιλογή χαρακτηριστικών είναι μια διαδικασία επιλογής ενός υποσυνόλου από το σύνολο των χαρακτηριστικών ικανών να υποστηρίξουν τη διαδικασία αντιστοίχησης επαρκώς. Στη συνέχεια, ένας ταξινομητής αναλαμβάνει την πρόβλεψη με βάση το επιλεγμένο σύνολο χαρακτηριστικών. Για το σύστημά μας χρησιμοποιήθηκε ο ταξινομητής Μείξης Εμπειρογνωμόνων (Mixture of Experts -ME) (Fritsch et al, 1997). Σύμφωνα με τους (Jordan et al, 2004) ο αλγόριθμος ΜΕ κατέχει μια ξεχωριστή θέση στην κατηγορία των δυναμικά συνδυαζόμενων μεθόδων. Ο αλγόριθμος ΜΕ βασίζεται στην αρχή του ‘‘διαίρει και βασίλευε’’. Αντί να λύσει το πρόβλημα κατηγοριοποίησης επί ολοκλήρου του χώρου επιλογής χαρακτηριστικών, το διαιρούμε σε μικρές περιοχές και επιχειρούμε να διασπάσουμε το πρόβλημα τοπικά και να συνδυάσουμε τις εξαγόμενες λύσεις. Οι υποχώροι καθορίζονται από τις συναρτήσεις εισόδου g_m. Σε κάθε περιοχή αντιστοιχίζονται τοπικοί ταξινομητές (“εμπειρογνώμονες - experts”) y_m που συνδυάζονται χρησιμοποιώντας τις εισόδους g_m. Ο κάθε ταξινομητής συνδυάζει τις εισόδους διαφόρων τοπικών ταξινομητών που αποτελούν εισόδους γι αυτόν. Ο αλγόριθμος επιχειρεί στην ουσία να επιλύσει το πρόβλημα αναλύοντας το σε απλούστερα. Οι συναρτήσεις που χρησιμοποιούν οι εμπειρογνώμονες (ΜΕ) ανήκουν στην κατηγορία πιθανοθεωρητικών συναρτήσεων με μια είσοδο που συνδυάζει τις πιθανότητες. Βάσει αυτών το δίκτυο εκπαιδεύεται και κατηγοριοποιεί το χώρο εισόδου. Η εικόνα 3.2 απεικονίζει ένα δίκτυο εμπειρογνωμόνων με δύο εμπειρογνώμονες και μια έξοδο.

Για το σχηματισμό των εμπείρων δικτύων οι τυπικές επιλογές είναι γενικευμένα γραμμικά μοντέλα (Jordan et al, 1994) και perceptrons (Koller et al, 1997) πολλαπλών επιπέδων.



Εικόνα 3. 2 Ένα μοντέλο δικτύου μίξης εμπειρογνωμόνων αποτελούμενο από δύο εμπειρογνώμονες E_1, E_2

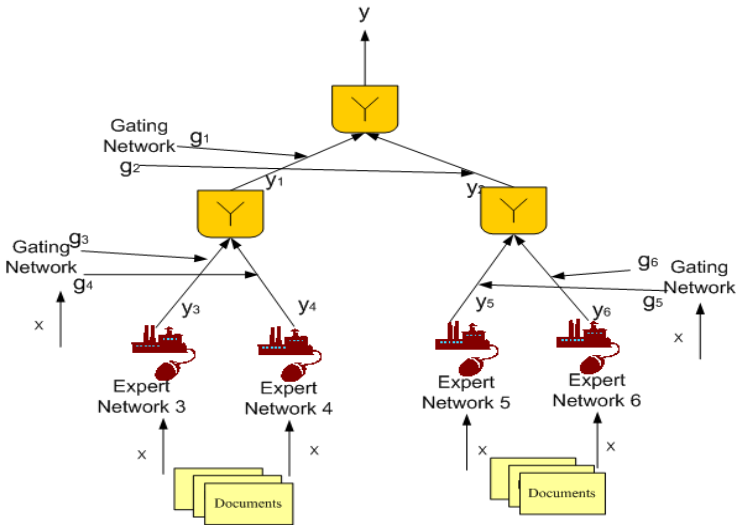
3.2.1 Γενικευμένα γραμμικά μοντέλα HME's

Θεωρούμε ότι το πρόβλημα μπορεί να απεικονιστεί χρησιμοποιώντας γενικευμένα γραμμικά μοντέλα της μορφής: $y_i = w_i^T x$, όπου w_i είναι οι παράμετροι. Η έξοδος του εμπείρου δικτύου του σχήματος 3.3 είναι η σταθμισμένη (από τις εξόδους των τοπικών δικτύων) μέση τιμή των εξόδων των εμπειρογνωμόνων που δίνεται από τη

σχέση: $y(x) = \sum_i g_i(x) y_i(x)$ (5), όπου $g_i(x)$ δηλώνει την πιθανότητα η είσοδος x να περικλείεται στο έμπειρο δίκτυο i. Σε ένα πρόβλημα κατηγοριοποίησης ενδιαφερόμαστε πάντοτε να υπολογίσουμε την πιθανότητα να προκύψει μια κατηγορία y θεωρώντας δεδομένο το x. Εναλλακτικά με όρους ενός μοντέλου ΜΕ υπολογίζουμε την υπό συνθήκη πιθανότητα $p(y|x)$ της εξόδου y δεδομένου του x. Αυτό μπορεί να υπολογιστεί από την εξίσωση (6): $p(y \mid x) = \sum_i g_i(x) \phi_i(y \mid x)$ (6), όπου φ_i (y_i στην Εικ. 3.3) αναπαριστά τις υπό συνθήκη βαρύτητες του Y δεδομένου του εμπειρογνώμονα i. Προκειμένου να διασφαλίσουμε μια πιθανοθεωρητική ερμηνεία του μοντέλου η συνάρτηση ενεργοποίησης g_i της εισόδου επιλέγεται με βάση τη συνάρτηση (Brindle, 1990):

$g_i = \exp(z_i) / \sum_j \exp(z_j)$ (7), όπου z_i είναι τα οι έξοδοι του δικτύου πριν τη θέσπιση ορίου. Με τη συνάρτηση αυτή, οι έξοδοι των δικτύων έχουν άθροισμα ίσο με τη μονάδα ένα και είναι πάντοτε θετικές.

Η ικανότητα να μοντελοποιούνται μη γραμμικές συναρτήσεις είναι ιδιαίτερα επιθυμητή σε στατιστικά μοντέλα. Ωστόσο οι μη γραμμικές συναρτήσεις που ένα μοντέλο ΜΕ μπορεί να αναπαραστήσει, είναι σχετικά περιορισμένες μεταξύ παρακείμενων περιοχών στο χώρο εισόδου δεδομένων. Μια συμπληρωματική προσέγγιση που προτάθηκε από τους Jordan and Jacobs (Jordan et al, 1994) είναι να χρησιμοποιούμε ως εισόδους στο δίκτυο τις εξόδους άλλων έμπειρων δικτύων. Το αποτέλεσμα είναι γνωστό σαν ιεραρχικό μοντέλο εμπείρων *hierarchical* mixtures-of-experts model (HME) και μπορεί να οπτικοποιηθεί σαν δέντρο. Ένα τέτοιο μοντέλο απεικονίζεται στην εικόνα 3.3. Η αρχιτεκτονική τέτοιων μοντέλων συνίσταται από εισόδους δύο επιπέδων με δυαδικά κλαδιά σε κάθε μη τερματικό κόμβο. Η έξοδος των εμπείρων E_3, E_4, E_5, E_6 είναι y_3, y_4, y_5, y_6 αντίστοιχα, οι έξοδοι των δικτύων G_1, G_2 στη βάση του δευτέρου επιπέδου είναι g_3, g_4, g_5, g_6. Για τις εξόδους των μη τερματικών κόμβων στη δεύτερη έχουμε $y_1=g_3y_3+g_4y_4$, $y_2=g_5y_5+g_6y_6$ και τελικά η έξοδος του συστήματος είναι $y=g_1y_1+g_2y_2$.



Εικόνα 3. 3 Δομή για ιεραρχικό δίκτυο μίξης εμπειρογνωμόνων με ύψος 2

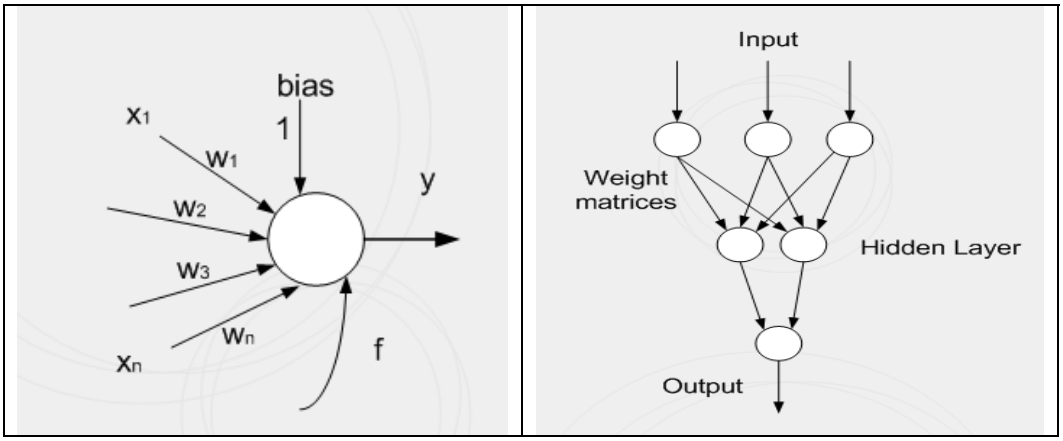
Η φάση εκπαίδευσης που αποσκοπεί στην εκτίμηση των παραμέτρων του συστήματος θεωρείται ζωτικής σημασίας για το σύστημα. Για τις ανάγκες της

κατηγοριοποίησης, το σύστημα πρέπει να εκπαιδευτεί με ένα κατάλληλο αριθμό παραμέτρων, που καθορίζουν τις τιμές των συναρτήσεων g_i, φ_i. Για την g_i χρησιμοποιούμε τη συνάρτηση της εξίσωσης 7 και για το έμπειρο δίκτυο γενικευμένα γραμμικά μοντέλα. Η κατανομή που περιγράφει η εξίσωση 6 αποτελεί τη βάση για τα έμπειρα δίκτυα και αποτελεί τη βάση για τη συνάρτηση εκτίμησης λάθους που μπορεί να βελτιστοποιηθεί χρησιμοποιώντας μια στοχαστική συνάρτηση με φθίνουσα κλίση ή χρησιμοποιώντας τον αλγόριθμο μεγιστοποίησης προσδοκιών (Expectation -Maximization EM) (Jordan et al, 1994). Στην περίπτωσή μας επιλέχτηκε ο αλγόριθμος EM.

Ο αλγόριθμος EM λειτουργεί με ένα επαναληπτικό τρόπο σε περιπτώσεις που λείπουν δεδομένα. Στην περίπτωση μας ως δεδομένα στον αλγόριθμο θεωρούνται οι έξοδοι των εμπείρων δικτύων των κατώτερων επιπέδων. Ένα από τα πλεονεκτήματα της χρήσης του συγκεκριμένου αλγορίθμου είναι ότι επιτρέπει την κατάτμηση των δεδομένων εισόδου σε υποσύνολα, ισάριθμα των επιμέρους εισόδων. Προκειμένου για την εκπαίδευση του συστήματος, χρησιμοποιούνται συνήθως Gaussian συναρτήσεις. Προκειμένου για την εκτίμηση της πιθανότητας λάθους, ένας συνήθης τρόπος είναι να εφαρμόσουμε την αρχή της μεγιστοποίησης της πιθανότητας που μπορεί να θεωρηθεί ότι αναπαρίσταται με τον όρο L. Δεδομένου ενός συνόλου ανεξάρτητων κατανεμημένων δεδομένων προς εκπαίδευση $\{x^n, t^n\}$, $n=1..N$, ή αντίστοιχα των δεδομένων προς κατηγοριοποίηση, η συγκεκριμένη παράμετρος δίνεται από τη σχέση: $L = \prod_n p(x,t) = \prod_n p(t \mid x)\, p(x)$ (8). Υπολογίζοντας τον αρνητικό λογάριθμο της πιθανότητας και εξαιρώντας τον όρο $p(x)$ επειδή δεν εξαρτάται από τις παραμέτρους του μοντέλου), μπορούμε να υπολογίσουμε μια συνάρτηση κόστους $E = -\sum_n p(t \mid x)$ (9). Λαμβάνοντας υπόψη τη συνάρτηση (6), η συνάρτηση κόστους για την κατάταξη μπορεί να υπολογιστεί ως ακολούθως: $E = -\sum_n \ln \sum_i g_i(x)\phi_i(t \mid x)$ (10). Αυτή η συνάρτηση κόστους πρέπει να ελαχιστοποιηθεί με χρήση του αλγορίθμου EM, μια πλήρης περιγραφή του οποίου μπορεί να αναζητηθεί στο (Jordan et al, 1994).

3.2.2 Perceptron μοντέλο HME's

Ένας εναλλακτικός τρόπος να μοντελοποιήσουμε το δίκτυο εμπειρογνωμόνων είναι να δημιουργήσουμε μια ιεραρχική δομή που αποτελείται από τεχνητούς νευρώνες, που αποτελούν μια αντιστοίχηση της μορφής $R^{k+1} \rightarrow Y \subseteq [-1, 1]$, όπου το Y μπορεί να είναι διακριτό, υποθέτοντας μόνο στοιχεία $\{\pm 1\}$. Η αντιστοίχηση δίνεται από μια συνάρτηση f(.), που αναφέρεται ως συνάρτηση ενεργοποίησης. Μια συνήθης επιλογή για τη συνάρτηση ενεργοποίησης είναι η σιγμοειδής μεταφοράς $1/(1+e^{-x})$ ή η υπερβολική εφαπτομένη tanh(x). Επιλέξαμε να μοντελοποιήσουμε το δίκτυο χρησιμοποιώντας ένα νευρώνα perceptron δύο επιπέδων. Το perceptron μπορεί να υπολογίσει μία έξοδο y από διαφορετικές εισόδους χρησιμοποιώντας μια μη γραμμική συνάρτηση ενεργοποίησης: $y = f(\sum_{i=1}^{n} w_i x_i + b)$, όπου w είναι ένα διάνυσμα βαρών, x είναι ένα διάνυσμα εισόδων και f είναι η συνάρτηση ενεργοποίησης.
Η έξοδος του νευρώνα τυπικά εξαρτάται από το σταθμισμένο άθροισμα των εισόδων και επηρεάζεται από το άθροισμα καθορίζοντας ορισμένα όρια τιμών.



Εικόνα 3.4α (αριστερά) Ένα απλό perceptron. 3.4β (δεξιά) Ένα perceptron δύο επιπέδων με ένα κρυμμένο επίπεδο.

Τα perceptrons μπορούν να χρησιμοποιηθούν σαν τμήματα μιας μεγαλύτερης και πιο πολύπλοκης δομής. Τα πολυεπίπεδα perceptrons, σε αναλογία με τη δημιουργία ιεραρχικών εμπείρων δικτύων που περιγράφηκαν στην προηγούμενη παράγραφο, είναι χρήσιμα εργαλεία που μπορούν να αξιοποιηθούν για την επίλυση δύσκολων προβλημάτων κατηγοριοποίησης όπου απαιτείται προηγούμενα εκπαίδευση του συστήματος. Ένα τυπικό πολυεπίπεδο δίκτυο perceptron (MLP) (εικ. 3.4β) αποτελείται από κόμβους που σχηματίζουν ένα στρώμα εισόδου, ένα ή περισσότερα επίπεδα και ένα στρώμα κόμβων εξόδου. Η μόνη αλλαγή σε σχέση με τα ιεραρχικά HME αναφέρεται στους τύπους των μονάδων που χρησιμοποιούνται, ενώ το υπόλοιπο σύστημα καθώς και ο αλγόριθμος Expectation -Maximization (EM) παραμένουν ίδιοι. Ο κύριος λόγος επίσης για την επιλογή της αρχιτεκτονικής perceptron είναι να διερευνηθεί το αν η συγκεκριμένη αρχιτεκτονική θα μπορούσε να λειτουργήσει καλύτερα με όρους απόδοσης σε σχέση με το γενικευμένο γραμμικό μοντέλο.

3.3 Συνοπτική περιγραφή πειραμάτων – Συμπεράσματα

Προκειμένου για την επαλήθευση της ικανότητας του συστήματος να ταξινομήσει ικανοποιητικά ένα δείγμα εγγράφων, διενεργήσαμε μια σειρά από πειράματα με διαθέσιμο στο διαδίκτυο δείγμα και με ιδιαίτερα χαρακτηριστικά δυσκολίας στην επεξεργασία και σωστή ταξινόμηση. Σαν υλικό επιλέχτηκε μια συλλογή από κείμενα ηλεκτρονικής αλληλογραφίας, για δύο κυρίως λόγους:

- λόγω της σημαντικότητας των κειμένων αυτών για το σύνολο σχεδόν των μελών ενός οργανισμού και
- λόγω του ότι παρουσιάζουν μια σειρά από ενδιαφέροντα χαρακτηριστικά και επίσης δεν στερούνται δομής, χωρίς ωστόσο να είναι και απόλυτα δομημένα. Ειδικότερα, ένα κείμενο ηλεκτρονικής αλληλογραφίας περιέχει μια σειρά από διαφορετικά πεδία, όπως για παράδειγμα το πεδίο αποστολέα, το θέμα, το κυρίως κείμενο, γεγονός που τους προσδίδει μερική δομή.

Ένα από τα προβλήματα επίσης είναι η αναζήτηση ενός αξιόλογου δείγματος για τη διεξαγωγή των πειραμάτων. Στη σχετική βιβλιογραφία πολύ λίγες αξιόπιστες συλλογές έχουν εμφανιστεί και καταστεί δημόσια διαθέσιμες. Για ορισμένες από αυτές ο ενδιαφερόμενος αναγνώστης μπορεί να αναφερθεί στις εργασίες των (Hidalgo 2002) και (Fawcett, 2003). Θα πρέπει να αναφέρουμε, ότι όπως και σε πολλές άλλες ερευνητικές προσεγγίσεις, τα πειράματά μας αποσκοπούσαν στην

κατάταξη σε δύο κυρίως κατηγορίες, συγκεκριμένα σε ενδιαφέροντα και μη κείμενα. Ωστόσο όπως αναφέρθηκε ήδη στην παράγραφο 3.1 η μέθοδος μας είναι πολύ εύκολα επεκτάσιμη στην περίπτωση που οι κλάσεις στις οποίες θέλουμε να κατατάξουμε τα έγγραφά μας είναι περισσότερες των δύο. Προκειμένου για τα πειράματά μας χρησιμοποιήθηκαν οι βάσεις της συλλογής *20030228_spam_2* που παρέχονται από το Spam Assassin (SpamAssassin, 2004). Η συλλογή αυτή περιλαμβάνει δύο βάσεις με έγγραφα τα οποία θα πρέπει να παραμείνουν μετά την επεξεργασία, τη 2*520030228_hard_ham_*2 που περιέχει 250 έγγραφα με ιδιαίτερης δυσκολίας χαρακτηριστικά και την *20030228_easy_ham* που περιέχει 2500 έγγραφα. Επίσης περιέχει και 1397 έγγραφα τα οποία έχουν χαρακτηριστεί εξαρχής ως μη ενδιαφέροντα. Στόχος των πειραμάτων είναι να διακρίνουμε την ικανότητα του συστήματος επιλέγοντας ένα μικρό δείγμα από κάθε βάση για να χρησιμοποιηθεί για την εκπαίδευσή του, να μπορέσει να κατατάξει τα υπόλοιπα έγγραφα και από τις δύο κατηγορίες σωστά.

3.3.1 Πειραματικά αποτελέσματα – η περίπτωση των γενικευμένων γραμμικών ιεραρχικών δικτύων εμπειρογνωμόνων

Προκειμένου για τον έλεγχο της αποτελεσματικότητας του συστήματος μας χρησιμοποιήθηκε αρχικά ο συνδυασμός των αλγορίθμων Ιεραρχικής Μίξης Εμπειρογνωμόνων (HME) και ο αλγόριθμος Simba για την επιλογή των χρησιμότερων χαρακτηριστικών. Από τα κείμενα χρησιμοποιήθηκαν χαρακτηριστικά από όλα τα διαθέσιμα πεδία.

Για τη συλλογή easy_ham το σύστημά μας έδειξε πολύ υψηλά ποσοστά στις επιτευχθείσες τιμές, αγγίζοντας οριακά το 100%. Στη συνέχεια, για τη συλλογή hard_ham, διαιρέσαμε τα 1397 μη ενδιαφέροντα μηνύματα σε 5 ομάδες, κάθε ένα από τα οποία περιείχε 240 μηνύματα (150 για εκπαίδευση και 90 για έλεγχο). Από τα 250 ενδιαφέροντα μηνύματα πήραμε τα 240 και από αυτά πάλι 150 χρησιμοποιήθηκαν για εκπαίδευση του συστήματος και 90 για τα πειράματα. Στη συνέχεια, προχωρήσαμε στη διενέργεια των πειραμάτων: Ο αριθμός του συνόλου των χαρακτηριστικών άγγιξε τις 515.219. Αντίστοιχα, ο αριθμός διακριτών χαρακτηριστικών άγγιξε τις 31.628. Κατόπιν με χρήση του Simba επιλέχτηκαν τα 300 πιο αντιπροσωπευτικά χαρακτηριστικά. Στον πίνακα 3.3 εμφανίζονται οι επιτευχθείσες τιμές για τις μετρικές ακρίβεια (precision) και ανάκληση (recall).

	Recall	**Precision**
Μη ενδιαφέροντα κείμενα	92.22%	80.58%
Ενδιαφέροντα κείμενα	77.78%	90.91%

Πίνακας 3.3 Επιτευχθείσες τιμές για τις μετρικές ανάκλησης(recall) και ακρίβειας (precision) κατάταξης.

3.3.2 Πειραματισμός με την αρχιτεκτονική perceptron HME

Στη συνέχεια αξιολογήθηκε και η δεύτερη τοπολογία που βασίζεται στη χρήση perceptron εμπείρων μονάδων χρησιμοποιώντας τόσο τον αλγόριθμο Simba όσο και τον αλγόριθμο επιλογής χαρακτηριστικών G-flip. Προκειμένου για μία συγκριτική μελέτη, συγκρίναμε την απόδοση του συστήματος μας με αυτή του naïve Bayes ταξινομητή. Στο πρώτο στάδιο, χρησιμοποιήσαμε τον αλγόριθμο G-flip στο ίδιο δείγμα δεδομένων με αυτό που χρησιμοποιήθηκε στην περίπτωση του αλγόριθμου Simba. Ο αλγόριθμος επέστρεψε ένα σύνολο από 5717 χαρακτηριστικά. Η τιμή της συνάρτησης αξιολόγησης (εξίσωση 4) μετά το πέρας του αλγορίθμου ήταν 2369.1.

Ο πίνακας 3.4 δείχνει τα πρώτα 20 χαρακτηριστικά που επέλεξε ο αλγόριθμος G-flip.

	Χαρακτηριστικό		**Χαρακτηριστικό**
1	to	11	ilug@jmason
2	com	12	x
3	receiv	13	authent
4	127	14	host
5	postfix	15	165
6	with	16	version
7	fetchmail	17	content
8	root@lugh	18	type
9	slashnull	19	text/plain
10	g72LqWv13294	20	ascii

Πίνακας 3.4 Τα 20 πιο αντιπροσωπευτικά χαρακτηριστικά για τη διαδικασία κατάταξης όπως προέκυψαν από την εφαρμογή του αλγόριθμου G-flip.

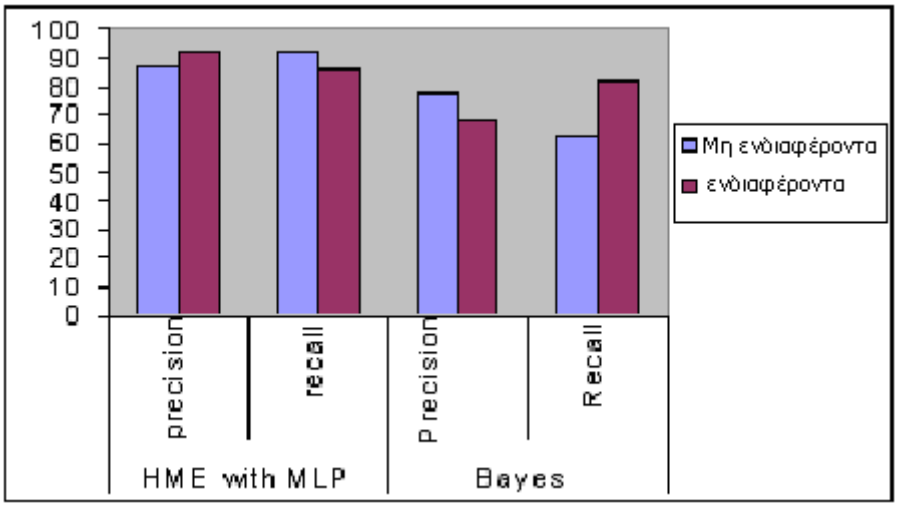
Στη συνέχεια χρησιμοποιήθηκε η συλλογή *20030228_spam_2* από την οποία πήραμε 50% από τα περιεχόμενά της για τη φάση εκπαίδευσης και τα υπόλοιπα για την εκτέλεση των πειραμάτων ταξινόμησης. Το δείγμα εκπαίδευσης παρουσίασε ένα σύνολο 2.105 χαρακτηριστικών.

Προκειμένου να ελέγξουμε την απόδοση του perceptron συστήματος, έγιναν δύο διαφορετικά πειράματα με τη συλλογή *20030228_spam_2*: στο πρώτο χρησιμοποιήθηκαν τα πρώτα 300 πιο αντιπροσωπευτικά χαρακτηριστικά από το σύνολο των χαρακτηριστικών. Στο δεύτερο πείραμα χρησιμοποιήθηκε το βέλτιστο σύνολο χαρακτηριστικών βάσει του αλγόριθμου G-Flip.

Μετρήσαμε την απόδοση του συστήματός μας και στις δύο περιπτώσεις με τα αντίστοιχα αποτελέσματα που επιτυγχάνει ο ταξινομητής Naïve Bayes που είναι ένας από τους πιο μαζικά αξιοποιημένους στη διεθνή βιβλιογραφία (Hidalgo 2002). Τα συγκριτικά αποτελέσματα εμφανίζονται σους πίνακες 3.5, 3.6 καθώς και στα σχήματα 3.5, 3.6 και δείχνουν ότι η προσέγγισή μας ξεπερνά σε απόδοση τον Bayesian ταξινομητή, που θεωρείται από τους πλέον αποδοτικούς.

Επιλογή αντιπροσωπευτικών χαρακτηριστικών βάσει Simba	**Ταξινομητής**			
	HME with Perceptron Experts		**Naïve Bayes Classifier**	
	Precision	**Recall**	**Precision**	**Recall**
Μη ενδιαφέροντα	86.79%	92%	77.5%	62%
Ενδιαφέροντα	91.49%	86%	68.33%	82%

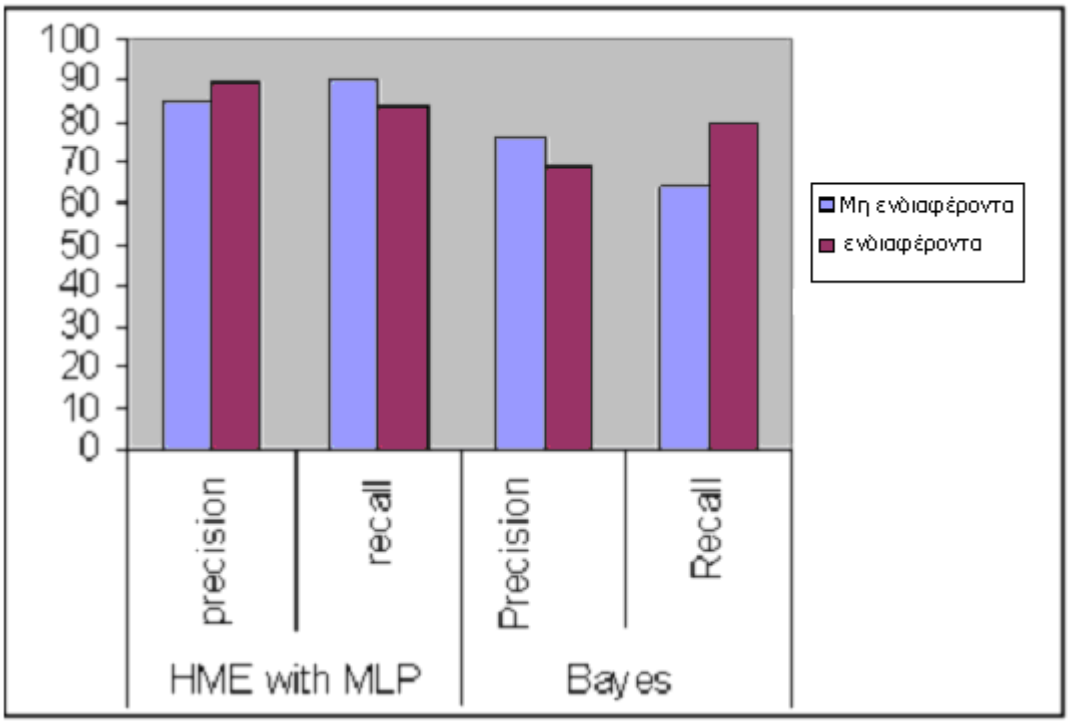
Πίνακας 3.5 Πειραματικά αποτελέσματα στη συλλογή 20030228_spam_2 για αρχιτεκτονική εμπειρογνωμόνων perceptron δύο επιπέδων εν συγκρίσει με το naïve Bayesian ταξινομητή. Και για τους δύο ταξινομητές χρησιμοποιήθηκε πρώτα ο αλγόριθμος Simba.



Εικόνα 3.5 Παρουσίαση σε γραφική μορφή των πειραματικών αποτελεσμάτων του πίνακα 3.5.

Επιλογή αντιπροσωπευτικών χαρακτηριστικών βάσει *G-Flip*	**Ταξινομητής**			
	HME with Perceptron Experts		Naïve Bayes Classifier	
	Precision	**Recall**	**Precision**	**Recall**
Μη ενδιαφέροντα	84.90%	90%	76.19%	64%
Ενδιαφέροντα	89.36%	84%	68.97%	80%

Πίνακας 3.6 Πειραματικά αποτελέσματα με χρήση της συλλογής 20030228_spam_2 και τον αλγόριθμο HME δίκτυο perceptron δύο επιπέδων έναντι του naïve Bayes έχοντας χρησιμοποιήσει τον αλγόριθμο G-Flip για επιλογή των χαρακτηριστικών.



Εικόνα 3.6 Οπτική παρουσίαση των αποτελεσμάτων του πίνακα 3.6

3.3.3 Αξιολόγηση των αποτελεσμάτων

Το σύστημα κατηγοριοποίησης εγγράφων αποτελεί βασικό δομικό πυρήνα ενός κατανεμημένου συστήματος διαχείρισης γνώσης. Μεαξύ των διαφορετικών πόρων γνώσης, μπορούμε να διακρίνουμε δομημένους πόρους (όπως για παράδειγμα μια σχεσιακή βάση), ημιδομημένους (όπως για παράδειγμα κείμενα ηλεκτρονικής αλληλογραφίας αλλά και αδόμητα. Σε κάθε περίπτωση απαιτείται ένας αποτελεσματικός μηχανισμός ανάκτησης και επιλογής της κατάλληλης πληροφορίας, από μεγάλα σύνολα δεδομένων. Μία επιπλέον απαίτηση αφορά στο ότι η λειτουργία αυτή του συστήματος πρέπει να γίνεται με τρόπο γενικό, ώστε να μπορεί να εφαρμοστεί ανάλογα και με τις προτιμήσεις των χρηστών, ή και ανάλογα με τις ανάγκες του εκάστοτε οργανισμού. Στα πλαίσια της διατριβής αναπτύχθηκε ένας τέτοιος αποδοτικός μηχανισμός ανάκτησης και διήθησης πληροφορίας, ο οποίος ελέγχθηκε σε απαιτητικά σύνολα δεδομένων και απέδειξε την αποτελεσματικότητά του επιτυγχάνοντας υψηλότερα ποσοστά ακρίβειας από προηγούμενες προσεγγίσεις.

Ένα άλλο αξιοσημείωτο χαρακτηριστικό της παραπάνω προσέγγισης είναι οι μικροί χρόνοι εκπαίδευσης που απαιτεί, καθώς επίσης και η ικανότητά του συστήματος να ενημερώνει με απλό τρόπο αλλαγές ή προσθήκες στα χαρακτηριστικά των κλάσεων που θα χρησιμοποιηθούν για την ταξινόμηση.

3.4 Αναζήτηση πόρων σε συνασπισμούς Π.Σ.

Μία από τις σημαντικές προκλήσεις σε ένα περιβάλλον συνασπισμών Π.Σ. είναι να δίνεται η δυνατότητα να υποβάλλονται ερωτήματα που αφορούν στην αναζήτηση γνωσιακών πόρων, στα διαφορετικά συστήματα που συμμετέχουν στο συνασπισμό. Ειδική μέριμνα θα πρέπει να λαμβάνει υπόψη της την ελαχιστοποίηση του δικτυακού φόρτου κατά την υποβολή των ερωτημάτων, ειδικά όταν στο σύστημα γίνεται χρήση συσκευών με περιορισμένους πόρους (κυρίως φορητές συσκευές). Σε ένα σύστημα συνασπιζόμενων Π.Σ. υπάρχουν διαφορετικοί, ετερογενούς φύσεως πόροι. Συνεπώς απαιτείται ένας μηχανισμός ενιαίας διαχείρισης και υποβολής ερωτημάτων ανεξάρτητα της φύσης τους και της δομής που υφίστανται. Παράλληλα, πρέπει να ληφθεί υπόψη ότι η ανταλλαγή μηνυμάτων μεταξύ δικτύων (ειδικά όταν τα μηνύματα πρέπει να κρυπτογραφηθούν ή όταν πρέπει να επαληθευτεί η αυθεντικότητά τους και η προέλευσή τους), είναι μια διαδικασία ιδιαίτερα απαιτητική τόσο σε υπολογιστικούς όσο και σε δικτυακούς πόρους. Συνεπώς, είναι ιδιαίτερα επιθυμητό να ελαττώσουμε όσο περισσότερο γίνεται τον αριθμό των μηνυμάτων που αποστέλλονται προκειμένου να ανακτηθεί η επιθυμητή πληροφορία. Ένας τρόπος για να το επιτύχουμε είναι να αυξήσουμε την απόδοση και αποτελεσματικότητα της διαδικασίας που φροντίζει για την αποστολή απάντησης στα ερωτήματα των χρηστών. Σε αυτή την κατεύθυνση προτάθηκε στα πλαίσια των εργασιών (Belsis et al, 2005g) (Gritzalis et al, 2006) (Malatras et al, 2005b), η έννοια των εικονικών δικτύων οντολογιών Virtual Ontology Networks (VON's) τα οποία αντανακλούν θεματικά το περιεχόμενο κάθε περιοχής σε τμήματα οντολογιών που χρησιμοποιούνται για να χαρακτηρίσουν σημασιολογικά τα περιβάλλοντα πολλαπλών πολιτικών. Αξιοποιώντας τα εικονικά δίκτυα οντολογιών, μπορούμε θεματικά να κατηγοριοποιήσουμε το κάθε σύστημα και να γνωρίζουμε εξαρχής τη συνάφεια ενός ερωτήματος με το περιεχόμενο των γνωσιακών πόρων των διαφορετικών Π.Σ. που συμμετέχουν στο συνασπισμό, απλά εξετάζοντας τη χαρακτηριστική οντολογία κάθε ενός.

Η υλοποίηση διαλειτουργικών συστημάτων αποδεικνύεται πολύπλοκη και επίπονη διαδικασία λόγω δύο θεμελιωδών χαρακτηριστικών: α) της διασποράς των πόρων στα διαφορετικά τμήματα του κατανεμημένου συστήματος και β) της ετερογένειας των παραπάνω πόρων. Μπορούμε να διακρίνουμε τα εξής είδη ετερογένειας:

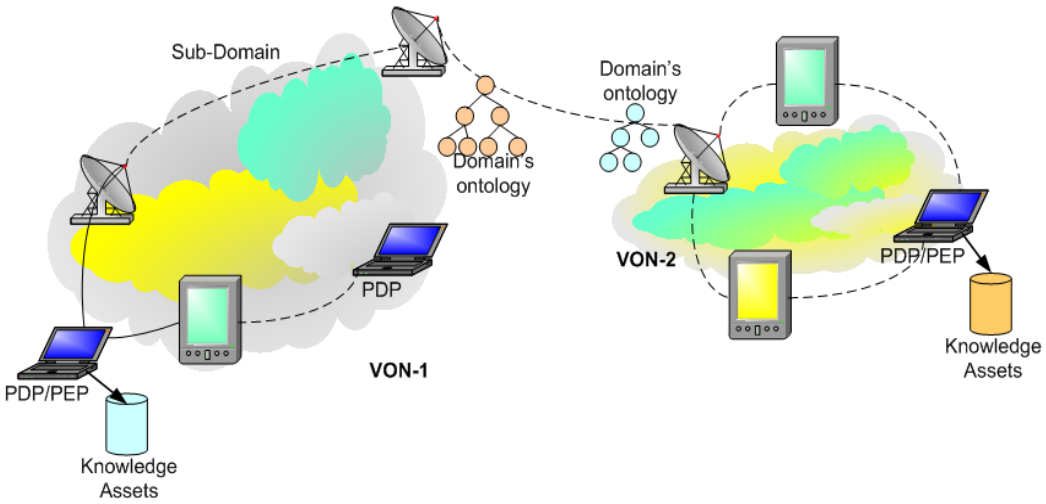
- *δομής (ετερογένεια σχήματος)*
- σημασιολογική (δεδομένων)
- συντακτική (βάσεων δεδομένων)

Η συντακτική ετερογένεια οφείλεται στο ότι διαφορετικά συστήματα βάσεων δεδομένων χρησιμοποιούν διαφορετικές γλώσσες (SQL, OQL, κοκ).
Η ετερογένεια δομής οφείλεται στις διαφορετικές μορφές με τις οποίες αποθηκεύονται σε διαφορετικά συστήματα τα δεδομένα.
Η σημασιολογική ετερογένεια αφορά στην διαφορά μεταξύ του περιεχομένου ενός πόρου και της έννοιας που αποδίδεται σε αυτό στα πλαίσια διαφορετικών συστημάτων. Οι σημασιολογικές διαφορές οφείλονται στην απόδοση διαφορετικής ερμηνείας των δεδομένων από διαφορετικά συστήματα, γεγονός που προκαλεί ποικίλα προβλήματα σε σχέση με τη διαλειτουργικότητα.
Προκειμένου για την επίλυση προβλημάτων ετερογένειας η χρήση των οντολογιών αποδεικνύεται πολύ σημαντική. Οι οντολογίες δηλώνουν τις έννοιες για την περιοχή ενδιαφέροντος, τις ιδιότητες και παρέχουν τη βάση για σημασιολογική ανακάλυψη πόρων (Belsis et al, 2004b). Οι οντολογίες συνεπώς μπορούν να αξιοποιηθούν προς αυτή την κατεύθυνση προκειμένου να παρέχουν περιγραφή των διαθέσιμων πόρων. Επιπλέον, όπως αναφέρθηκε η ανταλλαγή μηνυμάτων μεταξύ των διαφορετικών περιοχών προκειμένου για την υποβολή ερωτήσεων είναι μια διαδικασία που καταναλώνει σημαντικούς δικτυακούς πόρους και υπολογιστική ισχύ. Οι οντολογίες περιοχής μπορούν επομένως να χρησιμοποιηθούν για να καταγράψουν τις θεματικές περιοχές και τις συναφείς έννοιες που περιέχει η περιοχή ενδιαφέροντος με αποτέλεσμα διερευνώντας την οντολογία να είναι άμεσα γνωστό αν μια περιοχή διαθέτει γνωσιακούς πόρους σχετικούς με το ερώτημα που υποβάλλεται ή όχι.
Μπορούμε να διακρίνουμε δύο αναγκαίες φάσεις προκειμένου για την αξιοποίηση των οντολογιών σε ένα περιβάλλον που αποτελείται από διαφορετικά Π.Σ.: στην πρώτη φάση απαιτείται η δημιουργία των οντολογιών (μηχανικά), κάθε μία από τις οποίες περιγράφει μία σειρά από διαφορετικά χαρακτηριστικά. Με βάση τις οντολογίες που σχηματίστηκαν, στα πλαίσια κάθε αυτόνομου Π.Σ. μπορούμε να κατατάξουμε τους γνωσιακούς πόρους ως συναφείς ή όχι, ακολουθώντας τις διαδικασίες που περιγράφηκαν στις προηγούμενες παραγράφους του παρόντος κεφαλαίου. Στη δεύτερη φάση, ανάλογα με το ερώτημα του χρήστη ερωτάται η οντολογία περιοχής για το αν οι θεματικές κατηγορίες στις οποίες κατατάσσονται οι γνωσιακοί πόροι μιας περιοχής είναι συναφείς με το ερώτημα του χρήστη. Προκειμένου για τη διαχείριση των οντολογιών, αυτή μπορεί να γίνει με τη συγκέντρωσή τους σε ειδική βάση. Το ερώτημα του χρήστη συνεπώς κατευθύνεται πρώτα στη Γενική Βάση Οντολογιών (Global Ontology Repository) (Gritzalis 2005), όπου εντοπίζονται ποια από τα συμμετέχοντα στο συνασπισμό συστήματα είναι πιθανό να περιέχουν πόρους σχετικούς με το ερώτημα του χρήστη. Για όλες τις υπόλοιπες περιοχές το ερώτημα θεωρείται ως μη σχετικό με τα περιεχόμενά τους. Με αυτό τον τρόπο έχουμε επιτύχει να κατηγοριοποιήσουμε τα συμμετέχοντα Π.Σ σύμφωνα με ένα μεγαλύτερο σύνολο θεμάτων που κωδικοποιούνται σε κατάλληλες οντολογίες κάθε μία από τις οποίες συνιστά ένα εικονικό δίκτυο οντολογιών (Virtual Overlay Network -VON) (Belsis et al, 2005g) (Malatras et al, 2005b), (Gritzalis et al, 2006). Η εικόνα 3.7 απεικονίζει την έννοια των VONs στην πράξη.

Εφαρμογή: Ιατρικά περιβάλλοντα

Ας θεωρήσουμε την περίπτωση που ένας χρήστης αναζητά εγγραφές ιατρικού χαρακτήρα. Για παράδειγμα έστω ότι η υποβολή ερώτησης στο σύστημα αφορά στην αναζήτηση πληροφοριών που αφορούν σε μία ιατρική κατηγορία (όπως για παράδειγμα δεδομένα που αφορούν σε θέματα ανοσολογίας). Στην περίπτωση που ένα από τα συμμετέχοντα ιατρικά αυτόνομα περιβάλλοντα δεν διατηρεί καθόλου τέτοιου είδους δεδομένα τότε η υποβολή ερώτησης στο δίκτυο και η λήψη αρνητικής απάντησης μετά από το απαιτούμενο χρονικό διάστημα έχει αρνητική επίπτωση στην απόδοση του συστήματος. Προκειμένου να αποφευχθεί μία τέτοια επιβάρυνση, η χρήση της οντολογίας μπορεί να βοηθήσει σημαντικά. Κάθε Π.Σ. που συμμετέχει, με την αντίστοιχή του οντολογία μπορεί να θεωρηθεί σαν ένα ιδεατό -επικαλυπτόμενο της περιοχής- δίκτυο. Παρουσία της οντολογίας, μόνο τα σχετικά προς το περιεχόμενο των πόρων μιας περιοχής ερωτήματα κατευθύνονται προς το εσωτερικό της. Αντί λοιπόν να προωθηθεί το ερώτημα στους κόμβους του δικτύου και να ερωτηθούν οι τοπικοί εξυπηρετητές, πρώτα ερωτάται η οντολογία· αν το ερώτημα θεωρηθεί σχετικό, τότε υποβάλλεται το ερώτημα και προωθείται στο εσωτερικό του υποσυστήματος ενώ παράλληλα ενεργοποιείται το σύστημα επιβολής πολιτικών ασφάλειας.

Η ανάγκη για ελαχιστοποίηση της κατανάλωσης πόρων είναι εμφανής σε περιβάλλοντα που συμμετέχουν συσκευές με περιορισμένους πόρους (όπως για παράδειγμα φορητές συσκευές: PDA's, laptops κλπ). Η αναγκαία προσαρμογή του συστήματος επιβολής ελέγχου πρόσβασης για να αξιοποιηθεί σε περιβάλλοντα με περιορισμένους ιατρικούς πόρους θα περιγραφεί στα επόμενα κεφάλαια της διατριβής, συνοψίζοντας τα συμπεράσματα που καταγράφονται στις εργασίες (Gritzalis et al, 2006) και (Belsis et al, 2005g) (Belsis et al, 2005d) (που αφοροούν σε ασύρματα συνδεδεμένα ιατρικά περιβάλλοντα κυρίως).



Εικόνα 3.7 Ανεξάρτητες περιοχές κατηγοριοποιημένες σε διαφορετικά Εικονικά δίκτυα Οντολογιών Virtual Ontology Networks (VON's) σύμφωνα με τις θεματικές ενότητες που χαρακτηρίζουν τους πόρους κάθε περιοχής.

3.5 Συμπεράσματα

Ο δυναμικός χαρακτήρας και η φύση των περιβαλλόντων που σχηματίζονται από τη συνένωση διαφορετικών Π.Σ. με στόχο το διαμοιρασμό πόρων, εισάγουν μία σειρά από προκλήσεις που αφορούν τόσο στη σχεδίαση όσο και στην υλοποίηση τους.

Στα πλαίσια του παρόντος κεφαλαίου περιγράφηκαν δύο σημαντικές πτυχές της διαχείρισης συστημάτων που βασίζονται στην συνεργασία αυτόνομων Π.Σ.: αφενός μεν το ζήτημα της αξιοποίησης αποδοτικών τεχνικών για την κατηγοριοποίηση γνωσιακών πόρων στο εσωτερικό του κάθε αυτόνομου συστήματος, αφετέρου δε το πρόβλημα της διαχείρισης των προβλημάτων ετερογένειας.

Στα πλαίσια του πρώτου ζητήματος, περιγράφηκαν στα πλαίσια της διατριβής οι τεχνικές που αναπτύχθηκαν στα πλαίσια των εργασιών (Belsis et al, 2006a) (Belsis et al, 2006d) (Belsis, 2006e) και αφορούν στη χρήση τεχνικών που βασίζονται στην επιλογή κατάλληλων ταξινομητών και τεχνικών αναζήτησης των καλύτερων χαρακτηριστικών που μπορούν να βοηθήσουν στη γρήγορη και αποδοτική κατηγοριοποίηση μίας σειράς από γνωσιακούς πόρους σε προκαθορισμένες κατηγορίες. Μεταξύ των χαρακτηριστικών της προτεινόμενης λύσης είναι η υψηλή ακρίβεια, οι μικροί χρόνοι εκπαίδευσης του συστήματος και η δυνατότητα διαρκούς ενημέρωσης του με νέα χαρακτηριστικά. Η πειραματική διαδικασία που ακολουθήθηκε και καταγράφεται στις εργασίες (Belsis et al, 2006a) (Belsis et al, 2006d) απέδειξε την ανωτερότητα της παραπάνω προσέγγισης σε σχέση με άλλες αντίστοιχες της διεθνούς βιβλιογραφίας.

Εκτός από τα θέματα ασφάλειας που θα αποτελέσουν το κύριο αντικείμενο των επόμενων κεφαλαίων, υπάρχουν επιπλέον δύο βασικά προβλήματα που δυσχεραίνουν την αποδοτική λειτουργία ενός συστήματος αποτελούμενου από συνεργαζόμενα αυτόνομα Π.Σ.:

- Το πρόβλημα της ετερογένειας (Belsis et al, 2004b) (Belsis et al, 2005e) (Belsis et al, 2005f) (Shafiq et al, 2005)(Belokosztolszki, 2004), που αφορά στη δυσκολία διαχείρισης των πόρων των διαφορετικών οργανισμών λόγω της διαφορετικής φύσης των πόρων και των διαφορετικών δομών που υφίστανται για τους διαμοιραζόμενους πόρους και
- Το πρόβλημα της αξιοποίησης με ευέλικτο τρόπο των δικτυακών πόρων και της ελαχιστοποίησης της αποστολής μηνυμάτων ερωταποκρίσεων ανάμεσα στους συμμετέχοντες οργανισμούς (Malatras et al, 2005a)(Malatras et al, 2005b) (Belsis et al, 2005d) (Belsis et al, 2005f) (Gritzalis et al, 2006) (Belsis 2006e).

Στα πλαίσια της διατριβής και σε σχέση με τα παραπάνω προβλήματα, προτάθηκε η δημιουργία των εικονικών δικτύων οντολογιών, τα οποία συνιστούν μία ευέλικτη τεχνική βασισμένη στη χρήση οντολογιών, προκειμένου για την κατηγοριοποίηση σε θεματικές περιοχές των πόρων γνώσης που χαρακτηρίζουν τα συμμετέχοντα συστήματα. Διατηρώντας τις σχετικές οντολογίες σε συγκεκριμένη τοποθεσία (Belsis, 2006e) είναι εφικτό να γίνεται άμεσα αντιληπτό το αν ένας οργανισμός που συμμετέχει στο συνασπισμό διαθέτει συναφείς με το ερώτημα πόρους. Στην περίπτωση που διαθέτει, τότε το ερώτημα προωθείται στους εσωτερικούς κόμβους του συγκεκριμένου οργανισμού, σε αντίθετη περίπτωση το ερώτημα δεν προωθείται περαιτέρω. Τα πλεονεκτήματα από αυτήν την προσέγγιση είναι πολλαπλά και σημαντικά: Αφενός μεν η διαδικασία γίνεται πιο αποδοτική, αφού μειώνονται οι πόροι απόκρισης, αφετέρου δε γίνεται σημαντική εξοικονόμηση τόσο δικτυακών όσο

και υπολογιστικών πόρων. Το αποτέλεσμα αυτό έχει ιδιαίτερη βαρύτητα μιας και πληθαίνουν οι εφαρμογές περιβαλλόντων στα οποία συμμετέχουν υπολογιστικές συσκευές με περιορισμένους πόρους, όπως για παράδειγμα φορητές συσκευές (υπολογιστές – laptops, βοηθοί – PDAs, δίκτυα αισθητήρων- sensor networks), περιπτώσεις στις οποίες η εξοικονόμηση πόρων αποτελεί κύριο μέλημα.

ΜΕΡΟΣ Β

ΚΕΦΑΛΑΙΟ 4 - Διαχείριση Ασφάλειας σε περιβάλλοντα συνεργαζόμενων Πληροφοριακών Συστημάτων

Το βασισμένο σε ρόλους μοντέλο ασφάλειας (RBAC) όπως αναφέρθηκε ήδη στο δεύτερο κεφάλαιο, ομαδοποιεί τους ρόλους σε ένα οργανισμό και τα σχετικά με αυτούς προνόμια επί των αντικειμένων που διαθέτει ένας οργανισμός. Λόγω της απλότητας του καθώς και της γενικότητας που το χαρακτηρίζει μπορεί να αναπαραστήσει μια πληθώρα καταστάσεων και μπορεί να υποστηρίξει τα μοντέλα ασφάλειας πολλών και διαφορετικών οργανισμών με διαφορετικές απαιτήσεις.
Σε πολλούς οργανισμούς, όπου ο αριθμός των χρηστών κυμαίνεται σε μερικές χιλιάδες, ο αριθμός των ρόλων μπορεί να μεγαλώσει υπερβολικά. Σε εμπορικούς οργανισμούς, μελέτες που έχουν γίνει (Schaad et al, 2001) έδειξαν ότι ο αριθμός των ρόλων που απαιτούνται προκειμένου να εκφραστεί η πολιτική του οργανισμού μπορεί να ξεπεράσει τους χίλιους. Η πληροφορία που σχετίζεται με τους παραπάνω ρόλους, όπως για παράδειγμα η πληροφορία που αφορά στην αντιστοίχηση των χρηστών σε ρόλους, τα δικαιώματα που αντιστοιχούνται σε χρήστες, απαιτεί ειδικές τεχνικές διαχείρισης, κυρίως λόγω του όγκου της. Προκειμένου για την αποτελεσματικότερη διαχείριση της ασφάλειας, η κωδικοποίηση των κανόνων που περιγράφουν την παραπάνω πληροφορία μπορεί να γίνει με δομημένο τρόπο, όπως για παράδειγμα με χρήση γλωσσών περιγραφής πολιτικής ασφάλειας. Στη συνέχεια οι διαδικασίες μπορούν να γίνονται αυτοματοποιημένα με χρήση ειδικών εργαλείων λογισμικού που ερμηνεύουν τις αιτήσεις για πρόσβαση σε συγκεκριμένους πόρους σε επίπεδο εφαρμογής, ελαττώνοντας το διαχειριστικό φόρτο του συστήματος και αποσυνδέοντας τη διαχείριση ασφάλειας των εφαρμογών από το λειτουργικό σύστημα. Οι πραγματικές πολιτικές ασφάλειας ενός οργανισμού ωστόσο, εκφράζονται σε πολύ διαφορετική μορφή από αυτή των γλωσσών περιγραφής πολιτικών, όπως για παράδειγμα με μορφή οδηγιών, βέλτιστων πρακτικών (best practices) κοκ. Τη μετατροπή από τη μια μορφή στην άλλη είναι υπεύθυνοι να κάνουν οι διαχειριστές του συστήματος.

4.1 Γλώσσες αναπαράστασης πολιτικών – δυνατότητες και επιλογές

Οι περισσότερες γλώσσες περιγραφής πολιτικών ασφάλειας υποστηρίζουν διαφορετικούς τρόπους αναπαράστασης, άλλες δίνοντας απευθείας τη δυνατότητα καταγραφής σε φυσική γλώσσα, άλλες παρέχοντας δυνατότητα γραφικής αναπαράστασης των πολιτικών και άλλες κωδικοποιώντας την πολιτική σε μορφή XML (Damianou, 2002). Οι τελευταίες είναι και από τις πιο ελκυστικές, λόγω των αυξημένων χαρακτηριστικών διαλειτουργικότητας της γλώσσας XML που χρησιμοποιείται για την αναπαράστασή τους. Στην τελευταία κατηγορία ξεχωρίζουν οι γλώσσες X-RBAC (Joshi et al, 2004), XACML (XACML, 2004) και Rei (Patwardhan et al, 2004).
Η γλώσσα X-RBAC δημιουργήθηκε πρόσφατα για να καλύψει μέσα από τον ορισμό κατάλληλων σχημάτων περιγραφής εγγράφων XML, την ανάθεση δικαιωμάτων σε χρήστες, ανάθεση δικαιωμάτων σε πόρους για τους διάφορους χρήστες κλπ. (Joshi et al, 2004). Ωστόσο, ένα βασικό μειονέκτημα της παραπάνω γλώσσας είναι ότι δεν υπάρχουν διαθέσιμα εργαλεία λογισμικού να την υποστηρίξουν. Στην πράξη, ένα άλλο επίσης μειονέκτημά της είναι ότι δεν επιτρέπει την απεικόνιση ιεραρχιών.

Προκειμένου για την υλοποίηση των τεχνικών ελέγχου πρόσβασης που αναπτύχθηκαν στα πλαίσια της διατριβής και που περιγράφονται στις εργασίες (Belsis et al, 2005b) (Belsis et al, 2005c) (Belsis et al, 2005h) (Malatras et al, 2005a) (Malatras et al, 2005b) χρησιμοποιήθηκε η γλώσσα XACML που αποτελεί μια υλοποίηση του RBAC για την εφαρμογή κανόνων ελέγχου πρόσβασης. Η XACML είναι μια γλώσσα για την έκφραση πολιτικών ελέγχου πρόσβασης που κωδικοποιείται σε συντακτικό της γλώσσας XML. Η XACML παρέχει έλεγχο επί των ενεργειών ενώ υποστηρίζει επίσης τη δυνατότητα για επίλυση συγκρούσεων μέσω δηλώσεων που επιτρέπουν τον καθορισμό προτεραιοτήτων επί των πολιτικών. Ωστόσο, δεν υποστηρίζει ιεραρχίες ρόλων και δεν χαρακτηρίζεται από την εκφραστικότητα και την επεκτασιμότητα που παρέχουν οι γλώσσες που προορίζονται για χρήση στο σημασιολογικό ιστό (Patwardhan et al, 2004). Στην εργασία των (Patwardhan et al, 2004) περιγράφονται με γενικό τρόπο τα χαρακτηριστικά μιας νέας γλώσσας προσανατολισμένης στην υποστήριξη σημασιολογικών συσχετισμών, κάτι που είναι αναγκαίο σε περιβάλλοντα υπηρεσιών διαδικτύου (Web-Services) και σε περιβάλλοντα διεισδυτικού υπολογίζειν (pervasive computing)· ωστόσο δεν διατίθεται αναλυτική περιγραφή των κανόνων της γλώσσας, ενώ δεν υπάρχουν εργαλεία που να την υποστηρίζουν. Προκειμένου να αποφύγουμε τη δημιουργία μίας νέας γλώσσας, κρίθηκε προτιμότερη η επιλογή μίας (υπό ανάπτυξη) προτύπου γλώσσας και η τροποποίηση ορισμένων χαρακτηριστικών της προκειμένου να καλυφθούν συγκεκριμένοι περιορισμοί. Έτσι, ενώ διατηρούνται οι βασικές αρχές της γλώσσας XACML, με αποτέλεσμα να μπορεί να χρησιμοποιηθεί ο βασικός πυρήνας προγραμμάτων της προκειμένου για το σχηματισμό αιτήσεων και την αξιολόγηση της εγκυρότητας τους, επιλέχθηκε η γλώσσα RDF (Decker et al, 2000) για την αναπαράσταση των κανόνων της πολιτικής υψηλού επιπέδου. Με αυτό τον τρόπο επιτυγχάνουμε να είμαστε σε συμφωνία με τα πρότυπα και τις διεθνείς προσπάθειες (τόσο από την ακαδημαϊκή κοινότητα όσο και από την βιομηχανία) για την ανάπτυξη μιας κοινά αποδεκτής γλώσσας εφαρμογής πολιτικών ελέγχου πρόσβασης, ενώ χρησιμοποιούμε τις επεκτεταμένες ιδιότητες της γλώσσας RDF για να εκφράσουμε περισσότερη πληροφορία σε υψηλού επιπέδου πολιτική.
Η επιλογή μιας γλώσσας βασισμένης στο συντακτικό της XML για την αναπαράσταση της πληροφορίας που αφορά στους ρόλους και τα δικαιώματα, έγινε κυρίως λόγω των αυξημένων χαρακτηριστικών διαλειτουργικότητας της παραπάνω γλώσσας και της ικανότητας της να αξιοποιηθεί από πλήθος εφαρμογών και ανεξάρτητα λειτουργικού συστήματος.

Στον πίνακα 4.1 το παράδειγμα αναφέρεται στην δυνατότητα υποστήριξης της ενεργοποίησης ενός συνόλου ρόλων μέσα σε καθορισμένα χρονικά περιθώρια όπως επίσης και στη δυνατότητα εξουσιοδότησης χρηστών που προέρχονται από μια ορισμένη περιοχή, βάσει του γενικότερου πλαισίου (context) της περιοχής από την οποία προέρχονται οι αιτήσεις. Αυτό επιτυγχάνεται μέσω του κανόνα (rule) "EveryoneDuringBusinessHours" και της τιμής του αντίστοιχου πεδίου (attribute) που είναι ‘permit’, δηλαδή πιο απλά επιτρέπει σε οποιοδήποτε μέλος του οργανισμού να μπορεί να συνδέεται στις εργάσιμες ώρες μεταξύ 9.00 και 17.00.

```
<Rule RuleId="EveryoneDuringBusinessHours" Effect="Permit">
<Condition FunctionId=" Function#time-in-range"> <Apply
FunctionId="function:time-one-and-
only"><EnvironmentAttributeDesignator
DataType=http://www.w3.org/2001/XMLSchema#time
AttributeId=" environment:current-time"/></Apply>
<AttributeValue DataType="
http://www.w3.org/2001/XMLSchema#time"> 09:00:00
</AttributeValue>
<AttributeValue DataType="
http://www.w3.org/2001/XMLSchema#time">17:00:00
</AttributeValue>
</Condition></Rule>
```

Πίνακας 4.1 Παράδειγμα δυνατότητας εξουσιοδότησης πολλαπλών ρόλων, βάσει του πλαισίου περιβάλλοντος (context) στο οποίο ανήκουν και για συγκεκριμένο χρονικό διάστημα

4.1.1 Αναπαράσταση ρόλων με αξιοποίηση σημασιολογικών χαρακτηριστικών

Η αναπαράσταση πολιτικών με χρήση της XML έχει πολλαπλά πλεονεκτήματα κυρίως λόγω της μεγάλης της εξάπλωσης και των διαλειτουργικών χαρακτηριστικών της. Τα τελευταία χρόνια μάλιστα τείνει να γίνει και πρότυπο στο χώρο των κατανεμημένων συστημάτων. Ωστόσο, η αναπαράσταση συσχετίσεων μεταξύ ρόλων είναι σχετικά πολύπλοκη στην XML. Δηλαδή αν και η πληροφορία που αφορά σε ρόλους μεμονωμένα αναπαρίσταται ικανοποιητικά με τη βοήθεια της XML, σε περίπτωση που θέλουμε να αναπαραστήσουμε συσχετίσεις, ιεραρχίες και περιορισμούς μεταξύ ρόλων, αυτό θα πρέπει να γίνει με τρόπο ειδικό και να δομηθεί το XML έγγραφο με τέτοιο τρόπο που η επεξεργασία του θα εξαρτάται από την εκάστοτε εφαρμογή, γεγονός που ελαττώνει την ικανότητα γενίκευσης μιας λύσης. Έτσι, στα πλαίσια των εργασιών (Belsis et al, 2005h), (Belsis et al, 2005g), προτείνεται η αναπαράσταση ιδιοτήτων ρόλων σε γλώσσα RDF λόγω του ότι επιτρέπει πολύ ευκολότερα την έκφραση συσχετίσεων μεταξύ ρόλων, όπως για παράδειγμα ιεραρχιών. Ο πίνακας 4.2 αναπαριστά τμήμα ενός εγγράφου που ακολουθεί το συντακτικό της RDF που απεικονίζει την αναπαράσταση πληροφορίας που αφορά σε ρόλους. Το παράδειγμα αναφέρεται σε ένα μια ιεραρχία ρόλων ηλεκτρονικής διακυβέρνησης, συγκεκριμένα αφορά στην αναπαράσταση ρόλων ενός υπουργείου. Τα ονόματα των ρόλων βρίσκονται στην διεύθυνση http://defenseMinistry.org/roles, ενώ οι όροι που αφορούν στα δικαιώματα βρίσκονται στη διεύθυνση http://defenseMinistry.gov/permissions. Η ύπαρξη ιεραρχικής συσχέτισης μεταξύ δύο ρόλων δηλώνεται μέσω του κατηγορήματος “supervises” που περιέχει τους ρόλους που εποπτεύονται από το ρόλο που περιέχει τους συγκεκριμένους ρόλους που περιλαμβάνονται στο κατηγόρημα. Η ετικέτα (tag) “prm:supervises” περιλαμβάνει μια συλλογή από ονόματα ρόλων όπως διαφαίνεται από το συγκεκριμένο παράδειγμα του πίνακα 4.2, οι οποίοι βρίσκονται πιο κάτω από στην ιεραρχία από το ρόλο που βρίσκεται αμέσως ένα επίπεδο πιο πάνω και εντοπίζεται στο XML έγγραφο πριν από την ετικέτα “supervises”. Το παράδειγμα περιλαμβάνει δηλώσεις που δείχνουν την ώρα ενεργοποίησης – απενεργοποίησης για όλους τους ρόλους μέσω των στοιχείων “prm:activation-time” και “prm:deactivation-time”. Παράλληλα δηλώνονται μια σειρά από κατηγορήματα που αφορούν στις μεταβλητές περιβάλλοντος, για παράδειγμα το όνομα της περιοχής “intelligence.defenseMinistry.org” στην ετικέτα prm:DomainDescription μπορεί να χρησιμοποιηθεί σαν τιμή για αντίστοιχο κατηγόρημα και να επιτρέπεται μέσω αυτής της τιμής η πρόσβαση για όλα τα μέλη αυτής της περιοχής (του τμήματος του οργανισμού).

4.2 Διαχείριση ελέγχου πρόσβασης σε περιβάλλοντα πολλαπλών πολιτικών

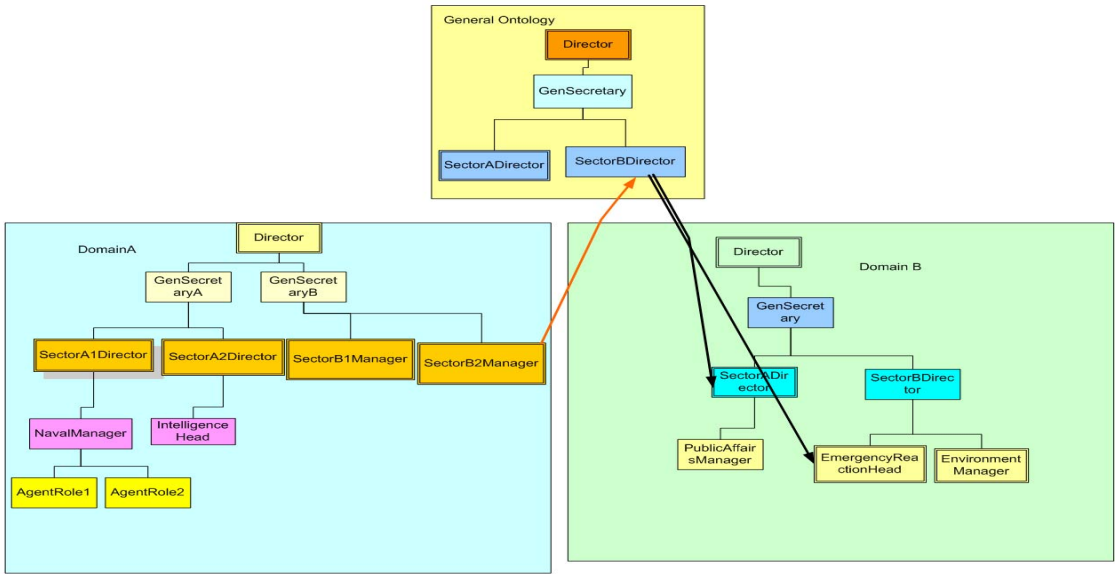
Η χρήση των πολιτικών ασφάλειας κωδικοποιημένων στο συντακτικό μιας ευρέως διαδεδομένης γλώσσας επιτρέπει την απλοποίηση της διαχείρισης της ασφάλειας, καθώς αυτή μπορεί να αναληφθεί από προγράμματα-πράκτορες που αναλαμβάνουν την ερμηνεία της πολιτικής και το χειρισμό των αιτήσεων. Μεταξύ των πλεονεκτημάτων της αυτοματοποιημένης διαχείρισης είναι η αδιάλειπτη λειτουργία του συστήματος, αφού η οποιαδήποτε αλλαγή μπορεί να κωδικοποιηθεί στο αρχείο καταγραφής της πολιτικής και απλά να ενημερωθεί το σημείο διερμηνείας της πολιτικής με το νέο αρχείο, ενώ παράλληλα αποσυνδέονται οι υπόλοιπες λειτουργίες του συστήματος από αυτή της διαχείρισης ασφάλειας. Ωστόσο, η περίπτωση της διαχείρισης ασφάλειας σε περιβάλλοντα πολλαπλών πολιτικών είναι αρκετά πιο πολύπλοκη. Στην περίπτωση αυτή, είναι αναγκαίο να δημιουργηθεί ένας μηχανισμός ικανός να στηρίξει μια διαλειτουργική λύση που θα υπόκειται επιπλέον σε μια σειρά από περιορισμούς (όπως για παράδειγμα ότι οποιαδήποτε μη επιτρεπτή πρόσβαση σε κάθε οργανισμό μεμονωμένα παραμένει μη επιτρεπτή στο περιβάλλον που θα προκύψει από τη συνεργασία). Παράλληλα, η προτεινόμενη λύση θα πρέπει να είναι συμβατή με την αρχή της αυτονομίας που δηλώνει ότι όλες οι επιτρεπτές πράξεις στα πλαίσια των μεμονωμένων πολιτικών πρέπει να επιτρέπονται επίσης στα πλαίσια των πολλαπλών πολιτικών (Gong et al, 1994). Η τελευταία αυτή απαίτηση δεν είναι τόσο περιοριστική όπως αναφέρεται στο (Shafiq et al, 2005), όπου προκειμένου για την επίλυση συγκρούσεων σε επίπεδο πολιτικής επιτρέπουν την μείωση της αυτονομίας σε τοπικό επίπεδο για τα συμμετέχοντα μέρη.

Στα πλαίσια της παρούσας διατριβής, υιοθετείται η λύση της δημιουργίας ενός μηχανισμού αντιστοίχησης του απομακρυσμένου ρόλου με κάποιον αντίστοιχο στην περιοχή που βρίσκονται οι αιτούμενοι πόροι (Belsis et al, 2005h). Η αντιστοίχηση ρόλων με διαφορετικό ωστόσο πλαίσιο από την δική μας προσέγγιση έχει εφαρμοστεί και σε άλλες ερευνητικές εργασίες (Belokosztolski, 2004),(Joshi et al, 2004). Ωστόσο οι περιορισμοί που κατά περίπτωση εισάγονται στις συγκεκριμένες εργασίες, επηρεάζουν τη γενικότητα των προτεινόμενων συστημάτων. Για παράδειγμα στην περίπτωση των (Joshi et al, 2004) προτείνεται η τεχνική αντιστοίχησης ρόλων κωδικοποιώντας σε XML αρχεία τις αντιστοιχίσεις και δημιουργώντας μια ένα-προς-ένα αντιστοίχηση των ρόλων μεταξύ διαφορετικών οργανισμών. Η προτεινόμενη αυτή τεχνική κλιμακώνεται δύσκολα, ενώ περιορίζει τα περιθώρια για τη δημιουργία ενός πλαισίου αυτοματοποιημένης διαχείρισης. Σε αντίστοιχη εργασία της ίδιας ομάδας (Shafiq et al, 2005) προτείνεται η τεχνική ενός αλγορίθμου που δημιουργεί μία καθολική πολιτική από τις επιμέρους. Ο αλγόριθμος αυτός απαιτεί πολυωνυμικό χρόνο αλλά και σημαντικούς υπολογιστικούς πόρους για την εκτέλεσή του. Παράλληλα, είναι δύσκολο να ενημερωθεί η καθολική πολιτική από τις μεταβολές στις επιμέρους πολιτικές.

Αντίστοιχα στην εργασία του (Belokosztolski, 2004) υιοθετείται μια προσέγγιση βασισμένη στην αντιστοίχηση ρόλων σε διαφορετικά συστήματα, που όμως λειτουργεί με διαφορετική φιλοσοφία, χρησιμοποιώντας τεχνικές περιορισμού της ροής των πληροφοριών ανάμεσα στα διαφορετικά συστήματα.

Στην προσέγγισή μας αφετηρία αποτελεί η ιδέα ότι σε οργανισμούς που λειτουργούν κάτω από κάποιο κοινό πλαίσιο όπως για παράδειγμα σε υπουργεία, υπάρχουν αρκετά κοινά χαρακτηριστικά στις δομές των ιεραρχιών ρόλων. Για παράδειγμα, όλα τα υπουργεία έχουν στην ανώτερη θέση τους το ρόλο του υπουργού, ακολουθεί η θέση ενός ή περισσότερων γενικών γραμματέων, κατόπιν διευθυντές τομέων κλπ.

Έτσι είναι προτιμότερη η δημιουργία μιας γενικευμένης ιεραρχίας ρόλων, στην οποία μπορούν να αντιστοιχιστούν τμήματα των επιμέρους τοπικών πολιτικών.
Στην περίπτωση του σχηματισμού ενός συνασπισμού με δυναμικό τρόπο, θα πρέπει να γίνει δυνατό ένας ρόλος σε ένα οργανισμό να μπορεί να αποκτήσει τα δικαιώματα σε κάποιον άλλο αντίστοιχο συνεργαζόμενο οργανισμό. Αυτό μπορεί να επιτευχθεί με την αντιστοίχηση των ρόλων των επιμέρους συστημάτων μέσω της χρήσης της ενδιάμεσης ιεραρχίας.
Η δική μας προσέγγιση, υπόκειται στον περιορισμό της ανάγκης για την ύπαρξη συμφωνίας μεταξύ των συνεργαζόμενων μερών στη διευθέτηση των αντιστοιχήσεων. Όπως όμως αναφέρθηκε, αφετηρία της προσέγγισης μας είναι η εφαρμογή των προτεινόμενων λύσεων σε συστήματα συνασπισμών στα πλαίσια του δημόσιου τομέα όπως σε ιατρικά περιβάλλοντα ή σε συστήματα ηλεκτρονικής διακυβέρνησης. Σε ένα τέτοιο περιβάλλον πολλαπλών πολιτικών είναι δεδομένη η παρουσία κανόνων που ρυθμίζουν το ευρύτερο πλαίσιο λειτουργίας του συνασπισμού (Ao et al, 2003). Η ύπαρξη άλλωστε των κανόνων που διαμορφώνουν τη λειτουργία του συνασπισμού είναι αναγκαία, μια και η εκ του μηδενός διαπραγμάτευση με αυτοματοποιημένο τρόπο πολιτικών, όπως αναφέρθηκε στο δεύτερο κεφάλαιο είναι NP-πλήρες πρόβλημα (McDaniel et al, 2002). Ένας άλλος περιορισμός αναφέρεται στο ότι πρέπει να θεωρείται δεδομένη η ύπαρξη εμπιστοσύνης μεταξύ των μερών, δηλαδή να μην υπάρχει κάποιο από τα μέρη που να θεωρηθεί ότι θα προσπαθήσει να αποκτήσει πρόσβαση σε πόρους άλλων μερών για ίδιο όφελος. Ο χειρισμός του προβλήματος χωρίς να ισχύσει ο παραπάνω περιορισμός απαιτεί την εφαρμογή αρχών της θεωρίας παιγνίων, χωρίς να είναι δεδομένο ότι θα επιτευχθεί κοινά αποδεκτή λύση (Gligor et al, 2001).



Εικόνα 4.1 Αντιστοίχηση ρόλων μεταξύ διαφορετικών περιοχών για συνεργαζόμενα συστήματα. Στο σχήμα ένας ρόλος που αντιστοιχεί σε ένα υπουργείο αντιστοιχείται στην κεντρική ιεραρχία και κατόπιν σε ένα δεύτερο υπουργείο.

Η κεντρική ιδέα της προτεινόμενης λύσης στο πρόβλημα της κατανεμημένης αυθεντικοποίησης, είναι αυτή της αντιστοίχησης ρόλων διαφορετικών συστημάτων που συμμετέχουν στο συνασπισμό. Παράλληλα επιχειρείται μια ομαδοποίηση των διαφορετικών αντιστοιχήσεων, με τρόπο διαλειτουργικό και με χρήση ενδιάμεσα οντολογιών. Δηλαδή επιχειρείται η αντιστοίχηση των ιεραρχιών ρόλων μεταξύ τους, διαμέσου μιας κεντρικής ιεραρχίας – οντολογίας - στην οποία οι τοπικές ιεραρχίες

υποχρεούνται να αντιστοιχηθούν. Η δυσκολία της παραπάνω προσέγγισης έγκειται στην δημιουργία της παραπάνω κεντρικής οντολογίας με τρόπο γενικό ώστε να καλύπτει κατά το δυνατόν τους περισσότερους ρόλους για ένα σύνολο οργανισμών (Belsis, 2006e). Όπως όμως αναφέρθηκε εξαρχής, στα περισσότερα περιβάλλοντα συνασπιζόμενων Π.Σ. (όπως π.χ. σε περιβάλλοντα ηλεκτρονικής διακυβέρνησης και σε ιατρικά διασυνδεδεμένα περιβάλλοντα), οι συμμετέχοντες οργανισμοί έχουν παρόμοια δομή, με αποτέλεσμα η δημιουργία της ενδιάμεσης οντολογίας να είναι εφικτή με σχετικά χαμηλή πολυπλοκότητα.

```
<?xml version="1.0" encoding="UTF-8"?>
<rdf:RDF>xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
xmlns:base="http://defenseMinistry.gov/roles"
xmlns:prm="http://defenseMinistry.gov/permissions">
<rdf:Description rdf:ID="GenSecretaryA">
<prm:activation-time>9:00</prm:activation-time>
<prm:dectivation-time>23:00</prm:dectivation-time>
<prm:DomainDescription>intelligence.defense.org</prm:DomainDescription
>
<prm:supervises parseType:="Collection">
<rdf:Description rdf:ID="SectorA2Director"/>
</prm:supervises>
</rdf:Description>
<rdf:Description rdf:ID="NavalManager">
<prm:activation-time>9:00</prm:activation-time>
<prm:deactivation-time>17:00</prm:deactivation-time>
<prm:DomainDescription>intelligence.defense.org</prm:DomainDescription
>
<prm:supervises parseType:="Collection">
   <rdf:Description rdf:ID="AgentRole1"/>
   <rdf:Description rdf:ID="AgentRole2"/>
</prm:supervises>
</rdf:Description>
</rdf:Description>
</rdf:RDF>
```

Πίνακας 4.2 Τμήμα εγγράφου περιγραφής ιδιοτήτων ρόλων και ιεραρχιών ρόλων

Στην προσέγγισή μας θεωρούμε ότι οι αντιστοιχίσεις ρόλων δεν υφίστανται υποχρεωτικά σε διπλή κατεύθυνση. Για παράδειγμα ένας ρόλος σε ένα οργανισμό μπορεί να αποκτήσει δικαιώματα για την εκτέλεση ενεργειών που προορίζονται για ένα αντίστοιχο ρόλο σε άλλο οργανισμό χωρίς ωστόσο να μπορεί να συμβεί και το αντίθετο. Επομένως μπορούμε να διακρίνουμε δύο τύπους αντιστοιχήσεων (Belsis et al, 2005h): τις έσω-αντιστοιχίσεις (in mappings) με κατεύθυνση προς την κεντρική οντολογία και τις έξω-αντιστοιχίσεις (out-mappings) με κατεύθυνση από την κεντρική οντολογία προς τις τοπικές. Αξίζει να σημειωθεί ότι η κεντρική οντολογία από μόνη της δεν χρήζει αντιστοιχήσεων.

Πρακτικά προκειμένου για την υλοποίηση ενός διαλειτουργικού μηχανισμού ικανού να ενσωματωθεί στο μηχανισμό επιβολής ελέγχου πρόσβασης, οι αντιστοιχίσεις φυλάσσονται σε ειδικό αρχείο που διατηρείται στο σύστημα επιβολής ελέγχου πρόσβασης, στο οποίο θα αναφερόμαστε ως μητρώο διαχείρισης συνασπισμού (coalition management registry). Εφόσον οι πολιτικές και οι κανόνες που αφορούν στις εξουσιοδοτήσεις και στις ιδιότητες που σχετίζονται με κάθε ρόλο κωδικοποιούνται σε RDF και XML μορφή, απαιτείται η χρήση αντίστοιχης κατάλληλης τεχνολογίας για την αποθήκευση των αντιστοιχήσεων. Για το σκοπό αυτό επιλέχτηκε η χρήση της τεχνολογίας XPath (XPath, 2005).

Η XPath αποσκοπεί στον προσδιορισμό τμήματος ενός XML εγγράφου. Αναπαριστά την τοποθεσία στην οποία βρίσκονται τα δεδομένα μέσα σε ένα XML κείμενο σωστά και αποδοτικά, γεγονός που την καθιστά κατάλληλη για την

υποβολή ερωτημάτων σε XML έγγραφα αλλά και αντίστοιχα σε XML μορφής πολιτικές ελέγχου πρόσβασης. Στον πίνακα 4.3 ρόλοι από ένα οργανισμό αντιστοιχούνται έμμεσα μέσω της κεντρικής ιεραρχίας ρόλων σε ρόλους άλλου συνεργαζόμενου οργανισμού με χρήση της γλώσσας XPath.

DefenseMinistry	CENTRAL
Minister/GenSecretaryB/SectorB2Manager	**Minister/GenSecretary/SectorBDirector**

Πίνακας 4.3α Αντιστοίχηση ρόλων (έσω αντιστοίχηση) με χρήση της XPath

PublicAffairsMinistry	CENTRAL
Minister/GenSecretary/SectorADirector	**Minister/GenSecretary/SectorBDirector**
Minister/GenSecretary/SectorBDirector/EmergencyReactionHead	**Minister/GenSecretary/SectorBDirector**

Πίνακας 4.3β Αντιστοίχηση ενός ρόλου από την κεντρική ιεραρχία σε δύο ρόλους τοπικής ιεραρχίας

Στην ουσία ανάγουμε την αντιστοίχηση ρόλων σε αντιστοίχηση διαφορετικών εγγράφων πολιτικών, καταγεγραμμένων σε XML. Αξίζει να σημειωθεί ότι λόγω της εκφραστικότητας της XPath, μπορούμε να αναπαραστήσουμε πολύπλοκες αντιστοιχήσεις ρόλων με ένα συμπαγή τρόπο, ομαδοποιώντας αντίστοιχους ρόλους σε μία μόνο σχέση XPath, χωρίς να χρειάζεται να γραφούν ξεχωριστοί κανόνες για κάθε ρόλο. Οι αντιστοιχήσεις μεταξύ των διαφόρων ιεραρχιών, αποθηκεύονται στο μητρώο διαχείρισης συνασπισμού, που αποτελεί τμήμα του συστήματος ελέγχου πρόσβασης που θα περιγραφεί αναλυτικότερα στην επόμενη παράγραφο.

4.3 Σύστημα επιβολής ελέγχων πρόσβασης

Όπως περιγράφηκε ήδη στο κεφάλαιο 3 ένα από τα βασικά προβλήματα που αφορούν στη διαχείριση συνεργαζόμενων Π.Σ. είναι η αντιμετώπιση του προβλήματος της ετερογένειας. Στα πλαίσια της αντιμετώπισης του προβλήματος αυτού, προτάθηκε η χρήση οντολογιών, για την παροχή μετα-δεδομένων που αφορούν στους πόρους που διαθέτει μια περιοχή και παράλληλα περιγράφηκε η διαδικασία δημιουργίας εικονικών δικτύων οντολογιών ανάλογα με τη θεματική κατηγορία στην οποία ανήκει καθένα τα συμμετέχοντα Π.Σ. Προκειμένου για το σχηματισμό των οντολογιών επιλέχθηκε το πλαίσιο περιγραφής πόρων (Resource Description Framework - RDF) (Decker et al, 2000). Η ικανότητα των οντολογιών RDF να επιτρέπουν τη σημασιολογική αναπαράσταση πόρων αξιοποιήθηκε στα πλαίσια των εργασιών (Belsis et al, 2005h)(Belsis et al, 2005g) και για την αναπαράσταση όρων πολιτικής ασφάλειας και των σχετικών τους ιδιοτήτων (attributes) όπως για παράδειγμα την περιγραφή των ρόλων που συμμετέχουν σε μια πολιτική, την περιγραφή των πόρων κλπ.

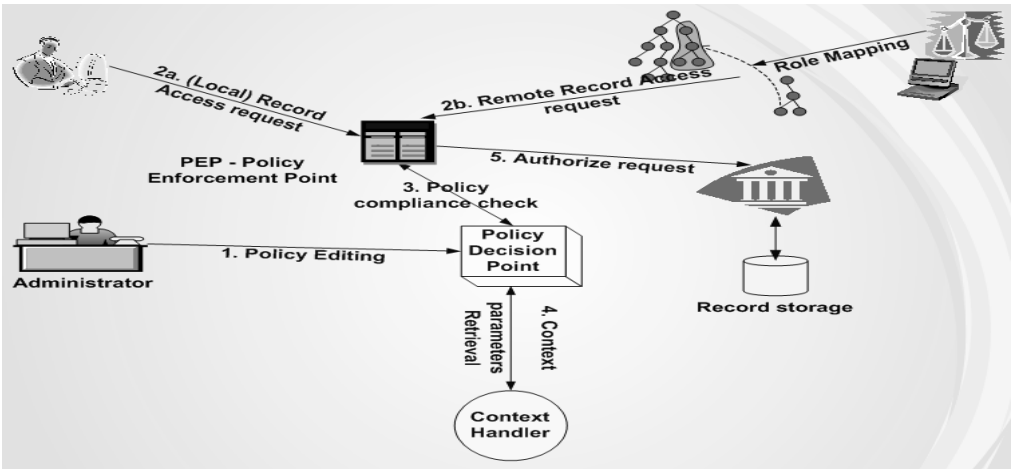
Στη συνέχεια, θα περιγράψουμε σε γενικές γραμμές τη λειτουργία του συστήματος επιβολής ελέγχων πρόσβασης. Τα βασικά τμήματα που το αποτελούν είναι: το σημείο επιβολής πολιτικών (Policy Enforcement Point - PEP) που είναι υπεύθυνο για την εφαρμογή των αρχών της πολιτικής, το σημείο αποφάσεων πολιτικής (Policy Decision Point - PDP) όπου εξετάζεται το σύννομο ενός αιτήματος σε σχέση με την υπάρχουσα πολιτική και που είναι υπεύθυνο επίσης για την τήρηση του μητρώου αντιστοιχήσεων ρόλων. Τέλος υπάρχει και ο χειριστής πλαισίου (context handler-CH) που συλλέγει πληροφορίες που αφορούν στη φύλαξη παραμέτρων συναφούς πλαισίου (context) όπως για παράδειγμα μεταβλητές περιβάλλοντος (που

διευκολύνουν την από κοινού αντιμετώπιση μίας σειράς ρόλων που προέρχονται από τον ίδιο οργανισμό).
Η βασική λειτουργία του συστήματος επιβολής ελέγχων πρόσβασης είναι η ακόλουθη: Ο διαχειριστής του συστήματος συγγράφει την πολιτική και τοποθετεί τις ενημερωμένες εκδόσεις της στο PDP. Όταν προκύψει ένα αίτημα για κάποιον πόρο αυτό απευθύνεται στο PEP. Το PEP με τη σειρά του δημιουργεί ένα κατάλληλο μήνυμα σε γλώσσα XML (πιν. 4.4α) και το αποστέλλει προς έλεγχο στο PDP. Το τελευταίο ελέγχει τη συμφωνία του αιτήματος με τις αρχές της πολιτικής. Ο Context Handler κατόπιν συλλέγει πληροφορίες που αφορούν στο πλαίσιο στο οποίο δρα το σύστημα. Όταν στο σημείο εφαρμογής πολιτικής καταφθάνει μια αίτηση για πρόσβαση σε πόρους τότε ερωτάται το σημείο απόφασης πολιτικής PDP. Στην περίπτωση που πρόκειται για ερώτημα που σχετίζεται με την τοπική πολιτική, τότε το ερώτημα απλά ελέγχεται σε σχέση με την υπάρχουσα πολιτική του οργανισμού (Εικ. 4.2, ενέργεια 2a). Στην περίπτωση που ο ρόλος δεν είναι γνωστός στο PDP τότε υποβάλλεται ερώτημα στο μητρώο διαχείρισης του συνασπισμού, προκειμένου να αναζητηθούν τυχόν αντιστοιχίσεις με υπάρχοντες ρόλους του συστήματος. (Εικ. 4.2, ενέργεια 2b). Κατόπιν, ανάλογα με το αν επιτρέπεται από την τοπική πολιτική (ή βάσει υπάρχουσας αντιστοίχησης με πολιτική συνεργαζόμενου οργανισμού) η πρόσβαση στον αιτούμενο πόρο, διαμορφώνεται κατάλληλο μήνυμα (πίν. 4.4β) το οποίο και αποστέλλεται στη συνέχεια προς εφαρμογή στο PEP.

```
<Subject>  <Attribute >   <AttributeValue>
          pbelsis@aegean.gr   </AttributeValue>
</Attribute>
</Subject><Resource>
<Attribute>
<AttributeValue>file://record/StudentlRecords/PeterBel
</AttributeValue></Attribute>
</Resource>
<Action><Attribute><AttributeValue>
read </AttributeValue></Attribute></Action>
          <Environment/></Request>
```

```
<Response>
          <Result>
<Decision>NotApplicable
</Decision>
          </Result>
</Response>
```

Πίνακας 4.4 α(αριστερά) Τμήμα από μήνυμα αιτήματος πόρου σε XACML 4.4β. (δεξιά) Τμήμα από μήνυμα απάντησης



Εικόνα 4.2 Λειτουργία επιβολής ελέγχου πρόσβασης σε βήματα (για τοπικές αλλά και απομακρυσμένες εξουσιοδοτήσεις).

Προκειμένου να αντιμετωπιστούν και περιπτώσεις σεναρίων υψηλών απαιτήσεων σε κατανεμημένα περιβάλλοντα, έχουμε επεκτείνει τις δυνατότητες του συστήματος μοιράζοντας το φόρτο επιβολής ελέγχων εξουσιοδότησης σε περισσότερα του ενός PDP, με στόχο την όσο το δυνατόν μεγαλύτερη διαθεσιμότητα του συστήματος. Δηλαδή αντί της δημιουργίας ενός κεντρικοποιημένου PDP μοιράζουμε το φόρτο μεταξύ διαφορετικών κατανεμημένων PDP που συνολικά επιτυγχάνουν το ίδιο αποτέλεσμα με τη λειτουργία ενός κεντρικού PDP (Belsis et al, 2005d)(Malatras et al, 2005b). Στα πλαίσια της παρούσας διατριβής παράλληλα αναπτύχθηκε πλαίσιο αυτοματοποιημένης διαχείρισης της ασφάλειας του συνασπισμού συστημάτων με στόχο την ελάττωση του διαχειριστικού φόρτου, το οποίο παρουσιάζεται στα επόμενα κεφάλαια. Λεπτομέρειες του μηχανισμού λειτουργίας των επιμέρους δομικών μονάδων του λογισμικού καθώς και η χρήση των διεπαφών του λογισμικού που αναπτύχθηκε και ενσωματώνει τις βασικές αρχές που περιγράφηκαν στο παρόν κεφάλαιο, θα παρατεθούν στο κεφάλαιο 7.

4.4 Περιβάλλοντα πολλαπλών πολιτικών με μερική εμπιστοσύνη μεταξύ των μερών

Μία από τις βασικές παραδοχές που έγιναν εξαρχής προκειμένου να ελαττωθεί η πολυπλοκότητα του προβλήματος, είναι αυτή της ύπαρξης ενός ρυθμιστικού μηχανισμού που εποπτεύει τη δημιουργία του συνασπισμού.

Μία άλλη αναγκαία προϋπόθεση είναι η ύπαρξη εμπιστοσύνης μεταξύ των συμμετεχόντων μερών (Bharadwaj et al, 2003), που σημαίνει ότι κανένα από τα συμμετέχοντα Π.Σ. δεν θα επιχειρήσει να αποκτήσει πρόσβαση σε περισσότερους πόρους από όσους είναι αναγκαίο για την επίτευξη του ρόλου του στα πλαίσια του συνασπισμού. Ένα άλλο πρόβλημα, έχει να κάνει με το ότι η πολιτική ενός οργανισμού κρύβει μια σημαντική ποσότητα ευαίσθητης πληροφορίας για τα συμμετέχοντα μέρη. Σε περιπτώσεις που μια σειρά οργανισμών επιθυμούν να συνεργαστούν, αλλά δεν διέπονται από κάποιο κοινό πλαίσιο, προκύπτει ένα πρόβλημα που αφορά στο πώς μπορεί να επιτευχθεί η δημιουργία του συνασπισμού, χωρίς να αποκαλυφθεί στο σύνολο της στα υπόλοιπα μέρη η πολιτική κάθε οργανισμού. Για παράδειγμα, στην περίπτωση υπουργείων που συνεργάζονται, το γεγονός ότι ανήκουν στο ίδιο πλαίσιο αμβλύνει τους πιθανούς ανταγωνισμούς και το ενδεχόμενο να προσπαθήσει κάποιο από τα εμπλεκόμενα μέρη να επωφεληθεί των άλλων. Δεν συμβαίνει όμως το ίδιο και στην περίπτωση οργανισμών του δημόσιου τομέα που συνεργάζονται με αντίστοιχους του ιδιωτικού. Στη δεύτερη περίπτωση, υπάρχει κίνητρο συνεργασίας αλλά και ενδεχόμενο να προσπαθήσει κάποιος ρόλος από τον ένα οργανισμό να αποκτήσει πρόσβαση σε μεγαλύτερο βαθμό σε κοινούς πόρους από ότι του είναι αναγκαίο.

Στη συνέχεια θα περιγραφεί μία λύση που αφορά στην απόκρυψη τμήματος της πολιτικής ασφάλειας των συμμετεχόντων μερών από το σύνολο των υπολοίπων οργανισμών που μετέχουν στη διαδικασία σχηματισμού του συνασπισμού, όπως προτάθηκε στα πλαίσια της εργασίας (Belsis et al, 2005f).

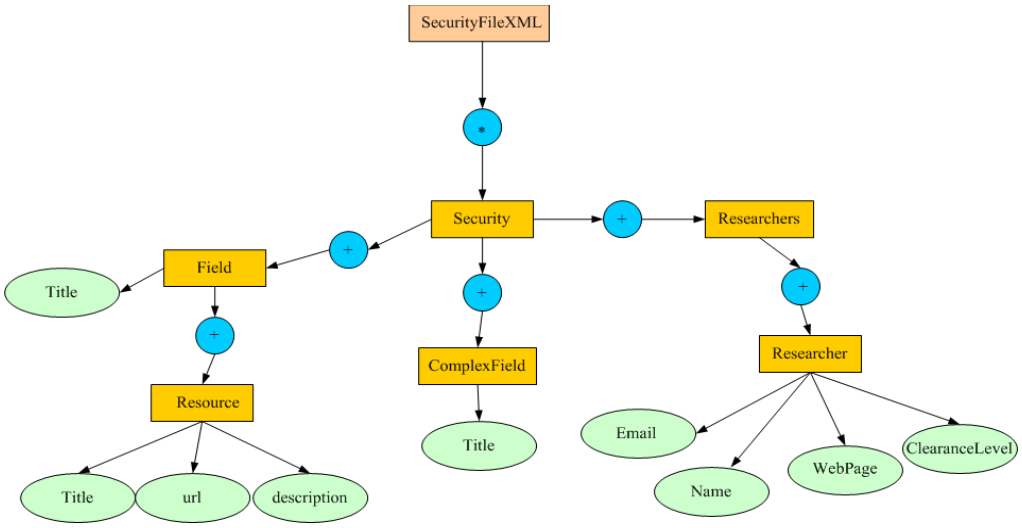
Στην περίπτωση σχηματισμού συνασπισμών μεταξύ Π.Σ. όπου υπάρχει (μερική) εμπιστοσύνη υπάρχει ανάγκη απόκρυψης κάθε επιπλέον πληροφορίας που αφορά στην πολιτική των Π.Σ. που συμμετέχουν στο συνασπισμό από τα υπόλοιπα συμμετέχοντα μέρη, ειδικά από όσα δεν έχουν υψηλό επίπεδο πρόσβασης σε κοινούς πόρους. Στην περίπτωση αυτή, είναι αναγκαίο να καθοριστούν ορισμένα κριτήρια που αφορούν στο ρόλο του κάθε συστήματος και τα δικαιώματα που μπορούν να αποδοθούν στους ρόλους του που συμμετέχουν στο συνασπισμό.

Μια δυνατότητα που μας δίνεται στο θέμα της απόκρυψης του συνόλου της πολιτικής είναι η μετατροπή του σχήματος XML σε σχεσιακή μορφή, όπου κατόπιν είναι δυνατό να εφαρμόσουμε τεχνικές απόκρυψης δεδομένων (και που υλοποιούνται εύκολα με βάση τα χαρακτηριστικά των περισσότερων εμπορικών συστημάτων διαχείρισης βάσεων δεδομένων - DBMS). Δηλαδή μπορούμε να αποκρύψουμε τις στήλες του σχεσιακού πίνακα που περιέχουν οποιαδήποτε πληροφορία αφορά σε κρίσιμα τμήματα της πολιτικής. Επομένως, κάθε σύστημα μπορεί να βλέπει από την πολιτική των άλλων μόνο ότι του έχει σαφώς επιτραπεί. Προκειμένου για την υλοποίηση της προτεινόμενης τεχνικής προτάθηκε στα πλαίσια της εργασίας (Belsis et al, 2005f) η τεχνική της μετατροπής εγγράφου ορισμού μορφής (Document Type Definition DTD) από την RDF πολιτική (ή ισοδύναμή της σε XML) σε σχεσιακή μορφή, με χρήση ενός αλγορίθμου που διενεργεί αυτόματα αυτή τη μετατροπή.
Για το σκοπό αυτό χρησιμοποιήθηκε ο αλγόριθμος hybrid inlining algorithm (Lee et al, 2001). Εννοιολογικά το DTD ενός XML εγγράφου έχει παρόμοια χαρακτηριστικά με το σχήμα μίας σχεσιακού τύπου βάσης δεδομένων (περισσότερες πληροφορίες για τη λειτουργία του αλγορίθμου μπορούν αν αναζητηθούν στην εργασία (Lee et al, 2001).
Στη συνέχεια δίνεται ένα παράδειγμα χρήσης του αλγορίθμου, που μετατρέπει ένα τμήμα από το έγγραφο περιγραφής του RDF σε κατάλληλο σχεσιακό σχήμα (εικ. 4.3). Το έγγραφο που αναλύεται, δεν αποτελεί έγγραφο πολιτικής σε XACML συμβατή μορφή (καθώς η XACML κωδικοποιείται σε XML και όχι σε RDF), βασίζεται στο παράδειγμα που αναλύεται στην εργασία (Belsis et al, 2005f) ενώ μπορεί εύκολα να αξιοποιηθεί για τη μετατροπή οποιασδήποτε τύπου XML πολιτικής σε σχεσιακή μορφή. Στο ακόλουθο παράδειγμα περιγράφονται μια σειρά ρόλων ενός οργανισμού, που στην προκειμένη περίπτωση διαδραματίζουν ερευνητές (Researchers) και για κάθε έναν παρατίθενται ως πεδία (attributes) περιγραφής ρόλων στο αρχείο καταγραφής της πολιτικής, πληροφορίες σχετικές με τον καθένα όπως η προσωπική σελίδα στο διαδίκτυο, το επίπεδο διαβάθμισης (ύψος στην ιεραρχία ρόλων κλπ.).

<?xml version="1.0" encoding="UTF-8"?>		
<! ELEMENT	SecurityFileXML	(Security*)>
<!ELEMENT	Security	(Field+,ComplexField+,Field+,Researchers+, Field+)>
<!ELEMENT	Field	(title, Resource+)>
<!ELEMENT	Title	(#PCDATA)>
<!ELEMENT	Resource	(title, url, description)>
<!ELEMENT	url	(#PCDATA)>
<!ELEMENT	Description	(#PCDATA)>
<!ELEMENT	ComplexField	(title, Field+)>
<!ELEMENT	Researchers	(Researcher+)>
<!ELEMENT	Researcher	(Name,Email, PersonalPage,ClearanceLevel)>
<!ELEMENT	Name	(#PCDATA)>
<!ELEMENT	Email	(#PCDATA)>
<!ELEMENT	PersonalPage	(#PCDATA)>
<!ELEMENT	ClearanceLevel	(#PCDATA)>

Πίνακας 4.5 Το έγγραφο περιγραφής μορφής DTD της RDF πολιτικής

Η βασική ιδέα είναι πρώτα η δημιουργία ενός γράφου όπου οι κύριες έννοιες αντιστοιχούν στους πίνακες που θα δημιουργηθούν, ενώ οι επιμέρους έννοιες αυτών είναι οι στήλες κάθε πίνακα. Ο γράφος του DTD σχήματος του Πίνακα 4.5 απεικονίζεται σχηματικά στην εικόνα 4.3.



Εικόνα 4.3 Μετατροπή RDF-DTD σε γράφο που παραπέμπει σε σχεσιακή μορφή

Παρατηρούμε ότι για μία σειρά από έννοιες που δηλώνονται σε ορισμένα πεδία του DTD υπάρχουν μια σειρά από υποκείμενα πεδία. Για παράδειγμα, για τους ερευνητές που συμμετέχουν σε ένα οργανισμό, χρησιμοποιούμε ως συσχετιζόμενα πεδία το όνομα, το email, το domain που ανήκουν. Η βασική έννοια του ερευνητή δίνει το έναυσμα για τη δημιουργία πίνακα, ενώ τα υποκείμενα πεδία αποτελούν τις στήλες του πίνακα (για κάθε νέο ερευνητή θα προσδιορίζονται οι αντίστοιχες τιμές των συγκεκριμένων πεδίων). Στη συνέχεια, με αντίστοιχη λογική μπορούμε να σχηματίσουμε και τους υπόλοιπους πίνακες. Αφού σχηματιστούν όλοι οι πίνακες είναι εύκολο να αποδώσουμε δικαιώματα ανάγνωσης σε συγκεκριμένες στήλες και για συγκεκριμένους ρόλους. Κατ' αυτόν τον τρόπο, το βασισμένο σε αντιστοίχηση ρόλων σύστημα μπορεί να λειτουργήσει προστατεύοντας τις πολιτικές των συμμετεχόντων μερών από την έκθεση στο σύνολο των υπολοίπων ρόλων.

4.5 Συμπεράσματα

Η εφαρμογή μηχανισμών επιβολής ελέγχου πρόσβασης σε περιβάλλοντα πολλαπλών πολιτικών και η λειτουργία ενός κλιμακούμενου μηχανισμού που επιτρέπει τη διασύνδεση διαφορετικών συστημάτων μεταξύ τους, αποτελεί τους κύριους στόχους του παρόντος κεφαλαίου. Μετά από μία επισκόπηση των δυνατοτήτων των γλωσσών περιγραφής πολιτικών ασφάλειας καθώς επίσης και συναφών ερευνητικών προσεγγίσεων στο χώρο της επιβολής ελέγχων πρόσβασης σε περιβάλλοντα συνεργαζόμενων συστημάτων, αναπτύχθηκαν οι προτεινόμενες στα πλαίσια της παρούσας διατριβής τεχνικές όπως αυτές περιγράφονται στις εργασίες (Belsis et al, 2005h) (Belsis et al, 2005b) (Belsis et al, 2005h) (Belsis et al, 2006c)(Belsis, 2006e). Το προτεινόμενο πλαίσιο διαθέτει μία σειρά από χαρακτηριστικά, σε αντιδιαστολή και με συναφείς επιστημονικές εργασίες:

- Χαρακτηρίζεται από χαμηλή πολυπλοκότητα στην υλοποίησή του ενώ στηρίζεται κατά κύριο λόγο σε διαλειτουργικές τεχνολογίες ενώ αξιοποιεί τεχνολογίες που τείνουν να αποκτήσουν χαρακτήρα προτύπου στην επεξεργασία και ανταλλαγή πληροφοριών.
- Διατηρεί τον αυτόνομο χαρακτήρα των συνεργαζόμενων συστημάτων.

- Επιτρέπει την υποβολή ερωτημάτων που αφορούν σε πόρους του συστήματος με ελάχιστη κατανάλωση δικτυακών και υπολογιστικών πόρων.
- Παράλληλα, προτείνεται στα πλαίσια της διατριβής μία τεχνική για την αντιμετώπιση του προβλήματος της απόκρυψης κρίσιμων τμημάτων της πολιτικής ασφάλειας από το σύνολο των συμμετεχόντων μερών. Όπως αναφέρθηκε το πρόβλημα της διαπραγμάτευσης χωρίς περιορισμούς περισσότερων από δύο πολιτικές ασφάλειας είναι NP-πλήρες. Έτσι κρίνεται αναγκαίο προκειμένου για την επίτευξη λύσης σε περιβάλλοντα πολλαπλών πολιτικών να τεθούν μία σειρά από περιορισμοί, όπως επίσης και να εισαχθεί ένα ρυθμιστικό πλαίσιο που εποπτεύει τη λειτουργία του συνασπισμού. Προκειμένου τέλος να αποφευχθεί η έκθεση του συνόλου της πολιτικής ενός οργανισμού από τα υπόλοιπα μέρη, αναπτύχθηκε μία τεχνική απόκρυψης κρίσιμων τμημάτων της πολιτικής των συνεργαζόμενων οργανισμών, μέσω της αυτοματοποιημένης μετατροπής της XML πολιτικής σε σχεσιακή μορφή. Έτσι δίνεται η δυνατότητα αυτοματοποιημένης μετατροπής των πολιτικών σε ισάριθμα σχεσιακά σχήματα, γεγονός που επιτρέπει την εφαρμογή της μεθόδου ακόμη και για μεγάλο σύνολο πολιτικών.

ΚΕΦΑΛΑΙΟ 5 - Αυτοματοποιημένη διαχείριση πολιτικών ασφάλειας

Η διαχείριση της ασφάλειας ενός συνασπισμού αυτόνομων συστημάτων είναι μια πολύπλοκη διαδικασία που επιφέρει ιδιαίτερο φόρτο τόσο στους διαχειριστές των μεμονωμένων συστημάτων όσο και σε αυτούς που είναι επιφορτισμένοι με τη διαχείριση του συνασπισμού, μέσω της δημιουργίας των αντιστοιχήσεων ρόλων, της διατήρησης ή της απομάκρυνσης ενός Π.Σ. στο συνασπισμό κοκ. Στις επόμενες παραγράφους θα παρουσιάσουμε τις γενικές αρχές ενός φορμαλισμού που επιτρέπει την αναπαράσταση προβλημάτων ελέγχου πρόσβασης που αφορούν τόσο σε επίπεδο ενός οργανισμού όσο και σε επίπεδο πολλαπλών συνεργαζόμενων οργανισμών, καθιστώντας παράλληλα εφικτή την ελάττωση του διαχειριστικού φόρτου. Στη συνέχεια, με την αναγωγή του προβλήματος της (ημι)αυτοματοποιημένης διαχείρισης του συνασπισμού σε ένα πρόβλημα επίλυσης χαλαρών περιορισμών (soft constraints) προτείνεται μία τεχνική εξεύρεσης επιτρεπτών αντιστοιχήσεων ακόμη και όταν αυτές δεν έχουν καθοριστεί ρητά, αλλά δεν απαγορεύονται από κάποιους κανόνες της πολιτικής.

Για τη δημιουργία του παραπάνω πλαισίου στηριχθήκαμε στην άλγεβρα των ημιδακτυλίων, χρησιμοποιώντας τη σημειολογία που εμφανίζεται στις εργασίες (Bistarelli, 2004) και (Bistarelli et al, 2001). Θα δείξουμε ότι η χρήση του συγκεκριμένου φορμαλισμού είναι επαρκής συνθήκη για την αναπαράσταση της ιεραρχίας ρόλων και δικαιωμάτων, ενώ τέλος θα εφαρμόσουμε τις βασικές του αρχές με στόχο τη βελτιστοποίηση της διαχείρισης ασφάλειας σε συνδυασμό με τη χρήση της τεχνικής αντιστοιχήσεων ρόλων. Οι αρχές που καταγράφονται στο παρόν κεφάλαιο έχουν καταγραφεί κατά κύριο ρόλο στις εργασίες (Belsis et al, 2006b) και (Belsis, 2006e).

5.1 Βασικές έννοιες – Ημιδακτύλιοι και προβλήματα ικανοποίησης χαλαρών περιορισμών (Semirings and Soft constraint satisfaction problems (SCSP's)

Οι ημιδακτύλιοι είναι αλγεβρικές δομές, κατάλληλες για την αναπαράσταση ποικιλίας προβλημάτων από διαφορετικές περιοχές. Στα (Bharadwaj et al, 2003)(Belsis et al, 2006b)(Bistarelli, 2004) βρίσκουμε εφαρμογές τους σε προβλήματα προσανατολισμένα στην ασφάλεια. Θα ξεκινήσουμε με μια σύντομη εισαγωγή στους ημιδακτυλίους και στα προβλήματα χαλαρών περιορισμών γενικότερα και θα δείξουμε πώς μπορούν να εφαρμοστούν σε προβλήματα που αφορούν στην ασφάλεια.

Ορισμός 1: Ένας ημιδακτύλιος είναι μια πλειάδα <A,+,*,**0,1**>, όπου

- A είναι ένα σύνολο **0,1** $\in$A
- Η πράξη + της πρόσθεσης είναι κλειστή, αντιμεταθετική, προσεταιριστική στο A με **0** το απορροφητικό στοιχείο
- Η πράξη * του πολλαπλασιασμού είναι κλειστή και επιμεριστική ως προς το A , με το **1** να είναι το μοναδιαίο στοιχείο και το **0** να είναι το απορροφητικό στοιχείο
- Η * είναι επιμεριστική επί της +

Θα πρέπει να σημειώσουμε τα εξής: Τόσο το σύνολο A, οι δύο πράξεις + και * όσο και το μοναδιαίο και απορροφητικό στοιχείο δεν παραπέμπουν στις συνήθεις πράξεις και στοιχεία από το σύνολο των ακεραίων, αλλά αναφέρονται με τη γενικευμένη τους μορφή. Το γεγονός επίσης ότι η + δηλώνεται επί συνόλων και όχι επί ζευγών ή

πλειάδων, κάνει την πράξη αντιμεταθετική, προσεταιριστική και ταυτοδύναμη (idempotent).

Ορισμός 2: Ένα σύστημα περιορισμών ορίζεται σαν μια πλειάδα CS=<S,D,V> όπου S είναι ένας κατάλληλος ημιδακτύλιος περιορισμών (c-ημιδακτύλιος), D είναι ένα πεπερασμένο σύνολο και V είναι ένα διατεταγμένο σύνολο μεταβλητών.

Ορισμός 3: Περιορισμός σε ένα αντίστοιχο σύστημα CS είναι μια πλειάδα <def,con> με con$\subseteq$V τη συνάρτηση σύνδεσης (connection function), τέτοια ώστε con(c)=<v_1,..,v_k> να περιγράφει ποιες μεταβλητές υπεισέρχονται σε ποιο περιορισμό, ενώ def είναι η συνάρτηση ορισμού (definition function), που προσδιορίζει ποιες πλειάδες επιτρέπονται από κάποιο περιορισμό. Επομένως η συνάρτηση def αντιστοιχεί μια τιμή στον ημιδακτύλιο σε κάθε συνδυασμό τιμών των μεταβλητών που περιέχονται στη συνάρτηση con. Αυτή η τιμή μπορεί να ισοδυναμεί με μια πιθανότητα, ένα κόστος, κάποια προτίμηση κλπ.

Με τις παραπάνω δομές μπορούμε να περιγράψουμε προβλήματα ελέγχου πρόσβασης και να μοντελοποιήσουμε τόσο ιεραρχίες ρόλων όσο και δικαιωμάτων. Επομένως η σχέση υποσυνόλου $\subseteq$ μας επιτρέπει να περιγράψουμε τα πλήρως διατεταγμένα σύνολα δικαιωμάτων και ρόλων. Επίσης, επιλέγοντας κατάλληλες πράξεις για τη γενικευμένη πρόσθεση και πολλαπλασιασμό, μπορούμε να μετατρέψουμε το πρόβλημα της αντιστοίχησης δικαιωμάτων σε ρόλους σε ένα πρόβλημα ικανοποίησης περιορισμών. Το πλεονέκτημα της χρήσης c-ημιδακτυλίων είναι ότι η ταυτοδυναμία (idempotency) της πράξης + βοηθά να ορίσουμε μια πράξη μερικής διάταξης $\leq_s$ στο σύνολο A, που επιτρέπει να συγκρίνουμε διαφορετικά στοιχεία του ημιδακτυλίου. Τυπικά μια έκφραση $a \leq_s b$ είναι ισοδύναμη με a+b=b, ή αλλιώς ότι ένα στοιχείο είναι προτιμότερο ανάμεσα στα a,b για την πράξη +. Επομένως μπορούμε να μοντελοποιήσουμε πράξεις όπου ένα δικαίωμα (ή ρόλος) είναι προτιμότερο, ανάλογα με το αν προτιμότερη κατάσταση για το σύστημα είναι η ανάθεση δικαιωμάτων σε ρόλους ή το αντίθετο (εξαρτάται από το είδος του συστήματος και τους περιορισμούς των πολιτικών).

Ορισμός 4 (προβολή - projection)**:** Δεδομένου ενός συστήματος περιορισμών (constraint system) CS=<S,D,V> με S=<A,+,×, **0**, **1**>, έναν περιορισμό c=<def,con> στο σύστημα αυτό και ένα σύνολο μεταβλητών I$\subseteq$V, τότε η προβολή του c επί του I αναπαριστώμενη ως $c\Downarrow_I$, είναι ένας νέος περιορισμός <def΄, con΄> με con΄=I$\cap$con και $def'(t') = \sum_{\{t | t\downarrow^{con}_{I\cap con} = t'\}} def(t)$.

Τυπικά η προβολή ισοδυναμεί με ελαχιστοποίηση του χώρου τιμών μόνο στις μεταβλητές ενδιαφέροντος. Εκτός από την προβολή, μια άλλη χρήσιμη πράξη με ιδιαίτερη σημασία είναι αυτή του συνδυασμού, που μας επιτρέπει να συνδυάζουμε περιορισμούς.

Ορισμός 5 (συνδυασμός - combination): Δοθέντων δύο περιορισμών c_1, c_2 στο προτεινόμενο σύστημα, ο συνδυασμός τους $c_1 \otimes c_2$ είναι ένας άλλος περιορισμός c= <def,con> όπου con=$con_1 \cup con_2$ και $def(t) = def_1(t\downarrow^{con}_{con_1}) \times def_2(t\downarrow^{con}_{con_2})$. Είναι προφανές ότι η $\otimes$ είναι αντιμεταθετική και προσεταιριστική, εφόσον είναι και η πράξη × .

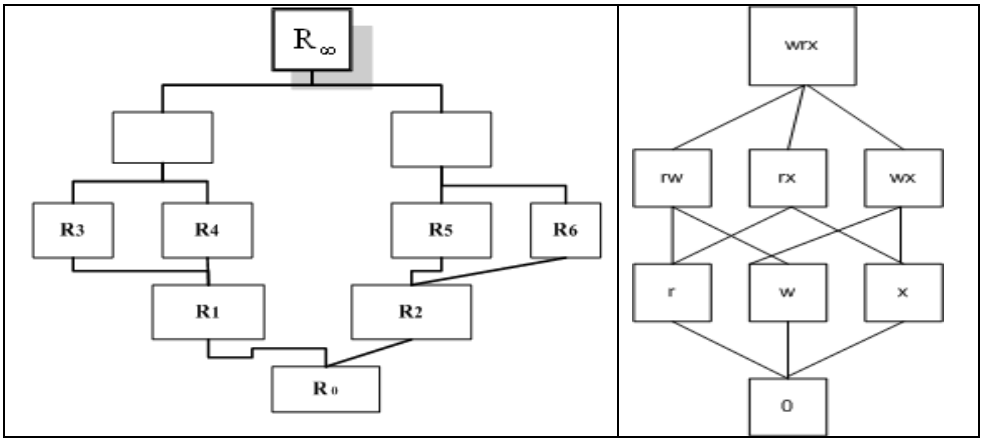
Η λύση sol(P) ενός προβλήματος περιορισμών P=<C,con> επί ενός αντίστοιχου συστήματος περιορισμών CS ορίζεται ως sol(P)= $(\otimes C)\Downarrow_{con}$, προκύπτει δε αν

συνδυάσουμε όλους τους υπό μελέτη περιορισμούς και τους προβάλλουμε επί των μεταβλητών που δηλώνονται στη συνάρτηση con.

Το βέλτιστο επίπεδο συνάφειας (best level of consistency) oLevel(P) είναι μια μετρική που αποδίδει μια εκτίμηση του πόσο η δοθείσα λύση ικανοποιεί τους περιορισμούς του προβλήματος και αποκτάται αν πρώτα πάρουμε την λύση και την προβάλλουμε επί του κενού συνόλου των μεταβλητών.

5.2 Καθορισμός κατάλληλων ημιδακτυλίων

Η εύρεση κατάλληλου ημιδακτυλίου που περιγράφει ικανοποιητικά ένα πρόβλημα, είναι ένα σημαντικό βήμα, εφόσον επηρεάζει σημαντικά την πορεία εξεύρεσης λύσης (αν υπάρχει). Στα προβλήματα ασφάλειας που μας ενδιαφέρουν, μπορούμε να διακρίνουμε δύο βασικές ιεραρχίες στα πλαίσια του μοντέλου RBAC: την ιεραρχία ρόλων και την ιεραρχία δικαιωμάτων.



Εικόνα 5-1 Αναπαράσταση ιεραρχιών ρόλων και δικαιωμάτων

Η ιεραρχία ρόλων μπορεί να αναπαρασταθεί από τον ημιδακτύλιο $< R,+_R, *_R, R_0, R_\infty>$, όπου:

- R είναι το σύνολο ρόλων στο σύστημα
- Η πράξη $+_R$ ορίζεται ως: $(R_1+_R R_2)$ και δηλώνει τον υψηλότερο απόγονο των ρόλων R_1 και R_2 στην ιεραρχία ρόλων
- Η πράξη $*_R$ ορίζεται ως ο κοινός πρόγονος των ρόλων R_1 και R_2 στην ιεραρχία ρόλων.
- R_∞, R_0 είναι οι ρόλοι που έχουν τα μέγιστα και ελάχιστα προνόμια αντίστοιχα σε ένα οργανισμό. Για παράδειγμα στην ιεραρχία της εικ. 5.1 ο R_∞ έχει μέγιστα προνόμια ενώ ο ρόλος R_0 είναι ο ρόλος με τα ελάχιστα προνόμια.

Το παραπάνω σύστημα περιορισμών μπορεί να χρησιμοποιηθεί ως ακολούθως (Bharadwaj et al, 2003): θεωρώντας ότι ένα σύστημα προσφέρει εξουσιοδότηση σε απομακρυσμένους χρήστες, μπορούμε να επιλέξουμε τον περιορισμό <R,V,C> όπου με R θεωρούμε τον ημιδακτύλιο ρόλων (Roles Semiring), C είναι τα διαπιστευτήρια-πιστοποιητικά που είναι γνωστά στο σύστημα και V είναι το σύνολο τιμών που μπορεί να πάρουν αυτοί οι τύποι πιστοποιητικών. Υπό αυτές τις συνθήκες κάθε πλειάδα αντιστοιχεί στην απόδοση ενός ρόλου στο συγκεκριμένο συνδυασμό τιμών πιστοποιητικών, ενώ σε οποιοδήποτε μη αποδεκτό συνδυασμό πιστοποιητικών αποδίδεται ο ρόλος R_0.

Ακολούθως, θεωρούμε την ιεραρχία δικαιωμάτων και δηλώνουμε ένα κατάλληλο ημιδακτύλιο $<P,+_P,*_P,P_\infty,P_0>$, όπου

- P είναι το σύνολο των δικαιωμάτων στο σύστημα
- Η πράξη $+_P$ δηλώνεται ως: $(P_1+_P P_2)$ και αντιπροσωπεύει το υψηλότερο δικαίωμα μεταξύ των P_1 και P_2
- Με την πράξη $*_P$ προκύπτει το χαμηλότερο δικαίωμα
- P_∞, P_0 είναι το υψηλότερο και το χαμηλότερο δικαίωμα στην ιεραρχία, αντίστοιχα

Ο ημιδακτύλιος των δικαιωμάτων μπορεί να αξιοποιηθεί ως ακολούθως: Θεωρούμε ένα σύστημα περιορισμών <R, O, P> που αποτελείται από τις δυνατές τιμές για τις μεταβλητές: R (ρόλοι), O (τα αντικείμενα προς προσπέλαση) και P (τα απαραίτητα δικαιώματα). Σε κάθε ρόλο στο σύστημα αντιστοιχείται μια πλειάδα t από δικαιώματα πρόσβασης. Το αποτέλεσμα είναι ένα SCSP του οποίου η λύση είναι σε κάθε περίπτωση ο χαμηλότερος ρόλος στην ιεραρχία που είναι αναγκαίο να ανατεθεί σε κάποιο χρήστη, προκειμένου να αποκτήσει πρόσβαση στους υπό διαπραγμάτευση πόρους.

Στην περίπτωση διαμοιρασμού πόρων από δύο αυτόνομα συστήματα, επιθυμούμε να αντιστοιχήσουμε δικαιώματα στους διαμοιραζόμενους πόρους για ένα συγκεκριμένο αριθμό ρόλων από κάθε υποσύστημα που συμμετέχει στο συνασπισμό. Ορίζουμε ένα νέο σύστημα περιορισμών $<P, L_1+L_2, R>$, όπου P είναι κατάλληλος ημιδακτύλιος, L_1 και L_2 είναι τα σύνολα τιμών που αντιστοιχούν στους τοπικούς ρόλους για κάθε σύστημα και R είναι το σύστημα της γενικευμένης ιεραρχίας ρόλων. Στη συνέχεια, προκειμένου να αντιστοιχίσουμε δικαιώματα στους απομακρυσμένους ρόλους πρέπει να εργαστούμε ως εξής: δημιουργούμε πρώτα ένα κατάλληλο πρόβλημα ικανοποίησης περιορισμών (CSP) αντιστοιχώντας δικαιώματα στους τοπικούς ρόλους $P \rightarrow L_1$ και $P \rightarrow L_2$ και κατόπιν κάνουμε αντιστοίχηση των τοπικών ρόλων σε ρόλους της κεντρικής ιεραρχίας. Στην περίπτωση που τα δικαιώματα που το σύνθετο CSP περιγράφει (και που έμμεσα έχουν αντιστοιχιστεί σε ένα γενικό ρόλο) υπερκαλύπτουν τα δικαιώματα του τοπικού ρόλου που διαθέτει πρόσβαση στους αιτούμενους πόρους, προκύπτει μια αποδεκτή λύση.

Συμπερασματικά μπορούμε να πούμε ότι οι αντιστοιχίσεις ρόλων μπορούν να θεωρηθούν σαν ορισμένες πλειάδες που είναι γνωστές εξαρχής. Προκειμένου για τη σύνθεση του προβλήματος ικανοποίησης περιορισμών, οι απαραίτητες πληροφορίες που αφορούν στις σχηματιζόμενες πλειάδες μπορούν να ανακτηθούν από το μητρώο αντιστοιχήσεων που διατηρείται για το συνασπισμό. Κατόπιν, ανάλογα με το αν το πρόβλημα έχει αποδεκτές λύσεις ή όχι μπορούμε να ικανοποιήσουμε το αίτημα πρόσβασης ή μπορούμε να αρνηθούμε στο χρήστη την πρόσβαση στους αιτούμενους πόρους.

5.3 Βελτιστοποίηση της τεχνικής αντιστοιχήσεων ρόλων

Σε πολλές περιπτώσεις αιτημάτων για πρόσβαση σε πόρους από απομακρυσμένους ρόλους, ενδέχεται να μην έχει καθοριστεί αντιστοίχηση με κάποιον ρόλο στο τοπικό σύστημα με αποτέλεσμα κανονικά να πρέπει να απορριφθεί το αίτημα. Αν ο απομακρυσμένος ρόλος ωστόσο έχει ιδιαίτερα αυξημένα προνόμια, τότε στις περισσότερες περιπτώσεις θα πρέπει να του αποδοθεί δικαίωμα πρόσβασης. Για να γίνει αυτό, θα πρέπει να απαιτηθεί η εμπλοκή των διαχειριστών του συστήματος οι

οποίοι θα δημιουργήσουν μια αντίστοιχη εγγραφή στο μητρώο διαχείρισης του συνασπισμού. Μας ενδιαφέρει από την άποψη αυτή να ελαχιστοποιήσουμε το διαχειριστικό φόρτο, που απαιτεί τη διαρκή εμπλοκή των διαχειριστών. Θα εξετάσουμε συνεπώς αν υπάρχει τρόπος ώστε να μπορέσει να βελτιστοποιηθεί η διαχείριση του συστήματος αποδίδοντας αυτόματα με ασφαλή τρόπο δικαιώματα σε ρόλους. Η βασική ιδέα είναι ότι είναι επιτρεπτή η ροή της πληροφορίας από κύριους (σημαντικούς) ρόλους προς δευτερεύοντες. Η βασική αρχή λειτουργίας μιας τέτοιας προσέγγισης είναι παρόμοια με τη φιλοσοφία των πολιτικών έλεγχου (release control policies) όπως περιγράφονται στο (Yao et al, 2005) και (Bettini et al, 2002). Στην περίπτωση των (Yao et al, 2005) εισάγεται ένα σημείο εφαρμογής φιλτραρίσματος (για παράδειγμα ένα τείχος προστασίας ειδικού σκοπού). Στην περίπτωσή μας ο έλεγχος μπορεί να γίνεται στο PDP. Η βασική αρχή πίσω από τη συγκεκριμένη προσέγγιση είναι ότι μία σειρά από αιτούμενες εξουσιοδοτήσεις (υπονοούμενες) μπορούν να προκύψουν από ρητά εκπεφρασμένες εξουσιοδοτήσεις με το συνήθη τρόπο με τον οποίο οι εξουσιοδοτήσεις διαδίδονται προς τα κάτω στην ιεραρχία εξουσιοδοτήσεων στα πλαίσια του RBAC (Yao et al, 2005). Μια τέτοιου είδους διάδοση επιτρέπει σε οντότητες χαμηλότερα στην ιεραρχία να γενικεύουν οντότητες που βρίσκονται χαμηλότερα, ή σε απλούστερη διατύπωση επιτρέπει στις οντότητες που βρίσκονται υψηλότερα στην ιεραρχία να κάνουν χρήση των δικαιωμάτων οντοτήτων που βρίσκονται πιο χαμηλά στην ιεραρχία.

Σε μια τέτοια περίπτωση για μια δεδομένη τριάδα (αντικειμένου, αποστολέα παραλήπτη) - (Object, Sender, Receiver) θα θέλαμε να καθορίσουμε ένα επιτρεπτό μονοπάτι που επιτρέπει τη ροή πληροφορίας με ασφαλή τρόπο. Λέγοντας ασφαλή τρόπο εννοούμε ότι δεν θα πρέπει να επιτρέψουμε σε ένα ρόλο με λιγότερα προνόμια από τα απαραίτητα να αποκτήσει πρόσβαση σε πόρους. Χρησιμοποιώντας το συμβολισμό των ημιδακτυλίων θα δείξουμε ότι μπορούμε να αναγάγουμε το πρόβλημά μας σε πρόβλημα εύρεσης ελάχιστου μονοπατιού με διαφορετικού τύπου βάρη.

Ας φανταστούμε το ακόλουθο σενάριο (Εικ. 5.2): ο ρόλος V που κατέχει μια υψηλή θέση στην ιεραρχία εξουσιοδοτήσεων στο Π.Σ. Β, επιθυμεί να αποκτήσει πρόσβαση σε πόρους από το Π.Σ. Α, για τους οποίους είναι αναγκαία η κατοχή προνομίων του ρόλου Τ2 (ή κάποιου ανώτερου) στην ιεραρχία Α. Επειδή δεν υπάρχει απευθείας αντιστοίχηση ανάμεσα στους δύο ρόλους αρχικό και τελικό, θα πρέπει να κληθούν οι διαχειριστές του συστήματος για να δημιουργήσουν νέα κατάλληλη αντιστοίχηση. Δεδομένου ότι ο ρόλος V μπορεί να αποκτήσει δικαιώματα του ρόλου U στην περιοχή Β και δεδομένου ότι υπάρχει αντιστοίχηση στον ρόλο Q στην περιοχή Α που μπορεί να αποκτήσει τα δικαιώματα του Τ2, μπορούμε να αντιληφθούμε ότι είναι δυνατό (αν δεν υπάρχουν άλλοι περιορισμοί) να θεωρήσουμε ότι ο ρόλος V κανονικά θα μπορούσε να αποκτήσει τα δικαιώματα του ρόλου Τ2. Επομένως το πρόβλημα ανάγεται πλέον στον εντοπισμό νόμιμων μονοπατιών (αν υπάρχουν). Θα πρέπει επίσης να τονίσουμε ότι υπάρχουν περιπτώσεις που δεν θα θέλαμε να ενεργοποιήσουμε κάποιο ενδιάμεσο ρόλο εξαιτίας της κρισιμότητας που τον χαρακτηρίζει.

Τέλος, θα πρέπει να αναφέρουμε ότι η συγκεκριμένη τεχνική ενδεχόμενα να μην είναι εφαρμόσιμη σε περιπτώσεις που τα δεδομένα είναι κρίσιμα ή ευαίσθητα (αν και η τεχνική των αντιστοιχήσεων μπορεί να εφαρμοστεί ακόμη και τότε). Εναλλακτικά, σε περίπτωση που η κρισιμότητα των δεδομένων το απαιτεί, η παραπάνω τεχνική μπορεί να εφαρμοστεί σαν εργαλείο υποστήριξης, όπου δεν θα λαμβάνονται απευθείας

αποφάσεις αλλά απλά θα προτείνονται ως δυνατότητες στο διαχειριστή του συστήματος.

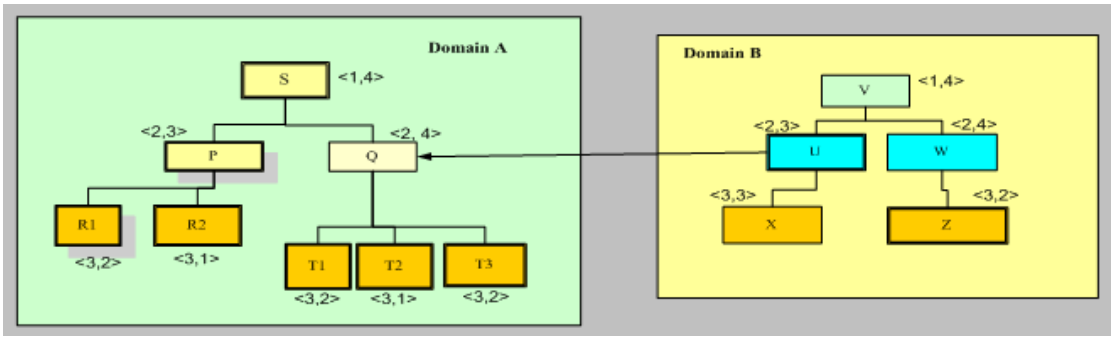
Προκειμένου να συμπεριλάβουμε στις υπό μελέτη περιπτώσεις ρόλους με μεγαλύτερη σημασία και κρισιμότητα για τον οργανισμό (που θα πρέπει να αποφεύγεται να ενεργοποιηθούν) δεν αναζητούμε απλά την ύπαρξη μονοπατιού, αλλά αναζητούμε την ύπαρξη του καλύτερου μονοπατιού υπολογίζοντας διαδρομές με βάρη. Ένα βάρος μπορεί να αποτελείται από ένα ζεύγος τιμών <a,b> όπου το "a" αναπαριστά το ύψος στην ιεραρχία ρόλων ενώ η παράμετρος "b" την κρισιμότητα κάθε ρόλου. Χρησιμοποιώντας ένα αλγόριθμο εκτίμησης μονοπατιών μπορούμε να προσδιορίσουμε όλες τις νόμιμες διαδρομές. Όταν ένας χρήστης αναζητά ένα μονοπάτι από κάποιο αποστολέα σε ένα συγκεκριμένο παραλήπτη, δεν αναζητά ένα τυχαίο μονοπάτι αλλά ένα βέλτιστο μονοπάτι. Σύμφωνα με τις αρχές της πολιτικής ελέγχου πρόσβασης, θεωρούμε δύο συνθήκες που μπορούν να ληφθούν υπόψη:

i) Ένας χρήστης δεν μπορεί να αποκτήσει δικαιώματα που συσχετίζονται με χρήστη που βρίσκεται υψηλότερα στην ιεραρχία και

ii) Ρόλοι που είναι πιο σημαντικοί (κρίσιμοι) θα πρέπει να είναι ενεργοποιούνται με χαμηλότερη σειρά προτίμησης.

5.4 Προσδιορισμός βέλτιστων μονοπατιών

Έστω η περίπτωση όπου έχουμε δύο διαφορετικές ιεραρχίες (Εικ. 5.2). Μπορούμε να αναπαραστήσουμε τους ρόλους σε κάθε ιεραρχία θεωρώντας το γράφο G=(N, E) όπου οι ρόλοι αναπαρίστανται σαν κόμβοι στο γράφο και αντιστοιχούμε ένα βάρος σε κάθε τόξο e $\in$E από τον κόμβο p μέχρι τον κόμβο q (p, q $\in$N). Αυτό το βάρος θα σχετίζεται με το ζεύγος τιμών που αναφέραμε και που συσχετίζεται με το επίπεδο στην ιεραρχία στο οποίο ανήκει κάθε ρόλος (μια παράμετρος που καθορίζει πόσο σημαντικός είναι κάθε ρόλος στην ιεραρχία) καθώς και την κρισιμότητα που χαρακτηρίζει κάθε ρόλο. Το παραπάνω πρόβλημα μπορεί να αναπαρασταθεί από δύο ημιδακτυλίους. Προκειμένου για τον υπολογισμό του κόστους βάσει της πρώτης παραμέτρου, μπορούμε να ορίσουμε ένα ημιδακτύλιο <N, +, $\min^*$, 0, +∞> όπου η πράξη $\min^*$ δηλώνει την ελάχιστη διαφορά (λαμβάνοντας υπόψη μόνο θετικές διαφορές) και την πράξη + με την κλασική έννοια. Για τον υπολογισμό του κόστους με βάση τη δεύτερη παράμετρο που σχετίζεται με την κρισιμότητα καθορίζουμε ένα ημιδακτύλιο <N, +, min, 0, +∞>, όπου min και + δηλώνονται με την κλασική τους σημασία. Σύμφωνα κατόπιν με τις αρχές που περιγράφηκαν στις προηγούμενες παραγράφους μπορούμε να εντοπίσουμε επιτρεπτά μονοπάτια βασισμένοι στις ακόλουθες αρχές: κάθε μονοπάτι δεν θα πρέπει να παραβιάζει τις αρχές της ιεραρχίας προχωρώντας στην κατεύθυνση της ενεργοποίησης ρόλων με περισσότερα προνόμια, που απαιτούν μεγαλύτερο βαθμό εξουσιοδότησης από ότι ο τρέχων κάθε φορά ρόλος. Παράλληλα θα πρέπει να αποφεύγουμε να ενεργοποιούμε ρόλους μείζονος σημασίας. Για να επιτύχουμε τα παραπάνω μπορούμε να χρησιμοποιήσουμε κάποιον από τους γνωστούς αλγόριθμους συντομότερου μονοπατιού (shortest path). Ωστόσο ο υπολογισμός με βάση τα βάρη των μονοπατιών είναι κάπως πιο πολύπλοκος όταν τα βάρη συσχετίζονται με τις ακμές και όταν χρησιμοποιούνται πολύπλοκοι τύποι για την εξαγωγή του βάρους.



Εικόνα 5.2 Παράδειγμα επίλυσης προβλήματος αντιστοίχησης ρόλων και αναπαράστασης ιεραρχιών με χρήση βαρών

Το πρόβλημα αυτό μπορεί να περιγραφεί με βάση το φορμαλισμό προγραμματισμού με χρήση χαλαρών περιορισμών (Soft Constraint Logic Programming - SCLP) (Bistarelli 2004)(Belsis et al, 2006b) που εφαρμόζεται επί ενός κατάλληλου ημιδακτυλίου. Προκειμένου να βρούμε ένα μονοπάτι που δεν παραβιάζει την ιεραρχία ρόλων αναζητούμε μόνο θετικές διαφορές ανάμεσα στην πρώτη παράμετρο του βάρους που συσχετίζεται με κάθε ρόλο. Επιτρέπουμε μόνο διαφορές με θετικό πρόσημο (ή μηδέν) που σημαίνει ότι ο ρόλος στον οποίο κατευθυνόμαστε πρέπει να βρίσκεται πιο κάτω στην ιεραρχία (θεωρούμε και για τους δύο οργανισμούς όλους τους ρόλους που βρίσκονται στο ίδιο επίπεδο ως ισοδύναμους) (Shafiq et al, 2005). Επιπλέον θέλουμε να υπολογίσουμε ελάχιστες διαφορές βασιζόμενοι στις τιμές του δεύτερου μέρους του ζεύγους τιμών, που σημαίνει ότι το άθροισμα των δεύτερων τιμών θα πρέπει να ελαχιστοποιείται.

Θα επιχειρήσουμε να εφαρμόσουμε τα παραπάνω με ένα συγκεκριμένο παράδειγμα που αναπαρίσταται στο Σχ. 5.2 όπου ο ρόλος V από την περιοχή B επιχειρεί να προσπελάσει πόρους που αντιστοιχούν στο ρόλο T2 από την περιοχή A. Παρατηρούμε ότι υπάρχει μία απευθείας αντιστοίχηση από το ρόλο u στο ρόλο q.

Ο υπολογισμός του βάρους με βάση το συνολικό κόστος για το μονοπάτι από το ρόλο V στο ρόλο U λειτουργεί ως εξής: [c_{vu}: <(2-1),(4+3)>=<1,7>]. Η πρώτη μεταβλητή του c_{vu} υπολογίζεται αφαιρώντας τις διαφορές στην ιεραρχία (θεωρώντας ότι το αποτέλεσμα της διαφοράς είναι πάντα θετικό) που υπολογίζονται από την παράσταση $\sum_{i}^{i,j:neighbours} \sum_{j,i\le j} (x_i - x_j)$, ενώ η δεύτερη τιμή στο βάρος δίνεται από το άθροισμα των κρισιμοτήτων που δίνεται από τν όρο $\{\min[\sum_{i}^{i,j:neighbours} \sum_{j} (y_i + y_j)]\}$ που μετρά το άθροισμα των κρισιμοτήτων (οι οποίες ορίζονται αυθαίρετα), ώστε να αποτρέψουν τους διαχειριστές από το να ενεργοποιήσουν κάποιους κρίσιμους ενδιάμεσους ρόλους. Για τη μετάβαση από το U στο Q έχουμε, [c_{uq} : <2-2, 4+3>= <0,7>]. Τέλος για τη μετάβαση από το Q στο T2: [c_{QT2}=<3-2,1+4>=<1,5>]. Στο παράδειγμά μας, έχουμε εντοπίσει το (μοναδικό) νόμιμο μονοπάτι. Στην περίπτωση που έχουμε πολλαπλές αντιστοιχίσεις και πολλαπλά δυνατά μονοπάτια μπορούμε να διαλέξουμε ένα που ελαχιστοποιεί το άθροισμα των κρισιμοτήτων.

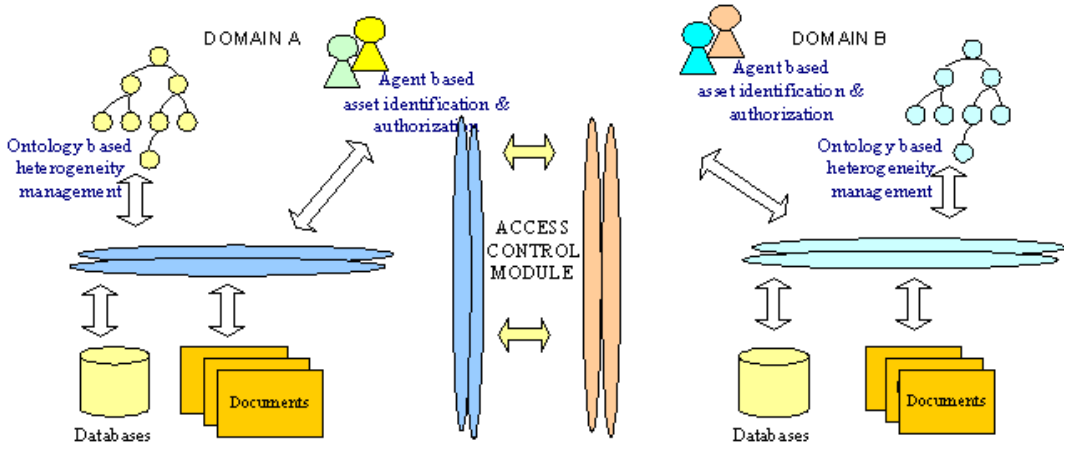
Αντί της παραμέτρου της κρισιμότητας που προαναφέρθηκε θα μπορούσαμε εναλλακτικά να παρακολουθήσουμε τη συμπεριφορά άλλων παραμέτρων. Επίσης θα πρέπει να σημειωθεί ότι θα μπορούσε η παραπάνω τεχνική να χρησιμοποιηθεί σαν εργαλείο υποστήριξης του διαχειριστή του συστήματος ο οποίος και θα παίρνει τις αποφάσεις σε αμφισβητούμενες περιπτώσεις και να μην επιτρέπουμε την προσπέλαση εκτός αν υπάρχει συγκεκριμένη και σαφής αντιστοίχηση ρόλων.

Το κέρδος που έχουμε χρησιμοποιώντας την συγκεκριμένη τεχνική είναι ότι μπορούμε να επιτύχουμε με ένα ευέλικτο και ασφαλή τρόπο την αντιστοίχηση πολιτικών υπακούοντας σε περιορισμούς ιεραρχίας ρόλων, επιτυγχάνοντας μια ασφαλή και κλιμακούμενη λύση στο πρόβλημα της διαλειτουργικότητας.

5.5 Γενική αρχιτεκτονική συστήματος

Προκειμένου για την πρακτική εφαρμογή των αρχών που περιγράφηκαν στα προηγούμενα και στο παρόν κεφάλαια, στα πλαίσια των εργασιών (Belsis et al, 2005f) (Belsis et al, 2004b) (Belsis et al, 2005e) περιγράφονται οι λεπτομέρειες μίας αρχιτεκτονικής γενικού σκοπού που υλοποιεί συγκεκριμένες λειτουργίες ενός κατανεμημένου συστήματος διαχείρισης γνώσης. Τμήματα των αντίστοιχων λειτουργιών έχουν αναπτυχθεί σε ανεξάρτητες ενότητες λογισμικού, λεπτομέρειες των οποίων έχουν περιγραφεί στις προαναφερθείσες εργασίες. Στις επόμενες ενότητες θα περιγραφεί μία γενικότερη αρχιτεκτονική, καθώς και μία σειρά από μελέτες περίπτωσης που αφορούν σε αναγκαίες τροποποιήσεις προκειμένου για την εφαρμογή των παραπάνω σε συστήματα με ειδικά χαρακτηριστικά και τα οποία μελετώνται κατά περίπτωση στο τέλος του κεφαλαίου, συνοψίζοντας τα συμπεράσματα των εργασιών (Belsis et al, 2005g) (Belsis et al, 2005d)(Malatras et al, 2005b) .

Οι δομικές μονάδες της αρχιτεκτονικής του κατανεμημένου συστήματος διαμοιρασμού πόρων γενικού σκοπού, είναι οι ακόλουθες (εικ. 5.3):



Εικ. 5.3 Γενική επισκόπηση της προτεινόμενης αρχιτεκτονικής

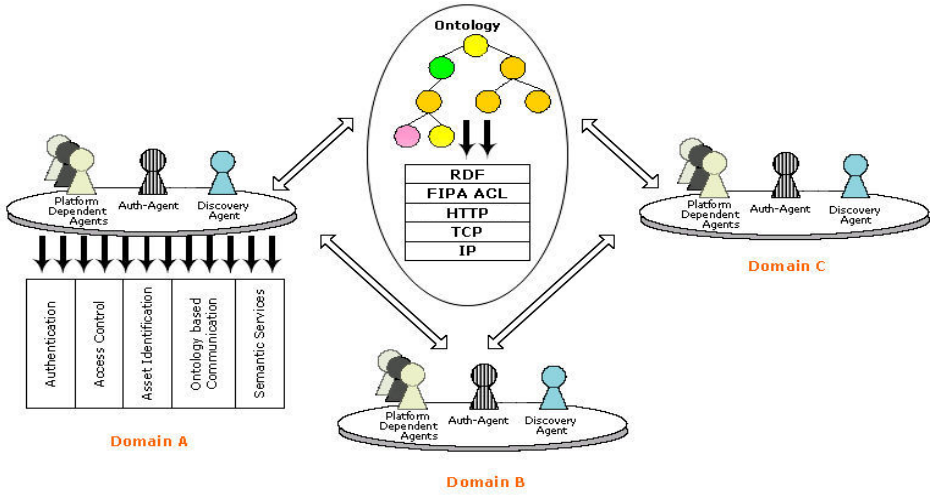
- Το σύστημα διαχείρισης εγγράφων, με έμφαση στην κατηγοριοποίησή τους σε διαφορετικές κατηγορίες σύμφωνα με τις τεχνικές που περιγράφηκαν στο κεφάλαιο 3. Οι κατηγορίες (κλάσεις) στις οποίες κατατάσσονται τα έγγραφα εξαρτώνται και από το δείγμα που παρέχουν οι χρήστες. Παράλληλα, μέσω ανεξάρτητης συνιστώσας, υποστηρίζεται η δυνατότητα διαχείρισης εικόνων και κειμένου μέσω ειδικής εφαρμογής που λειτουργεί σαν οργανωσιακή μνήμη ενός οργανισμού και έχει τη δυνατότητα αποθήκευσης ετερογενών στοιχείων καθώς επίσης και μετα-δεδομένων που τα περιγράφουν (Belsis et al, 2005e)(Belsis et al, 2005f). Η οργανωσιακή μνήμη (Belsis et al, 2005e), έχει τη δυνατότητα αποθήκευσης ημι-δομημένων κειμένων, τα οποία αφορούν σε

διαφορετικές θεματικές κατηγορίες και τα οποία εισάγονται κατόπιν κρίσης από ειδικούς. Στις επιλογές των χρηστών υπάρχει η δυνατότητα αναζήτησης κειμένου βάσει θέματος, ενώ μπορούν να αναζητηθούν και πληροφορίες από τους ειδικούς του οργανισμού ανάλογα με τους τομείς εξειδίκευσης τους. Επίσης ο χρήστης μπορεί να αναζητήσει περισσότερες πληροφορίες στην κατηγορία ενός κειμένου που τον ενδιαφέρει, ή μπορεί να αναζητήσει τους κριτές του κειμένου και να βρει σχετικές πληροφορίες ερχόμενος σε άμεση επικοινωνία μαζί τους αξιοποιώντας τις δυνατότητες της πλατφόρμας (Belsis et al, 2004b) (Belsis et al, 2004a) ή μπορεί να αναζητήσει άλλα κείμενα των ίδιων συγγραφέων. Η πλατφόρμα επίσης έχει τη δυνατότητα χειρισμού εκτός από κείμενα και συνοδευτικού πολυμεσικού υλικού, όπως για παράδειγμα εικόνων, οι οποίες μπορούν να αντιστοιχούνται σε συγκεκριμένο κείμενο. Η υλοποίηση της συγκεκριμένης εφαρμογής έχει γίνει σε Java και Oracle 9ι. Προκειμένου για την επιτυχή διαχείριση των ετερογενών πόρων, διατηρείται ένα σύνολο από μετα-δεδομένα που βοηθούν στην ενιαία διαχείριση των διαφορετικής φύσεως πόρων. Παράλληλα, υπάρχει η δυνατότητα ανάπτυξης της συγκεκριμένης αρχιτεκτονικής σε κατανεμημένη μορφή, με την εγκατάσταση του λογισμικού σε διαφορετικές δικτυακές περιοχές που συνεργάζονται μεταξύ τους, ενώ παράλληλα κάθε μία διατηρεί την αυτονομία της.

- Το σύστημα επιβολής ελέγχων πρόσβασης που είναι υπεύθυνο για την εφαρμογή των πολιτικών ασφάλειας. Αποτελείται από τα PDP, PEP και το χειριστή πλαισίου (Context Manager). Παράλληλα, στο PDP έχει ενσωματωθεί το μητρώο διαχείρισης συνασπισμού (coalition management registry) που είναι υπεύθυνο για την τήρηση των αντιστοιχήσεων μεταξύ των διαφορετικών περιοχών.

- Το σύστημα διαχείρισης οντολογιών που επιτρέπει την κατηγοριοποίηση των πόρων κάθε περιοχής σε διαφορετικές θεματικές περιοχές, επιτρέποντας κατ' αυτόν τον τρόπο την καταπολέμηση της ετερογένειας. Επιπλέον με τη χρήση οντολογιών, καθίσταται εφικτή η θέσπιση κοινά αποδεκτής ορολογίας για την επικοινωνία μεταξύ πρακτόρων λογισμικού. Έτσι σε κάθε περιοχή μπορεί να αντιστοιχιστεί (Belsis et al, 2005f) ένα ζεύγος πρακτόρων εκ των οποίων ένας πράκτορας αναλαμβάνει την αναζήτηση πόρων (Search Agent/ S-Agent) και ένας την αυθεντικοποίηση των χρηστών (Authorization agent/ A-agent). Ο τελευταίος, αναλαμβάνει την επικοινωνία με το PDP για λογαριασμό του χρήστη. Ο S- Agent φροντίζει για τον εντοπισμό πόρων σε διαφορετικές περιοχές ενώ ο A-Agent φροντίζει να παρέχει με διαφανή τρόπο στο χρήστη εξουσιοδότηση μεταφέροντας για λογαριασμό του τα πιστοποιητικά. Η παρουσία των πρακτόρων αποσκοπεί στο να γίνεται η διαδικασία αναζήτησης όρων και η εξουσιοδότηση του χρήστη με διαφανή τρόπο. Τα μηνύματα που ανταλλάσσονται μεταξύ των πρακτόρων ακολουθούν τα πρωτόκολλα FIPA (FIPA, 2005) ενώ οι οντολογίες σε RDF αξιοποιούνται για την επίλυση των προβλημάτων ετερογένειας. Στο σχήμα 5.4 απεικονίζεται η γενικότερη αρχιτεκτονική μαζί με τους πράκτορες που για κάθε περιοχή αναλαμβάνουν την αναζήτηση πόρων και την αυθεντικοποίηση των χρηστών όπως επίσης και οι πράκτορες που είναι εγγενείς στη χρησιμοποιούμενη πλατφόρμα JADE και αναλαμβάνουν διεργασίες όπως

η αναζήτηση των διευθύνσεων άλλων πρακτόρων και άλλες λειτουργίες που σχετίζονται με την επικοινωνία και το συντονισμό άλλων πρακτόρων.



Εικόνα 5.4 Αρχιτεκτονική συστήματος βασισμένη σε πράκτορες.

5.5.1 Εφαρμογή σε περιβάλλοντα διεισδυτικού υπολογίζειν (pervasive environments)

Τα περιβάλλοντα διεισδυτικού υπολογίζειν (ή ευρύτερα γνωστά ως pervasive environments) υλοποιούνται πάνω από ασύρματα δίκτυα ειδικού σκοπού (mobile ad-hoc networks - MANETs), τα οποία διακρίνονται από την αστάθεια των κόμβων που τα αποτελούν λόγω της κινητικότητας τους, καθώς και από την περιορισμένη αυτονομία και υπολογιστική ισχύ των συσκευών που τα απαρτίζουν. Η παρούσα παράγραφο βασίζονται στις εργασίες (Belsis et al, 2005g) (Belsis et al, 2005d) και αφορούν κυρίως σε ζητήματα ασφάλειας και αρχιτεκτονικής προκειμένου για την αξιοποίηση των παραπάνω περιβαλλόντων σε ιατρικά ασύρματα διασυνδεδεμένα περιβάλλοντα, όπως για παράδειγμα διασυνδεδεμένες ιατρικές κλινικές. Ένα από τα κύρια κίνητρα για την εφαρμογή των παραπάνω τεχνολογιών προκειμένου για τη διασύνδεση ιατρικών κλινικών είναι η ικανότητα αναζήτησης της πληροφορίας από το γιατρό όταν βρίσκεται κοντά στο χώρο του ασθενή και με πολύ γρήγορους χρόνους απόκρισης (Choudhri et al, 2003). Η ιδιαιτερότητα των παραπάνω περιβαλλόντων έγκειται στην κρισιμότητα και στον ευαίσθητο χαρακτήρα των προσωπικών ιατρικών δεδομένων, που επιβάλλουν τη λήψη μίας σειράς από μέτρα προκειμένου για τη διαφύλαξη του ιατρικού απορρήτου.

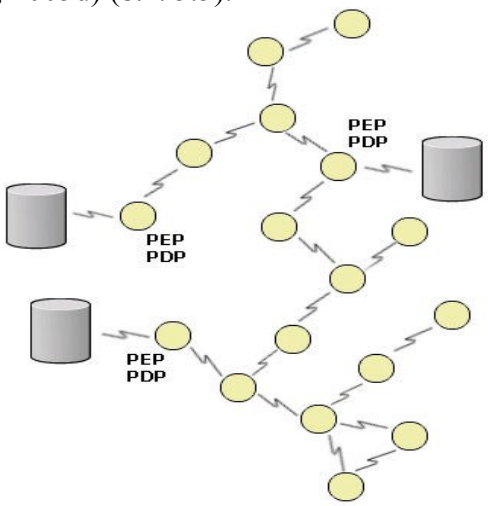
5.5.1.1 Διαφύλαξη εμπιστευτικότητας

Οι περισσότερες από τις φορητές συσκευές σήμερα υποστηρίζουν την αυθεντικοποίηση των χρηστών με χρήση κρυπτογραφίας δημόσιου κλειδιού (PKI - Public Key Infrastructure). Η αυθεντικοποίηση χρηστών σε επίπεδο συσκευής επιτυγχάνεται με την εισαγωγή ενός προσδιοριστικού ταυτότητας (PIN identifier), ενώ το ιδιωτικό κλειδί που επιτρέπει την αντιστοίχηση του χρήστη με τον κάτοχο του ιδιωτικού κλειδιού και νόμιμο χρήστη της συσκευής μπορεί να φυλάσσεται σε ένα ασφαλές αφαιρούμενο μέσο όπως για παράδειγμα σε μία έξυπνη κάρτα (smart card). Αν και η υπολογιστική ισχύς αποτελεί ένα περιορισμό για τις περισσότερες φορητές

συσκευές, οι περισσότεροι κατασκευαστές υποστηρίζουν την χρήση συμμετρικής κρυπτογραφίας μεγέθους κλειδιού 128-bit για την κρυπτογράφηση όλων των δεδομένων που ανταλλάσσονται καθώς και επίσης τη χρήση ψηφιακών πιστοποιητικών προκειμένου για την αυθεντικοποίηση των οντοτήτων που θα επικοινωνήσουν μεταξύ τους.

5.5.1.2 Αποθήκευση πολιτικών

Διαφορετικές προτάσεις έχουν γίνει τελευταία σε σχέση με την αποθήκευση αλλά και επιβολή πολιτικών όταν γίνεται χρήση φορητών συσκευών. Σύμφωνα με τους (Jansen et al, 2002) οι πολιτικές μπορούν να φυλάσσονται σε μία έξυπνη κάρτα ενώ η συσκευή να επιτηρεί διαρκώς αν η κάρτα έχει αφαιρεθεί από τη συσκευή ή όχι. Στην προσέγγιση μας δεν απαιτείται όλες οι συσκευές να έχουν αποθηκευμένη την πολιτική ασφάλειας του οργανισμού εφόσον δεν είναι απαραίτητο όλες οι συσκευές να παρέχουν υπηρεσίες. Η πολιτική αποθηκεύεται μόνο στα σημεία αποφάσεων πολιτικής (Policy Decision Points -PDPs) τα οποία ελέγχουν την συμβατότητα ενός αιτήματος για πρόσβαση σε πόρους (ιατρικές εγγραφές) με τα αρχεία καταγραφής της πολιτικής ασφάλειας, τα οποία κρατούνται σε συγκεκριμένα σημεία μόνο και όχι στο σύνολο των συσκευών όπως στην περίπτωση των (Jansen et al, 2002). Έτσι η πολιτική φυλάσσεται μόνο σε συγκεκριμένα σημεία τα οποία φροντίζουν για την επιβολή των ελέγχων πρόσβασης για οποιαδήποτε περίπτωση αιτήματος πρόσβασης σε πόρους (Belsis et al, 2005d) (εικ. 5.5).

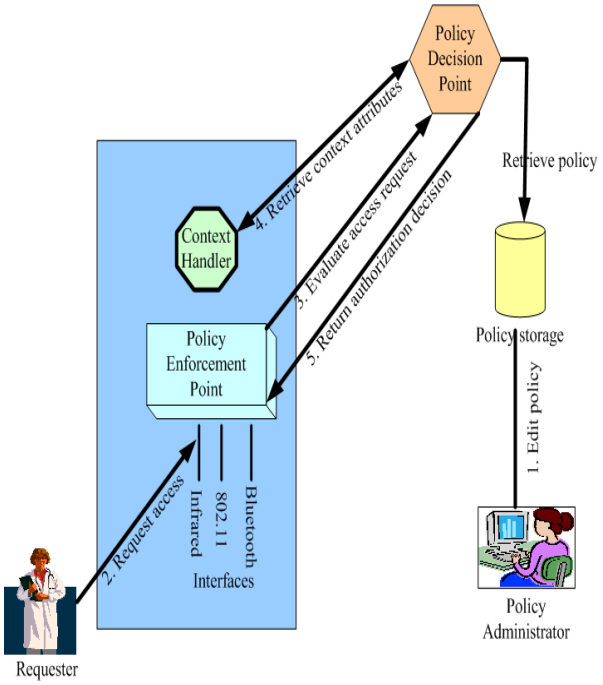


Εικόνα 5.5 Προσαρμογή του συστήματος επιβολής ελέγχων πρόσβασης σε περιβάλλοντα μειωμένων υπολογιστικών πόρων

5.5.1.3 Δικτυακή τοπολογία

Η μεταφορά του σεναρίου συνεργασίας ιατρικών συστημάτων σε ασύρματα περιβάλλοντα, εισάγει μία σειρά από προκλήσεις. Τα pervasive περιβάλλοντα χαρακτηρίζονται από μεγάλο αριθμό χρηστών γεγονός που δυσχεραίνει τη διαχείριση της ασφάλειας. Ορισμένες προσεγγίσεις κάνουν χρήση των βασισμένων στην εμπιστοσύνη μοντέλων (Choudhri et al, 2003). Στην περίπτωσή μας επιχειρείται η παροχή υπηρεσιών όχι σε όλους τους χρήστες τους δικτύου, αλλά μόνο σε όσους εμπλέκονται ενεργά στην διαδικασία περίθαλψης και για τους οποίους είναι αναγκαία η πρόσβαση σε ιατρική πληροφορία.

Σενάρια χρήσης του συστήματος

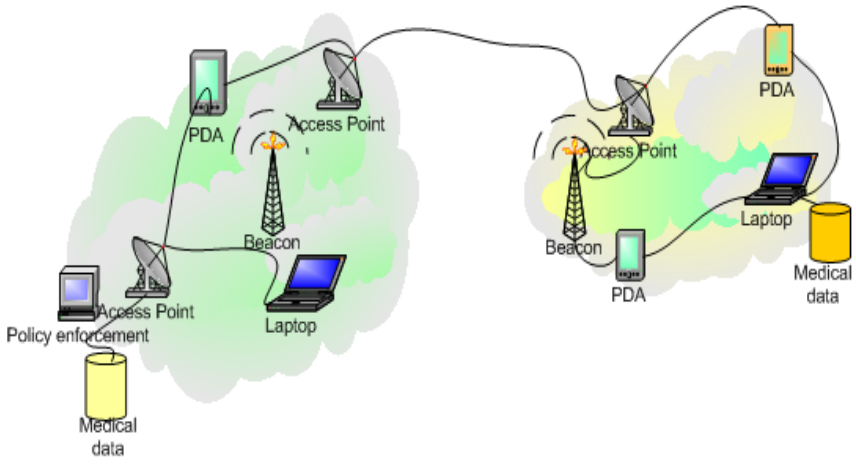


Εικόνα 5.6 Σενάριο εξουσιοδότησης σε ασύρματα διασυνδεδεμένο περιβάλλον.

Ας θεωρήσουμε το ακόλουθο σενάριο χρήσης: Ένας γιατρός που ανήκει στον τομέα Α ενός νοσοκομείου, επιθυμεί πρόσβαση σε αρχεία που αφορούν σε αιματολογικά δεδομένα κάποιου ασθενούς που νοσηλεύεται στη μονάδα εντατικής θεραπείας και δεν είναι σε θέση να δώσει ο ίδιος οποιαδήποτε πληροφορία.

Προκειμένου να αποκτήσει άμεση πρόσβαση στα δεδομένα μέσω μίας φορητής συσκευής (ψηφιακού βοηθού – PDA) ο γιατρός υποβάλλει το ερώτημα δίνοντας τα στοιχεία του ασθενούς σε κατάλληλο πεδίο και επιλέγοντας από τις διαθέσιμες κατηγορίες στις οποίες έχουν κατηγοριοποιηθεί θεματικά τα δεδομένα. Η αίτηση υποβάλλεται στο αντίστοιχο PDP του τομέα που καταχωρούνται τα αιματολογικά δεδομένα, και παράλληλα υποβάλλονται από τη φορητή συσκευή του γιατρού τα πιστοποιητικά με την οποία το PDP θα κάνει την αυθεντικοποίηση και θα επιβάλλει τον έλεγχο πρόσβασης βάσει των κανόνων της πολιτικής. Στην περίπτωση που ο γιατρός δεν ανήκει στο αιματολογικό τμήμα, θα αναζητηθεί η αντίστοιχη εγγραφή που επιτρέπει την αντιστοίχηση του γιατρού του τομέα Α με αντίστοιχο ρόλο του αιματολογικού τμήματος. Η επικοινωνία κρυπτογραφείται με τεχνικές που θα αναφερθούν εκτενέστερα στην επόμενη παράγραφο, ενώ και σε φορητές συσκευές υπάρχει η δυνατότητα να έχουμε μήκος χρησιμοποιούμενου κλειδιού 128-bit.

Η αναγνώριση του αν η συσκευή βρίσκεται στον τομέα που ανήκει ο συγκεκριμένος ρόλος στον οποίο ανήκουν τα πιστοποιητικά που φυλάσσονται στην κάρτα ή όχι, γίνεται μέσω της χρήσης ενός ραδιοφάρου (beacon) (εικ. 5.6) που εκπέμπει σε ορισμένη συχνότητα, ενώ στην έξυπνη κάρτα φυλάσσονται μία σειρά από μηνύματα τα οποία αντιστοιχούν στην παραπάνω ή στις παραπάνω συχνότητες και τα οποία αναγνωρίζει η συσκευή. Έτσι για όσο διάστημα η συσκευή βρίσκεται στον τομέα της το PDP αναζητά στην τοπική του πολιτική αν πρέπει να επιτραπεί η πρόσβαση σε αιτούμενους πόρους, αλλιώς ενεργοποιείται πρώτα η διαδικασία αναζήτησης αντίστοιχων ρόλων (στο μητρώο διαχείρισης συνασπισμού) από απομακρυσμένα συνεργαζόμενα συστήματα.



Εικόνα 5.6 Ασύρματα διασυνδεδεμένα περιβάλλοντα. Η παρουσία του ραδιοφάρου σε κάθε περιοχή σηματοδοτεί για μία συσκευή αν βρίσκεται στην περιοχή που υπάγεται και ο χρήστης-κάτοχος για τη διευκόλυνση της διαδικασίας εξουσιοδότησης

5.5.2 Ζητήματα διαλειτουργικότητας για διασυνδεδεμένα ιατρικά συνεργαζόμενα συστήματα

Στα πλαίσια της εργασίας (Gritzalis et al, 2006) περιγράφεται μία υποδομή που επιτρέπει τη διασύνδεση ιατρικών περιοχών καθώς και την ανταλλαγή μεταξύ τους σε ηλεκτρονική μορφή ιατρικών αρχείων. Προκειμένου η όλη υποδομή να διαθέτει χαρακτηριστικά διαλειτουργικότητας, θα πρέπει στην ανάπτυξη της αρχιτεκτονικής να αξιοποιηθούν μία σειρά από πρότυπες τεχνικές και τεχνολογίες. Έτσι, τα ανταλλασσόμενα μηνύματα θα πρέπει να υποβάλλονται σε μία μορφή αναγνωρίσιμη και κατανοητή από όλα τα συμμετέχοντα μέρη. Το HL7 είναι ένα διεθνές πρότυπο που αποσκοπεί στο να διευκολύνει την επικοινωνία μεταξύ διαφορετικών πλατφορμών. Έτσι η επικοινωνία μέσω HL7 επιτυγχάνεται μέσα από συντακτικά αλλά και σημασιολογικά προτυποποιημένα μηνύματα. Η ανταλλαγή τύπου HL7 μηνυμάτων μπορεί να επιτευχθεί μέσα από χαμηλού κόστους διαύλους επικοινωνίας όπως για παράδειγμα το διαδίκτυο. Η χρήση ωστόσο αυτών των τεχνικών εισάγει μία σειρά από κινδύνους, όπως:

- Έκθεση των δεδομένων του χρήστη σε μη εξουσιοδοτημένη αποκάλυψη
- Δυνητική τροποποίηση του μηνύματος, γεγονός που διακυβεύει την εγκυρότητα του τελικού μηνύματος.
- Μη αποποίηση της λήψης των μηνυμάτων, γεγονός που επιτρέπει σε ένα από τα συμμετέχοντα μέρη να αρνηθούν την παραλαβή ενός συγκεκριμένου μηνύματος

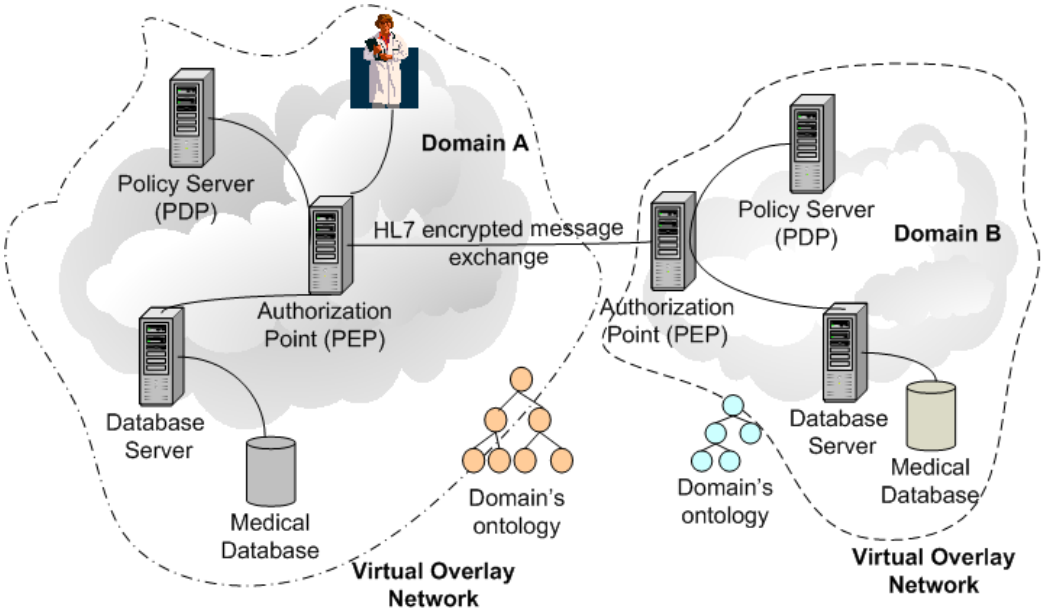
Προκειμένου για την αντιμετώπιση των παραπάνω κινδύνων, μπορούν να χρησιμοποιηθούν υπάρχουσες κρυπτογραφικές τεχνικές, οι οποίες είναι αρκετά αξιόπιστες ώστε να παρέχουν υπηρεσίες ασφάλειας υψηλού επιπέδου. Υπάρχουν ήδη αρκετά πρότυπα ικανά να παρέχουν τεχνικές ικανές να διαφυλάξουν την ακεραιότητα, εμπιστευτικότητα και μη-αποποίηση των αποστελλόμενων μηνυμάτων. Τεχνικές συμμετρικής κρυπτογράφησης βασισμένες σε ένα κλειδί κοινό για τα δύο μέρη, παρέχουν λύσεις στο θέμα της εμπιστευτικότητας, μόνο που προϋποθέτει ότι οι δύο πλευρές που μοιράζονται το κοινό κλειδί εμπιστεύονται η μία την άλλη. Στα μειονεκτήματα της μεθόδου μπορούμε να παρατηρήσουμε ότι δεν υπάρχει τρόπος να επαληθευτεί ποιος ήταν ο αποστολέας του μηνύματος μεταξύ αυτών που μοιράζονται το κοινό κλειδί. Παράλληλα, μια και πολλά μέρη μοιράζονται το ίδιο κλειδί, η

μυστικότητα του κλειδιού δεν μπορεί να διαφυλαχτεί για μεγάλες περιόδους. Εάν ένα από τα συμμετέχοντα μέρη δεν μπορέσει να διαφυλάξει την ασφάλεια του κλειδιού, τότε η ασφάλεια διακυβεύεται για το σύνολο των μερών. Συνεπώς ένα από τα προβλήματα είναι η διαφύλαξη της μυστικότητας του κλειδιού για μεγάλο διάστημα, ενώ απαιτείται επίσης η ύπαρξη ενός ασφαλούς διαύλου επικοινωνίας προκειμένου για την ανταλλαγή του κλειδιού μεταξύ των συμμετεχόντων μερών.
Εξαιτίας αυτών των προβλημάτων στη χρήση συμμετρικής κρυπτογράφησης, κατά κανόνα αξιοποιείται η ασύμμετρη κρυπτογραφία για την κρυπτογράφηση μηνυμάτων HL7. Η ασύμμετρη κρυπτογραφία λειτουργεί στη βάση της αντιστοίχησης μίας οντότητας σε ένα ζεύγος κλειδιών, με μονοσήμαντο τρόπο. Μέσω της κοινοποίησης του δημόσιου κλειδιού στους πάντες και της χρήσης του ιδιωτικού κλειδιού μόνο από τον ιδιοκτήτη του, η κρυπτογραφία δημόσιου κλειδιού παρέχει τις ακόλουθες υπηρεσίες:

- Εμπιστευτικότητα: Τα δεδομένα μπορούν να σταλούν στον αποστολέα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα. Έτσι καθίσταται ικανός μόνο ο παραλήπτης πλέον να διαβάσει το μήνυμα. Ούτε ο αποστολέας δεν μπορεί να διαβάσει το κρυπτογραφημένο πλέον μήνυμα
- Αυθεντικοποίηση: Η προέλευση των δεδομένων μπορεί εύκολα να επαληθευτεί από οποιονδήποτε χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα.
- Μη αποποίηση της λήψης του μηνύματος: Σαν συνέπεια της αυθεντικοποίησης ο αποστολέας δεν μπορεί να αρνηθεί την αποστολή του μηνύματος καθώς κανείς άλλος δεν θα μπορούσε να χρησιμοποιήσει το ιδιωτικό του κλειδί.

Τα HL7 μηνύματα σε συνδυασμό με τη χρήση τεχνικών ασύμμετρης κρυπτογραφίας είναι ιδανικά για τη διατήρηση της εμπιστευτικότητας, ακεραιότητας και την μη-αποποίηση λήψης του μηνύματος, καθώς κάθε επικοινωνία σε HL-7 αποτελείται από δύο μηνύματα: ένα μήνυμα αιτήματος και ένα απάντησης. Το μήνυμα απάντησης είναι συνήθως ένα μήνυμα επιβεβαίωσης (αλλά μπορεί να είναι και οποιοδήποτε άλλο μήνυμα αυτής της μορφής).
Βασισμένες στην εμπειρία διαφορετικών ευρωπαϊκών ερευνητικών έργων (Blobel, 2004) (Ruotsalainen, 2004) οι περισσότερες κατανεμημένες ιατρικού χαρακτήρα αρχιτεκτονικές χρησιμοποιούν ισχυρούς κρυπτογραφικούς αλγορίθμους, έξυπνες κάρτες ενώ βασίζονται σε Έμπιστες Τρίτες Οντότητες-ETT (Trusted Third Party - TTP) για την επαλήθευση των ψηφιακών υπογραφών που όλων των χρηστών. Η χρήση επίσης ειδικού υλικού (hardware) διευκολύνει τη φύλαξη των υπογραφών, ελαχιστοποιώντας έτσι τυχόν αδυναμίες στην διαδικασία φύλαξης των υπογραφών.
Η ασφαλής μεταφορά αρχείων πάνω από δίκτυα επιτυγχάνεται με τη χρήση του πρωτοκόλλου ασφαλούς μεταφοράς (secure file transfer protocol - SFTP) που έχει γίνει αποδεκτό σαν ένα από τα HL7/ANSI πρότυπα. Το SFTP επίσης μπορεί να χρησιμοποιηθεί για την αποστολή εικόνων. Επιπλέον, για την υλοποίηση του HL7 και την κωδικοποίηση δεδομένων χρησιμοποιείται η XML που θεωρείται ως de-facto πρότυπο κωδικοποίησης δεδομένων και χρήσης στο διαδίκτυο.
Η εικόνα 5.7 παρουσιάζει την αρχιτεκτονική ενός συστήματος που υλοποιεί τις παραπάνω απαιτήσεις και που επιτρέπει την ανταλλαγή μηνυμάτων τύπου HL7 μεταξύ διαφορετικών συστημάτων (Gritzalis et al, 2006). Ένα παράδειγμα σεναρίου χρήσης ανάλογου συστήματος είναι το ακόλουθο: Έστω ότι ένας γιατρός από τον τομέα Α ζητά κάποια ιατρικά αρχεία. Το αίτημά του απευθύνεται στο σημείο επιβολής πολιτικής του τομέα του (PEP). Το PEP δημιουργεί κατάλληλο μήνυμα στον εξυπηρετητή στον οποίο λειτουργεί το σημείο επιβολής πολιτικής. Ανάλογα με

τα πιστοποιητικά που υπέβαλλε ο χρήστης, ελέγχεται αν υπάρχει δικαίωμα πρόσβασης στους αιτούμενους πόρους και ανάλογα αξιολογείται το αίτημα με βάση την υπάρχουσα πολιτική. Στην περίπτωση που ο γιατρός αιτείται πόρους που αντιστοιχούν σε διαφορετική περιοχή, τότε αναζητείται η κατάλληλη αντιστοίχηση και κατόπιν του ανατίθεται ένας ρόλος από τους αντίστοιχους στο απομακρυσμένο σύστημα (αν υπάρχει). Υπεύθυνα για τη λειτουργία αντιστοίχησης είναι τα δύο PDP των περιοχών. Το PDP του τομέα Α δημιουργεί ένα κατάλληλο μήνυμα, στο οποίο περιγράφονται οι αιτούμενοι πόροι, ο ρόλος που αντιστοιχεί στον απομακρυσμένο τομέα ανάλογα με το τι έχει καταγραφεί στο μητρώο διαχείρισης συνασπισμού και στο μήνυμα επισυνάπτεται η ψηφιακή υπογραφή προκειμένου με το κλειδί του αποστολέα (το κλειδί που αντιστοιχεί στην περιοχή Α, αν το σύστημα λειτουργεί με ένα κλειδί για την κρυπτογράφηση όλων των μηνυμάτων των χρηστών του για ευκολία, αλλιώς με το κλειδί του κάθε χρήστη που αιτείται τους πόρους). Το PDP της περιοχής Β χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για να επαληθεύσει την αυθεντικότητα του μηνύματος και τον πραγματικό αποστολέα, ενώ στη συνέχεια χρησιμοποιώντας το ιδιωτικό του κλειδί αποκρυπτογραφεί το μήνυμα. Στη συνέχεια συμβουλεύεται τον εξυπηρετητή που είναι υπεύθυνος για τη φύλαξη της πολιτικής και ελέγχεται αν πρέπει να εξουσιοδοτηθεί το αίτημα. Στη συνέχεια, ο εξυπηρετητής της περιοχής Β δημιουργεί ένα κλειδί που θα χρησιμοποιηθεί για μία σύνοδο, προκειμένου να μεταδοθούν τα δεδομένα κρυπτογραφημένα με αυτό το κλειδί. Στην πράξη δηλαδή το κλειδί μίας συνόδου αποστέλλεται με τεχνικές ασύμμετρης κρυπτογραφίας και χρησιμοποιείται για την κρυπτογράφηση δεδομένων λόγω του ότι οι τεχνικές συμμετρικής κρυπτογραφίας είναι πιο γρήγορες και απαιτούν λιγότερους υπολογιστικούς πόρους. Το κλειδί της συνόδου κρυπτογραφείται με το ιδιωτικό κλειδί του Β και με το δημόσιο κλειδί του Α και αποστέλλεται σε ένα HL7 συμβατό μήνυμα. Ο εξυπηρετητής της περιοχής Α, χρησιμοποιεί το δημόσιο κλειδί του Β για να επαληθεύσει την προέλευση του μηνύματος και με το ιδιωτικό του κλειδί αποκρυπτογραφεί το κλειδί συνόδου. Με αυτό το κλειδί αποστέλλει την τύπου HL7 απάντηση στον Α. Στη συνέχεια πλέον με χρήση πρωτοκόλλου SSL κρυπτογραφούνται τα μηνύματα μεταξύ των περιοχών Α και Β.



Εικόνα 5.7 Διασυνδεδεμένα ιατρικά περιβάλλοντα

5.6 Συμπεράσματα

Στο παρόν κεφάλαιο, αναπτύχθηκε μία τεχνική ημι-αυτοματοποιημένης διαχείρισης του συστήματος επιβολής ελέγχων πρόσβασης σε περιβάλλοντα πολλαπλών πολιτικών, με χρήση ενός φορμαλισμού που βασισμένου στην άλγεβρα ημιδακτυλίων και με χρήση προγραμματισμού με περιορισμούς, όπως περιγράφηκε στις εργασίες (Belsis et al, 2006b) (Belsis 2006e).

Παράλληλα, στο δεύτερο μέρος του κεφαλαίου, αναπτύχθηκαν τα χαρακτηριστικά μιας αρχιτεκτονικής που αξιοποιεί τα συμπεράσματα των εργασιών (Belsis et al, 2005f)(Belsis et al, 2004c) (Belsis et al, 2005e). Παράλληλα, μελετήθηκαν διαφορετικές παραλλαγές της συγκεκριμένης αρχιτεκτονικής προκειμένου να προσαρμοστεί σε περιβάλλοντα με ειδικές απαιτήσεις, όπως για παράδειγμα ασύρματα διασυνδεδεμένα περιβάλλοντα (με χρήση συσκευών με περιορισμένους υπολογιστικούς πόρους) και ιατρικά διασυνδεδεμένα περιβάλλοντα. Τα χαρακτηριστικά των μελετών περίπτωσης που παρουσιάστηκαν έχουν καταγραφεί στις εργασίες (Belsis et al, 2005d) (Belsis et al, 2005g)(Gritzalis et al, 2006)(Malatras et al, 2005b).

Η προτεινόμενη λύση μεταξύ άλλων, διαθέτει τα εξής χαρακτηριστικά:

- Ικανότητα κλιμάκωσης, εφόσον ο τρόπος με τον οποίο καθορίζονται οι αντιστοιχίσεις ρόλων επιτρέπει στο σύστημα να μεγαλώνει χωρίς μεγάλο κόστος και χωρίς να αυξάνει την πολυπλοκότητά του.
- Ανθεκτικότητα (robustness), εφόσον η λύση που προτείνεται χαρακτηρίζεται από την απλότητα αλά ταυτόχρονα και την αποτελεσματικότητά της. Παράλληλα, επιτυγχάνεται η διατήρηση των ιδιοτήτων της ασφάλειας και της αυτονομίας για τις διαφορετικές περιοχές.
- Ευελιξία, καθώς δεν υπάρχει ανάγκη για τη διαρκή παρακολούθηση και τροποποίηση του συστήματος, μέσω του μηχανισμού βελτιστοποίησης της λειτουργίας του και της ελάττωσης του απαιτούμενου διαχειριστικού φόρτου.

ΚΕΦΑΛΑΙΟ 6 - Εφαρμογές τεχνικών μερικής ικανοποίησης περιορισμών και ασαφούς λογικής για την υποστήριξη δημιουργίας συνασπισμών Π.Σ.

6.1. Εισαγωγή

Στην προηγούμενη ενότητα περιγράφηκε η χρήση τεχνικών ικανοποίησης χαλαρών περιορισμών (soft constraints) προκειμένου για την επίτευξη μίας τεχνικής ημι-αυτοματοποιημένης διαχείρισης της ασφάλειας ενός συνασπισμού συστημάτων. Οι τεχνικές ικανοποίησης περιορισμών βρίσκουν πολλαπλές εφαρμογές σε προβλήματα τεχνητής νοημοσύνης, στην επίλυση προβλημάτων χρονοπρογραμματισμού, μηχανικής όρασης (Freuder et al, 1992), ενώ τελευταία κερδίζουν διαρκώς έδαφος οι εφαρμογές τους σε προβλήματα ασφάλειας (Bistarelli, 2004)(Barker et al, 2003)(Ahn et al, 2000).

Οι περιορισμοί αποτελούν σημαντική πτυχή του RBAC, που συγκεντρώνουν ιδιαίτερο ενδιαφέρον λόγω της ικανότητας μέσω αυτών να περιγράψουμε πληθώρα προβλημάτων ελέγχου πρόσβασης. Η αναπαράσταση και επίλυση προβλημάτων ασφάλειας σε περιβάλλοντα πολλαπλών πολιτικών με συνδυασμένη χρήση περιορισμών και ασαφούς λογικής, αποτελεί μία καινοτομία που προτείνεται στα πλαίσια της παρούσας διατριβής. Στις επόμενες παραγράφους θα περιγραφεί η χρησιμότητα των τεχνικών μερικής ικανοποίησης περιορισμών καθώς και της θεωρίας ασαφών περιορισμών στην αναπαράσταση προβλημάτων ασφάλειας.

Στα πλαίσια του παρόντος κεφαλαίου η συνεισφορά της διατριβής είναι η ακόλουθη:

Αξιοποιούνται οι τεχνικές μερικής ικανοποίησης περιορισμών για την επίλυση ανταγωνιστικών καταστάσεων σε περιβάλλοντα πολλαπλών πολιτικών. Παρέχεται ένας τρόπος για την ανάνηψη από καταστάσεις αδιεξόδου, στις οποίες ο συνασπισμός Π.Σ. δεν μπορεί να επιτρέψει την ανταλλαγή πόρων λόγω της ύπαρξης υπερβολικού αριθμού περιορισμών.

Εισάγεται ένα πλαίσιο στο οποίο προβλήματα ασφάλειας αναπαρίστανται με χρήση χαλαρών περιορισμών, οι οποίοι στη συνέχεια με τη συνδυασμένη χρήση τεχνικών μερικής ικανοποίησης και ασαφούς λογικής, επιλύονται με κριτήριο το βαθμό ικανοποίησής τους. Ο προαναφερθείς μηχανισμός επίλυσης ανταγωνισμών βασίζεται στη χαλάρωση κάποιων από τους (μη κρίσιμους) περιορισμούς. Παράλληλα με χρήση ασαφούς λογικής παρέχεται ένα πλαίσιο υποστήριξης του συνασπισμού Π.Σ. που επιτρέπει να λαμβάνονται υπόψη οι προτιμήσεις των συμμετεχόντων μερών. Κατ' αυτόν τον τρόπο η διαχείριση της ασφάλειας γίνεται πιο ευέλικτη, ενώ επιτυγχάνουμε την ελάττωση του διαχειριστικού φόρτου. Το παρόν κεφάλαιο στηρίζεται κατά κύριο λόγο στην εργασία (Belsis et al, 2006c).

6.2. Βασικές έννοιες

6.2.1 Ικανοποίηση περιορισμών (Constraint satisfaction)

Σχετικά πρόσφατα εμφανίζεται έντονο ερευνητικό ενδιαφέρον για τις εφαρμογές του προγραμματισμού με χρήση περιορισμών σε προβλήματα ασφάλειας (Ahn et al, 2000) (Barker et al, 2003). Ιδιαίτερο ενδιαφέρον αποκτά η δυνατότητα εφαρμογής των τεχνικών ικανοποίησης περιορισμών σε περιβάλλοντα πολλαπλών πολιτικών. Στην παρούσα ενότητα θα αξιοποιηθούν τεχνικές μερικής ικανοποίησης περιορισμών

σε συνδυασμό με τη χρήση ασαφούς λογικής, προκειμένου για την κωδικοποίηση των προτιμήσεων των συμμετεχόντων μερών σε περιβάλλοντα πολλαπλών πολιτικών.

Ένα πρόβλημα ικανοποίησης περιορισμών (constraint satisfaction problem - CSP) αποτελείται από ένα σύνολο μεταβλητών του προβλήματος, μία περιοχή τιμών που δυνητικά μπορούν να ανατεθούν στις παραπάνω μεταβλητές και από ένα σύνολο περιορισμών που καθορίζουν τους επιτρεπτούς συνδυασμούς ανάθεσης τιμών στις μεταβλητές. Άτυπα, μπορούμε να πούμε ότι ένας περιορισμός είναι ένας συνδυασμός επιτρεπτών τιμών για ένα σύνολο μεταβλητών. Μπορούμε να διακρίνουμε τους περιορισμούς (και τα προβλήματα περιορισμών) σε άκαμπτους (crisp) - ή στην περίπτωση που επιτρέπουν κάποιο βαθμό ευελιξίας ως προς το βαθμό ικανοποίησής τους - σε χαλαρούς περιορισμούς (soft constraints). Στη δεύτερη περίπτωση θα μελετήσουμε τεχνικές μερικής ικανοποίησης (partial constraint satisfaction), όπου υπό προϋποθέσεις μπορούμε να παραβιάζουμε κάποιους περιορισμούς (χαμηλής κρισιμότητας) προκειμένου να επιτευχθεί μία λύση στο πρόβλημα, ειδικά σε περιπτώσεις που υπάρχει πολύ μεγάλος αριθμός περιορισμών. Συναφής με την εισαγωγή τεχνικών μερικής ικανοποίησης περιορισμών είναι και η χρήση ασαφούς λογικής, που επιτρέπει την έκφραση προτιμήσεων σχετικά με την ικανοποίηση συγκεκριμένων περιορισμών στην κλίμακα [0,1], με καταστάσεις που πλησιάζουν το βαθμό 1 να είναι πλήρως αποδεκτές ενώ καταστάσεις που προσεγγίζουν το 0 να θεωρούνται απορριπτέες (κάτι που αποτελεί και βασική αρχή της θεωρίας ασαφών συνόλων.

6.2.2 Αρχές Ασαφούς λογικής (fuzzy logic principles)

Η θεωρία ασαφούς λογικής εισήχθη για να περιγράψει με μαθηματικό τρόπο την ασάφεια που χαρακτηρίζει πλήθος καταστάσεων στην καθημερινή ζωή. Η κύρια ιδέα είναι ότι συχνά μία σειρά από καταστάσεις ικανοποιούνται σε μερικό βαθμό και όχι απόλυτα. Για παράδειγμα το να κατατάξουμε κάποιο άτομο ως 'νέο' είναι σχετικό, αφού τα όρια της νεότητας δεν μπορούν να εκφραστούν με απόλυτο τρόπο. Έτσι, μπορούμε πλέον να εκφράσουμε το βαθμό ικανοποίησης μίας συνθήκης δια μέσου της αντιστοίχησης μίας τιμής από το σύνολο [0,1], με το 1 να αντιστοιχεί στην πλήρη ικανοποίηση της συνθήκης και το 0 να αντιστοιχεί στην πλήρη παραβίασή της.

Σε διακριτά σύνολα, μπορούμε να ορίσουμε μία συνάρτηση μέλους X_A που παίρνει τιμή 1 αν $\chi \in A$ και 0 αν $\chi \notin A$. Η έννοια της συμμετοχής ή όχι σε ένα σύνολο γενικεύεται στα πλαίσια της χρήσης ασαφούς λογικής, όπου η συμμετοχή στο σύνολο παριστάνεται με μία συνάρτηση $U \rightarrow [0,1]$. Δύο χαρακτηριστικές πράξεις επί των ασαφών συνόλων είναι η γενικευμένη 'τομή' και 'ένωση' επί δύο συνόλων, ή στη γλώσσα της ασαφούς λογικής $(A \wedge B)(x)=\inf\{A(x),B(x)\}$ και $(A \vee B)(x)=\sup\{A(x),B(x)\}$, όπου sup (supremum) είναι το ελάχιστο άνω φράγμα του συνόλου και inf (infimum) είναι το μέγιστο κάτω φράγμα του αντίστοιχου συνόλου (Kaburlasos, 2006). Αντίστοιχα το γενικευμένο συμπλήρωμα ορίζεται ως $A'(\chi)=1-A(\chi)$.

Με τον ορισμό μίας σχέσης μερικής διάταξης $\leq$ το σύνολο [0,1] ικανοποιεί τις ιδιότητες ενός δικτυώματος, δηλαδή κάθε υποσύνολό του να έχει ουδέτερο στοιχείο ως προς τις πράξεις $\wedge$ και $\vee$, να ισχύει η επιμεριστική και προσεταιριστική ιδιότητα και επιπλέον κάθε υποσύνολο του να έχει sup (Kaburlasos et al, 2002). Το δικτύωμα $([0,1], \leq)$ έχει ιδιαίτερη σημασία, καθώς τόσο μία σειρά από μοντέλα ασφάλειας αξιοποιούν τις βασικές αρχές της θεωρίας δικτυωμάτων όπως αναφέρθηκε ήδη στο κεφάλαιο 2, αλλά και γιατί επιτρέπουν την εισαγωγή ενός μοντέλου ασαφούς λογικής

για την περιγραφή του βαθμού ικανοποίησης μίας σειράς περιορισμών (προσανατολισμένων σε θέματα ασφάλειας).

6.2.3 Εφαρμογή των περιορισμών στο μοντέλο RBAC

Σε περιβάλλοντα πολλαπλών πολιτικών, είναι συχνό το φαινόμενο της ύπαρξης αντικρουόμενων απαιτήσεων και περιορισμών από τα συμμετέχοντα μέρη. Η ενδεχόμενη χρησιμότητα της ασαφούς λογικής στις παραπάνω περιπτώσεις έχει καταγραφεί αρκετά νωρίς, στις εργασίες της Hosmer (Hosmer, 1992)(Hosmer, 1993). Μια πολιτική μπορεί σύμφωνα με τη Hosmer να θεωρηθεί ως ένα σύνολο περιορισμών από μια αποδεκτή αρχή που διευκολύνει κάποια ομαδική δραστηριότητα. Σε ένα περιβάλλον του πραγματικού κόσμου, η τεκμηριωμένα απόλυτη ασφάλεια αν και επιθυμητή δεν είναι πάντοτε εφικτή. Μία από τις αιτίες είναι ότι η επίτευξη μίας ασφαλούς κατάστασης με ακρίβεια, αναγκαστικά μπορεί να ισχύσει μόνο για περιπτώσεις απλών συστημάτων (Hosmer, 1992).

Η πολυπλοκότητα στον χειρισμό καταστάσεων που αφορούν στη διαχείριση πολλαπλών πολιτικών οδηγεί στην ανάγκη χρήσης μιας λογικής που επιτρέπει τον καθορισμό του βαθμού επίτευξης ασφάλειας με χρήση διαφόρων παραμέτρων, καθώς και τον καθορισμό του βαθμού αβεβαιότητας ή του βαθμού ικανοποίησης των διαφορετικών απαιτήσεων. Μέχρι τώρα, οι περισσότερες εργασίες στο χώρο της διαπραγμάτευσης πολλαπλών πολιτικών στηρίζονται στη χρήση πρώτου βαθμού λογικής (Bonatti et al, 2000)(Bonatti et al, 2002) (Khurana, 2002). Η χρήση του παραπάνω φορμαλισμού ωστόσο παρουσιάζει ιδιαίτερη δυσκολία όσον αφορά τη δυνατότητα υλοποίησης λειτουργικών λύσεων και συστημάτων, κυρίως λόγω της πολυπλοκότητας που χαρακτηρίζει τα περιβάλλοντα πολλαπλών πολιτικών και αναγκαστικά εισάγει μια σειρά από περιορισμούς στις λύσεις που μπορούμε να επιτύχουμε. Η ασαφής λογική αντίθετα, αποτελεί ένα καλό πεδίο για να εκφράσουμε την αβεβαιότητα και την ασάφεια κάνοντας εφικτή την ενσωμάτωση ρεαλιστικών καταστάσεων στα μοντέλα ασφάλειας (Hosmer, 1993). Ωστόσο, η άποψη της Hosmer όπως διατυπώνεται στις εργασίες της είναι περισσότερο διαισθητική και εκφράζει τη δυνατότητα της ασαφούς λογικής να εφαρμοστεί στο πρόβλημα των πολλαπλών πολιτικών, μέσω της έκφρασης του βαθμού ικανοποίησης απαιτήσεων στη βάση του συνόλου [0,1], χωρίς ωστόσο να προχωρά σε κάποια περαιτέρω θεωρητική διαπραγμάτευση του προβλήματος.

Εφαρμογή της ασαφούς λογικής σε μοντέλα ασφάλειας έχουμε και στην εργασία του Ovchinikov (Ovchinikov, 1994). Το μοντέλο του Ovchnikov αφορά στην εφαρμογή των αρχών της ασαφούς λογικής στο μοντέλο Bell-LaPadula, που είναι ένα ιεραρχικό μοντέλο όπου οι χρήστες και οι πόροι κατατάσσονται σε διαφορετικά ιεραρχικά επίπεδα. Όπως ήδη αναφέρθηκε στο κεφάλαιο 2, η βασική αρχή λειτουργίας του διέπεται από τις δύο βασικές αρχές ‘no read-up’ (δεν επιτρέπεται η ανάγνωση στοιχείων που βρίσκονται σε ανώτερο επίπεδο) και ‘no write-down’ (δεν επιτρέπεται η τροποποίηση αρχείων που ανήκουν σε κατώτερα επίπεδα). Το μοντέλο Bell-LaPadula ωστόσο είναι εφαρμόσιμο κατά κύριο λόγο σε οργανισμούς που έχουν ιεραρχική δομή, όπως για παράδειγμα είναι τα στρατιωτικά περιβάλλοντα. Όπως περιγράφηκε συνοπτικά και στο δεύτερο κεφάλαιο οι βασικές έννοιες του παραπάνω μοντέλου στην κλασσική του μορφή, είναι:

το σύνολο των υποκειμένων $S=\{S_1,\ldots,S_n\}$ (διεργασίες ή άτομα), το σύνολο αντικειμένων $O=\{O_1, \ldots, O_m\}$ (αρχεία, συσκευές, προγράμματα) και τέλος $C=\{C_1,\ldots,C_q\}$ είναι το σύνολο των ιεραρχικών επιπέδων με $C_1>C_2>\ldots>C_q$. Στην τυπική εκδοχή του μοντέλου μια κατάσταση v είναι ένας συνδυασμός (b, M, f) όπου

$b \subseteq S \times O$ που χαρακτηρίζει ποιο υποκείμενο έχει πρόσβαση σε ποια αντικείμενα, M είναι ο πίνακας πρόσβασης στην κατάσταση, ενώ f είναι ένα διάνυσμα κατάταξης αντικειμένου/υποκειμένου. Σε ένα περιβάλλον που διέπεται από τη χρήση ασαφών (fuzzy) κανόνων το b είναι ένα ασαφές υποσύνολο του $S \times O$. Δηλαδή b είναι μια δυαδική συσχέτιση που ορίζεται στο $S \times O$ και το b (s,o) μπορεί να ερμηνευθεί ως ο βαθμός στον οποίο το υποκείμενο s έχει πρόσβαση στο αντικείμενο o (Ovchinikov, 1994).

Το μειονέκτημα του Bell-LaPadula μοντέλου είναι ότι δεν είναι ικανό να αποτελέσει το μοντέλο ασφάλειας ενός μεγάλου εύρους οργανισμών και ειδικά όσων δεν έχουν την αυστηρή ιεραρχική δομή που χαρακτηρίζει τα στρατιωτικά συστήματα. Στην πράξη από τα μοντέλα ασφάλειας που αναφέρθηκαν στο δεύτερο κεφάλαιο, το πλέον καθιερωμένο είναι το βασισμένο σε ρόλους μοντέλο ελέγχου πρόσβασης (Role Based Access Control – RBAC). Η λογική του RBAC είναι ότι τα δεδομένα ανήκουν στον οργανισμό και όχι στους χρήστες. Έτσι, τα δικαιώματα επί των πόρων του συστήματος ορίζονται στη λογική ρόλων, αντίστοιχων με τους οργανωσιακούς ρόλους. Δηλαδή ομάδες χρηστών που επιτελούν ανάλογο έργο στα πλαίσια του οργανισμού ομαδοποιούνται σε ρόλους και αντιστοιχούνται δικαιώματα σε αυτούς τους ρόλους ανάλογα με τα καθήκοντα που αντιστοιχούν στον καθένα. Για κάθε νέο χρήστη στο σύστημα αντιστοιχείται ένας υπάρχων (ή ένας νέος) ρόλος, οπότε αυτόματα του αποδίδονται τα καθήκοντα που το σύστημα αποδίδει σε κάθε χρήστη που ανήκει στο ρόλο αυτό. Άλλο πλεονέκτημα του RBAC είναι ότι είναι πιο απλό στη διαχείριση αφού ακόμη και για πολύ μεγάλους αριθμούς χρηστών το σύνολο των δυνατών ρόλων είναι αρκετά μικρότερο, ενώ η πληροφορία που σχετίζεται με την απόδοση δικαιωμάτων πρόσβασης ομαδοποιείται και διαχειρίζεται πιο εύκολα.

Σε επίπεδο ενός οργανισμού, ο καθορισμός προνομίων πρόσβασης και η διαχείριση της ασφάλειας υπόκειται σε μια σειρά περιορισμούς, που από τη στιγμή που ικανοποιούνται το σύστημα μπορεί πλέον να λειτουργεί αυτόνομα. Η κατάσταση περιπλέκεται σε περιβάλλοντα πολλαπλών πολιτικών, όπου επιχειρείται ο συνδυασμός διαφορετικών πολιτικών και η ταυτόχρονη ικανοποίηση διαφορετικών απαιτήσεων ασφάλειας και όπου η ανάγκη για διαμοιρασμό πόρων (αρχείων ή εφαρμογών) έρχεται συχνά σε αντίθεση με την απαίτηση για διατήρηση δύο βασικών αρχών (Gong et al, 1994):

- Της αρχής της ασφάλειας, που δηλώνει ότι κάθε μη επιτρεπτή πρόσβαση σε επίπεδο μιας πολιτικής, θα πρέπει να είναι επίσης μη επιτρεπτή στο προκύπτον περιβάλλον πολλαπλών πολιτικών.
- Της αρχής της αυτονομίας, που δηλώνει ότι μια επιτρεπτή πράξη στα πλαίσια ενός οργανισμού πρέπει επίσης να επιτρέπεται στα πλαίσια του περιβάλλοντος πολλαπλών πολιτικών.

Η παρουσία πολλών περιορισμών - συχνά ανταγωνιστικών - από διαφορετικά περιβάλλοντα που συμμετέχουν στο συνασπισμό των διαφορετικών περιβαλλόντων, καθιστά συχνά αδύνατη την ικανοποίηση του συνόλου αυτών. Αποτέλεσμα του να υπόκειται το πρόβλημα σε υπερβολικά μεγάλο αριθμό περιορισμών, είναι να διακυβεύεται η επίτευξη του αναγκαίου διαμοιρασμού πόρων. Σε περιπτώσεις όπως αυτή, η χρήση ασαφών συσχετίσεων και η αξιολόγηση του βαθμού ικανοποίησης των περιορισμών μπορεί να βοηθήσει σημαντικά στην εξεύρεση λύσης. Η φιλοσοφία της προσέγγισης που θα αναπτυχθεί στις επόμενες παραγράφους είναι ότι συχνά η επίτευξη του συνασπισμού μπορεί να καταρρεύσει από την παρουσία ενός ελάσσονος σημασίας περιορισμού, που δεν διακυβεύει την ασφάλεια όλου του συστήματος. Σε

αυτή την περίπτωση υπό προϋποθέσεις μπορεί να αρθεί η απαίτηση ικανοποίησης του. Ένα ακόμη από τα προβλήματα που σχετίζονται με τη διαχείριση της ασφάλειας συνασπισμών, είναι ότι η αύξηση της πολυπλοκότητάς τους λειτουργεί αντίστροφα ανάλογα με την ευκολία διαχείρισής τους, η οποία γίνεται μια χρονοβόρα και επιρρεπής σε λάθη διαδικασία, αν βασιστούμε κατά κύριο λόγο στον ανθρώπινο παράγοντα και λιγότερο σε αυτοματοποιημένα εργαλεία (Khurana 2002).

Η ύπαρξη ανταγωνιστικών και συχνά αντικρουόμενων περιορισμών από κάθε Π.Σ. είναι συχνό φαινόμενο. Προκειμένου για την επίλυση των ανταγωνισμών και των αδιεξόδων, συχνά είναι αναγκαία η εμπλοκή των διαχειριστών του συστήματος. Αυτό δημιουργεί επιπλέον φόρτο στη διαχείριση του συστήματος, όπως επίσης και κινδύνους στη διαχείριση της ασφάλειας. Στο παρόν κεφάλαιο περιγράφεται η ανάγκη μιας εκ νέου θεώρησης του προβλήματος της διαχείρισης ασφάλειας συνασπισμών Π.Σ. όπου λαμβάνεται κυρίως μέριμνα για την αντιμετώπιση προβλημάτων μεγάλου αριθμού περιορισμών, καθώς και για την κατά το δυνατόν επίτευξη αυτοματοποιημένης διαχείρισης του συστήματος. Υπό αυτές τις συνθήκες, οι αποφάσεις εξουσιοδότησης προσπέλασης μπορούν πολλές φορές να υπακούουν στον κανόνα της ασάφειας, αναζητώντας κατά κύριο λόγο την ικανοποίηση των κρίσιμων περιορισμών, ενώ οι λιγότερο σημαντικοί περιορισμοί μπορούν υπό συνθήκες να θεωρηθούν ως δευτερεύουσας σημασίας και / ή να αγνοηθούν .

6.3 Μερική ικανοποίηση περιορισμών – Ασαφείς περιορισμοί

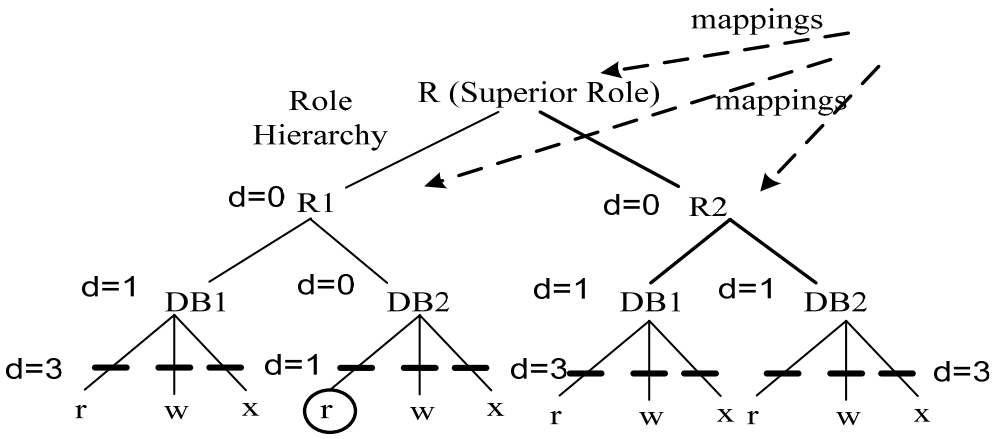
6.3.1 Φορμαλιστική περιγραφή του προβλήματος – Παράδειγμα διαμοιρασμού κοινών πόρων

Στις επόμενες παραγράφους, στα πλαίσια της εφαρμογής τεχνικών μερικής ικανοποίησης περιορισμών με συνδυασμένη χρήση ασαφούς λογικής για την επίλυση ανταγωνιστικών καταστάσεων (conflicts) σε περιβάλλοντα πολλαπλών πολιτικών, θα αξιοποιηθεί ένα παράδειγμα ανταγωνισμού με χαμηλής κρισιμότητας περιορισμούς.

Σε πρώτη φάση θα επιχειρήσουμε να περιγράψουμε τους σχετικούς περιορισμούς με ένα ποιοτικό τρόπο, προχωρώντας με εφαρμογή σε σχετικό παράδειγμα. Κατόπιν θα επεκτείνουμε την εφαρμογή του παραδείγματος εισάγοντας ασαφείς περιορισμούς (fuzzy constraints). Με όμοιο τρόπο θα μπορούσαμε να καλύψουμε ένα πολύ μεγαλύτερο εύρος περιορισμών (όπως για παράδειγμα διαχωρισμού καθηκόντων - separation of duty) σε συστήματα συμβατά με το μοντέλο RBAC. Στην περίπτωση μας θα θεωρήσουμε ένα παράδειγμα δύο διασυνδεδεμένων περιοχών που προσπαθούν να επικοινωνήσουν με χρήση του πρωτοκόλλου IPSec (IPSec, 1998).

Έστω ότι δύο Π.Σ. τα Α και Β επιχειρούν τη σύναψη συνασπισμού όπου στο Π.Σ. Α υπάρχουν δύο πόροι που τίθενται σε κοινή χρήση, οι βάσεις δεδομένων DB_1 και DB_2. Ο ρόλος R_1 μπορεί να διαβάσει (read access) τοπικά τη βάση DB_2. Η βάση DB_1 θεωρούμε ότι έχει πιο ευαίσθητα δεδομένα, γι' αυτό και δεν επιτρέπουμε σε κάποιον μεμονωμένο ρόλο να την προσπελάσει (απαιτούνται πιο σύνθετοι έλεγχοι προκειμένου να επιτραπεί η προσπέλαση σε αυτήν). Στο ρόλο R_2 δεν επιτρέπουμε κάποιο δικαίωμα πρόσβασης στις δύο βάσεις.

Σύμφωνα με τις αντιστοιχήσεις ρόλων όπως έχουν καταγραφεί από τους διαχειριστές του συνασπισμού των δύο Π.Σ. ένας ρόλος από το απομακρυσμένο Π.Σ. Β έχει οριστεί στο Π.Σ. Α σαν αντίστοιχος του ρόλου R (Εικ. 6.1) .



Εικόνα 6.1 Πρόβλημα αντιστοίχησης ρόλων με υπερβολικό αριθμό περιορισμών

Βάσει των κανόνων του μοντέλου RBAC ο R μπορεί να κληρονομήσει τα δικαιώματα των κατώτερων ρόλων R_1, R_2. Θεωρώντας δεδομένη τώρα αυτή την αντιστοίχηση του ρόλου R στον απομακρυσμένο ρόλο του Π.Σ. Β, αναζητούμε ένα μηχανισμό (ημι-) αυτόματης αντιστοίχησης προνομίων πρόσβασης με στόχο ο χρήστης από το σύστημα Β να μπορεί να έχει πρόσβαση σε συγκεκριμένους πόρους του συστήματος Α, λαμβάνοντας υπόψη και τους τοπικούς περιορισμούς. Η χρήση ωστόσο του πρωτοκόλλου IPSec σε κάθε περιοχή (που μπορεί να επιβάλλει πρόσθετους κανόνες, αποθηκευμένους στο τείχος προστασίας του κάθε οργανισμού), είναι δυνατό να αποτρέψει τη σύναψη του διαύλου επικοινωνίας, ειδικά αν γίνεται με χρήση κρυπτογραφικών τεχνικών, με αποτέλεσμα να είναι αδύνατη η πρόσβαση σε οποιοδήποτε πόρο του συστήματος Α. Στην περίπτωση αυτή οδηγούμαστε σε μία κατάσταση αδιεξόδου.

6.3.2 Μη-πλήρης ικανοποίηση σε προβλήματα πολλαπλών περιορισμών

Προκειμένου για την εύρεση αποδεκτών συνδυασμών της μορφής, <R,O,P> η πιο πρόσφορη τεχνική που θα μπορούσε να αξιοποιηθεί είναι η τεχνική της οπισθοδρόμησης (backtracking) που ψάχνει διεξοδικά όλους τους δυνατούς συνδυασμούς της μορφής <R, O, P> (προκειμένου να βρει μία αποδεκτή λύση και να αντιστοιχιστούν δικαιώματα πρόσβασης σε κάποιον από τους ρόλους του Π.Σ. Β). Όπως εύκολα μπορεί να διαπιστωθεί, όλοι οι δυνατοί συνδυασμοί αποτυγχάνουν (εφόσον αναφερόμαστε σε προσπάθεια απομακρυσμένης και κρυπτογραφημένης επικοινωνίας), με αποτέλεσμα κανένας συνδυασμός να μην μπορεί να ικανοποιήσει το σύνολο των περιορισμών (κάτι τέτοιο αναπαρίσταται στο σχήμα 6.1 με τις διακεκομμένες γραμμές στα δικαιώματα που αντιστοιχούν στους διαμοιραζόμενους πόρους).

Σε αντίθεση με την μέθοδο εξαντλητικής αναζήτησης όλων των δυνατών συνδυασμών με στόχο την επίλυση του προβλήματος, η μέθοδος διακλάδωσης και φραγμού (branch and bound) δεν αναζητεί την ιδανική λύση που ικανοποιεί το σύνολο των περιορισμών, αλλά μία που ικανοποιεί όχι λιγότερους από ένα προκαθορισμένο όριο N περιορισμών (όπου το N μπορεί και δυναμικά να μεταβάλλεται κατά τη διαδικασία αναζήτησης λύσης). Στον αλγόριθμο που παρατίθεται στον πίνακα 6.1, η παράμετρος distance που μετράται από τη μεταβλητή N μπορεί να ρυθμιστεί εξαρχής σύμφωνα με κάποια a-priori γνώση (ή σύμφωνα με τις προτιμήσεις που εκφράζει ένα Π.Σ.) και δηλώνει την προτίμηση μία αποδεκτή λύση να ικανοποιεί όχι λιγότερο από N περιορισμούς. Κατά τη διάρκεια αναζήτησης λύσης, ένα μονοπάτι αναζήτησης (search path) συνίσταται από ένα σύνολο τιμών που

αντιστοιχούνται στις μεταβλητές που μας ενδιαφέρουν. Ένα μονοπάτι αναζήτησης που οδηγεί στην πιο πρόσφατη ανάθεση τιμής για μια μεταβλητή, αποτελεί το τρέχον μονοπάτι αναζήτησης (current search path). Στον αλγόριθμο του πίνακα 6.7 κάθε ρόλος στην ιεραρχία του Π.Σ. Β ελέγχεται πρώτα για την ύπαρξη αντιστοίχησης σε κάποιο ρόλο του Π.Σ. Α. Στη συνέχεια, για τις προκαθορισμένες αντιστοιχίσεις ρόλων, γίνεται μια ανάθεση Αντικειμένων (O-Objects) και δικαιωμάτων (P-Permissions) προσέχοντας να ικανοποιηθούν όσο το δυνατόν περισσότεροι περιορισμοί. Τα N, S, Best-solution είναι καθολικές μεταβλητές στον αλγόριθμο, που περιέχουν τις αναγκαίες και επαρκείς συνθήκες (προτιμήσεις των Π.Σ.) καθώς και την βέλτιστη μέχρι στιγμής λύση κατά τη διάρκεια των επαναλήψεων του αλγορίθμου.
Στην προσέγγισή μας αναζητούμε για όλα τα ζεύγη ρόλων που σχηματίζονται από τους δύο συνεργαζόμενους οργανισμούς, τις δυνατές αντιστοιχήσεις διαμοιραζόμενων αντικειμένων και δικαιωμάτων επί αυτών. Δηλαδή το σχηματισμό των επιτρεπτών τιμών για πλειάδες του τύπου $<R_i, R_j, O, P>$, όπου R_i, R_j δύο ρόλοι αντίστοιχοι που ανήκουν ο κάθε ένας σε διαφορετικό σύστημα. Προκειμένου για την αναζήτηση των αποδεκτών λύσεων χρησιμοποιούμε τεχνικές μέγιστης ικανοποίησης περιορισμών, που συνιστούν μια μορφή βελτιστοποίησης. Το πλεονέκτημα της τεχνικής διακλάδωσης και φραγμού που χρησιμοποιείται, είναι ότι δε χρειάζεται να αναζητήσει όλα τα δυνατά μονοπάτια αλλά ότι μπορεί να σταματήσει όταν ανιχνεύσει μια ικανοποιητική λύση (επιτυγχάνοντας κατ' αυτόν τον τρόπο καλύτερους χρόνους απόκρισης και κατ' επέκταση καλύτερη απόδοση για το σύστημα).

Για κάθε ρόλο r_I { r_I είναι ένας ρόλος από το απομακρυσμένο Π.Σ. }

Για κάθε ρόλο r_j { r_j είναι ρόλος που ανήκει στο Π.Σ. στο οποίο απευθύνεται το αίτημα πρόσβασης }

Αν υπάρχει αντιστοίχηση_ρόλων ($r_I \rightarrow r_j$) τότε

Classify_PA_BB_S (role-hierarchy-path, Distance, DomainA-roles, Objects, Permissions, Values) {PA_BB_S: Κατάταξε με βάση το κριτήριο διακλάδωσης και φραγμού } {Αναζήτηση μερικών λύσεων με στόχο την εύρεση συνδυασμών τιμών στο μονοπάτι αναζήτησης και να συσχετίσουμε δικαιώματα πρόσβασης με αντικείμενα}

Τέλος_κυρίως προγράμματος

Υπορουτίνα Classify_PA_BB_S (Search_path, Distance, Variables, Values)

[Variables: οι μεταβλητές χώρου ενδιαφέροντος]

[Values: Τιμές που αντιστοιχούνται στις μεταβλητές]

[Search_path: σύνολο τιμών που αντιστοιχούνται στις μεταβλητές χώρου αναζήτησης]

[Dimension: Αριθμός περιορισμών που παραβιάζονται από το συγκεκριμένο συνδυασμό τιμών]

{S_Bound: Δυναμικά υπολογιζόμενο σε κάθε επανάληψη όριο }

Αν Variables=nil τότε

{έχουμε αντιστοιχίσει τιμές σε όλες τις μεταβλητές στο Search-path}

Best-solution ← Search-path

N ← Distance

Αν N≤ S_Bound τότε επέστρεψε ' ΤΕΛΟΣ'

{βρέθηκε ικανοποιητική λύση }

αλλιώς επέστρεψε "ΣΥΝΕΧΙΣΕ_ΑΝΑΖΗΤΗΣΗ"

{επανέλαβε μέχρι μια άλλη τιμή για την τελευταία τιμή αντιστοιχιστεί στο Search-path}

αλλιώς αν Distance =N τότε

```
   { Το Search-path επεκτείνεται μέχρι να αντιστοιχιστούν τιμές στις υπόλοιπες μεταβλητές που να μην παραβιάζουν περισσότερους περιορισμούς }
    επέστρεψε "ΣΥΝΕΧΙΣΕ_ΑΝΑΖΗΤΗΣΗ"
αλλιώς  {προσπάθησε να επεκτείνεις το Search-Path}
    Current-value ← πρώτη τιμή από το σύνολο τιμών
    New_Distance ← Distance
δοκίμασε επιλογές στο Search-path, από την τελευταία στην πρώτη,
      μέχρις ότου New_Distance <N:
  Αν η επιλογή είναι ασύμβατη με την τρέχουσα τιμή Current-value τότε
            New_Distance  ← New_Distance+1
   Αν  New_Distance < N και
    Classify_PA_BB_S (Search-path συν τρέχουσα τιμή current-value,
                          New_Distance,
                          Variables μείον την πρώτη μεταβλητή,
                          Τιμές της δεύτερης μεταβλητής στην Variables) = ' ΤΕΛΟΣ'
                              Τότε επέστρεψε 'ΤΕΛΟΣ'  {Το Search-path επεκτάθηκε επαρκώς }
 Αλλιώς {έλεγξε για μια άλλη τιμή (value)}
επέστρεψε Classify_PA_BB_S (Search-path, Distance, Variables, Values εκτός της τρέχουσας )
```

Πίνακας 6.7 Αλγόριθμος αντιστοίχησης δικαιωμάτων σε απομακρυσμένους ρόλους με εφαρμογή τεχνικών μερικής ικανοποίησης περιορισμών.

Ο αλγόριθμος διασχίζει το δέντρο αναζήτησης μετακινούμενος προς τα κάτω στο κατώτερο επίπεδο του δέντρου, κάθε επίπεδο του οποίου αντιστοιχεί σε μια μεταβλητή. Ένα σύνολο τιμών που αντιστοιχούν σε κάποιες από τις μεταβλητές του προβλήματος συνιστούν ένα μονοπάτι αναζήτησης (search-path). Ο όρος απόσταση (distance) αναφέρεται στον αριθμό περιορισμών που παραβιάζονται από ένα συνδυασμό τιμών.

Στο παράδειγμά μας, αντιστοιχίζοντας στο ρόλο R τα δικαιώματα του ρόλου R_2 (θεωρώντας ότι ο ανώτερος στην ιεραρχία ρόλος κληρονομεί τα δικαιώματα του κατώτερου ρόλου) και τη στιγμή που προσπαθούμε να αποδώσουμε στη δεύτερη μεταβλητή {O} την τιμή DB_1, έχουμε την πρώτη παραβίαση περιορισμού κάτι που δίνει την τιμή στη μεταβλητή d=1. Επιχειρώντας να αντιστοιχίσουμε δικαιώματα (ένα επίπεδο πιο κάτω) στον πιο πάνω πόρο, έχουμε d=3, λόγω του ότι η DB_1 δεν μπορεί να προσπελαστεί ή να τροποποιηθεί απομακρυσμένα από κανένα ρόλο, ενώ ο ρόλος R_2 δεν θα πρέπει να έχει σε καμία περίπτωση πρόσβαση στους συγκεκριμένους πόρους. Το N στον αλγόριθμο χρησιμοποιείται σαν μεταβλητή που κρατάει τον αριθμό των ασυμβατοτήτων στη μέχρι στιγμής καλύτερη λύση. Καθώς η τεχνική διακλάδωσης και φραγμού προχωρά, προκύπτει μια καλύτερη λύση η οποία παραβιάζει ένα μόνο περιορισμό: (R_1, DB_2, r). Τυπικά στην αντιστοίχηση δικαιωμάτων, αντί απλής ανάγνωσης r θα μπορούσαμε να γράψουμε r-r (απομακρυσμένη ανάγνωση, remote read). Στην περίπτωση αυτή, ο συνδυασμός (R_1, DB_2) είναι επιτρεπτός, το ίδιο και ο συνδυασμός (R_1, r) και μόνο ο συνδυασμός (R_1, DB_2, r-r) αποτελεί παραβίαση των περιορισμών που επιβάλλουν οι πολιτικές ασφάλειας. Χαλαρώνοντας αυτή την απαίτηση, η συγκεκριμένη πολιτική πρόσβασης

φαίνεται πώς μπορεί να βρει μια ικανοποιητικά αποδεκτή λύση (στο σχήμα 6.1 η λύση υποδεικνύεται με ένα κύκλο).

Συμπεραίνουμε πώς με τη χρήση τεχνικών μερικής ικανοποίησης περιορισμών, είναι δυνατόν να επιτύχουμε λύσεις στο πρόβλημα της ικανοποίησης πολλαπλών πολιτικών, με την προϋπόθεση οι περιορισμοί οι οποίοι δεν ικανοποιούνται πλήρως να μην επισύρουν γενικότερους κινδύνους για τη διαχείριση ασφάλειας του συστήματος (να μην πρόκειται ουσιαστικά για κρίσιμους περιορισμούς).

6.3.3 Ασαφείς περιορισμοί (fuzzy constraints)

Σε αντίθεση με τους συμπαγείς περιορισμούς, οι χαλαροί (soft) περιορισμοί επιτρέπουν τον καθορισμό προτιμήσεων ανάμεσα στις τιμές (κ-πλειάδες) που μπορούν να αντιστοιχιστούν σε ένα σύνολο μεταβλητών. Οι μεταβλητές αυτές μπορούν να θεωρηθούν ως μέλη σε μια ολικά διατεταγμένη ασαφή (fuzzy) σχέση, που αντιστοιχεί σε κάθε πλειάδα ένα βαθμό προτίμησης $\mu_e(u_{1,\ldots,}u_k)$ σε ένα ολικά διατεταγμένο σύνολο [0,1]. Μπορούμε συνεπώς να επεκτείνουμε την έννοια ενός προβλήματος ικανοποίησης περιορισμών (CSP) ώστε να συμπεριλαμβάνει και ασαφείς προτιμήσεις (fuzzy preferences). Σαν ένα πρόβλημα ικανοποίησης ασαφών περιορισμών (fuzzy-CSP) θεωρούμε ένα πρόβλημα που περιλαμβάνει ένα σύνολο από μεταβλητές $(x_{1,\ldots}x_k)$, ένα πεπερασμένο σύνολο $(D_1,\ldots,D_k)$ τιμών που οι μεταβλητές μπορούν να λάβουν και τέλος ένα σύνολο από ασαφείς περιορισμούς $(c_1,\ldots\ldots,c_k)$. Ένα στιγμιότυπο $v^* \in D$ θεωρείται ως η καλύτερη λύση, αν ο βαθμός ικανοποίησης όλων των περιορισμών C $((c_1,c_{2,..,}c_k)\underline{v^*})$ είναι ο μέγιστος δυνατός (Dubois et al, 1993). Χρησιμοποιώντας χαλαρούς περιορισμούς μπορούμε με πολλούς διαφορετικούς τρόπους να χειριστούμε τις προτιμήσεις των συμμετεχόντων στο συνασπισμό μερών. Θεωρούμε πως αυτές οι προτιμήσεις μπορούν να κωδικοποιηθούν σε μια συσχέτιση R ασαφούς λογικής, που συσχετίζει κάθε κ-πλειάδα $(u_{1,\ldots,}u_k)$ με ένα βαθμό προτίμησης. Έτσι $P_R(u_{1,\ldots,}u_k)$, $>P_R(u_1', \ldots,u_k')$ σημαίνει ότι η πλειάδα $(u_{1,\ldots,}u_k)$ είναι προτιμότερη της $(u_{1,\ldots,}u_k)$. $P_R(u_{1,\ldots,}u_k)=0$ σημαίνει ότι η πλειάδα $(u_{1,\ldots,}u_k)$ παραβιάζει πλήρως τον περιορισμό ενώ $P_R(u_{1,\ldots,}u_k)=1$ σημαίνει ότι ο περιορισμός ικανοποιείται πλήρως.

6.4 Ασαφείς συσχετίσεις (Fuzzy relations)

Στην προηγούμενη παράγραφο εξετάστηκε πώς μια ασαφής συσχέτιση R αντιστοιχεί σε κάθε k-πλειάδα ένα επίπεδο προτίμησης $\mu_R(u_{1,\ldots,}u_k)$ σε ένα πλήρως διατεταγμένο σύνολο L. Αυτό το σύνολο συνήθως επιλέγεται στο διάστημα [0,1]. $\mu_R(u_{1,\ldots,}u_k) > \mu_R(u_1', \ldots,u_k')$ σημαίνει ότι η $(u_{1,\ldots,}u_k)$ είναι προτιμότερη της $(u_1', \ldots,u_k')$.

Οι ασαφείς περιστολές (fuzzy restrictions) προσφέρουν ένα εναλλακτικό φορμαλισμό, δίνοντας τη δυνατότητα να αντιστοιχίσουμε προτεραιότητες – παρόμοια με τις προτιμήσεις - στους περιορισμούς, εκπεφρασμένες στην κλίμακα [0,1].

Ένας συντελεστής a_c εκφράζει το βαθμό προτεραιότητας κάθε περιορισμού C και υποδεικνύει το βαθμό στον οποίο ο περιορισμός αυτός C θα πρέπει να ικανοποιηθεί. Πιο αναλυτικά, $a_c=1$ σημαίνει ότι ο περιορισμός πρέπει να ικανοποιηθεί απόλυτα, ενώ $a_c=0$ σημαίνει ότι μπορεί και να αγνοηθεί εντελώς. Συνεπώς μια ασαφής συσχέτιση S σε ένα σύνολο $U_1 \times\ldots\times U_k$ μπορεί να μοντελοποιήσει το ζεύγος περιορισμού-βαθμού προτεραιότητας (C, a_c) με μία συνάρτηση $\mu_S(u_{1,\ldots,}u_k)=1$ στην περίπτωση που ο συνδυασμός $(u_{1,\ldots,}u_k)$ ικανοποιεί τη σχέση, ή ως $\mu_S(u_{1,\ldots,}u_k)=1-a_c$ στην περίπτωση που το παραβιάζει. Εναλλακτικά θα μπορούσαμε να πούμε ότι η μ_S

καθορίζεται ανάλογα με το αν η μέγιστη τιμή επιτυγχάνεται ικανοποιώντας τον περιορισμό ή παραβιάζοντάς τον. Για ένα χαλαρό περιορισμό C που μοντελοποιείται από τη συσχέτιση R το ζεύγος (C, a_c) μοντελοποιείται από τη συνάρτηση $\mu_S(u_{1,\ldots,}u_k)=\max(1-a_c, \mu_R(u_{1,\ldots,}u_k))$.

Ιδιαίτερο ενδιαφέρον έχει η ικανότητα χειρισμού ταυτόχρονα πολλαπλών περιορισμών. Για το σκοπό αυτό, μπορούμε να ορίσουμε δύο πράξεις: την προβολή (projection) και το συνδυασμό (combination). Δοθέντων δύο υποσυνόλων $W=\{w_1,\ldots,w_k\}$ και $Y=\{y_1,\ldots,y_i\}$ του συνόλου $(x_{1,\ldots}x_k)$ των μεταβλητών, δεδομένου $W\subseteq Y$ και θεωρώντας μια ασαφή συσχέτιση T που περιορίζει τις δυνατές τιμές του Y, η προβολή του T στο W είναι μια επίσης ασαφής συσχέτιση $R=T\downarrow W$, που ορίζεται από τη σχέση $\mu_R(u_{w1,\ldots,}u_{wk})= \sup_{\{(u_{y1,\ldots,}u_{yh})\,/(u_{y1,\ldots,}u_{yh})\downarrow W=(u_{w1,\ldots,}u_{wk})\}} \mu_{T(}u_{w1},\ldots,u_{wk})$ όπου $(u_{w1,\ldots,}u_{wk})$ δηλώνει την περιστολή του $(u_{y1},\ldots,u_{yi})$ στο W. Άτυπα, η ασαφής συσχέτιση μ_R δηλώνει σε ποιο βαθμό ένα μερικό στιγμιότυπο $(u_{w1,\ldots,}u_{wk})$ του συνόλου Y μπορεί να επεκταθεί σε ένα πλήρες στιγμιότυπο του Y που ικανοποιεί την σχέση T. Αυτή η παρατήρηση έχει ιδιαίτερη σημασία στην περίπτωση που έχουμε επιλέξει πρώτα ένα στιγμιότυπο ενός περιορισμού που μας ενδιαφέρει κύρια και θέλουμε να επεκτείνουμε ώστε να συμπεριλάβουμε τους λιγότερο σημαντικούς περιορισμούς, με στόχο να ικανοποιήσουμε (μερικώς) το δοθέν πρόβλημα στο μέγιστο δυνατό βαθμό.

Ο συνδυασμός δύο ασαφών περιστολών R και S που περιορίζει τις δυνατές τιμές των δύο συνόλων μεταβλητών X και Y, μπορεί να οριστεί ως η ασαφής συσχέτιση $T=R\otimes S$ επί των δυνατών τιμών της ένωσης $W=X\cup Y$ των δύο συνόλων. Ορίζεται ως $\mu_{T\,(}u_{w1,\ldots,}u_{wk)}=\min\{\,(\mu_R(u_{w1,\ldots,}u_{wk})\downarrow X),\, \mu_S((u_{w1,\ldots,}u_{wk})\downarrow Y)\}$. Τυπικά το αποτέλεσμα $\mu_{R1\otimes R2\otimes R3\otimes..\otimes Rm}(u_1,..,u_n)$ εκτιμά σε ποιο βαθμό ο συνδυασμός $(u_1,..,u_n)$ τιμών ικανοποιεί ταυτόχρονα τους δοθέντες περιορισμούς. Ο συνδυασμός επιτρέπει να μετασχηματίσουμε το επίπεδο προτίμησης σε περιορισμούς, σε βαθμούς προτίμησης στις προκύπτουσες λύσεις.

Εναλλακτικά, μπορούμε και τους ατομικούς περιορισμούς να τους θεωρήσουμε σαν αποδόμηση μιας καθολικής fuzzy συσχέτισης $\rho=R_1\otimes R_{2\ldots}\otimes R_n$ που περιορίζει το συνδυασμό τιμών που μπορούν να αντιστοιχιστούν σε ένα σύνολο μεταβλητών $(x_{1,\ldots.}x_n)$. Ακόμη και αν δεν υπάρχει συσχετισμός στο σύνολο των περιορισμών $\{R_1,R_2,\ldots,R_m\}$, η ρ υπονοεί μια περικοπή στις επιτρεπόμενες τιμές για μια μεταβλητή, ανεξάρτητα του ποιες τιμές έχουν αντιστοιχιστεί σε μια άλλη μεταβλητή. Στις περισσότερες περιπτώσεις, υφίσταται μια υπονοούμενη μεταβολή των τιμών που μπορούν να αντιστοιχιστούν σε άλλες μεταβλητές: $\rho^{\downarrow\{x_{i,}\,x_j\}}\subset\rho^{\downarrow\{x_i\}}\otimes\rho^{\downarrow\{x_j\}}$.

6.4.1 Αναζήτηση λύσεων στις ασαφείς συσχετίσεις

Η επίλυση προβλημάτων ασαφών περιορισμών στις περισσότερες περιπτώσεις προκύπτει σαν επέκταση μιας μερικής λύσης που αντιστοιχεί τιμές στις υπάρχουσες μεταβλητές, κατά τέτοιο τρόπο ώστε ένα στιγμιότυπο να ικανοποιεί όλους τους δοσμένους περιορισμούς. Η έννοια της μερικής ικανοποίησης είναι ζωτικής σημασίας στην άλγεβρα των προβλημάτων ασαφών περιορισμών. Τα κριτήρια στην αναζήτηση λύσης μπορεί να είναι η απόδοση τιμής στις πιο κρίσιμες μεταβλητές ή εναλλακτικά στις πλέον περιορισμένες.

Μία χρήσιμη μετρική που μπορεί να αξιοποιηθεί στην εκτίμηση της πιο κρίσιμης παραμέτρου, στην οποία πρέπει να ανατεθούν τιμές πρώτα, είναι η καταλληλότητα. Η καταλληλότητα $a_i(v)$ μιας τιμής $v\in D_i$ για μία μεταβλητή x_i εκτιμάται επί τη βάσει του βαθμού μέγιστης ικανοποίησης των περιορισμών αναφορικά με τη x_i. Ορίζεται ως

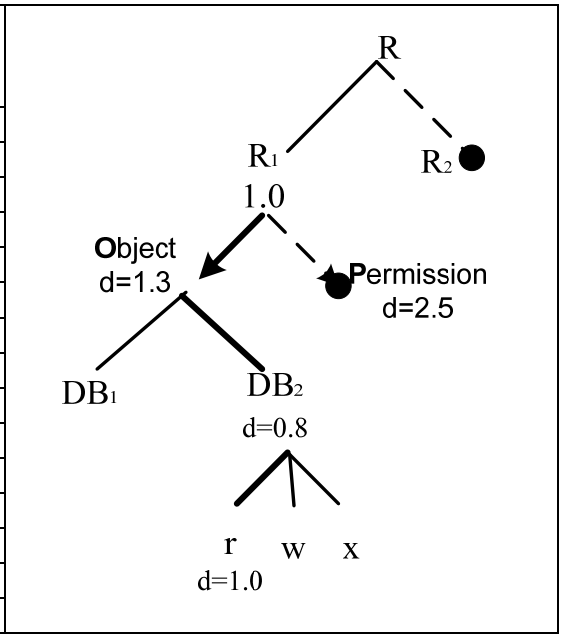
$a_i(v)=\max\{C((c_{i1},..,c_{ih}),\underline{v}) \mid \underline{v} \in D_{i1},\times\ldots\times D_{ik-1} \times\{v\}\times D_{ik+1} .. \times D_{ih}\}$. Από την καταλληλότητα μπορούμε να εκτιμήσουμε τη μετρική d_i (δυσκολία – difficulty) μίας μεταβλητής, η οποία προκύπτει από το άθροισμα των δυνατών τιμών που προκύπτουν για την καταλληλότητα, για όλες τις δυνατές αναθέσεις τιμών στη συγκεκριμένη μεταβλητή. Η μετρική αυτή μπορεί να υπολογιστεί σύμφωνα με τη σχέση $d_i = \sum_{v \in D_i} a_i(v)$ (Ruttkay, 1994).

Αναζητώντας τη βέλτιστη λύση, πρώτα αντιστοιχούμε τιμές σε μεταβλητές με περιορισμένο αριθμό παραμέτρων, προκειμένου στη συνέχεια να εφαρμόσουμε ευκολότερα τεχνικές διακλάδωσης και φραγμού (που κρατούν ίχνη της λύσης που επιτυγχάνει το μέγιστο βαθμό ικανοποίησης σε δεδομένη χρονική στιγμή). Όλες οι μερικές αναθέσεις τιμών για τις οποίες ο βαθμός ικανοποίησης δεν ξεπερνά αυτόν της μέχρι στιγμής βέλτιστης λύσης, απομακρύνονται πλέον από περαιτέρω διερεύνηση.

6.4.2 Εφαρμογές των ασαφών περιορισμών σε προβλήματα ελέγχου πρόσβασης

Επιστρέφοντας στο πρόβλημα της παραγράφου 6.3.1, θα επιχειρήσουμε να το περιγράψουμε ως πρόβλημα ικανοποίησης ασαφών περιορισμών (fuzzy constraint satisfaction problem – FCSP) με μεταβλητές R (role), O (object) P (permission) με χώρους μεταβλητών $\{R_1, R_2\}$, $\{DB_1 , DB_2\}$, και {w,r,x} αντίστοιχα. Έχουμε ορίσει μια αντίστοιχη προτίμηση για διαφορετικούς συνδυασμούς μεταβλητών, η οποία αναπαρίσταται στην εικ. 6.2α (οι συνδυασμοί που είναι μη επιτρεπτοί δεν αναπαρίστανται). Όπως έχει ήδη περιγραφεί το πρόβλημα υπόκειται σε μεγάλο αριθμό περιορισμών και δεν υπάρχει ακριβής λύση. Χρησιμοποιώντας ως μετρικές την καταλληλότητα και τη δυσκολία μιας μεταβλητής όπως περιγράφηκαν στην προηγούμενη παράγραφο, θα επιχειρήσουμε να υπολογίσουμε βέλτιστες λύσεις που ικανοποιούν τους δοθέντες περιορισμούς στο μέγιστο δυνατό βαθμό. Συνεπώς υπολογίζουμε τις τιμές των μετρικών δυσκολίας και καταλληλότητας για όλες τις μεταβλητές του δοθέντος χώρου, ξεκινώντας από τη μεταβλητή R:

Con-straint	Satisfa-ction	R (role)	P (permi-ssion)	O (Object)
C_1	0.8	R1	w	
	1	R1	r	
	0.7	R1	x	
	0.1	R2	w	
	0.2	R2	r	
C_2	0.5	R1		DB1
	0.8	R1		DB2
	0.1	R2		DB1
	0.3	R2		DB2
C_3	0.4		w	DB1
	0.8		w	DB2
	0.5		r	DB1
	0.8		r	DB2
	0.5		x	DB1
	0.7		x	DB2



Εικόνα 6.2α(αριστερά) Έκφραση προτιμήσεων επί περιορισμών 6.2β (δεξιά) Υπολογισμός των τιμών των μεταβλητών για την προσέγγιση λύσης

$a_R(R_1)=1$, $a_R(R_2)=0.2$ και $d_R=1.2$, Για τη μεταβλητή P (permissions) έχουμε $a_p(r)= 1$ $a_p(w)=0.8$, $a_p(x)=0.7$ $d_p=2.5$ ενώ για τη μεταβλητή O (object) έχουμε $a_o(DB_1)=0.5$ και $a_o(DB_2)=0.8$ δίνοντας $d_O=1.3$.

Από τα παραπάνω προκύπτει ότι θα πρέπει να αποδώσουμε τιμή πρώτα στην μεταβλητή R, η οποία επιτυγχάνει τη χαμηλότερη τιμή δυσκολίας. Από τις δυνατές τιμές της μεταβλητής, πρέπει να αποδώσουμε αυτήν με τη μεγαλύτερη καταλληλότητα, δηλαδή την τιμή R_1. Στη συνέχεια, από τις δύο εναπομένουσες μεταβλητές, θα πρέπει να εντοπιστεί η επόμενη σε σημαντικότητα. Ο χώρος αναζήτησης μετά την αντιστοίχηση τιμής στην R έχει μειωθεί μόνο στους συνδυασμούς που περιλαμβάνουν την τιμή R_1 για τη μεταβλητή R. Επομένως από τα δεδομένα της εικ. 6.2α υπολογίζουμε με όμοιο τρόπο για τις δύο μεταβλητές: $a_P(w)=0.8$, $a_P(r)=1$, $a_P(x)=0.7$, με $d_P=2.5$ και $a_O(DB_1)=0.5$, $a_O(DB_2)=0.8$ με $d_O=1.3$. Από τους τελευταίους υπολογισμούς είναι προφανές πώς η επόμενη μεταβλητή στην οποία πρέπει να αποδώσουμε τιμή είναι το αντικείμενο (Object - O) και η πιο κατάλληλη τιμή για τη μεταβλητή αυτή - που μπορεί να αντιστοιχιστεί στην ήδη επιλεγμένη τιμή R_1 για τη μεταβλητή R - είναι η DB_2. Μέχρι στιγμής έχουμε επιτύχει να αντιστοιχίσουμε την DB_2 ως τον πιο κατάλληλο πόρο για το ρόλο R_1 και το επόμενο βήμα είναι να ελέγξουμε για αποδεκτούς συνδυασμούς δικαιωμάτων. Όπως προκύπτει σχετικά εύκολα, η καταλληλότερη τιμή είναι η r, που επιτυγχάνει και τη μέγιστη τιμή καταλληλότητας. Συνεπώς έχουμε επιτύχει να έχουμε ως πιο κατάλληλο συνδυασμό για την τριάδα <R,O,P>, το <R_1, DB_2, r> (εικ. 6.2β). Ο ολικός βαθμός ικανοποίησης της λύσης που προέκυψε, μπορεί να υπολογιστεί με βάση την αρχή του συνδυαστικού γινομένου (που βοηθά στην εκτίμηση του συνολικού βαθμού ταυτόχρονης ικανοποίησης των περιορισμών) και δίνεται από τη σχέση: $C_{prod}((c_1,..,c_n), \underline{v})=\prod_{i=1}^{n} c_i(v_i)$. Στην περίπτωσή μας επιτυγχάνεται ένας συνολικός βαθμός ικανοποίησης ίσος με 0.8.

Ενσωμάτωση στο σύστημα επιβολής ελέγχων πρόσβασης

Οι προτιμήσεις ενός Π.Σ. σε ένα συνασπισμό μπορούν να φορτωθούν δυναμικά κατά τη διάρκεια εκτίμησης του αιτήματος από το σημείο εκτίμησης αποφάσεων πολιτικής (PDP), ενώ μπορούν να κωδικοποιηθούν με τη μορφή που απεικονίζεται στην εικ. 6.2α και να αποθηκευτούν σε αρχεία XML. Σύμφωνα λοιπόν με την παραπάνω διαδικασία κωδικοποιούνται οι προτιμήσεις κάθε Π.Σ. ανά ρόλο, πόρο και τύπο δικαιώματος, εκφράζοντας την κρισιμότητα πόρων καθώς και την προτίμηση σε ρόλους ανάλογα με τη σημαντικότητά τους στην ιεραρχία. Η ανάγνωση των προτιμήσεων γίνεται από το PDP κατά τη διάρκεια του υπολογισμού της εγκυρότητας του αιτήματος, και κατόπιν με τον υπολογισμό των μετρικών που περιγράφονται στις §6.4.2 και §6.4.3 μπορεί να εκτιμηθεί αν παραβιάζονται κάποιοι περιορισμοί και αν ναι σε ποιο βαθμό (προκύπτει μία εκτίμηση για το αν είμαστε πλησιέστερα στην ικανοποίηση των σχετικών αιτημάτων ή όχι).

6.5. Συζήτηση – συγκριτική αποτίμηση

Η αναπαράσταση προβλημάτων ασφάλειας με χρήση περιορισμών αποκτά ιδιαίτερη βαρύτητα στη σχετική ερευνητική βιβλιογραφία τελευταία. Οι Ahn και Sandhu, (Ahn et al, 2000) δημιούργησαν μια γλώσσα ικανή να αναπαραστήσει περιορισμούς εξουσιοδότησης, βασισμένη στη χρήση πρώτου βαθμού λογικής με κατηγορήματα (predicate first order logic). Στη δουλειά τους αυτή υποστηρίζεται η δυνατότητα

αναπαράστασης διαφορετικού τύπου περιορισμούς πρόσβασης, όπως για παράδειγμα περιορισμούς διαχωρισμού καθηκόντων (separation of duty) κοκ. Στο παρόν κεφάλαιο επεκτείναμε το πεδίο εφαρμογής του προγραμματισμού περιορισμών στην περίπτωση πολλαπλών πολιτικών και δείξαμε ότι η δημιουργία συνασπισμού και η επίτευξη συμφωνίας είναι δυνατή με τη χρήση τεχνικών μερικής ικανοποίησης και τεχνικών ασαφούς λογικής για την ικανοποίηση των περιορισμών.

Οι (Khurana et al, 2002) δημιούργησαν ένα μοντέλο για συνασπισμούς αυτόνομων συστημάτων χρησιμοποιώντας τη γλώσσα RCL 2000 των Ahn και Sandhu (Ahn and Sandhu, 2000). Στο μοντέλο τους τα συμμετέχοντα περιβάλλοντα παίρνουν σειρά κυκλικά και προτείνουν τους πόρους που επιθυμούν να συνεισφέρουν στον κοινά διαμοιραζόμενο χώρο. Στο μοντέλο τους, η διαπραγμάτευση γίνεται με βάση ρόλους που έχουν προκαθορισμένα δικαιώματα. Ωστόσο, για μεγάλο αριθμό χρηστών με βάση το μοντέλο αυτό, καθίσταται δύσκολη η διαχείριση των πληροφοριών που αφορούν σε ρόλους και δικαιώματα, λόγω του μεγάλου αριθμού πινάκων που απαιτούνται και λόγω του μεγάλου αριθμού παραμέτρων των πινάκων αυτών που απαιτούνται προκειμένου για τη διαχείριση του συνασπισμού.

Οι (Shafiq et al, 2005) περιγράφουν ένα αλγόριθμο σχηματισμού μιας καθολικής πολιτικής που ενοποιεί τις μεμονωμένες πολιτικές πρόσβασης των συμμετεχόντων Π.Σ. Στη συνέχεια προκειμένου για την επίλυση των αντικρουόμενων περιορισμών περιγράφεται μια τεχνική βασισμένη στη χρήση τεχνικών ακέραιου προγραμματισμού. Στην προσέγγιση αυτή, ένα κύριο μειονέκτημα σχετίζεται με την ικανότητα χειρισμού των αλλαγών στις επιμέρους πολιτικές, αφού για να εκτελεστεί κάθε φορά ο αλγόριθμος απαιτείται πολυωνυμικός χρόνος. Επίσης δεν υπάρχει η δυνατότητα να ληφθούν υπόψη οι προτιμήσεις των συμμετεχόντων περιοχών, όπως γίνεται στη δική μας περίπτωση με τη χρήση ασαφούς λογικής. Οι Barker και Stuckey (Barker et al, 2003) χρησιμοποιούν λογικό προγραμματισμό με περιορισμούς και παρουσιάζουν μια τεχνική αναπαράστασης πολλαπλών πολιτικών. Η προσέγγιση αυτή δεν λαμβάνει υπόψη της υποστήριξη για περιορισμούς που οφείλονται στις επιμέρους περιοχές (όπως για παράδειγμα περιορισμοί πρόσβασης σε συγκεκριμένους πόρους), ενώ και η αντιστοίχηση δικαιωμάτων γίνεται με μη ευέλικτο τρόπο. Αντίθετα στη δική μας προσέγγιση προτείνεται μια λύση που επιτρέπει ένα ευέλικτο τρόπο επίλυσης του προβλήματος, που λαμβάνει υπόψη του και τις προτιμήσεις των συμμετεχόντων Π.Σ. (εκπεφρασμένων με τη μορφή ασαφών συσχετίσεων).

Στην προσέγγιση των Bonatti και λοιπών (Bonatti et al, 2000)(Bonatti et al, 2002), προτείνεται μια άλγεβρα για τη δημιουργία μιας συνολικής πολιτικής από απλούστερες πολιτικές. Η γλώσσα αυτή βασίζεται στη χρήση λογικής πρώτου βαθμού. Στις αδυναμίες της συγκεκριμένης προσέγγισης μπορούμε να διακρίνουμε τη δυσκολία υλοποίησης των προτεινόμενων λύσεων και ενσωμάτωσης τους σε κάποιον από τους υπάρχοντες μηχανισμούς πρόσβασης. Παράλληλα δεν υπάρχει και σε αυτή την προσέγγιση δυνατότητα να καθοριστούν οι προτιμήσεις των συμμετεχόντων μερών.

6.6. Συμπεράσματα

Η δημιουργία δυναμικά μεταβαλλόμενων συνασπισμών είναι μια πολύπλοκη διαδικασία, λόγω της αναγκαιότητας να ικανοποιηθούν μια σειρά από περιορισμοί συχνά αντικρουόμενων συμφερόντων. Προκειμένου για την επίτευξη ικανοποιητικής λύσης στο πρόβλημα της διαλειτουργικότητας και της συνεργασίας των Π.Σ. που διέπονται από διαφορετικές πολιτικές, η εισαγωγή τεχνικών μερικής ικανοποίησης των περιορισμών προκύπτει ως ευέλικτη λύση. Στα πλαίσια αυτά, δείξαμε ότι σε

προβλήματα όπου η παράλληλη ύπαρξη πολλαπλών περιορισμών οδηγεί το σύστημα σε αδιέξοδα, η χρήση τεχνικών μερικής ικανοποίησης περιορισμών και οι συναφείς τεχνικές ασαφούς λογικής μπορούν να οδηγήσουν σε λύσεις που κατά τα άλλα δεν θα ήταν εφικτό να επιτευχθούν.

Επίσης δείξαμε πώς μπορούν να ενσωματωθούν οι μετρικές ασαφούς λογικής στη διαδικασία εκτίμησης του βαθμού ικανοποίησης περιορισμών, και να ενσωματωθούν στο σύστημα επιβολής ελέγχων πρόσβασης (συγκεκριμένα στο PDP) κατά τη διαδικασία εκτίμησης των αιτημάτων προσπέλασης. Με αυτή τη διαδικασία μπορούμε να περιορίσουμε δραστικά το διαχειριστικό φόρτο του συστήματος αφού μη κρίσιμοι περιορισμοί (που θα οδηγούσαν σε αποτυχία τις προσπάθειες δημιουργίας συνασπισμού ή θα απαιτούσαν ειδικό χειρισμό από τους διαχειριστές του συστήματος), τώρα μπορούν να ικανοποιηθούν.

ΚΕΦΑΛΑΙΟ 7 - Περιβάλλον διαχείρισης πολλαπλών πολιτικών ασφάλειας και επιβολής ελέγχου πρόσβασης σε συνεργαζόμενα συστήματα.

Στο παρόν κεφάλαιο παρουσιάζεται το σύστημα επιβολής ελέγχου πρόσβασης και διαχείρισης πολλαπλών πολιτικών σε περιβάλλον συνασπιζόμενων Π.Σ. Η λειτουργία του και ο σχεδιασμός του βασίζονται στα ερευνητικά συμπεράσματα των κεφαλαίων 4, 5 και 6 όπως αυτά διατυπώνονται και στις δημοσιεύσεις (Belsis et al, 2005b), (Belsis et al, 2005c), (Belsis et al, 2005d), (Belsis et al, 2005e), (Belsis et al, 2005g), (Belsis et al, 2005h), (Malatras et al, 2005a), (Malatras et al, 2005b), (Belsis et al, 2006c). Προκειμένου για τη σχεδίαση του συστήματος, κύρια μέριμνα ήταν το σύστημα που θα υλοποιηθεί να διαθέτει τα ακόλουθα χαρακτηριστικά:

- Να αξιοποιεί μία υπάρχουσα γλώσσα περιγραφής πολιτικών, με στόχο να είναι εφικτή η μεταφορά των προτεινόμενων λύσεων σε περιβάλλοντα πολλαπλών πολιτικών, χωρίς ωστόσο να απαιτείται η δημιουργία μιας καινούργιας γλώσσας και των συνοδευτικών της εργαλείων.
- Να διαθέτει μια σειρά από διαλειτουργικά χαρακτηριστικά που να του δίνουν τη δυνατότητα να μπορεί να εγκατασταθεί σε πολλές διαφορετικές κατηγορίες εφαρμογών ανεξάρτητα από το περιβάλλον ανάπτυξής τους.
- Να διαθέτει δυνατότητα κλιμάκωσης, υποστηρίζοντας τη δυνατότητα συνεργασίας μεταξύ μεγάλου αριθμού διαφορετικών οργανισμών.

Στο πιλοτικό σύστημα που αναπτύχθηκε λεπτομέρειες του οποίου θα περιγραφούν στη συνέχεια, υποστηρίζεται η δυνατότητα επιβολής ελέγχων πρόσβασης μεταξύ δύο συστημάτων αμοιβαία και για οποιονδήποτε ρόλο, ανεξάρτητα από το σύστημα στο οποίο ανήκει, λετουργεί δηλαδή ως κατανεμημένο σύστημα. Ωστόσο, η εμφάνιση δύο μόνο συστημάτων αποφάσεων πολιτικής (PDP) και ενός σημείου επιβολής πολιτικής (PEP) είναι εντελώς τυπική και μπορεί να επεκταθεί με χρήση περισσότερων από τρεις υπολογιστές (όπως ίσχυε στα πειράματα που έγιναν για να ελέγξουν την ορθή λειτουργία του συστήματος).

7.1 Σύστημα επιβολής ελέγχων πρόσβασης σε κατανεμημένα περιβάλλοντα

Το προτεινόμενο σύστημα επιβολής ελέγχων πρόσβασης σε περιβάλλοντα συνεργαζόμενων αυτόνομων συστημάτων, έχει σκοπό την εφαρμογή των αρχών που αναπτύχθηκαν στα κεφάλαια 4 και 6. Συγκεκριμένα αποσκοπεί:

- Στην αξιοποίηση διαδεδομένων και πρότυπων τεχνολογιών που αφορούν σε πολιτικές ασφάλειας, με στόχο τη δυνατότητα πρακτικής εφαρμογής του σε μεγάλο πλήθος εφαρμογών.
- Στο να δώσει ιδιαίτερη έμφαση στο διαλειτουργικό χαρακτήρα της αναπτυσσόμενης λύσης.
- Στην υποστήριξη του νέου μεθοδολογικού πλαισίου για την επίλυση συγκρούσεων μεταξύ διαφορετικών πολιτικών με χρήση ασαφούς λογικής όπως αυτό περιγράφηκε στο κεφάλαιο 6.

Μεταξύ των χαρακτηριστικών που θα πρέπει ένα τέτοιο σύστημα να διαθέτει είναι:

- Η υποστήριξη της δυνατότητας αναπαράστασης των πολιτικών να γίνεται από κατάλληλο γραφικό περιβάλλον.

- Να προσφέρει τη δυνατότητα ελέγχου της εφαρμογής των πολιτικών (Κοκολάκης 2000).
- Να μπορεί να δίνει με απλό τρόπο, έλεγχο στο χρήστη επί των ενεργειών στα αρχεία πολιτικής. Η συγκεκριμένη απαίτηση επιβάλλεται λόγω του μειονεκτήματος της XACML να είναι κάπως δυσνόητη στο χρήστη, λόγω του βασισμένου στην XML συντακτικού της (Damianou, 2002).
- Το σύστημα επιβολής πολιτικής (PEP) καθώς και το σύστημα επιβολής αποφάσεων πολιτικής (PDP) να αυτοματοποιούν τη διαδικασία αποστολής και λήψης των συνταγμένων σε XML μηνυμάτων αιτήσεων πρόσβασης, καθώς και των σχετικών απαντήσεων.

Αν και το σύνολο των απαιτήσεων περιλαμβάνει ενδεχόμενα περισσότερες και πιο εκτενείς προδιαγραφές, πολλές από τις οποίες έχουν γίνει σαφείς και από τα προηγούμενα κεφάλαια, τα συγκεκριμένα χαρακτηριστικά που αναφέρθηκαν καλύπτουν μία σειρά από τις πλέον σημαντικές προδιαγραφές και περιορισμούς για τους οποίους έγινε προσπάθεια να ενσωματωθούν στο αναπτυσσόμενο σύστημα, στα πλαίσια της υλοποίησης που περιγράφεται στη συνέχεια.

7.2 Αρχιτεκτονική του συστήματος

7.2.1 Λειτουργικά χαρακτηριστικά του συστήματος

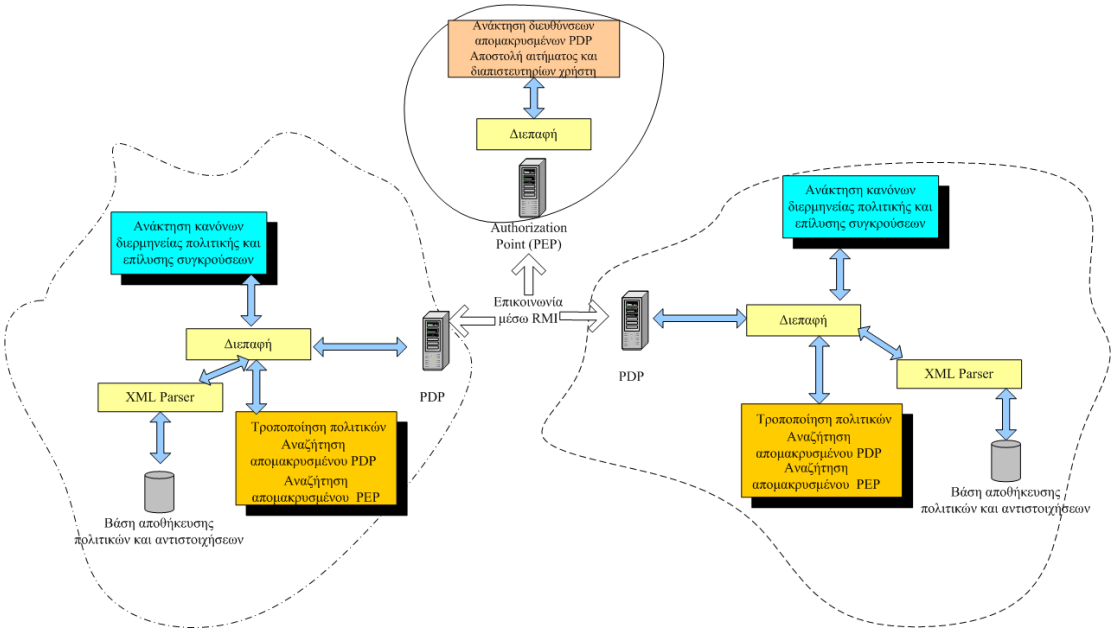
Μεταξύ των βασικών απαιτήσεων για την ανάπτυξη του συστήματος κατανεμημένης επιβολής ελέγχου πρόσβασης και αντιστοίχησης των διαφορετικών πολιτικών μεταξύ συνασπισμών αυτόνομων συστημάτων, είναι η ανάγκη ανεξαρτησίας του από το είδος της εφαρμογής, καθώς και η ανάγκη ενσωμάτωσης όσο το δυνατόν περισσότερων διαλειτουργικών χαρακτηριστικών, ώστε να καθιστούν εφικτή την αξιοποίησή του από μεγάλο πλήθος εφαρμογών.

Το πρωτότυπο που αναπτύχθηκε βασιζόμενο κατά κύριο λόγο στα συμπεράσματα των κεφαλαίων 4 και 6, επικοινωνεί με το εκάστοτε σύστημα σε επίπεδο εφαρμογής, χωρίς να απαιτείται η ενσωμάτωσή του στην εκάστοτε εφαρμογή.

Τα επιμέρους τμήματα του συστήματος είναι:

1. Το σύστημα αποφάσεων πολιτικής, (Policy Decision Point – PDP)
2. Το σύστημα επιβολής πολιτικής (Policy Enforcement Point – PEP)
3. Η βάση αποθήκευσης πολιτικών
4. Το σύστημα ανάκτησης πολιτικών και εξαγωγής της πληροφορίας από το XML αρχείο
5. Τα γραφικά εργαλεία διεπαφής που επιτρέπουν την διαχείριση των αιτήσεων και την τροποποίηση των αρχείων πολιτικής και τη διαμόρφωση των αιτήσεων σε XACML συμβατή μορφή

Η εικ. 7.1 απεικονίζει τη γενική αρχιτεκτονική του συστήματος, όπου εμφανίζονται οι δομικές μονάδες που το αποτελούν καθώς και ο μηχανισμός επικοινωνίας μεταξύ τους.



Εικόνα 7-1 Γενική αρχιτεκτονική του συστήματος επιβολής ελέγχου προσπέλασης

7.2.2 Η βάση αποθήκευσης πολιτικών

Στη βάση αποθήκευσης πολιτικών αποθηκεύονται οι πολιτικές όπως αυτές έχουν δημιουργηθεί σε XML συμβατή μορφή από τους διαχειριστές του συστήματος. Η τροποποίηση των πολιτικών μπορεί να γίνει και με τη βοήθεια της διεπαφής διαχείρισης του συστήματος, που έχει ενσωματωθεί στη διεπαφή διαχείρισης του PDP. Σαν ενότητα λογισμικού ωστόσο η βάση διαχείρισης πολιτικών, καθώς και το γραφικό κομμάτι διαχείρισης των πολιτικών, είναι ανεξάρτητα ως προς τη λειτουργία τους από το PDP.

7.2.3 Το σύστημα αποφάσεων πολιτικής (Policy Decision Point-PDP)

Η ενότητα λογισμικού που διαχειρίζεται τις αποφάσεις που αφορούν στη διερμηνεία και εφαρμογή των πολιτικών, αποτελείται από την αντίστοιχη διεπαφή που δίνει τη δυνατότητα αποστολής αιτήσεων για συγκεκριμένους πόρους και από το τμήμα που ανακτά την κατάλληλη πολιτική από τη βάση φύλαξης πολιτικών και αξιολογεί το αίτημα σε σχέση με την υπάρχουσα πολιτική. Δεδομένης της ύπαρξης συγκεκριμένου αιτήματος από κάποιο ρόλο, το PDP μέσω της διεπαφής κωδικοποιεί το αίτημα σε XACML συμβατή μορφή και αναλαμβάνει να ελέγξει την εγκυρότητά του σε σχέση με τις διαθέσιμες πολιτικές. Ανάμεσα στις δυνατότητες του PDP, είναι η σύνδεση του συστήματος με το απομακρυσμένο PDP με χρήση της τεχνολογίας Remote Method Invocation (Java-RMI) δίνοντας ως μοναδική παράμετρο τη διεύθυνση του απομακρυσμένου PDP. Έτσι, πρώτα ελέγχεται η τοπική πολιτική για το αν ένα αίτημα για τη λήψη πόρων είναι έγκυρο. Σε περίπτωση που είναι, δίνεται εντολή στο PEP να επιτρέψει το αίτημα και να δώσει πρόσβαση στον αιτούμενο πόρο. Σε αντίθετη περίπτωση, πριν να δοθεί αρνητική απάντηση, ελέγχεται το απομακρυσμένο PDP αν υπάρχει σχετική αντιστοίχηση και στην περίπτωση που υπάρχει εξουσιοδοτείται ο χρήστης. Σε αντίθετη περίπτωση, το αίτημα απορρίπτεται.

7.2.4 Το σημείο επιβολής της πολιτικής (Policy Enforcement Point - PEP)

Το σημείο επιβολής της πολιτικής έχει ως αντικείμενο την επιβολή των τελικών αποφάσεων που λαμβάνονται από το PDP και ουσιαστικά αποτελεί το σημείο που αναλαμβάνει την εφαρμογή των κανόνων πρόσβασης. Στην υλοποίηση που έλαβε χώρα στα πλαίσια της διατριβής (Belsis et al, 2005b) (Belsis et al, 2005c) (Belsis et al, 2006b) (Belsis et al, 2006c), προκειμένου για τη δυνατότητα εφαρμογής ελέγχου πρόσβασης σε περιβάλλοντα πολλαπλών πολιτικών το PEP ενημερώνεται για τη διεύθυνση ενός από τα PDP και κάθε φορά που αποστέλλεται ένα αίτημα για κάποιους πόρους, αυτό προωθείται στο PDP προκειμένου να διερευνηθεί η εγκυρότητά του. Σε περίπτωση που το PDP δεν μπορέσει να αποφανθεί σύμφωνα με τις διαθέσιμες πολιτικές, αναζητά το απομακρυσμένο PDP προκειμένου να ελεγχθεί βάσει του μηχανισμού αντιστοιχήσεων (policy mappings), αν υπάρχει σε αυτό πολιτική που να επιτρέπει την εξουσιοδότηση του αιτήματος. Σε περίπτωση που δεν υπάρχει σε κανένα PDP, τότε το μήνυμα που εμφανίζεται είναι ‘‘not-applicable’’. Αν υπάρχει σαφώς εκπεφρασμένη πολιτική που δείχνει ότι το αίτημα δεν πρέπει να γίνει αποδεκτό, τότε λαμβάνεται μήνυμα deny.

7.2.5 Υποσύστημα ανίχνευσης – επίλυσης συγκρούσεων με χρήση ασαφούς λογικής

Όπως περιγράφηκε στο προηγούμενο κεφάλαιο και στην εργασία (Belsis et al, 2006c), στα πλαίσια της διατριβής προτείνεται μία τεχνική επίλυσης αντικρουόμενων απαιτήσεων πολιτικών βασισμένου στη χρήση ασαφούς λογικής και προγραμματισμού με χρήση ασαφών περιορισμών ειδικότερα. Ο μηχανισμός επίλυσης συγκρούσεων είναι ενσωματωμένος στην επεκταμένη έκδοση του PDP, δίνει δε τη δυνατότητα εκτίμησης του βαθμού ικανοποίησης των προτιμήσεων των διαφορετικών περιοχών που συμμετέχουν στο συνασπισμό. Παράλληλα, από τη διεπαφή διαχείρισης του PDP παρέχεται η δυνατότητα καταχώρησης νέων πολιτικών που αφορούν σε επιτρεπτούς συνδυασμούς της μορφής <R.O,P> (εικ. 7.7). Κατόπιν, δίνεται η δυνατότητα αξιολόγησης του βαθμού ικανοποίησης των διαφόρων τριάδων, και με βάση αντίστοιχα τον καθορισμό μίας τιμής κατωφλίου για τις επιτρεπτές τριάδες, την εύρεση συνδυασμών που μπορούν να επιτραπούν (και συνεπώς και αυτών που δεν είναι επιτρεπτοί).

7.3 Πιλοτική εφαρμογή

Το πιλοτικό σύστημα που περιγράφεται στη συνέχεια, αναπτύχθηκε στα πλαίσια του ελέγχου της δυνατότητας εφαρμογής των αρχών και των προτεινόμενων λύσεων που περιγράφηκαν στις εργασίες (Belsis et al, 2005e) (Belsis et al, 2005h), (Belsis, 2006e) (Belsis et al, 2006c). Προκειμένου για την ανάπτυξη του γραφικού περιβάλλοντος, των PDP, PEP καθώς και του υποσυστήματος ανίχνευσης και επίλυσης συγκρούσεων χρησιμοποιήθηκε η γλώσσα Java, ενώ για τη σύνταξη των πολιτικών και των αιτημάτων πρόσβασης χρησιμοποιήθηκε το συντακτικό της γλώσσας XACML. Η επικοινωνία των διαφορετικών PDP, PEP γίνεται με χρήση τεχνολογίας Remote Method Invocation (RMI).

7.3.1 Η γλώσσα XACML

Η γλώσσα XACML είναι μία πρότυπη γλώσσα περιγραφής πολιτικών η οποία κωδικοποιείται σε XML. Υποστηρίζει τη δυνατότητα περιγραφής χρονικών περιορισμών, επίλυσης συγκρούσεων, περιγραφής κανόνων πρόσβασης για ένα

σύνολο αντικειμένων ανάλογα με τα χαρακτηριστικά του περιβάλλοντος στο οποίο ανήκουν (context based authorization) κοκ.
Στον πίνακα 7.1 εμφανίζεται μία πολιτική σε XACML που επιτρέπει σε όλους τους χρήστες που προέρχονται από μία περιοχή (domain) να εξουσιοδοτούνται να έχουν πρόσβαση σε όλους τους πόρους ενός καταλόγου. Στον πίνακα 7.2 περιγράφεται μία πολιτική που επιτρέπει σε όλους τους χρήστες που ανήκουν σε μία συγκεκριμένη περιοχή να αποκτούν δικαίωμα ανάγνωσης στους πόρους που ελέγχει το PDP και για όλες τις ώρες μεταξύ 9:00 και 17:00. Κάθε αίτημα πρόσβασης που δεν υπακούει στον παραπάνω κανόνα απορρίπτεται. Τα σημαντικά σημεία των δύο αυτών πολιτικών έχουν υπογραμμιστεί, ώστε να γίνονται ευκολότερα αντιληπτά στον αναγνώστη. Ένα από τα 'μειονεκτήματα' της συγκεκριμένης γλώσσας είναι το δύσκολο συντακτικό της που την καθιστά δυσανάγνωστη (Damianou 2002). Οι περιορισμοί αυτοί ωστόσο οφείλονται στην ανάγκη υποστήριξης αναπαράστασης σε XML μορφή, γεγονός ωστόσο που της δίνει σημαντικό προβάδισμα έναντι άλλων γλωσσών σε σχέση με τα διαλειτουργικά της χαρακτηριστικά. Άλλωστε πολλές από τις υπάρχουσες γλώσσες καταγραφής είτε δεν έχουν υποστήριξη από εργαλεία ή δεν διαθέτουν επαρκή τεκμηρίωση, είτε έχουν ως μελλοντικό στόχο την υποστήριξη της αναπαράστασης τους σε XML συμβατή μορφή (Belsis et al, 2005h).

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy xmlns="urn:oasis:names:tc:xacml:1.0:policy"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
PolicyId="ObligationPolicy"RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">
<Description>
This protects access to all documents in the "sensitive" directory.
All users @users.example.com are allowed to read this documents,
but to all other access is denied. Logging is done all access attempts
using Obligations, though the logged information is different
depending on whether or not the access attempt is allowed.
  </Description>

  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
          <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">users.example.com</AttributeValue>
          <SubjectAttributeDesignator
DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name"

AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"/>
        </SubjectMatch>
      </Subject>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-match">
          <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">http://server.example.com/sensitive/.*</AttributeValue>
          <ResourceAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#string"

```

```
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"/>
        </ResourceMatch>
      </Resource>
    </Resources>
    <Actions>
      <AnyAction/>
    </Actions>
  </Target>

  <Rule RuleId="AllowAllReads" Effect="Permit">
    <Target>
      <Subjects>
        <AnySubject/>
      </Subjects>
      <Resources>
        <AnyResource/>
      </Resources>
      <Actions>
        <Action>
          <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">read</Attrib
uteValue>
            <ActionAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#string"

AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"/>
          </ActionMatch>
        </Action>
      </Actions>
    </Target>
  </Rule>

  <Rule RuleId="DenyOtherActions" Effect="Deny"/>

  <Obligations>
    <Obligation ObligationId="LogSuccessfulRead"
FulfillOn="Permit">
      <AttributeAssignment AttributeId="user"
DataType="http://www.w3.org/2001/XMLSchema#anyURI">urn:oasis:
names:tc:xacml:1.0:subject:subject-id</AttributeAssignment>
      <AttributeAssignment AttributeId="resource"
DataType="http://www.w3.org/2001/XMLSchema#anyURI">urn:oasis:
names:tc:xacml:1.0:resource:resource-id</AttributeAssignment>
    </Obligation>
    <Obligation ObligationId="LogInvalidAccess" FulfillOn="Deny">
      <AttributeAssignment AttributeId="user"
DataType="http://www.w3.org/2001/XMLSchema#anyURI">urn:oasis:
names:tc:xacml:1.0:subject:subject-id</AttributeAssignment>
      <AttributeAssignment AttributeId="resource"
DataType="http://www.w3.org/2001/XMLSchema#anyURI">urn:oasis:
names:tc:xacml:1.0:resource:resource-id</AttributeAssignment>
      <AttributeAssignment AttributeId="action"
DataType="http://www.w3.org/2001/XMLSchema#anyURI">urn:oasis:
names:tc:xacml:1.0:action:action-id</AttributeAssignment>
    </Obligation>
  </Obligations>
</Policy>
```

Πίνακας 7.8 XACML πολιτική που επιτρέπει εξουσιοδότηση βάσει μεταβλητών περιβάλλοντος

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy xmlns="urn:oasis:names:tc:xacml:1.0:policy"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      PolicyId="TimeRangePolicy"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:ordered-permit-overrides">

  <Description>
    Between 9am and 5pm local time, allow anyone to open the main door. All other times, only allow authorized people (ie, those with an email address @users.example.com). Deny in all other cases.
  </Description>

  <Target>
    <Subjects>
      <AnySubject/>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">main-door</AttributeValue>
          <ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"/>
        </ResourceMatch>
      </Resource>
    </Resources>
    <Actions>
      <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">open</AttributeValue>
          <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"/>
        </ActionMatch>
      </Action>
    </Actions>
  </Target>

  <Rule RuleId="EveryoneDuringBusinessHours" Effect="Permit">
    <Condition FunctionId="http://research.sun.com/projects/xacml/names/function#time-in-range">
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">
        <EnvironmentAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#time"
          AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"/>
      </Apply>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">09:00:00</AttributeValue>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">17:00:00</Attrib
```

```
uteValue>
    </Condition>
  </Rule>

  <Rule RuleId="EmployeesAlways" Effect="Permit">
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">users.example
.com</AttributeValue>
            <SubjectAttributeDesignator
DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name"

AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"/>
          </SubjectMatch>
        </Subject>
      </Subjects>
      <Resources>
        <AnyResource/>
      </Resources>
      <Actions>
        <AnyAction/>
      </Actions>
    </Target>
  </Rule>

  <Rule RuleId="DenyAllOthers" Effect="Deny"/>

</Policy>
```

Πίνακας 7.9 XACML πολιτική που επιτρέπει την εξουσιοδότηση μεταξύ συγκεκριμένων χρονικών ορίων.

7.3.2 Δημιουργία αιτήσεων – απαντήσεων σε συντακτικό XACML

Στα επόμενα θα θεωρήσουμε ένα παράδειγμα αιτήματος ανάγνωσης ενός πόρου στην XACML (OASIS, 2004). Το παραπάνω αίτημα υποβάλλεται στο PDP, το οποίο φορτώνει από τη βάση πολιτικών το αντίστοιχο αρχείο πολιτικής. Για περισσότερες πληροφορίες ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει στο εγχειρίδιο της γλώσσας XACML. Στο συγκεκριμένο παράδειγμα ο χρήστης με email: pbelsis@aegean.gr ζητά να αποκτήσει πρόσβαση στο αρχείο file://aegean/members/docs/pbelsis, του στο domain: aegean.gr, που περιέχει προσωπικά στοιχεία του.

Στην XACML, το αίτημα μοιάζει ως ακολούθως:

```
[a38]  <?xml version="1.0" encoding="UTF-8"?>
[a39]  <Request xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:cd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
[a40]  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:cd
http://docs.oasis-open.org/xacml/access_control-xacml-2.0-context-schema-
cd.xsd">
[a41]   <Subject>
[a42]    <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name">
[a43]     <AttributeValue>
[a44]     pbelsis@aegean.gr
[a45]     </AttributeValue>
[a46]    </Attribute>
[a47]   </Subject>
[a48]   <Resource>
```

```
[a49]    <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI">
[a50]     <AttributeValue>
[a51]      file://aegean/members/docs/pbelsis
[a52]     </AttributeValue>
[a53]    </Attribute>
[a54]   </Resource>
[a55]   <Action>
[a56]    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-
id" DataType="http://www.w3.org/2001/XMLSchema#string">
[a57]     <AttributeValue>
[a58]      read
[a59]     </AttributeValue>
[a60]    </Attribute>
[a61]   </Action>
[a62]   <Environment/>
[a63]  </Request>
```

Πίνακας 7.10 Αίτημα ανάγνωσης πόρου στην XACML

Οι γραμμές [a38] - [a40] περιέχουν τις πληροφορίες επικεφαλίδας από ο αίτημα. Το στοιχείο <Subject> περιέχει ένα ή περισσότερα πεδία (*attributes*) της οντότητας που αιτείται ένα πόρο. Μπορούμε να έχουμε πολλαπλά υποκείμενα (*subjects)*, και καθένα να έχει πολλαπλά πεδία (*attributes*). Στο παράδειγμά μας στις γραμμές [a41] - [a47] υπάρχει μόνο ένα υποκείμενο και αυτό έχει μόνο ένα πεδίο: την ταυτότητα του υποκειμένου που εκφράζεται από το email του: pbelsis@aegean.gr. Το στοιχείο <Resource> περιέχει ένα ή περισσότερα attributes στα οποία το υποκείμενο έχει πρόσβαση. Στις γραμμές [a48] - [a54] περιέχεται ο πόρος στον οποίο αιτείται η πρόσβαση που προσδιορίζεται από το (Universal Resource Identifier –URI) του πόρου, που είναι " file://aegean/members/docs/pbelsis ".
Το στοιχείο <Action> περιέχει ένα ή περισσότερα πεδία (attributes) της πράξης την οποία το υποκείμενο αιτείται επί του πόρου. Σε κάθε αίτημα μπορούμε να υποβάλουμε την εκτέλεση μίας μόνο ενέργειας επί ενός πόρου. Οι γραμμές [a55] - [a61] περιγράφουν την ταυτότητα της ενέργειας που στην προκειμένη περίπτωση είναι ανάγνωση "read".
Το στοιχείο περιβάλλοντος <Environment> [a62], είναι κενό.
Στη γραμμή [a63] κλείνει το αίτημα.
Το PDP επεξεργάζεται το αίτημα εντοπίζοντας την κατάλληλη πολιτική στη βάση πολιτικών. Συγκρίνει το υποκείμενο (subject), τον αιτούμενο πόρο (resource), την αιτούμενη ενέργεια (action) και τις μεταβλητές περιβάλλοντος (environment) με αυτά της διαθέσιμης πολιτικής.
Σαν αποτέλεσμα της αξιολόγησης του αιτήματος και της διαθέσιμης πολιτικής, επιστρέφεται η απάντηση από το PDP. Στην προκειμένη περίπτωση, ο αλγόριθμος συνδυασμού κανόνων (***rule-combining algorithm)*** που έχει καθοριστεί για την πολιτική καθορίζει ότι η απάντηση που πρέπει να δοθεί στο παραπάνω αίτημα είναι "NotApplicable". Το μήνυμα απάντησης είναι όπως το ακόλουθο (Πιν. 7.11):

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
[a64] <Response xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:cd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:cd
http://docs.oasis-open.org/xacml/xacml-core-2.0-context-schema-cd.xsd">
[a65]  <Result>
[a66]   <Decision>NotApplicable</Decision>
[a67]  </Result>
[a68] </Response>
```

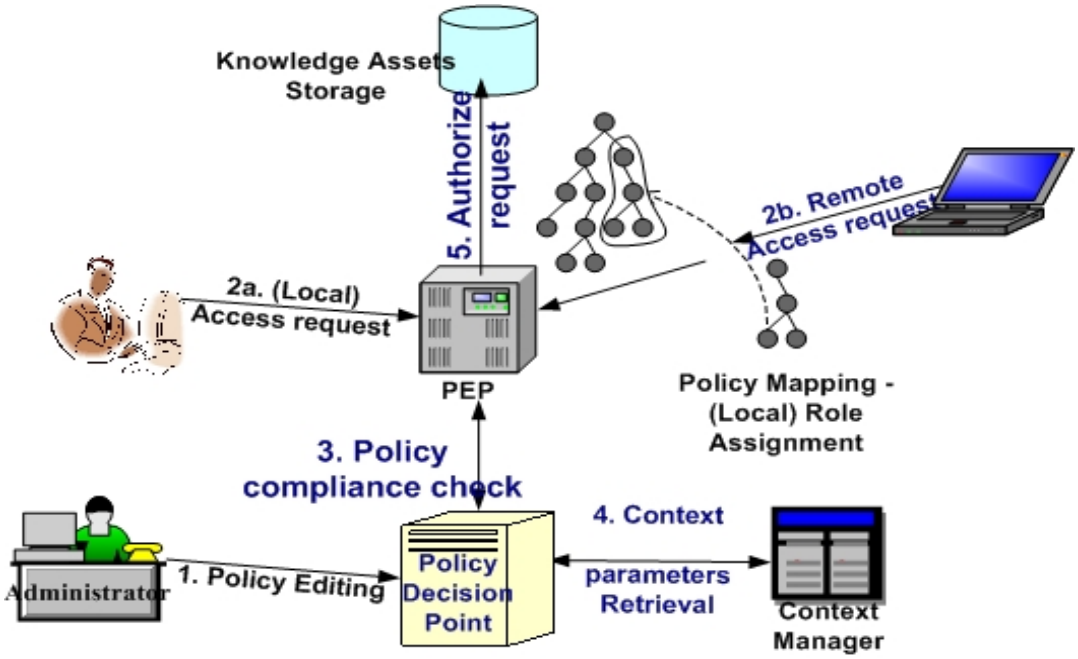
Πίνακας 7.11 Μύνημα απάντησης σε μορφή XACML

Οι γραμμές 0 - [a64] περιέχουν την πληροφορία επικεφαλίδων αντίστοιχα όπως και στο αρχείο πολιτικής αλλά και στο αντίστοιχο του αιτήματος. Το στοιχείο <Result> στις γραμμές [a65] - [a67] περιέχει το αποτέλεσμα αξιολόγησης της απόφασης με βάση την πολιτική. Η απάντηση μπορεί να είναι (επιτρεπτό αίτημα) "Permit", (άρνηση) "Deny", (μη εφαρμόσιμο) "NotApplicable" ή ακαθόριστο "Indeterminate". Επομένως το PEP πρέπει να αρνηθεί την πρόσβαση σε αυτή την περίπτωση. Στη γραμμή [a68] κλείνει η απάντηση.

Το σύστημα εφαρμογής κανόνων προσπέλασης που υλοποιεί τις παραπάνω αρχές για τη δημιουργία ενός κατανεμημένου συστήματος εξουσιοδότησης έχει υλοποιηθεί με βάση της βασικές αρχές της XACML, με κυριότερη διαφορά την επέκταση που αφορά στην εφαρμογή των κανόνων για περιβάλλοντα πολλαπλών πολιτικών.

Όπως αναφέρθηκε σε προηγούμενη ενότητα, τα βασικά τμήματα του πλαισίου επιβολής ελέγχου πρόσβασης είναι: το σημείο επιβολής πολιτικών Policy Enforcement Point (PEP) που είναι υπεύθυνο για την εφαρμογή των αρχών της πολιτικής, το σημείο αποφάσεων πολιτικής Policy Decision Point (PDP), όπου εξετάζεται το σύννομο ενός αιτήματος σε σχέση με την υπάρχουσα πολιτική και που είναι υπεύθυνο επίσης για την τήρηση του μητρώου αντιστοιχήσεων ρόλων και ο χειριστής πλαισίου (context handler- CH) που συλλέγει πληροφορίες που αφορούν στη φύλαξη παραμέτρων πλαισίου και παραμέτρους που αφορούν στην αξιολόγηση μεταβλητών που αφορούν στην διευκόλυνση της εφαρμογής της πολιτικής για μια σειρά από ρόλους που προέρχονται από τον ίδιο οργανισμό.

Η γενική λειτουργία του συστήματος επιβολής ελέγχων πρόσβασης είναι η ακόλουθη (εικ. 7.2): Ο διαχειριστής του συστήματος συγγράφει την πολιτική και τοποθετεί τις ενημερωμένες εκδόσεις της στο PDP. Όταν προκύψει ένα αίτημα για κάποιον πόρο αυτό απευθύνεται στο PEP. Το PEP με τη σειρά του δημιουργεί ένα κατάλληλο μήνυμα σε γλώσσα XML (Πιν.7.3) και το αποστέλλει προς έλεγχο στο PDP. Το τελευταίο ελέγχει τη συμφωνία του αιτήματος με τις αρχές της πολιτικής. Ο Context Handler κατόπιν συλλέγει πληροφορίες που αφορούν στο πλαίσιο στο οποίο δρα το σύστημα. Όταν στο σημείο εφαρμογής πολιτικής καταφθάνει μια αίτηση για πόρους, τότε ερωτάται το σημείο απόφασης πολιτικής PDP. Στην περίπτωση που πρόκειται για ερώτημα που σχετίζεται με την τοπική πολιτική, τότε το ερώτημα απλά ελέγχεται σε σχέση με την υπάρχουσα πολιτική του οργανισμού. Στην περίπτωση που ο ρόλος δεν είναι γνωστός στο PDP τότε υποβάλλεται ερώτημα στο μητρώο διαχείρισης του συνασπισμού, προκειμένου να αναζητηθούν τυχόν αντιστοιχίσεις με υπάρχοντες ρόλους του συστήματος. Παράλληλα, με βάση την κωδικοποίηση των παραμέτρων (σε αρχείο που αποθηκεύεται στο μητρώο διαχείρισης συνασπισμού στο PDP) που αφορούν στις προτιμήσεις των συμμετεχόντων μερών, δίνεται η δυνατότητα εκτίμησης του βαθμού ικανοποίησης των αιτημάτων πρόσβασης με χρήση ασαφούς λογικής όπως περιγράφηκε στο κεφάλαιο 6.



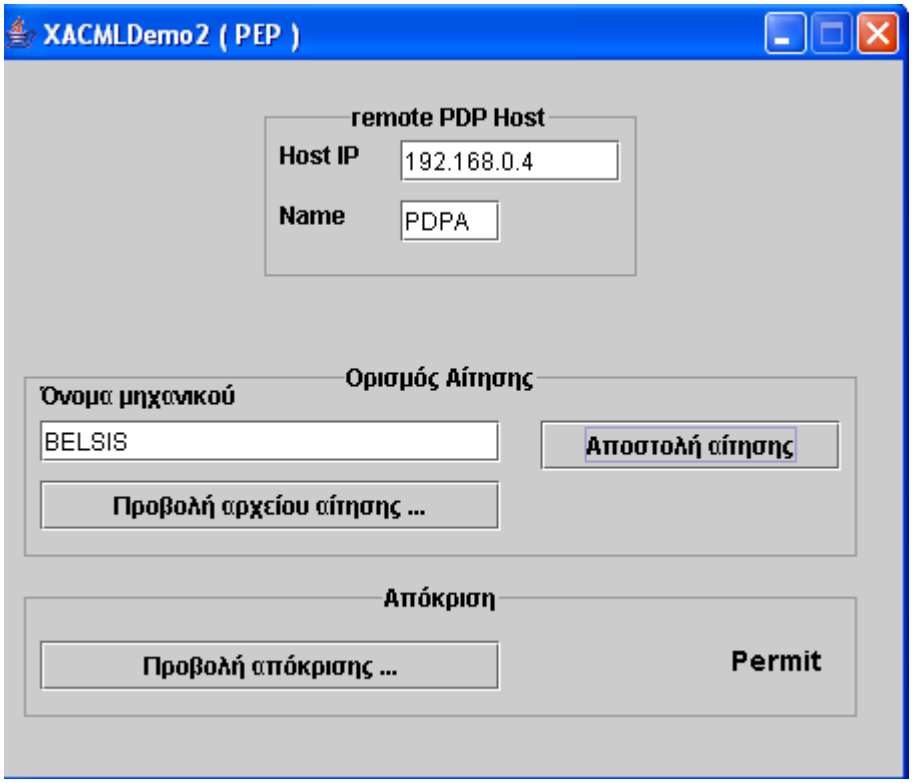
Εικόνα 7-2 Λειτουργία συστήματος επιβολής ελέγχων πρόσβασης

7.4 Σύστημα επιβολής κατανεμημένων ελέγχων πρόσβασης

Το σύστημα επιβολής ελέγχου πρόσβασης αναπτύχθηκε εξ' ολοκλήρου σε γλώσσα Java ενώ η επικοινωνία των αντίστοιχων ενοτήτων λογισμικού που το αποτελούν γίνεται με χρήση RMI. Αποτελείται στην πιλοτική του μορφή από δύο PDP και ένα PEP. Μέσω της διεπαφής διαχείρισης του PDP μπορεί ο χρήστης να διαμορφώσει την τοπική πολιτική, προσθέτοντας ή αφαιρώντας χρήστες. Η αρχική έκδοση του λογισμικού σχεδιάστηκε παρέχοντας δικαιώματα προσπέλασης σε προκαθορισμένους πόρους. Δηλαδή δεν υποστήριζε η διεπαφή την δυνατότητα τροποποίησης των αντικειμένων και των σχετικών δικαιωμάτων παρά μόνο έδινε τη δυνατότητα τροποποίησης των στοιχείων που αφορούν στους χρήστες – μηχανικούς που χρησιμοποιούν το σύστημα (εικ. 7.6). Στην εξελιγμένη έκδοση του συστήματος που αναπτύχθηκε, υπάρχει η δυνατότητα τροποποίησης των αντικειμένων που διαχειρίζεται η πολιτική καθώς επίσης και των δικαιωμάτων επί αυτών για τις διάφορες κατηγορίες χρηστών (εικ. 7.7). Παράλληλα μπορούν για κάθε τριάδα <υποκείμενο, αντικείμενο, δικαίωμα> να αντιστοιχείται και ένας βαθμός ικανοποίησης που θα αξιοποιηθεί από το τμήμα του λογισμικού που είναι υπεύθυνο για τον υπολογισμό του βαθμού ικανοποίησης του αντίστοιχου περιορισμού.

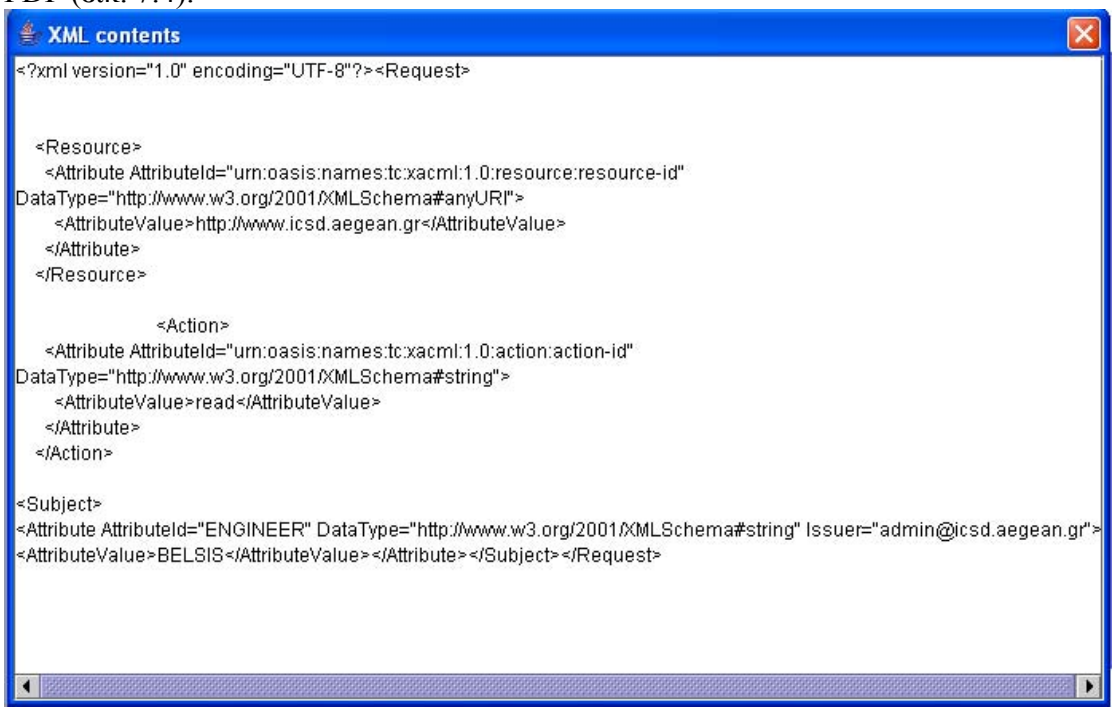
7.4.1 Το σύστημα επιβολής αποφάσεων PEP

Στην εικόνα 7.3 φαίνεται η λειτουργία του συστήματος επιβολής πολιτικής (PEP). Κατά τη λειτουργία του PEP, δίνεται σε αυτό η διεύθυνση ενός από τα PDP και κατόπιν τα PDP αναζητούν πρώτα στην τοπική πολιτική - που ανακτάται από τη βάση φύλαξης πολιτικών - την ύπαρξη σχετικής δήλωσης, που επιτρέπει την εξουσιοδότηση του αιτούμενου υποκειμένου. Σε περίπτωση που δεν υπάρχει στην τοπική πολιτική κατάλληλη δήλωση, το PDP αναζητά τα αντίστοιχα PDP άλλων οργανισμών που συμμετέχουν στο συνασπισμό, προκειμένου να ελεγχθεί (μέσω του μηχανισμού αντιστοίχησης) αν πρέπει να εγκριθεί το αίτημα ή όχι.



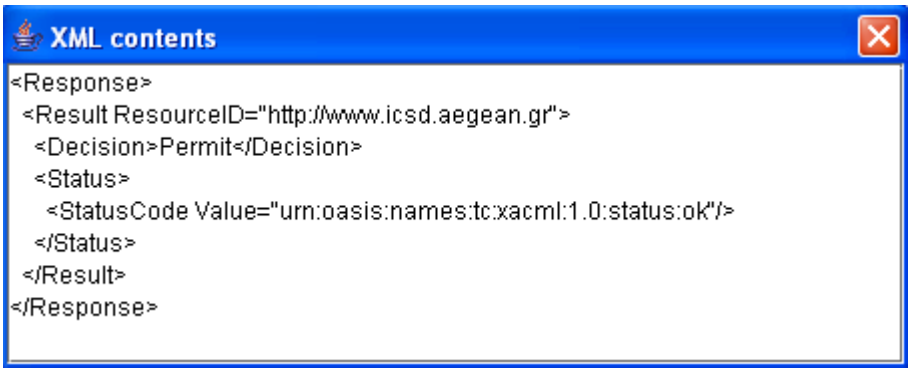
Εικόνα 7-3 Σύστημα επιβολής πολιτικής (PEP) σε λειτουργία. Στέλνοντας το PEP το αίτημα σε ένα από τα δύο PDP μπορεί η αυθεντικοποίηση να γίνεται λαμβάνοντας υπόψη τους κανόνες και των δύο. Στην προκειμένη περίπτωση για τον αιτούμενο μηχανικό η απάντηση είναι θετική (permit).

Επιλέγοντας από τη διεπαφή την επιλογή προβολής του αρχείο υ αίτησης μπορούμε να δούμε σε XACML συμβατή μορφή το μήνυμα που αποστέλλεται από το PEP στο PDP (εικ. 7.4).



Εικόνα 7-4 Το αίτημα του PEP σε XACML συμβατή μορφή

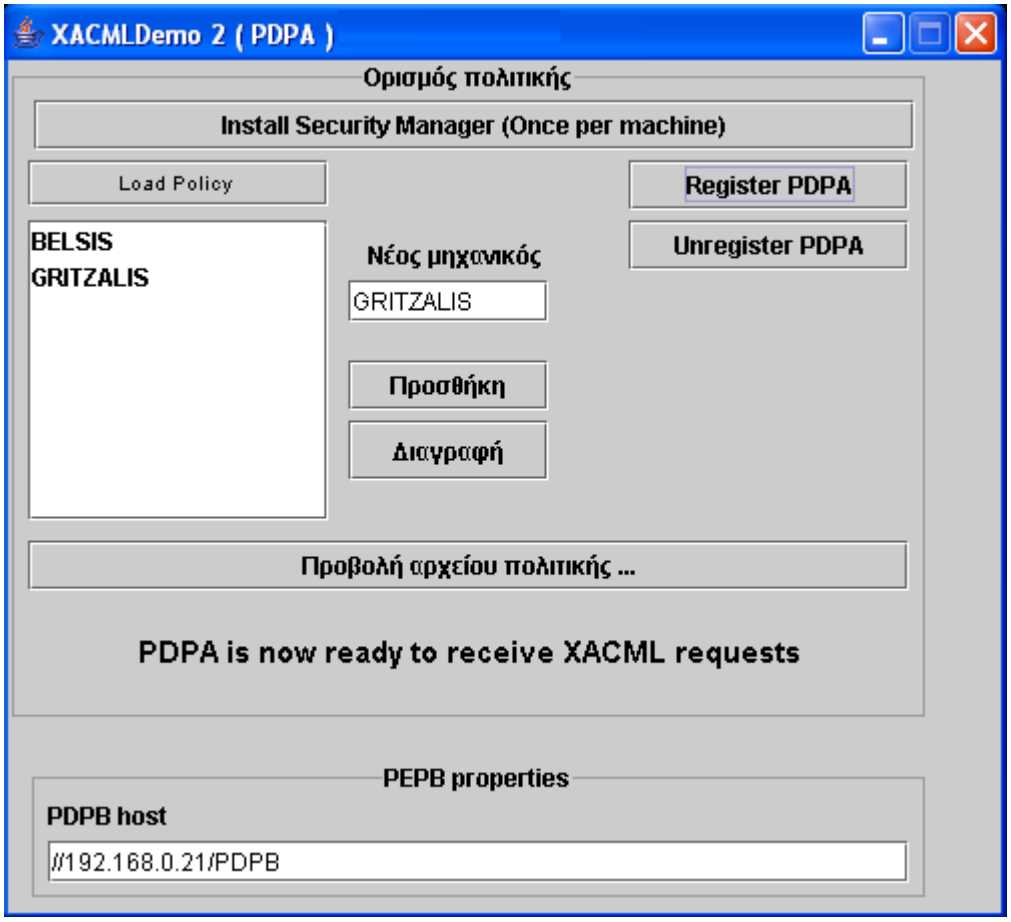
Στην εικόνα 7.5 φαίνεται το μήνυμα απόκρισης το οποίο διαμορφώνεται με βάση την απόφαση του PDP και το οποίο μπορεί να αναζητήσει ο χρήστης με την επιλογή ‘Προβολή απόκρισης’.



Εικόνα 7-5 Με την κατάλληλη επιλογή από τη διεπαφή φαίνεται η απάντηση σε XACML συμβατή μορφή. Στην περίπτωση μας είναι “permit”.

7.4.2 Το σύστημα λήψης αποφάσεων πολιτικής - PDP

Στην εικόνα 7.6 φαίνεται η λειτουργία του συστήματος λήψης αποφάσεων (PDP). Ενσωματωμένη στη διεπαφή είναι η δυνατότητα τροποποίησης των αρχείων πολιτικής, με την προσθήκη νέων ρόλων. Στην πρώτη έκδοση του συστήματος, οι πολιτικές αφορούν στην τροποποίηση ενός αρχείου το οποίο αφορά σε ένα πόρο /κατάλογο πόρων. Με βάση την τρέχουσα έκδοση και τα εργαλεία που παρέχονται από το διαδίκτυο για την XACML δεν υπάρχει έτοιμο λογισμικό που να επιτρέπει τη διαχείριση πολλαπλών πόρων με χρήση πολιτικών. Παράλληλα δεν υπάρχουν μέχρι στιγμής γραφικά εργαλεία διαχείρισης όπως τα συγκεκριμένα που αναπτύχθηκαν στα πλαίσια της υλοποίησης πρωτοτύπου για τις ανάγκες της παρούσας διατριβής. Στην εξελιγμένη έκδοση του λογισμικού που περιλαμβάνει και το σύστημα υπολογισμού του βαθμού ικανοποίησης ενός αιτήματος με χρήση ασαφούς λογικής δίνεται η δυνατότητα δημιουργίας διαφορετικών πολιτικών που αφορούν σε διαφορετικούς συνδυασμούς υποκειμένου (ρόλου), αντικειμένου (πόρου) και δικαιώματος, ενώ παράλληλα καταγράφεται για κάθε μία από τις επιθυμητές τριάδες και ο βαθμός προτίμησης του συστήματος στην ικανοποίηση του αιτήματος που αφορά σε συγκεκριμένο συνδυασμό (εικ. 7.7).
Το κάθε PDP μπορεί λαμβάνοντας τη διεύθυνση του απομακρυσμένου PDP να ελέγχει (με το μηχανισμό αντιστοίχησης), την ύπαρξη στην πολιτική του απομακρυσμένου PDP δηλώσεων που σχετίζονται με το συγκεκριμένο αίτημα.

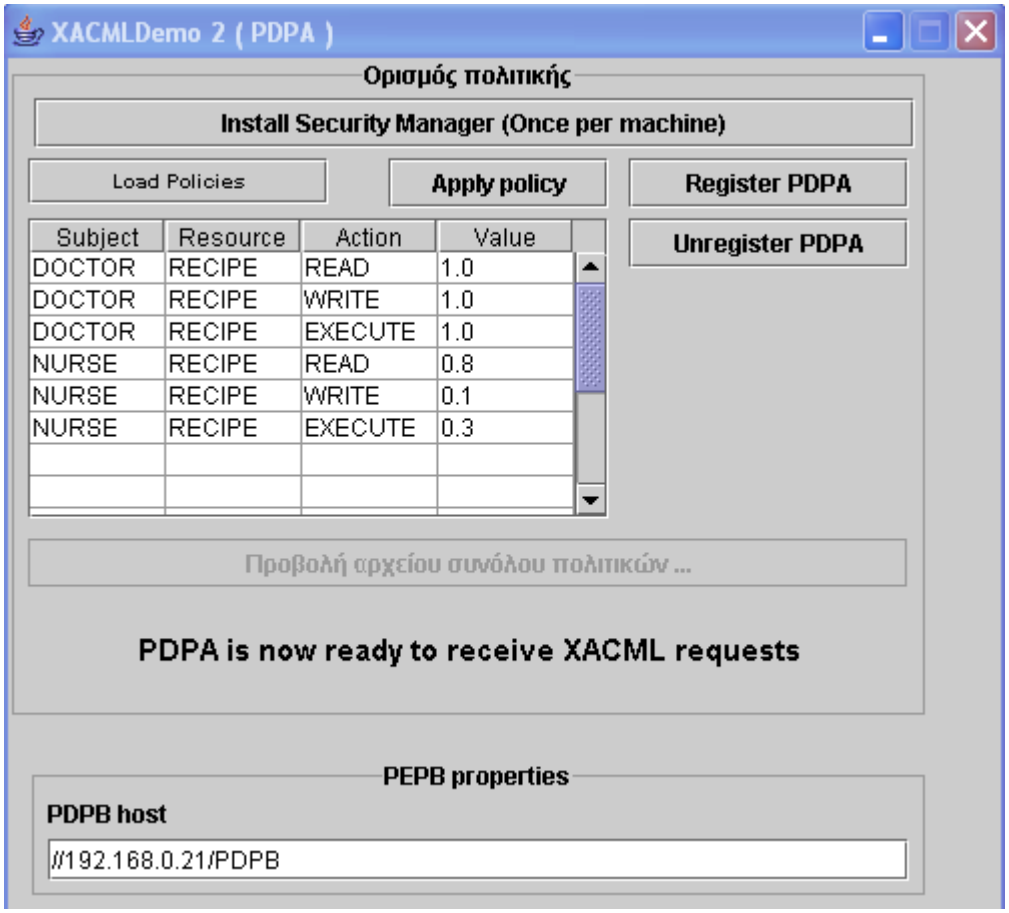


Εικόνα 7-6 Το σύστημα PDP για τον ένα οργανισμό

7.4.3 Επεκταμένη έκδοση συστήματος αυθεντικοποίησης

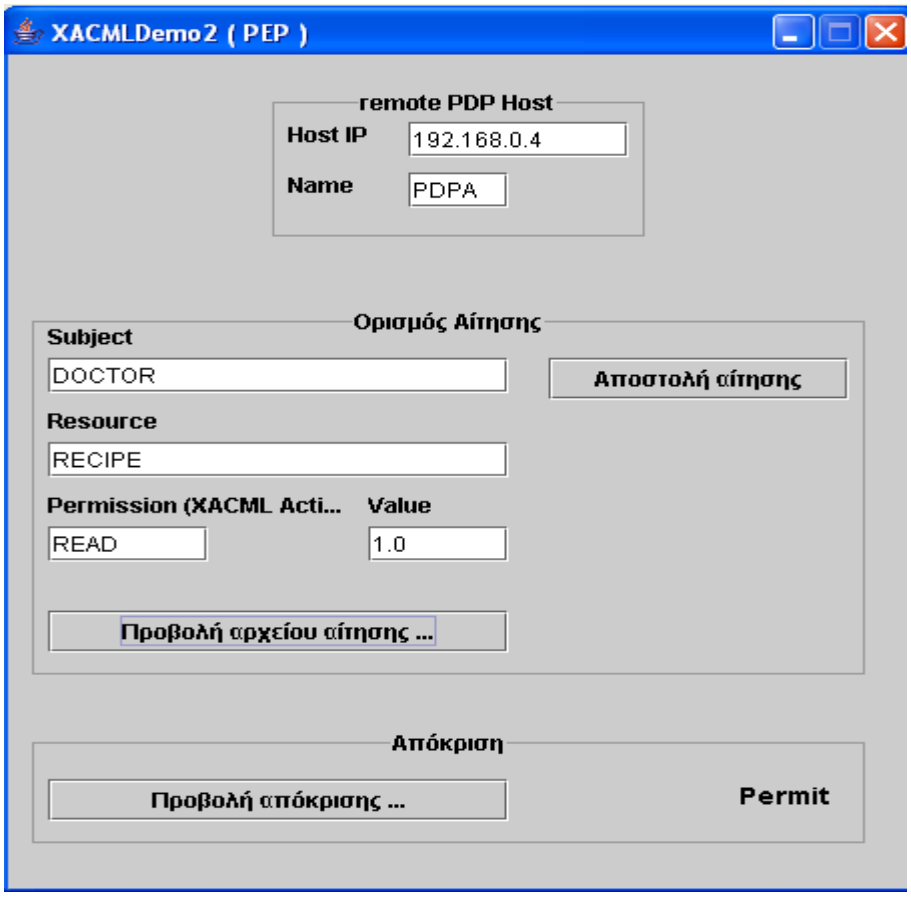
Στη δεύτερη έκδοση του συστήματος, που έχει περιγραφεί στην εργασία (Belsis et al, 2006c) ενσωματώνεται στη λειτουργία του συστήματος αφενός μεν η δυνατότητα δημιουργίας διαφορετικών πολιτικών που αφορούν σε διαφορετικούς πόρους, αφετέρου δε ή δυνατότητα καθορισμού για διαφορετικούς συνδυασμούς υποκειμένου - αντικειμένου- δικαιώματος ενός βαθμού προτίμησης που μπορεί να αξιολογεί την ικανοποίηση αιτημάτων σε περιβάλλοντα πολλαπλών πολιτικών με χρήση ασαφούς λογικής.

Όπως φαίνεται και στην εικόνα 7.7 υπάρχει η δυνατότητα τροποποίησης της πολιτικής προσθέτοντας νέους ρόλους (Roles), νέους πόρους (Resources), ενώ επίσης για τους διαφορετικούς επιτρεπτούς συνδυασμούς των παραπάνω με τους δυνατούς τύπους δικαιωμάτων μπορούμε να αντιστοιχίσουμε μία τιμή στην κλίμακα [0,1]. Το PDP αποκτώντας τη διεύθυνση του απομακρυσμένου PDP μπορεί να ανακτά τις αντιστοιχίσεις ρόλων και στο περιβάλλον πολλαπλών πολιτικών να ελέγχει την ικανοποίηση διαφορετικών αιτημάτων που σχετίζονται είτε με την τοπική πολιτική είτε με την πολιτική του PDP του συνεργαζόμενου οργανισμού.



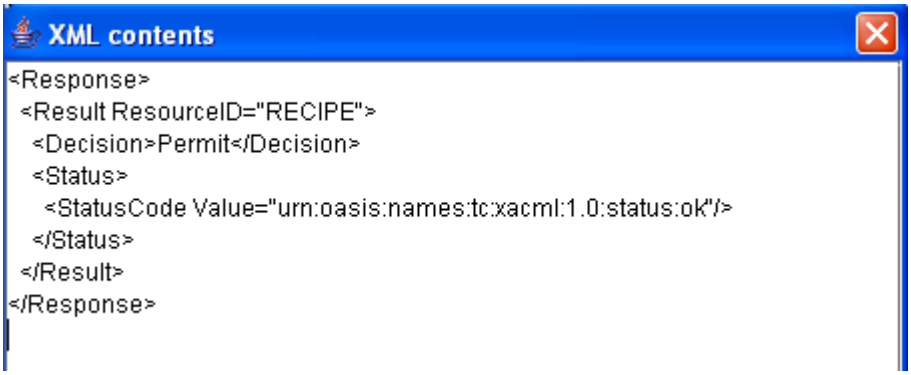
Εικόνα 7-7 Επεκταμένη έκδοση του PDP

Στην εικόνα 7.8 παρουσιάζεται το τροποποιημένο PEP που αναλαμβάνει την αποστολή αιτημάτων ως τριάδα συνδυασμού <υποκείμενο, αντικείμενο, δικαίωμα>. Στις εικόνες 7.9 και 7.10 φαίνεται το αντίστοιχο αίτημα σε XACML μορφή καθώς και η απάντηση που λαμβάνει από το PDP (στην περίπτωσή μας είναι permit).



Εικόνα 7-8 Επεκταμένη έκδοση PEP

Εικόνα 7-9 Μήνυμα αίτησης προς το PDP με ενσωμάτωση προτεραιοτήτων



Εικόνα 7-10 Μήνυμα απόκρισης προς το PEP

7.5 Συμπεράσματα

7.5.1 Αποτίμηση της λειτουργίας του συστήματος

Με βάση την αξιολόγηση της πιλοτικής υλοποίησης από τη δοκιμαστική της εφαρμογή σε κατανεμημένο περιβάλλον, προκύπτουν μία σειρά από συμπεράσματα που αφορούν στις δυνατότητες αλλά και στους περιορισμούς χρήσης του συστήματος:

- Η λειτουργία του συστήματος απευθύνεται σε διαχειριστές με καλή γνώση των τεχνικών θεμάτων που άπτονται των πολιτικών ασφάλειας αλλά και εξειδικευμένων τεχνολογιών όπως για παράδειγμα XML, RMI, Java.
- Η μετατροπή των πολιτικών από τη μορφή των οδηγιών εφαρμογής που δίνονται σε επίπεδο οργανισμού, σε πολιτικές κατώτερου επιπέδου διερμηνεύσιμες από το σύστημα επιβολής πολιτικών, απαιτεί ανθρώπινη εμπλοκή και αρκετό κόστος.
- Σε περιβάλλοντα πολλαπλών πολιτικών απαιτείται ιδιαίτερη προσοχή προκειμένου για τη δημιουργία σωστών αντιστοιχήσεων (μία λανθασμένη αντιστοίχηση δημιουργεί κίνδυνο στην ασφάλεια του συστήματος).
- Στην παρούσα μορφή, το σύστημα δεν υποστηρίζει ένα αναλυτικό μηχανισμό ανίχνευσης και επίλυσης όλων των δυνατών τύπων συγκρούσεων. Ωστόσο, με τη χρήση υπαρχόντων αλγορίθμων και τεχνικών επίλυσης όπως για παράδειγμα κανόνων τύπου "Deny-overrides" (μεταξύ δύο αντικρουόμενων πολιτικών επικρατεί η άρνηση), ή με χρήση προτεραιοτήτων ανάμεσα σε πολιτικές κοκ, μπορεί να αντιμετωπιστεί εν μέρει το πρόβλημα των συγκρούσεων. Η ενσωμάτωση όμως ενός μηχανισμού ολοκληρωμένης αντιμετώπισης συγκρούσεων με χρήση και του πλαισίου που βασίζεται στην ασαφή λογική, αποτελεί ένα πεδίο έρευνας με αρκετό ενδιαφέρον το οποίο αποτελεί ανοικτό ερευνητικό ζήτημα στη διεθνή βιβλιογραφία.

7.5.2 Συνεισφορά του πρωτοτύπου- ενδεχόμενες μελλοντικές επεκτάσεις

Μετά και από τη δοκιμαστική εφαρμογή του συστήματος αλλά και τη μελέτη συναφών συστημάτων αλλά και προγενέστερων υλοποιήσεων στα πλαίσια της ανάπτυξης της XACML μπορούμε να παρατηρήσουμε τα εξής:

- Το σύστημα επιβολής ελέγχου πρόσβασης, μπορεί να αξιοποιηθεί προκειμένου για τη δημιουργία συστημάτων συνασπισμών Π.Σ. και να επιτρέψει τη συνεργασία σε επίπεδο εφαρμογής.
- Το σύστημα που υλοποιήθηκε διαθέτει μια σειρά από διαλειτουργικά χαρακτηριστικά, που του δίνουν ένα σαφές πλεονέκτημα έναντι άλλων υλοποιήσεων, μία και η συνεργασία επιτυγχάνεται ακόμη και για συστήματα που βασίζονται σε διαφορετικές πλατφόρμες λογισμικού και διαφορετικά λειτουργικά συστήματα.
- Οι διεπαφές που αναπτύχθηκαν καθιστούν πιο εύκολη τη διαχείριση των βιβλιοθηκών που παρέχονται από την τρέχουσα υλοποίηση της XACML στα πλαίσια του OASIS. Παράλληλα επεκτείνουν τις δυνατότητες του συστήματος, επιτρέποντας τη δημιουργία και διαχείριση σύνθετων πολιτικών, καθώς και τη δυνατότητα απεικόνισης πολιτικών διαφορετικών αυτόνομων συστημάτων.
- Το σύστημα επίλυσης συγκρούσεων που βασίζεται στη χρήση ασαφούς λογικής, αποτελεί καινοτομία στον τομέα της επίλυσης συγκρούσεων μεταξύ αντιφατικών πολιτικών.

Ωστόσο, θα μπορούσαμε να καταγράψουμε και μία σειρά από ενδεχόμενες βελτιώσεις που θα μπορούσαν να γίνουν στο μέλλον προκειμένου για την επέκταση των δυνατοτήτων του συστήματος που αναπτύχθηκε στα πλαίσια της διατριβής:

- Η διεπαφή μπορεί να επεκταθεί αλλά και να βελτιωθεί η σχεδίαση της, με στόχο την μεγαλύτερη λειτουργικότητά της, αλλά και ενδεχόμενα την υποστήριξη περισσότερων χρηστών με λιγότερο εξειδικευμένη γνώση των σχετικών τεχνολογιών.
- Το σύστημα ανίχνευσης συγκρούσεων μπορεί να επεκταθεί ώστε να υποστηρίζει μία ευρεία γκάμα συγκρούσεων.
- Το σύστημα επιβολής ελέγχων πρόσβασης μπορεί να τροποποιηθεί κατάλληλα ώστε να διερμηνεύει αναπαραστάσεις ρόλων που βασίζονται σε τεχνολογίες σημασιολογικού ιστού (όπως η RDF) και να αξιολογεί συσχετίσεις μεταξύ ιεραρχιών ρόλων.
- Στην τρέχουσα μορφή του συστήματος, προκειμένου για την επιβολή ελέγχων πρόσβασης, προϋποτίθεται ότι έχει ολοκληρωθεί η διαδικασία αυθεντικοποίησης των χρηστών του συστήματος με κάποια αξιόπιστη μέθοδο. Προκειμένου για τη δημιουργία ενός ολοκληρωμένου συστήματος αυθεντικοποίησης / επιβολής ελέγχων πρόσβασης μπορεί στο σύστημα να ενσωματωθεί ένας LDAP server και κατάλληλο λογισμικό, ενώ προκειμένου για τη διασφάλιση της κρυπτογράφησης των επικοινωνιών σε περιβάλλοντα όπου αυτό είναι αναγκαίο μπορούν να εφαρμοστούν οι τεχνικές που περιγράφονται στις εργασίες (Belsis et al, 2005g), (Gritzalis et al, 2006).
- Ενδιαφέρον τέλος, παρουσιάζει ως μελλοντική δραστηριότητα η μέτρηση της απόδοσης του συστήματος και η ικανότητα ανταπόκρισης του σε μικρά χρονικά διαστήματα σε μεγάλο αριθμό αιτημάτων που κατευθύνονται στο PDP από διαφορετικά Π.Σ.

Σαν γενικό συμπέρασμα μπορούμε να πούμε ότι η ανάπτυξη του πιλοτικού συστήματος απέδειξε την εφικτότητα υλοποίησης των τεχνικών αντιστοίχησης των διαφορετικών πολιτικών, όπως αυτή περιγράφεται στα (Belsis et al, 2005h)(Belsis 2006e)(Gritzalis et al, 2006) (Belsis et al, 2006c) (Belsis et al, 2005c) (Belsis et al, 2005b) (Belsis et al, 2005f) (Belsis et al, 2005d) (Belsis et al,

2005e). Η δημιουργία ενός ολοκληρωμένου μηχανισμού επίλυσης διαφορετικών τύπων συγκρούσεων καθώς και η ανάπτυξη ενός φορμαλισμού υποστήριξης και επίλυσης των διαφορετικών αυτών τύπων συγκρούσεων σε συνδυασμό με τη χρήση ασαφούς λογικής μπορεί να χαρακτηριστεί σαν ένα ανοικτό ερευνητικό ζήτημα.

ΚΕΦΑΛΑΙΟ 8 - Συμπεράσματα – ανοικτά ερευνητικά ζητήματα

Η διαρκής ανάπτυξη των τεχνολογιών πληροφορικής και επικοινωνιών δημιουργεί νέες δυνατότητες όσον αφορά τη δυνατότητα διασύνδεσης των πληροφοριακών συστημάτων. Από τις πιο ενδιαφέρουσες προκλήσεις είναι αυτή του διαμοιρασμού πόρων και δεδομένων στα πλαίσια ενός ευρύτερου πλαισίου συνεργασίας των συμμετεχόντων οργανισμών. Χαρακτηριστικά παραδείγματα του πεδίου εφαρμογής των παραπάνω, είναι η συνεργασία οργανισμών του δημόσιου τομέα με στόχο την παροχή καλύτερων υπηρεσιών προς τον πολίτη, η συνεργασία υπηρεσιών συλλογής πληροφοριών με στόχο την πρόληψη και αντιμετώπιση παρανόμων ενεργειών, η συνεργασία επιστημονικών και ερευνητικών ιδρυμάτων στα πλαίσια κοινών ερευνητικών δράσεων, η διασύνδεση πληροφοριακών συστημάτων υγείας κοκ.
Στα πλαίσια της υποστήριξης των παραπάνω στόχων, η παρούσα διατριβή επικεντρώθηκε κυρίως στην αντιμετώπιση των ακόλουθων ζητημάτων:

- Τη δημιουργία ενός μηχανισμού ανάκτησης και διήθησης πληροφοριών στο περιβάλλον των συνεργαζόμενων Π.Σ. (Belsis et al, 2006a) (Belsis 2006e) (Belsis et al, 2006d)
- Την αντιμετώπιση του προβλήματος της ετερογένειας των γνωσιακών πόρων και την πρόταση ενός μηχανισμού αποτελεσματικής διαχείρισης των διαμοιραζόμενων πόρων, λαμβάνοντας υπόψη τις μειωμένες δυνατότητες αυτόνομης λειτουργίας και τους μειωμένους πόρους συσκευών σε ειδικού τύπου περιβάλλοντα (ad-hoc δίκτυα, ασύρματα περιβάλλοντα εν γένει) (Belsis et al, 2005f) (Belsis et al, 2005e)
- Τη δημιουργία ενός μηχανισμού που θα καθιστά εφικτή τη διαχείριση ασφάλειας και το χειρισμό διαφορετικών ρόλων σε περιβάλλοντα πολλαπλών πολιτικών, χωρίς να είναι αναγκαία η εξαρχής σχεδίαση του συστήματος επιβολής ελέγχου πρόσβασης (Belsis et al, 2005h) (Belsis et al, 2005g)
- Τη δημιουργία ενός πλαισίου ημι-αυτοματοποιημένης διαχείρισης ασφάλειας των συνασπισμών αυτόνομων Π.Σ. το οποίο μπορεί να χρησιμοποιηθεί τόσο για την εφαρμογή των κανόνων πολιτικής ασφάλειας όσο και ως υποστηρικτικό εργαλείο για τους διαχειριστές του συστήματος (Belsis et al, 2006b) (Belsis 2006e).
- Την πρόταση υιοθέτησης, ως επέκταση του παραπάνω πλαισίου αυτοματοποιημένης διαχείρισης, ενός καινοτόμου συστήματος επίλυσης συγκρούσεων (conflicts) μεταξύ διαφορετικών πολιτικών, βασισμένο στη χρήση ασαφούς λογικής (Belsis et al, 2006c).

8.1 Αντιμετώπιση του ζητήματος της ανάπτυξης τεχνικών διήθησης πληροφορίας σε κατανεμημένα περιβάλλοντα

Στα πλαίσια της αντιμετώπισης του προβλήματος της ανάκτησης επιλεγμένης πληροφορίας και της κατηγοριοποίησης της αδόμητης πληροφορίας που εντοπίζεται στα διαφορετικά συστήματα που διαμοιράζονται πόρους, προτάθηκε η συνδυασμένη χρήση: α) τεχνικών επιλογής βέλτιστων χαρακτηριστικών και β) αλγορίθμων ταξινόμησης σε προεπιλεγμένες κλάσεις. Προκειμένου για την αξιολόγηση της ποιότητας μίας λύσης χρησιμοποιήθηκε μία τεχνική εκτίμησης της ποιότητας των επιλεγμένων χαρακτηριστικών που βασίζεται στην έννοια των περιθωρίων (margins) (Belsis et al, 2006a) (Belsis et al, 2006d). Ο πειραματισμός με ειδικά σύνολα δεδομένων ανέδειξε τα θετικά στοιχεία της προτεινόμενης τεχνικής έναντι συναφών

λύσεων, κυρίως εξαιτίας της δυνατότητάς της να επιτυγχάνει υψηλότερα ποσοστά ακρίβειας αλλά και λόγω του πλεονεκτήματος να γίνεται εύκολα η ενημέρωση του χρησιμοποιούμενου δείγματος με νέα σύνολα δεδομένων.

8.1.1 Τεχνικές αντιστοίχησης ρόλων σε περιβάλλοντα πολλαπλών πολιτικών.

Προκειμένου για τη δημιουργία ενός κλιμακούμενου, χαμηλής πολυπλοκότητας, μηχανισμού επιβολής ελέγχου πρόσβασης σε περιβάλλοντα πολλαπλών πολιτικών προτάθηκε στα πλαίσια των (Belsis et al, 2005h) (Belsis et al, 2005g) η τεχνική της αντιστοίχησης ρόλων, που επιτρέπει την απονομή δικαιωμάτων σε ρόλους που ανήκουν σε διαφορετικό οργανισμό. Η χρήση διαλειτουργικών, καθώς και σημασιολογικά ενδυναμωμένων, τεχνικών βασισμένων κυρίως σε τεχνολογίες που χρησιμοποιούν τη γλώσσα XML επιτρέπουν την αναπαράσταση και διερμηνεία από το σύστημα επιβολής ελέγχου πρόσβασης της πληροφορίας που αφορά στους ρόλους με διαλειτουργικό τρόπο. Η πιλοτική υλοποίηση που περιγράφηκε στο κεφάλαιο 7 υλοποιεί τους παραπάνω μηχανισμούς αντιστοίχησης σε επίπεδο εφαρμογής, και επειδή έχει βασιστεί στην τεχνολογία Java δίνει τη δυνατότητα αξιοποίησης σε μεγάλο πλήθος εφαρμογών. Παράλληλα, στο πλαίσιο της εργασίας (Belsis et al, 2005f) προτείνεται μία τεχνική που επιτρέπει την απόκρυψη κρίσιμων σημείων πολιτικής από το σύνολο των συμμετεχόντων μερών στο συνασπιζόμενο περιβάλλον.

8.1.2 Ημι-αυτοματοποιημένη διαχείριση ρόλων

Με δεδομένη την ανάγκη δημιουργίας συσχετίσεων με εμπλοκή των διαχειριστών του συνασπισμού, ο διαχειριστικός φόρτος ενδέχεται να γίνεται δύσκολα διαχειρίσιμος. Στην περίπτωση αυτή απαιτείται η δημιουργία ενός μηχανισμού που θα επιτρέπει την ελάττωση του παραπάνω διαχειριστικού φόρτου, αξιολογώντας την εγκυρότητα ορισμένων αιτήσεων για τις οποίες δεν υπάρχει ρητά καθορισμένη αντιστοίχηση των αντίστοιχων ρόλων και οι οποίες δεν αναφέρονται σε κρίσιμους πόρους (Belsis et al, 2006b) (Belsis 2006e). Ο προτεινόμενος μηχανισμός αξιοποιεί τεχνικές ικανοποίησης χαλαρών περιορισμών (soft constraints).
Παράλληλα, ένα από τα προβλήματα που διέπουν τη λειτουργία συνασπισμών αυτόνομων Π.Σ. είναι και αυτό της επίλυσης συγκρούσεων μεταξύ των διαφορετικών απαιτήσεων των πολιτικών του συστήματος. Στο πλαίσιο της αντιμετώπισης αυτών των συγκρούσεων προτείνεται ένας μηχανισμός που βασίζεται στην εκτίμηση του βαθμού ικανοποίησης μίας σειράς από προϋποθέσεις με χρήση ασαφούς λογικής (Belsis et al, 2006c).

8.1.3 Αντιμετώπιση προβλημάτων ετερογένειας

Ένα από τα βασικά προβλήματα στην περίπτωση της συγχώνευσης διαφορετικών συστημάτων είναι αυτό της αντιμετώπισης της ετερογένειας που αφορά στη διαφορετική αναπαράσταση ομοειδών πόρων σε διαφορετικά συστήματα, ή στη διαφορετική κωδικοποίηση των πόρων κοκ. Στη βάση της επίλυσης αυτού του προβλήματος προτάθηκε στα πλαίσια των εργασιών (Gritzalis et al, 2006), (Malatras et al, 2006b) (Belsis et al, 2005d) η τεχνική δημιουργίας των εικονικών δικτύων οντολογιών που επιτρέπουν την κατηγοριοποίηση των διαφορετικών συστημάτων ανάλογα με το θεματικό περιεχόμενο των πόρων που αυτά διαθέτουν.
Εφαρμογές των παραπάνω τεχνικών σε συγκεκριμένες μελέτες περίπτωσης έχουμε σε συγκεκριμένες μελέτες περίπτωσης που αφορούν σε συστήματα κυρίως ιατρικού χαρακτήρα (Belsis et al, 2005g) (Belsis et al, 2005d) (Gritzalis et al, 2006) αλλά και

σε περιβάλλοντα ειδικού σκοπού, όπως αυτά που στηρίζονται σε ad-hoc δίκτυα (Malatras et al, 2005b).

8.2 Πεδία μελλοντικής έρευνας

Με βάση τα όσα αναφέρθηκαν και στα προηγούμενα κεφάλαια, καθίσταται προφανές πως ανακύπτουν μία σειρά από ερευνητικά ζητήματα που θα μπορούσαν να τύχουν διεξοδικότερης μελλοντικής έρευνας:

- Στον τομέα της αποτελεσματικής διήθησης της πληροφορίας, ένας διεξοδικότερος πειραματισμός με διαφορετικούς συνδυασμούς αλγορίθμων, τόσο για επιλογή του βέλτιστου συνόλου χαρακτηριστικών αλλά και για κατηγοριοποίηση με βάση τα επιλεχθέντα χαρακτηριστικά, ενδέχεται να αναδείξει αποδοτικότερους συνδυασμούς από αυτούς που παρουσιάστηκαν στο πλαίσιο της παρούσας έρευνας. Παράλληλα, οι δυνατότητες της μεθόδου που αναπτύχθηκε στα πλαίσια των εργασιών (Belsis et al, 2006a) (Belsis et al, 2006c) ξεπερνούν αυτές της απλής ταξινόμησης κειμένων και μπορούν να χρησιμοποιηθούν και για την ανίχνευση των χαρακτηριστικών ενός συγγραφέα και κατ' επέκταση του εντοπισμού του συγγραφέα κειμένων από μία συλλογή διαφορετικών κειμένων με βάση ένα δείγμα κειμένων που χρησιμοποιείται ως πρότυπο και ενδεικτικό του ύφους του συγκεκριμένου συγγραφέα. Είναι επίσης προφανές πως οι εφαρμογές της τελευταίας αυτής τεχνικής μπορούν να υποστηρίξουν ζητήματα από το χώρο της δικανικής πληροφορικής.
- Το πλαίσιο επίλυσης συγκρούσεων μεταξύ διαφορετικών πολιτικών μπορεί να επεκταθεί υποστηρίζοντας διαφορετικούς τύπους συγκρούσεων σε σχέση με το παράδειγμα που αναφέρεται στο (Belsis et al, 2006c). Ενδιαφέρον επίσης αποκτά και η δημιουργία ενός ολοκληρωμένου θεωρητικού υπόβαθρου, βασισμένου στη χρήση ασαφούς λογικής, για τη διαπραγμάτευση αιτήσεων σε περιβάλλοντα συνεργαζόμενων αυτόνομων Π.Σ.
- Παράλληλα ανοικτό παραμένει το ερευνητικό πρόβλημα της διαπραγμάτευσης σε περιβάλλοντα που υπάρχει έλλειψη εμπιστοσύνης. Στα πλαίσια της παρούσας διατριβής προτάθηκε μία τεχνική απόκρυψης του συνόλου της πολιτικής από τα διαπραγματευόμενα μέρη, ωστόσο είναι ενδιαφέρουσα ερευνητικά η προοπτική αναζήτησης αποδοτικών τεχνικών στο πρόβλημα της διαπραγμάτευσης.

Βιβλιογραφία:

Abadi M., Burrows M., Lampson B., and Plotkin G. (1998) A calculus for access control in distributed systems. In J. Feigenbaum, editor, *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference*, pages 1–23, Aug. 1991. LNCS 576.

Ahn G. J., Sandhu R. (2000), "Role-based Authorization Constraints Specification", *ACM Transactions on Information and Systems Security (TISSEC),* Vol. 3, No.4, November 2000, pp. 207-206

Ahn J.G., Sandhu R. (2000), "Role-based Authorization Constraints Specification", *ACM Transactions on Information and Systems Security (TISSEC),* Vol. 3, No.4, November 2000, pp. 207-206

Ahn, G. J. and Sandhu R. (1999), The RSL99 Language for Role-Based Separation of Duty Constraints. In Proceedings of the Fourth ACM Workshop on Role-Based Access Control, Fairfax, Virginia, USA, ACM Press, pp. 43-54, 28-29 October 1999.

Ao X. and Minsky N. H. (2003), Flexible regulation of distributed coalitions. In LNCS 2808: the Proc. of the European Symposium on Research in Computer Security (ESORICS) 2003.

Aura T. (1998), "On the Structure of Delegation Networks", Proceedings of the 11th IEEE Computer Security Foundations Workshop, Rockport, MA.

Bachrach G., Navot A., Tishby N. (2004), "Margin Based Feature Selection - Theory and Algorithms". In Proc of Int. Conference on Machine learning (ICML, Alberta, Canada

Barker S., Stuckey P. (2003), "Flexible Access Control Policy Specification with Constraint logic programming *ACM Transactions on Information and Systems Security (TISSEC)*. 6, 4 (Nov. 2003), 501-546

Barker S., Stuckey P. (2003), "Flexible Access Control Policy Specification with Constraint logic programming *ACM Trans. Inf. Syst. Secur.* 6, 4 (Nov. 2003), 501-546

Belokolsztolszki A., Eyers D., Moody K (2003), "Policy Contexts: Controlling Information Flow in Parameterised RBAC", Proceedings of the 4th International Workshop on Policies for Distributed Systems and Networks (POLICY'03), IEEE press, pp.99-110.

Belokosztolszki A. (2004), "Role based access control for policy administration", available at *http://www.cl.cam.ac.uk/* as technical report No 586, university of Cambridge, UK.

Belsis P., Gritzalis S., Skourlas C., Drakopoulos I. (2004a). "Implementing Knowledge Management techniques for security purposes", 6th International Conference on Enterprise Information Systems (in Collaboration with ACM, AAAI, IEICE and APPIA), Porto, Portugal, April 14-17, 2004, Proceedings, Vol. 2, pp 535-540.

Belsis P., Gritzalis S. (2004b), "Distributed Autonomous Knowledge Acquisition and Dissemination Ontology based Framework" in Proceedings of the PAKM 2004 5th International Conference on Practical Aspects of Knowledge Management -

Workshop on Enterprise Modeling and Ontology: Ingredients for Interoperability, D. Karagiannis (Ed.), December 2004, Vienna, Austria, Univ. of Vienna, pp. 100-104

Belsis P., Kokolakis S, Kiountouzis E. (2005a) "Information systems security from a knowledge management perspective" Information Management & Computer security, vol. 13, number3, March 2005 (pp. 189 – 202)

Belsis P., Malatras A., Gritzalis S., Skourlas C., Chalaris I. (2005b), "Flexible Secure heterogeneous File Management in Distributed Environments ", IADAT Journal of Advanced Technology, vol. 1 Number 2, pp. 66-68, December 2005, published by IADAT International Association for the Development of Advances in Technology

Belsis P., Malatras A., Gritzalis S., Skourlas C., Chalaris I. (2005c), "Semantically enabled Secure Multimedia content delivery using GIS principles", in Proceedings of the IADAT-micv2005 International Conference on Multimedia, Image Processing and Computer Vision, J. Larrauri et al, (Eds.), April 2005, Madrid, Spain, Proceedings by IADAT International Association for the Development of Advances in Technology pp. 34-39

Belsis P., Malatras A., Gritzalis S., Skourlas C., Chalaris I. (2005d), "Pervasive Secure Electronic Healthcare Records Management", in Proceedings of the ICEIS 7th International Conference on Enterprise Information Systems - Workshop on Ubiquitous Computing, S. K. Mostefaoui (Ed.), May 2005, Miami, USA, published by ICEIS, pp. 101-109

Belsis P., Gritzalis S., Skourlas C.(2005e), "Security Enhanced Distributed Knowledge Management Architecture", in *Proceedings of the I-KNOW'05 5th International Conference on Knowledge Management*, K. Tochtermann, H. Maurer (Eds.) July 2005, Graz, Austria, Springer

Belsis P., Gritzalis S., Malatras A., Skourlas C., Chalaris I. (2005f), "Sec-Shield: Security Preserved Distributed Knowledge Management between Autonomous Domains" in Proceedings of the DEXA'05 TrustBus'05 2nd International Conference on Trust, Privacy, and Security in the Digital Business, J. Lopez, G. Pernul, (Eds.), August 2005, Copenhagen, Denmark, Lecture Notes in Computer Science LNCS 3592, Springer, pp. 10-20

Belsis P., Gritzalis S. (2005g), "Security Control Schemes for Pervasive Medical Environments", in Proceedings of the 1st IEEE International Conference on Pervasive Services ICPS 2005 - Workshop on Security, Privacy, and Trust in Pervasive and Ubiquitous Computing SecPerU'05, July 2005, P. Georgiadis, S. Gritzalis, Y. Marias (Eds.) Santorini, Greece, Diaylos Press

Belsis P., Gritzalis S., Katsikas S. (2005h), "A Scalable Security Architecture enabling Coalition Formation between Autonomous Domains", in Proceedings of the 5th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'05), December 2005, Athens, Greece, IEEE Computer Society Press

Belsis P., Fragos K., Gritzalis S., Skourlas C. (2006a), The SF-HME System : A Hierarchical Mixtures-of–Experts classification system for spam filtering, 21st ACM symposium on Applied Computing (SAC 06), Dijon France, 23-27 April 2006

Belsis P, Gritzalis S., Katsikas S. (2006b) Optimized Multi-Domain Secure Interoperation using Soft Constraints, 3rd IFIP Conference on Artificial Intelligence

Applications and Innovations (AIAI) 2006, Athens June 7 - 9, 2006, Springer.

Belsis P., Gritzalis S., Katsikas S.K. (2006c), Partial and fuzzy constraint satisfaction to support coalition formation*, ENTCS Electronic Notes on Theoretical Computer Science*, 2006, Elsevier.

Belsis P., Fragos K., Gritzalis S., Skourlas C. (2006d) Applying effective feature selection techniques with Hierarchical Mixtures of Experts for spam classification, submitted for publication

Belsis P (2006e) "Challenges and Potential Solutions for Secure and Efficient Knowledge Leveraging in Coalitions" *eJETA, The electronic Journal for e-Commerce Tools & Applications,* 2006

Bertino E., Jajodia S., Samarati P (1995), 'Database Security: Research and Practice' Information Systems, Vol. 20, No 7, pp. 537-556, Elsevier.

Bertino, E., Bonatti, P. A., & Ferrari, E. (2001), *TRBAC: A Temporal Role-based Access Control Model*, ACM Transactions on Information and System Security, 4(3), 191-233.

Bettini C., Jajodia S., Wang X. S., Wijesekera D. (2002), "Provisions and Obligations in Policy Management and Security Applications", proceedings of 28th VLDB conference, China 2002, pp. 502-513.

Bharadwaj V. and Baras J.(2003) "Towards automated negotiation of access control policies", *In Proc. of the 4th IEEE International workshop on Policies for distributed Systems and Networks (POLICY 03), pp. 77-86, IEEE press*

Bharadwaj V., Baras J (2003), "Towards automated negotiation of access control policies", In proceedings of third IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'03), 2003

Bhatti R., Joshi J., Bertino E., Ghafoor A. (2004), A: X-GTRBAC admin: a decentralized administration model for enterprise wide access control. SACMAT 2004: 78-86

Bidan C., Issarny V. (1998), "Dealing with Multi-Policy Security in Large Open Distributed Systems" ESORICS 1998, 51-66.

Bistarelli S. (2004), "Semirings for Soft Constraint Solving and Programming", Springer Lecture Notes in Computer Science, Vol. 2962.

Bistarelli S., Montanari U., Rossi F (2001). "Semiring-Based Constraint Logic Programming: Syntax and Semantics, , in *ACM TOPLAS*, ACM Press New York, NY, USA, Pages: 1 - 29 Vol. 23, issue 1, 2001

Blaze M., Feigenbaum J., and Lacy J. (1996), " Decentralized Trust Management", Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA.

Blaze, M., Feigenbaum J. and Keromytis A. (1998), *Keynote: Trust Management for Publc-Key Infrastructures*. In Proceedings of the Security Protocls International Workshop, Cambridge, England, Springer-Verlag LNCS, pp. 59 - 63, April 1998.

Blobel B. (2004), "Authorization and access control for EHR systems". International Journal of Medical Informatics, (2004) 73, 251-25)

Bonatti, P., de Capitani di Vimercati, S., and Samarati, P. (2000), A modular approach to composing access control policies. In *Proceedings of the 7th ACM Conference on Computer and Communications Security* (Athens, Greece, November 01 - 04, 2000). P. Samarati, Ed. CCS '00. ACM Press, New York, NY, 164-173

Bonatti, P., De Capitani di Vimercati, S., and Samarati, P. (2002), An algebra for composing access control policies. *ACM Trans. Inf. Syst. Secur.* (TISSEC) 5, 1 (Feb. 2002), 1-35.

Brewer, D.F.C. and Nash, M.J. (1989), The Chinese Wall security policy. In proceedings of the 1989 IEEE symposium on security and privacy, IEEE Press, USA.

Bridle J. S. (1990), "Probabilistic interpretation of feed forward classification network outputs with relationships to statistical pattern recognition". In F. Fogelman S and J. Herault, editors, Neurocomputing: Algorithms, Architectures, and Applications, pages 227--236. Springer Verlag, New York, 1990

Brutlag J. D. and Meek. C. (2000), "Challenges of the Email Domain for Text Classification". In *Proc. of the 17th International Conference on Machine Learning*, pages 103–110, Stanford University, USA.

Chen F. and Sandhu R. (1995), 'Constraints for role-based access control'. In Proceedings of the First ACM Workshop on Role-Based Access Control (RBAC'95), pages II–39–46, 1995.

Choudhri A, Kagal L., Joshi A., Finin T., and Yesha Y. (2003), PatientService: Electronic Patient Record Redaction and Delivery in Pervasive Environments, Fifth International Workshop on Enterprise Networking and Computing in Healthcare Industry (Healthcom 2003), Santa Monica, June 2003

Chu Y., Feigenbaum Joan, LaMacchia B., Resnick P., Strauss M. (1997), "{REFEREE}: Trust management for {Web} applications",Computer Networks and ISDN Systems, 29, 8, p. 953-964, 1997.

Cohen W (1996), "Learning Rules that Classify E-mail". In Proceedings of the 1996 AAAI Spring Symposium on Machine Learning in Information Access, California.

Crammer K., Bachrach K.G., Navot A., Tishby N. (2002), "Margin analysis of the lvq algorithm", Proc. of the 17th Conference on Neural Information Processing Systems.

Damianou N. (2002), "A Policy Framework for management of Distributed Systems", Phd Thesis, Imperial College, London.

Decker S., Melnik S., van Harmelen, F, Fensel D., Klein M., Broekstra J., Erdmann M., Horrocks I, (2000), 'The semantic web: the roles of XML and RDF', IEEE Internet Computing 4 (5) (2000) 63–74.

Denning, D.E. (1976), "A Lattice Model of Secure Information Flow" Communications of ACM 19(5):236-243 (1976)

Drucker H., Vapnik V, Wu. D (1999), Support Vector Machines for Spam Categorization. *IEEE Trans. on Neural Networks,* 10(5).

Dubois D., Fargier H., and Prade H (1993), The calculus of fuzzy restrictions as a basis for flexible constraint satisfaction. *In Proc. IEEE International Conference on Fuzzy Systems*, pages 1131–1136. IEEE Computer Society.

Ellison C. , Frantz B, Lampson B, Rivest R, Thomas B, and Ylonen. T. (1999), SPKI certificate theory. RFC 2693,Sept. 1999.

Ellison C. M. (1998), SPKI Certificate documentation, http://www.clark.net/pub/cme/html/spki.html.

Fawcett T. (2003) "In vivo" spam filtering: A challenge for KDD. SIGKDD explorations, vol 5,issue 2, 2003, pp. 140-149.

FIPA, (2005) FIPA standard status specifications www.fipa.org/repository/standardspecs.html

Freuder E. C., Wallace R. J. (1992), "Partial constraint satisfaction", *Artificial Intelligence* 58 (1992), pp.21-70

Fritsch J., Finke M., and Waibel. A., (1997), Context dependent hybrid HME/HMM speech recognition using polyphone clustering decision trees". In Proceedings of ICASSP-97, 1997

Gee K. (2003), "Using Latent Semantic Indexing to Filter spam", proceedings of ACM Symposium on Applied Computing SAC 2003, 460-464, Florida, USA, ACM Press

Gibson T. (2001), "An Architecture for Flexible, High Assurance, Multi-Security Domain Networks", Proceedings of the Network and Distributed Systems Security Symposium, San Diego.

Gligor V., Khurana H., Koleva, R., Bharadwaj,V. and Baras J.(2001), "On the Negotiation of Access Control Policies", 9th Security Protocols Workshop, Cambridge, UK, Springer-Verlag, 2001.

Gligor, V. (1995), *Characteristics of Role Based Access Control*. In Proceedings of the First ACM/NIS, Role Based Access Control Workshop, Gaithersburg, Maryland, USA, ACM Press, November 1995.

Gong and X. Qian.(1994), "The Complexity and Composability of Secure Interoperation" In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 190–200, Oakland, California, May 1994. IEEE.

Gritzalis S. (2005) 'A policy ruled Knowledge dissemination architecture for supporting Multi-Domain Secure Interoperation", the eJournal for Electronic Commerce Tools and Applications, vol. 1 no. 4 Dec. 2005

Gritzalis S., Belsis P., Katsikas S. (2006) "Interconnecting autonomous medical domains: a security perspective", IEEE Engineering in Medicine and Biology (accepted)

Gritzalis S., Iliadis J., Gritzalis D., Spinellis D., Katsikas S. (1999) "Developing Secure Web-based Medical Applications", *Medical Informatics and the Internet in Medicine,* Vol.24, No.1, pp.75-90, 1999, Cambridge University Press - Taylor & Francis Publications

Herzberg, A., Y. Mass, Michaeli J., Naor D. and Ravid Y. (2000), *Access Control Meets Public Key Infrastructure, or: Assigning Roles to Strangers*. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California, USA, 14-17 May 2000.

Hidalgo J (2002), Evaluating Cost Sensitive Bulk Email Categorization, pp 615-620, SAC 2002, Madrid, Spain

Hitchens, M. and Varadharajan V. (2001), Tower: A Language for Role Based Access Control. In Proceedings of the Policy Workshop 2001, HP Labs, Bristol, UK, Springer-Verlag, 29-31 January 2001.

Hoagland, J. A., Pandey R. and Levitt K. N. (1998). *Security Policy Specification Using a Graphical Approach*. Technical report CSE-98-3, UC Davis Computer Science Department, 22 July 1998.

Hosmer Hillary H. (1992), "The Multilpolicy Paradigm", Proceedings of the 15th National Computer Security Conference, Baltimore, October, 1992

Hosmer, H. H. (1993), "Security is fuzzy!: applying the fuzzy logic paradigm to the multipolicy paradigm". In *Proceedings on the 1992-1993 Workshop on New Security Paradigms* (Little Compton, Rhode Island, United States). J. B. Michael, V. Ashby, and C. Meadows, Eds. NSPW '92-93. ACM Press, New York, NY, 175-184

IPSEC, (1998), RFC 2401, Security Architecture for the Internet Protocol, http://rfc.net/rfc2401.html

ISO 17799 (2003) "Information Technology – Code of Practice for information security management", ISO/IEC 17799

Jacobs R. A., Jordan M. I., Nowlan S. J., and Hinton G. E. (1991), "Adaptive mixtures of local experts. Neural Computation", 3(1):79--87, 1991.

Jansen W. A., Karygiannis T., Gavrila S., and Korolev V. (2002), "Assigning and Enforcing Security Policies on Handheld Devices". In Proceedings of the Canadian Information Technology Security Symposium, May 2002

Jordan M. I. and Jacobs. R. A (1994) "Hierarchical mixtures of experts and the EM algorithm". Neural Computation, 6(2):181--214.

Joshi J.B.D., Bhatti R., Bertino E., Ghafoor A.(2004), "Access Control Language for Multi-Domain Environments", *IEEE Internet Computing*, Nov. 2004, pp. 40-50.

Kaburlasos V.G., and Petridis V. (2002), "Learning and Decision-Making in the Framework of Fuzzy Lattices", in *New Learning Paradigms in Soft Computing*, L.C. Jain and J. Kacprzyk (eds.), pp. 55-96, 2002, Heidelberg, Germany: Physica-Verlag GmbH, Studies in Fuzziness and Soft Computing series, vol. 84,

Kaburlasos, V.G. (2006), "Towards a Unified Modeling and Knowledge-Representation based on Lattice Theory", Computational Intelligence and Soft Computing Applications Series: Studies in Computational Intelligence , Vol. 27

Keromytis, A. D., Ioannidis S., Greenwald M. and Smith J. M. (2001), *Scalable Security Policy Mechanisms*. Technical Report, MS-CIS-01-05, University of Pennsylvania CIS Dept., January 2001.

Khurana H.(2002), "Negotiation and Management of Coalition Resources", Phd Thesis, University of Maryland.

Khurana H., Gligor V. D. and Linn J. (2002), "Reasoning about Joint Administration of Coalition Resources", In *Proc. of IEEE International Conference on Distributed Computing Systems (ICDCS)*, pp.429-439, Vienna, Austria, July 2002, IEEE press.

Kira K., Rendell L. (1992), "A practical approach to feature selection", In Proc. of 9th International workshop on machine learning (pp. 249-256.

Kokolakis S. and Kiountouzis E. (2000). "Interoperability in Multi-Policy Environments", Computers & Security, vol. 19, No. 3.

Kokolakis S., Gritzalis D., Katsikas S. (1998). "Generic security Policies for Health Care Information Systems", Health Informatics Journal, Vol.4 no.3, pp. 184-195, 1998.

Koller D., and Sahami M. (1997), "Hierarchically classifying documents using very few words", in I*nternational Conference on Machine Learning (ICML)*, pp. 170-178.

Lee D., Chu W., (2001), CPI: Constraints- Preserving Inlining algorithm for mapping XML DTD to relational schema, Data and Knowledge Engineering, 39, pp. 3-25.

Lewis D. (1992), "Feature selection and feature extraction for text categorization", Morgan Kaufmann, San Francisco, pp. 212-217.

Lobo, J., Bhatia R. and Naqvi S. (1999). A Policy Description Language. In Proceedings of the Sixteenth National Conference on Artificial Intelligence Eleventh Innovative Applications of AI Conference, Orlando,Florida, USA, 18-22 July 1999.

Lupu, E., Sloman M., Dulay N. and Damianou N. (2000). Ponder: Realising Enterprise Viewpoint Concepts. In Proceedings of the 4th International Enterprise Distributed Object Computing Conference (EDOC 2000), Makuhari, Japan, 25-28 September 2000.

Malatras A., Pavlou G, Belsis P., Gritzalis S., Skourlas C., Chalaris I. (2005a), "Secure and Distributed Knowledge Management in Pervasive Environments", in *Proceedings of the 1st IEEE International Conference on Pervasive Services ICPS 2005*, V.Kalogeraki (Ed.), July 2005, Santorini, Greece, IEEE Computer Society Press

Malatras A., Pavlou G., Belsis P., Gritzalis S., Skourlas C., Chalaris I. (2005b), "Deploying Pervasive Secure Knowledge Management Infrastructures", in International Journal of Pervasive Computing and Communications, 2005, Troubador Publishing (best papers of IEEE ICPS 2005)

McDaniel P and Prakash A. (2002), Methods and Limitations of Security Policy Reconciliation. *2002 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, pages 73-87, MAY 2002. Oakland, CA

Mladenic D. (1998), "Feature subset selection in text-learning", in *Proc. of the 10th European Conference on Machine Learning*.

Mukkamala R., Atluri V. and Warner J. (2005), ``A Distributed Service Registry for Resource Sharing among Ad-hoc Dynamic Coalitions," proc. of IFIP Joint Working Conference on Security Management, Integrity, and Internal Control in Information Systems, Springer

Nejdl, W., Wolf, B., Qu, C., Decker, S., Sintek, M., Naeve, A., Nilsson, M., Palmer, M., Risch, T. (2002), "Edutella: A P2P networking infrastructure based on rdf". In: Proceedings to the Eleventh International World Wide Web Conference, Honolulu, Hawaii, USA (2002

OASIS (2004), Organization for the Advancement of Structured Information Standards, ''XACML Extensible access control markup language specification 2.0'', OASIS Standard, (available at http://www.oasis-open.org, March 2004

Ovchinnikov S. (1994), Fuzzy sets and secure computer systems, *Proc. of the New Security Paradigms Workshop*, August 3 - 5, 1994, Little Compton, RI.

Patwardhan A., Korolev V., Kagal L., Joshi A. (2004), "Enforcing Policies in Pervasive Environments", In Proc. of the MobiQuitous 2004 1st Annual Conference on Mobile and Ubiquitous Systems, IEEE Press

Ruotsalainen P. (2004), "A cross platform model for secure Electronic health record communication", International Journal of Medical Informatics, (2004) 73, 291-295.

Ruttkay Z. (1994) "Fuzzy constraint satisfaction." *In Proc. 3rd IEEE International Conference on Fuzzy Systems,* pages 1263–1268.

Sahami M., Dumais S., Heckerman D., and Horvitz. E. (1998), "A Bayesian Approach to Filtering Junk E-Mail". Learning for Text Categorizaton - Papers from the AAAI Workshop, 1998, pages 55-62, Madison Wisconsin. AAAI Technical Report WS-98-05.

Samarati P., Sabrina de Capitani di Vimercati (2001), "Access Control: Policies, Models, and Mechanisms", R. Focardi and R. Gorrieri (Eds.): FOSAD 2000, LNCS 2171, pp. 137–196, 2001.

Sandhu R (1995), 'Roles versus groups'. In Proceedings of the First ACM Workshop on Role-Based Access Control (RBAC'95), pages I–25–26, 1995.

Sandhu R. (1995), Roles versus groups. In Proceedings of the First ACM Workshop on Role-Based Access Control (RBAC'95), pages I–25–26.

Sandhu R. and Munawer Q (1998), "How to do discretionary access control using roles. In Proceedings of the Third ACM Workshop on Role-Based Access Control (RBAC'98), pages 47–54.

Sandhu R. and Samarati P. (1994), Access control: Principles and practice. IEEE Communications Magazine, 32(9):40–48, 1994.

Sandhu, R. S., E. J. Coyne, H. L. Feinstein and C. E. Youman (1996),. *Role-Based Access Control Models*.IEEE Computer, vol. 29(2), pp. 38-47.

Sandhu.R. (1993), "Lattice-based access control models". IEEE Computer, 26(11):9–19, 1993.

Schaad A and Moffett J. **(2002),** 'A lightweight approach to specification and analysis of role-based access control extensions'. In Seventh ACM Symposium on Access Control Models and Technologies (SACMAT'02), pages 13–22. ACM Press

Schapire R. E. and Freund Y. and Bartlett P. and Lee W. Sun (1997), "Boosting the margin: a new explanation for the effectiveness of voting methods", Proc. 14th International Conference on Machine Learning", Morgan Kaufmann, 322--330, 1997

Schapire R., Singer Y. (1999), "Improved boosting algorithms using confidence-rated predictions. Machine learning 37(3): pp. 297-336.

Schroeder M.D., Saltzer J. (1975), "The protection of information in computer systems. IEEE, 63(9):1278–1308, September 1975.

Seamons K., Winsborough W., and Winslett M. (1997), "Internet Credential Acceptance Policies", Proceedings of the Workshop on Logic Programming for Internet Applications, Leuven, Belgium.

Seleznyov A., Mohamed A., Hailes S. (2004), "ADAM: An agent-based Middleware Architecture for Distributed Access Control" in *Proceedings of the 22nd International Multi-Conference on Applied Informatics: Artificial Intelligence and Applications,* 2004

Shafiq B., Joshi J., Bertino E., Ghafoor A. (2005), "Secure Interoperation in a Multidomain Environment Employing RBAC Policies," IEEE TKDE, vol. 17, No. 11, pp. 1557-1577, Nov., 2005

Shands D., Yee R., Jacobs J. (2000), "Secure Virtual Enclaves: Supporting Coalition Use of Distributed Application Technologies", Proceedings of the Network and Distributed Systems Security Symposium, San Diego, February 2000.

SpamAssassin (2004) http://spamassassin.org/publiccorpus

Tempich C., Ehrig M., Fluit C., Haase P., Marti E.L., Plechawski M., Staab S. (2004), "XAROP: A Midterm Report on Introducing a Decentralized Semantics based Application", in *Proceedings of Practical Aspects of Knowledge Management (PAKM 2004),* Vienna Austria, LNAI vol. 3336 Springer, pp. 259-270, 2004

Waterhouse S. R. and Robinson A. J. (1994) "Classification using hierarchical mixtures of experts". In Proceedings 1994 IEEE Workshop on Neural Networks for Signal Processing, pages 177--186, Long Beach CA, 1994. IEEE Press

Weippl E., Schatten A., Karim S., Tjoa A. (2004), "SemanticLIFE Collaboration: Security Requirements and solutions – security aspects of semantic knowledge management", in *Proceedings of Practical Aspects of Knowledge Management (PAKM 2004),* Vienna Austria, LNAI 3336 Springer, pp. 365-377, 2004

Winsborough W., K. E. Seamons, and V. E. Jones (2000), "Automated Trust Negotiation", DARPA Information Survivability Conference and Exposition, Hilton Head, January 2000.

X.509 (1997), I. T. Union. ITU-T recommendation X.509 (08/97) – information technology – open systems interconnection – the directory: Authentication framework, Aug. 1997. Internet X509 Public Key Infrastructure documents, http://www.ietf.org/rfc/rfc2459.txt

XML (2004), extensible Markup Language Specification (XML), http://www.w3.org/XML/, March 2004

XPATH (2005), XML Path Language, http://www.w3.org/TR/xpath

Yao C., Winsborough W., Jajodia S. (2005), "A hierarchical Release Control Framework", proceedings of IFIP 11.1 \& 11.5 Joint Working Conference on Security Management, Fairfax USA, December 2005.

Κοκκολάκης Σ. (2000). ''Ανάπτυξη και Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων'', Διδακτορική διατριβή, Οικονομικό Πανεπιστήμιο Αθηνών.