ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Έλεγχος Πρόσβασης Πληροφοριακών Συστημάτων με «Επίγνωση Πλαισίου» Βασισμένος σε Οντολογίες

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Άννα Π. Αντωνακοπούλου

Αθήνα, Οκτώβριος 2014

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Έλεγχος Πρόσβασης Πληροφοριακών Συστημάτων με «Επίγνωση Πλαισίου» Βασισμένος σε Οντολογίες

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Άννα Π. Αντωνακοπούλου

Συμβουλευτική Επιτροπή : Ι. Στ. Βενιέρης
Δήμητρα-Θεοδώρα Ι. Κακλαμάνη
Μιχαήλ Ε. Θεολόγου

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 29η Οκτωβρίου 2014.

.....	.....	.....
Ιάκωβος Βενιέρης	Δήμητρα-Θεοδώρα Κακλαμάνη	Μιχαήλ Θεολόγου
Καθηγητής Ε.Μ.Π	Καθηγήτρια Ε.Μ.Π	Καθηγητής Ε.Μ.Π
.....	.....	.....
Νικόλαος Ουζούνογλου	Χρήστος Δουληγέρης	Συμεών Παπαβασιλείου
Καθηγητής Ε.Μ.Π	Καθηγητής Παν. Πειραιώς	Αναπλ. Καθηγητής Ε.Μ.Π
	.....	
	Χρήστος Κακλαμάνης	
	Καθηγητής Παν. Πατρών	

Αθήνα, Οκτώβριος 2014

.....

Άννα Π. Αντωνακοπούλου

Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Copyright © Άννα Π. Αντωνακοπούλου, 2014.
Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

Στον πατέρα μου που έφυγε …
Στην κόρη μου που ήρθε…

Περίληψη

Η συνεχώς εξελισσόμενη φύση των υπολογιστικών συστημάτων και του όγκου συλλογής και ροής των πληροφοριών σε οργανισμούς και επιχειρήσεις, έχει ως αποτέλεσμα την έγερση ανησυχιών σχετικά με την ορθή διάθεση και χρήση των πληροφοριών και συνεπώς την ανάπτυξη λύσεων που εφαρμόζουν τις κατάλληλες πολιτικές ελέγχου πρόσβασης για την εκπλήρωση των απαιτήσεων ασφαλείας. Ως εκ τούτου, η παρούσα διατριβή έχει ως αντικείμενο τη σχεδίαση μοντέλου ελέγχου πρόσβασης (access control) με περιορισμούς «επίγνωσης πλαισίου» (context-aware) και «επίγνωσης ιδιωτικότητας» (privacy-aware) βασισμένο σε ρόλους (Role-based access control – RBAC). Εξετάζονται προτεινόμενες στη βιβλιογραφία λύσεις οι οποίες αφορούν σε μοντέλα ελέγχου πρόσβασης που ενσωματώνουν χαρακτηριστικά τα οποία έχουν σχεδιαστεί για την επιβολή πολιτικών προστασίας ασφαλείας και ιδιωτικότητας.

Η προσέγγιση που ακολουθεί η παρούσα διατριβή αφορά στην ενίσχυση και επέκταση των παραδοσιακών μοντέλων με χαρακτηριστικά και τεχνολογίες που έχουν αρχίσει να εφαρμόζονται έτσι ώστε οι πολιτικές ελέγχου πρόσβασης να γίνουν πληρέστερες και αποτελεσματικότερες, έχοντας επιπρόσθετα ως στόχο την εκπλήρωση των απαιτήσεων της νομοθεσίας και των προτιμήσεων ιδιωτικότητας των χρηστών αναφορικά με τη συλλογή και χρήση προσωπικών δεδομένων κατά την παροχή υπηρεσιών. Οι τεχνολογίες που εφαρμόζονται λαμβάνουν κυρίως υπ’ όψιν παραμέτρους «ευρύτερου πλαισίου» και «επίγνωσης ιδιωτικότητας» στη διαδικασία λήψης απόφασης, οι οποίες εκφράζουν χωρο-χρονικούς, ιστορικούς και άλλους περιβαλλοντικούς περιορισμούς.

Ως βάση του μοντέλου, σχεδιάστηκε ένα σημασιολογικό πλαίσιο, βασισμένο σε μία οντολογία για την ενίσχυση της εκφραστικότητας και επεξεργασίας των πληροφοριών πλαισίου/πολιτικών, το οποίο μοντελοποιεί επιπλέον τις θεμελιώδεις αρχές αναφορικά με την προστασία των προσωπικών δεδομένων, όπως αυτές πηγάζουν από τη νομοθεσία. Το μοντέλο επιπλέον τεκμηριώνεται και αξιολογείται με παράδειγμα της λειτουργίας του σε συγκεκριμένη περίπτωση χρήσης η οποία αφορά σε περιβάλλοντα παρακολούθησης δικτύων.

Λέξεις κλειδιά: εξουσιοδότηση, έλεγχος πρόσβασης, ιδιωτικότητα, πληροφορίες πλαισίου, οντολογία, σημασιολογικό μοντέλο, συλλογισμός, ψηφιακά πιστοποιητικά, Υποδομή Δημόσιου Κλειδιού, Υποδομή Διαχείρισης Δικαιωμάτων

Abstract

The constantly evolving nature of computer systems and the volume of information collection and flow in organizations and businesses have resulted in raising concerns about the proper disposal and use of information and thus development of solutions that apply the appropriate access control policies in order to meet safety requirements. Therefore, this doctoral thesis deal with the design of a privacy and context aware access control model based on roles (Role-based access control - RBAC). The thesis examines some proposed in the literature solutions related with access control models that incorporate features which are designed to enforce policies for the protection of security and privacy.

The approach taken in this doctoral thesis concerns the strengthening and expansion of traditional models with features and technologies that have started to be implemented so that access control policies to be more comprehensive and effective, having additionally as goal to meet the requirements of legislation and the privacy preferences of users regarding the collection and usage of personal data in the provision of services. The technologies applied mainly take into account parameters of “broader context” and “awareness of privacy” in the decision-making process. These parameters express spatio-temporal, historical and other environmental constraints.

As the basis of the model, a semantic framework has been designed, based on an ontology in order to enhance expressiveness and processing of contextual information or policies, which additionally models the fundamental principles regarding the protection of personal data, such as those stemming from the legislation. The model is further evaluated and documented through an example of its operation at a particular use case related to network monitoring environments.

Keywords: authorization, access control, privacy, contextual information, semantic model, ontology, reasoning, digital certificates, Public Key Infrastructure, Privilege Management Infrastructure.

Ευχαριστίες

Η παρούσα διδακτορική διατριβή αποτελεί το επιστέγασμα μιας ερευνητικής προσπάθειας που διήρκησε αρκετά χρόνια. Θα ήθελα μέσα από την καρδιά μου να ευχαριστήσω τον επιβλέποντά μου κ. Ιάκωβο Βενιέρη, Καθηγητή Ε.Μ.Π., για την εμπιστοσύνη που επέδειξε στις δυνατότητές μου αλλά και τη στήριξή του για όλα αυτά τα χρόνια, καθώς και την Καθηγήτρια Ε.Μ.Π. κα. Δήμητρα-Θεοδώρα Κακλαμάνη για τη συνεχή υποστήριξη και καθοδήγηση.

Ένα ιδιαίτερο ευχαριστώ αρμόζει σε όλους τους συναδέρφους μου στο εργαστήριο «Ευφυών Επικοινωνιών και Δικτύων Ευρείας Ζώνης».

Ιδιαίτερα θα ήθελα να ευχαριστήσω τους τρείς κοντινότερους συνεργάτες μου. Πρώτα το Δρ. Γιώργο Λιουδάκη, για την καθοδήγηση και τη στήριξή του και στη συνέχεια τους Δρ. Φώτη Γώγουλο και Δρ. Αζίζ Μουσά για τη συμμετοχή και τη βοήθειά τους καθ’ όλη τη διάρκεια της διατριβής.

Τέλος, ένα μεγάλο ευχαριστώ στην οικογένεια μου, τους γονείς μου Παναγιώτη και Μαρία, τον αδερφό μου Φώτη, το σύζυγο μου Δημήτρη και τους αγαπημένους μου φίλους για τη συνεχή συμπαράσταση και την πίστη που έδειξαν καθ’ όλη τη διάρκεια των σπουδών μου.

Περιεχόμενα

Περίληψη 6
Abstract 8
Ευχαριστίες 9
Περιεχόμενα 11
Ευρετήριο Εικόνων 13
Ευρετήριο Πινάκων 14
Κεφάλαιο 1 16
Εισαγωγή 16
1.1 Πλαίσιο της διατριβής 16
1.1.2 Έλεγχος πρόσβασης πληροφοριακών συστημάτων 20
1.1.3 Ιδιωτικότητα 22
1.1.4 Ορισμοί Οντολογιών 24
1.2 Διάρθρωση Διατριβής 26
Κεφάλαιο 2 28
Τεχνολογίες και απαιτήσεις ελέγχου πρόσβασης 28
2.1 Παραδοσιακές λύσεις ελέγχου πρόσβασης 28
2.1.1 Προαιρετικός και Υποχρεωτικός έλεγχος πρόσβασης (DAC & MAC) 29
2.1.2 Έλεγχος πρόσβασης βάσει ρόλων (RBAC) 32
2.2 Αξιοποιώντας τον έλεγχο πρόσβασης για την προστασία της ιδιωτικότητας 36
2.2.1 Ιδιωτικότητα και νομοθεσία 37
2.2.2 Ζητήματα και απαιτήσεις ελέγχου πρόσβασης για την εφαρμογή προστασίας της ιδιωτικότητας 46
2.2.3 Μειονεκτήματα του μοντέλου RBAC όσον αφορά την ιδιωτικότητα 49
2.3 Μηχανισμοί εξουσιοδοτήσεων 51
2.3.1 Κρυπτογραφία 52
2.3.2 Ψηφιακές υπογραφές και Ψηφιακά πιστοποιητικά 52
2.3.4 Υποδομή Δημόσιου Κλειδιού και Υποδομή Διαχείρισης Δικαιωμάτων 55
2.4 Επίγνωση πλαισίου στον έλεγχο πρόσβασης 57
2.4.1 Παράμετροι επίγνωσης πλαισίου 59
2.4.2 Περιορισμοί πλαισίου που στοχεύουν στην προστασία της ιδιωτικότητας . 60

2.5 Σημασιολογικές τεχνολογίες στον έλεγχο πρόσβασης με επίγνωση πλαισίου και επίγνωση ιδιωτικότητας 66
2.5.1 Δομικά στοιχεία οντολογιών 67
2.5.2 Οντολογίες σχετικές με την ιδιωτικότητα 68
2.5.3 Σύγκριση και παρατηρήσεις 75
Κεφάλαιο 3 78
Συγκριτική μελέτη και εξαγωγή απαιτήσεων μοντέλων ελέγχου πρόσβασης 78
3.1 Μοντέλα ελέγχου πρόσβασης με επίγνωση πλαισίου 78
3.2 Μοντέλα ελέγχου πρόσβασης με επίγνωση ιδιωτικότητας και επίγνωση πλαισίου 83
3.3 Σημασιολογικά μοντέλα ελέγχου πρόσβασης με επίγνωση πλαισίου 90
3.4 Σύνοψη χαρακτηριστικών μοντέλων ελέγχου πρόσβασης επίγνωσης πλαισίου και ιδιωτικότητας 94
3.4.1 Ενσωμάτωση του πλαισίου ιδιωτικότητας 96
3.4.2 Πλεονεκτήματα και Περιορισμοί 97
Κεφάλαιο 4 100
Μοντέλο ελέγχου πρόσβασης 100
4.1 Βασικές αρχές της προτεινόμενης λύσης 101
4.2 Συσχετίσεις μεταξύ των συνόλων 102
4.3 Κανόνες ελέγχου πρόσβασης 105
4.4 Πληροφορίες πλαισίου 106
Κεφάλαιο 5 109
Οντολογία ελέγχου πρόσβασης 109
5.1 Βασικές Κλάσεις Οντολογίας ελέγχου πρόσβασης 110
5.1.1 Η κλάση PersonalData 110
5.1.2 Η κλάση Purposes 111
5.1.3 Η κλάση Roles 112
5.1.4 Η κλάση Actions 112
5.2 Η κλάση Rules 113
5.3 Βοηθητικές Κλάσεις 114
5.3.1 Η κλάση ExclusiveCombinations 114
5.3.2 Η κλάση Obligations 114
5.3.3 Η κλάση Conditions και συμπληρωματικές κλάσεις πλαισίου 115
5.3.4 Η κλάση ContextualBase 117

Κεφάλαιο 6 125
Αρχιτεκτονική προτεινόμενης λύσης 125
6.1 Εξαγωγή πολιτικών πρόσβασης 126
6.2 Περιγραφή του συστήματος 128
6.3 Διαδικασία συλλογιστικής 129
6.3.1 Στατική συλλογιστική 130
6.3.2 Δυναμική συλλογιστική 139
6.4 Ψηφιακά Πιστοποιητικά: Δομή και Διαχείριση 142
6.5 Δομή Πλατφόρμας Εξουσιοδοτήσεων 149
6.5.1 Διαχειριστής Συναλλαγών 150
6.5.2 Διαχειριστής Συνόδων 151
6.6 Ελεγκτής Διασφάλισης Ιδιωτικότητας 152
6.6.1 Λογισμικό Προδιαγραφής Μοντέλου Ελέγχου Πρόσβασης 153
6.7 Διαδικασία αυθεντικοποίησης και εξουσιοδότησης 155
Κεφάλαιο 7 159
Παράδειγμα Χρήσης και Αξιολόγηση 159
7.1 Σχετικό Υπόβαθρο 160
7.2 Ζητήματα προστασίας της ιδιωτικότητας σε περιβάλλοντα παρακολούθησης δικτύων 162
7.3 Βασικό Σενάριο Χρήσης 164
7.4 Αξιολόγηση 167
Συμπεράσματα και μελλοντική εργασία 170
Βιβλιογραφία 174
Δημοσιεύσεις 183
Διεθνή επιστημονικά περιοδικά 183
Κεφάλαια σε βιβλία 183
Πρακτικά διεθνών επιστημονικών συνεδρίων 183
Συνοπτικό Βιογραφικό Σημείωμα 185

Ευρετήριο Εικόνων

Εικόνα 1. Στοιχεία Πληροφοριακού Συστήματος 20
Εικόνα 2: Η λογική του ελέγχου πρόσβασης με βάση τους ρόλους 33
Εικόνα 3: Οικογένεια RBAC 34

Εικόνα 4: Επιμέρους χαρακτηριστικά RBAC....36
Εικόνα 5: Οι βασικές Αρχές Ιδιωτικότητας....41
Εικόνα 6: Εφαρμογή Ιδιωτικότητας στον έλεγχο πρόσβασης....49
Εικόνα 7: Πληροφορίες Επίγνωσης Πλαισίου....65
Εικόνα 8: Πλαίσιο Ιδιωτικότητας....66
Εικόνα 9: Το μοντέλο GEO-RBAC....79
Εικόνα 10: Το σύστημα X-GTRBAC....81
Εικόνα 11: Προφίλ επέκτασης RBAC για XACML....82
Εικόνα 12: Ιεραρχία Σκοπών στο μοντέλο Pu-BAC....84
Εικόνα 13: Το μοντέλο PuRBAC....86
Εικόνα 14: Το μοντέλο OrBAC....88
Εικόνα 15: Οικογένεια μοντέλου P-RBAC....89
Εικόνα 16: Εξουσιοδότηση στο P-RBAC....90
Εικόνα 17: Το πλαίσιο RBAC with XACML+OWL....92
Εικόνα 18: Το σύστημα GTHBAC....93
Εικόνα 19: Το προτεινόμενο σημασιολογικό μοντέλο....110
Εικόνα 20: Ο γράφος δεδομένων....111
Εικόνα 21: Παράδειγμα συνθήκης χρονικού τύπου πλαισίου....118
Εικόνα 22: Παράδειγμα συνθήκης χρονικού τύπου πλαισίου....119
Εικόνα 23: Εκτεταμένο σχήμα της Οντολογίας....120
Εικόνα 24: Η κλάση IDMEFalert....120
Εικόνα 25: Οι κλάσεις AlertTarget και AlertSource....121
Εικόνα 26: Αρχιτεκτονική του συστήματος....128
Εικόνα 27: Ενδεικτικός κανόνας SWRL....133
Εικόνα 28: Χρόνος εκτέλεσης λογισμικού Pellet....133
Εικόνα 29: Αλγόριθμος υπολογισμού των αντικειμένων του συνόλου *PDT*....137
Εικόνα 30: Χρόνος εκτέλεσης λογισμικού παραγωγής συμπερασμάτων (1)....137
Εικόνα 31: Χρόνος εκτέλεσης λογισμικού παραγωγής συμπερασμάτων (2)....137
Εικόνα 32: Permanent Public Key Certificates – P-PKCs....143
Εικόνα 33: User Public Key Certificates – U-PKCs....144
Εικόνα 34: Role Attribute Certificates – R-ACs....145
Εικόνα 35: Permitted Data Types Attribute Certificates – PDT-ACs....146
Εικόνα 36: Δομή Πλατφόρμας Διαχείρισης Εξουσιοδοτήσεων....149
Εικόνα 37: Ο γράφος ρόλων....154
Εικόνα 38: Βήμα προς βήμα προδιαγραφή κανόνων εξουσιοδότησης....154
Εικόνα 39: Οθόνη ενημέρωσης λίστας ανάκλησης πιστοποιητικών....155
Εικόνα 40: Διαδικασία αυθεντικοποίησης και εξουσιοδότησης....158
Εικόνα 41: Οντολογική αναπαράσταση κανόνα σεναρίου χρήσης....166

Ευρετήριο Πινάκων

Πίνακας 1: Σύγκριση Οντολογιών Ιδιωτικότητας....76
Πίνακας 2: Συγκριτική μελέτη των μοντέλων ελέγχου πρόσβασης....95
Πίνακας 3: Οι OWL ιδιότητες της κλάσης Alerts....122

Πίνακας 4: Οι OWL ιδιότητες της Οντολογίας 124
Πίνακας 5: Διαφορετικές εκδόσεις εικονικών Οντολογιών Εξουσιοδότησης 132
Πίνακας 6: Χρόνος εξαγωγής μοναδικών αντικειμένων του συνόλου *PDT* 138

Κεφάλαιο 1

Εισαγωγή

1.1 Πλαίσιο της διατριβής

Οι πρόσφατες τεχνολογικές εξελίξεις όσον αφορά στην επεξεργασία των δεδομένων και τις επικοινωνιακές δυνατότητες της τεχνολογίας των πληροφοριών παρακινούν μια πληροφοριακή επανάσταση που επιφέρει σημαντικές βελτιώσεις στην ποιότητα της ζωής των πολιτών, νέες δυνατότητες και προοπτικές για τις επιχειρήσεις, συμπεριλαμβανομένων τη λειτουργική αποδοτικότητα, τη βελτίωση της ποιότητας των προϊόντων και υπηρεσιών, καθώς και τις δυνατότητες για καινοτομία.

Το γεγονός αυτό προβάλλει σοβαρούς κινδύνους για την ιδιωτικότητα, εννοώντας με αυτό την «απαίτηση των ατόμων, ομάδων, ή θεσμικών οργάνων να καθορίζουν κατά το δοκούν πότε, πώς, και σε ποιο εύρος οι πληροφορίες που τους αφορούν κοινοποιούνται σε τρίτους» (Westin, 1967). Η κλίμακα της προσωπικής συλλογής δεδομένων αυξάνεται, η πρόσβαση στις πληροφορίες, η επεξεργασία, η συγκέντρωση, ο συνδυασμός και η διασύνδεση διευκολύνονται, οι νέοι τύποι των δεδομένων που συλλέγονται και η αλυσίδα παροχής υπηρεσιών γίνεται πολύπλοκη, εμπλέκοντας πολλούς φορείς στην ανταλλαγή και την κοινή χρήση δεδομένων. Πάνω από έναν αιώνα μετά το δοκίμιο που προσδιορίζει ότι η προστασία της ιδιωτικής ζωής, ως θεμελιώδες ανθρώπινο δικαίωμα, είχε τεθεί σε κίνδυνο από τις τεχνολογικές εξελίξεις (Warren & Brandeis, 1890), οι πολίτες ποτέ πριν στην ιστορία δεν ήταν τόσο ανήσυχοι για την προστασία της και τις απειλές που προέρχονται από τις αναδυόμενες τεχνολογίες (Gallup Organization, 2008).

Από την άλλη πλευρά, η προστασία της ιδιωτικότητας έχει εξελιχθεί σε ένα εξέχον θέμα και αποτελεί επιχειρησιακή απαίτηση ακόμα και για τους οργανισμούς που αποτελούν συλλέκτες και επεξεργαστές προσωπικών δεδομένων. Καθώς η εμπιστοσύνη αναδεικνύεται στον πυρήνα της κοινωνικής τάξης, η έγκριση και η διάθεση των προϊόντων και των υπηρεσιών τους καθορίζεται από την αντίληψη του κινδύνου και του οφέλους των πιθανών χρηστών. Ως εκ τούτου, από την οπτική γωνία των οργανισμών, η αναγνώριση τη σημασίας της προστασίας της ιδιωτικότητας

έχει ως κίνητρο τις απώλειες των επιχειρήσεων λόγω παραβιάσεών της και τις ατυχίες που υποστηρίζουν τη δυσπιστία των χρηστών: η οικονομία αντιμετωπίζει εμπόδια λόγω των κινδύνων για την ιδιωτικότητα (Acquisti, 2010).

Επιπλέον, ο τομέας της ιδιωτικότητας αποτελεί μια νομοθετημένη περιοχή (Solove, 2006) και αρκετές χώρες, π.χ., του Καναδά και των μελών της Ευρωπαϊκής Ένωσης, έχουν υιοθετήσει νομοθεσία για την προστασία των δεδομένων, η οποία γενικά αντανακλά τις θεμελιώδεις αρχές, που θεμελιώθηκαν από τον Οργανισμό για την Οικονομική Συνεργασία και Ανάπτυξη στις κατευθυντήριες γραμμές ορόσημό του (OECD, 1980). Ως εκ τούτου, η κανονιστική συμμόρφωση και το δυναμικό των κυρώσεων αποτελούν τους κύριους λόγους για να δοθούν κίνητρα στις επιχειρήσεις για την υιοθέτηση δίκαιων επιχειρηματικών πρακτικών σε σχέση με τη διαχείριση των προσωπικών πληροφοριών. Προκειμένου οι επιχειρήσεις να εμπνεύσουν εμπιστοσύνη στους πελάτες τους, καθώς και να συμμορφωθούν με τη νομοθεσία προστασίας της ιδιωτικότητας, θεσπίζουν πρακτικές διαχείρισης δεδομένων που αντανακλώνται από τις πολιτικές προστασίας.

Πρόσφατα, αρκετά πλαίσια έχουν προκύψει για την τυποποίηση των προδιαγραφών των πολιτικών ιδιωτικότητας, ενώ τα προγράμματα της "σφραγίδας σεβασμού των προσωπικών δεδομένων" συχνά εντάσσονται ως μέτρα οικοδόμησης εμπιστοσύνης. Παρ 'όλα αυτά, οι πολιτικές προστασίας της ιδιωτικής ζωής και οι σφραγίδες από μόνες τους δεν είναι αποτελεσματικές από λειτουργική άποψη. Μια κρίσιμη πρόκληση αφορά την αυτοματοποίηση της εφαρμογής τους ή, με άλλα λόγια, την υλοποίησή τους από τεχνικά μέσα και την ενσωμάτωσή τους με τα υποκείμενα συστήματα Τεχνολογίας της Πληροφορίας και Τηλεπικοινωνιών (ΤΠΤ).

Μία από τις πιο σημαντικές τεχνολογίες που επιτρέπουν την επιβολή των δίκαιων πρακτικών δεδομένων είναι ο έλεγχος πρόσβασης. Στην πραγματικότητα, οποιαδήποτε παραβίαση της ιδιωτικής ζωής σίγουρα περιλαμβάνει μερική πρόσβαση στα προσωπικά δεδομένα και, κατά συνέπεια, ο έλεγχος πρόσβασης αποτελεί θεμελιώδη πτυχή της προστασίας της ιδιωτικότητας.

Η ανάπτυξη ενός συστήματος ελέγχου πρόσβασης γίνεται συνήθως με μια πολυφασική προσέγγιση που βασίζεται στις ακόλουθες αρχές: τις πολιτικές ελέγχου πρόσβασης, τα μοντέλα ελέγχου πρόσβασης, και τους μηχανισμούς ελέγχου

πρόσβασης (Samarati, 2001). Οι πολιτικές ελέγχου πρόσβασης είναι στην πραγματικότητα υψηλού επιπέδου κανόνες που καθορίζουν τον τρόπο με τον οποίο η πρόσβαση τελεί υπό τη διαχείριση των μηχανισμών ελέγχου πρόσβασης, πως τα υποκείμενα μπορούν να έχουν πρόσβαση σε πόρους και υπό ποιες συνθήκες. Οι πολιτικές ελέγχου πρόσβασης εξασφαλίζονται και υλοποιούνται με ένα μηχανισμό ελέγχου πρόσβασης που μεταφράζει τα αιτήματα πρόσβασης με βάση τη δομή που παρέχει το σύστημα ελέγχου πρόσβασης. Για παράδειγμα, μια λίστα ελέγχου πρόσβασης (ACL) είναι ένα γνωστός μηχανισμός ελέγχου πρόσβασης. Τα μοντέλα ελέγχου πρόσβασης γεφυρώνουν το χάσμα αφαιρετικότητας ανάμεσα στην πολιτική ελέγχου πρόσβασης και στο μηχανισμό ελέγχου πρόσβασης που την εφαρμόζει. Ένα μοντέλο ελέγχου πρόσβασης παρέχει μια επίσημη εκπροσώπηση του πώς λειτουργεί η πολιτική ελέγχου πρόσβασης, επιτρέποντας να επαληθεύσει τις ιδιότητες και την ασφάλεια που παρέχεται από το σχεδιασμένο σύστημα ελέγχου πρόσβασης. Αντί να προσπαθεί να αξιολογήσει και να αναλύσει τα συστήματα ελέγχου πρόσβασης αποκλειστικά στο επίπεδο του μηχανισμού, τα μοντέλα ελέγχου πρόσβασης συνήθως γράφονται για να περιγράψουν τις ιδιότητες ασφάλειας ενός συστήματος ελέγχου πρόσβασης.

Ως εκ τούτου, τα μοντέλα ελέγχου πρόσβασης αποτελούν την επίσημη παρουσίαση της πολιτικής ασφάλειας που επιβάλλεται από το σύστημα και είναι χρήσιμα για την απόδειξη των θεωρητικών ορίων και μειονεκτημάτων ενός συστήματος ελέγχου πρόσβασης.

Τα παραδοσιακά μοντέλα ελέγχου πρόσβασης, όπως ο Προαιρετικός Έλεγχος πρόσβασης (Discretionary Access Control - DAC) (NCSC, 1987), ο Υποχρεωτικός Έλεγχος Πρόσβασης (Mandatory Access Control (MAC) (Pfleeger, 1997) και ο Έλεγχος Πρόσβασης βασισμένος σε Ρόλους (Role based Access Control - RBAC) (Ferraiolo et al, 2001), (Sandhu et al, 1996) αποτυγχάνουν να ανταποκριθούν στις απαιτήσεις που απορρέουν από τις θεμελιώδεις αρχές προστασίας της ιδιωτικότητας (OECD, 1980) οι οποίες απαιτούν την ενσωμάτωση διαφορετικών κριτηρίων στις αποφάσεις ελέγχου πρόσβασης και όχι μόνο πληροφορίες για το ποιος χρήστης, με ποιο ρόλο, εκτελεί ποια δράση και σε ποιο δεδομένο. Από την άποψη αυτή, η ανάπτυξη μοντέλων ελέγχου πρόσβασης ειδικά προσαρμοσμένων για την προστασία

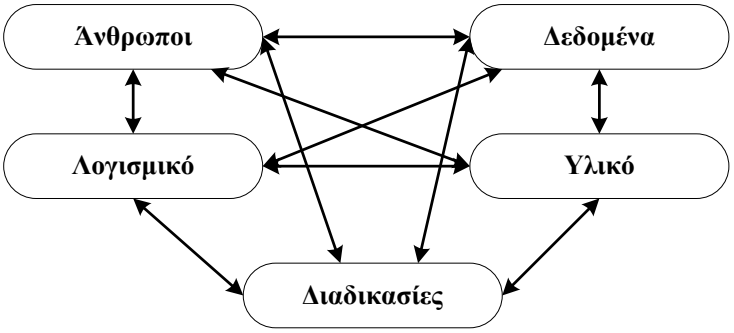
της ιδιωτικότητας αποτελεί το επίκεντρο εντατικής έρευνας τα τελευταία χρόνια. Η τάση αυτή, η οποία αναφέρεται ως "έλεγχος πρόσβασης με επίγνωση ιδιωτικότητας", αφορά συνήθως την ενίσχυση των παραδοσιακών προσεγγίσεων με άλλες τεχνολογίες που έχουν αρχίσει να εφαρμόζονται στον έλεγχο πρόσβασης που είναι ή θα πρέπει να λειτουργήσουν ως μοχλός σε συνδυασμό με την προστασία της ιδιωτικότητας, προκειμένου οι πολιτικές ελέγχου πρόσβασης να γίνουν πιο αποτελεσματικές. Σε αυτά περιλαμβάνονται παράμετροι πλαισίου ως μέρος της διαδικασίας λήψης αποφάσεων, καθώς και η χρήση σημασιολογικών τεχνολογιών για την ενίσχυση της εκφραστικότητας και των δυνατοτήτων επεξεργασίας.

Τα μοντέλα ελέγχου πρόσβασης που θα παρουσιαστούν στις επόμενες ενότητες παρέχουν τα πιο αντιπροσωπευτικά και πλήρη πλαίσια στη βιβλιογραφία όσον αφορά στις προδιαγραφές, στη διαχείριση και στην επιβολή τόσο του παραδοσιακού ελέγχου πρόσβασης με επίγνωση πλαισίου όσο και των πολιτικών προστασίας ιδιωτικότητας, εκμεταλλευόμενα τα οφέλη του μοντέλου RBAC. Η χρήση του μοντέλου RBAC βοηθά τους οργανισμούς να διαχειρίζονται με ασφάλεια το ολοένα και πιο μεγάλο αριθμό χρηστών. Οδηγεί διαισθητικά στον τρόπο με τον οποίο διαχειρίζονται οι εργασιακοί ρόλοι και οι αρμοδιότητες, και επομένως είναι εύκολο στην κατανόηση και τη χρήση. Οι επιχειρήσεις μπορούν να ομαδοποιήσουν μεμονωμένους χρήστες σε ομάδες που έχουν παρόμοιες αρμοδιότητες εργασίας ή κοινά προνόμια ασφάλειας και ως εκ τούτου να διαχειρίζονται περιορισμένο αριθμό χρηστών σε ομάδες, σε αντίθεση με τη διαχείριση εκατοντάδων ή εκατομμύριων μεμονωμένων χρηστών. Οι επιχειρήσεις με τη σειρά τους, μπορούν να διαθέσουν αυτούς τους ρόλους και τις πολιτικές ασφαλείας σε κατ' εξουσιοδότηση διαχειριστές εντός της εταιρείας ή σε οργανισμούς-εταίρους τους, οι οποίοι μπορούν αποτελεσματικά να ελέγχουν και να διαχειρίζονται τις δικές τους ομάδες χρηστών. Επιπλέον, το μοντέλο RBAC είναι ιδιαίτερα ευέλικτο και μπορεί να έχει πολλές παραλλαγές με εξελιγμένα χαρακτηριστικά (π.χ. ιεραρχίες ρόλων, δυναμικούς περιορισμούς διαχωρισμού καθηκόντων), καθιστώντας δυνατή την επίτευξη πιο πολύπλοκων επιχειρησιακών αναγκών. Ως αποτέλεσμα, οι χρήστες αποκτούν πρόσβαση σε εκείνες μόνο τις πληροφορίες που χρειάζονται για να εκπληρώσουν τις ευθύνες και τα καθήκοντά τους, προκειμένου να προστατευθεί η ιδιωτικότητα των δεδομένων και να επιτευχθεί ο έλεγχος πρόσβασης.

1.1.2 Έλεγχος πρόσβασης πληροφοριακών συστημάτων

Ο όρος πληροφοριακό σύστημα είναι ένας γενικότερος όρος που συμπεριλαμβάνει την υποδομή της πληροφορικής τεχνολογίας. Αποτελεί ένα γενικό όρο που αντιστοιχεί συνήθως στο σύνολο των πληροφοριακών συστημάτων που αποτελούνται από την υποδομή της πληροφορικής τεχνολογίας και άλλων παραγόντων, πχ. άνθρωποι. Πιο συγκεκριμένα, είναι ένα σύνολο διασυνδεδεμένων συστημάτων που συλλέγουν, επεξεργάζονται, αποθηκεύουν και διανέμουν την πληροφορία σχετικά με την επιχείρηση ή το περιβάλλον της για την υποστήριξη της λήψης απόφασης, το συντονισμό και τον έλεγχό της.

Τα βασικά στοιχεία ενός πληροφοριακού συστήματος, όπως δείχνει και η Εικόνα 1 είναι το υλικό (hardware), το λογισμικό (software), το δίκτυο, η βάση δεδομένων, οι διαδικασίες (δηλ. το σύνολο των οδηγιών για τη χρήση και το συνδυασμό όλων των στοιχείων της υποδομής του πληροφοριακού συστήματος) και οι άνθρωποι (δηλ. το σύνολο των ανθρώπων που εργάζονται με το πληροφοριακό σύστημα σε διάφορους ρόλους πχ. χρήστες, διαχειριστές, κατασκευαστές κ.α.).



Εικόνα 1. Στοιχεία Πληροφοριακού Συστήματος

Ο έλεγχος της πρόσβασης σε ένα Πληροφοριακό Σύστημα επιτυγχάνεται με ένα σύνολο μηχανισμών και τεχνικών με τους οποίους οριοθετείται η ελεγχόμενη πρόσβαση στους πόρους του συστήματος. Οι πόροι που πρέπει να προστατευθούν από μη εξουσιοδοτημένη πρόσβαση είναι, μεταξύ άλλων, η μνήμη, οι συσκευές εισόδου/εξόδου, οι διαμοιραζόμενες εφαρμογές/εργαλεία και τα δεδομένα τους. Για να επικοινωνήσει ένας χρήστης με ένα πληροφοριακό σύστημα πρέπει πρώτα από όλα το ένα μέρος (το σύστημα) να βεβαιωθεί για την ταυτότητα του άλλου. Έτσι η σύνδεση και επικοινωνία μεταξύ του χρήστη και του πληροφοριακού συστήματος

γίνεται στο σημείο διεπαφής και προϋποθέτει την τήρηση μιας διαδικασίας η οποία εξασφαλίζει ότι το άλλο μέρος είναι αυτό που πρέπει να είναι. Η διαδικασία της αλληλεπιβεβαίωσης περιέχει τα ακόλουθα στάδια:

Α) Στάδιο ταυτοποίησης (identification)

Στο στάδιο αυτό ο χρήστης καλείται να αναφέρει την ταυτότητά του, δηλαδή να διευκρινίσει στο σύστημα ποιος αιτείται προσπέλασης. Ο χρήστης εισάγει μια συμβολοσειρά που γνωρίζει (π.χ. ένα κωδικό όνομα) ή κάτι που κατέχει (π.χ. μια κάρτα), τα οποία είναι γνωστά εκ των προτέρων στο σύστημα και δεν είναι απαραίτητο να τηρούνται μυστικά ούτε να λαμβάνεται κάποιο μέτρο για την προστασία της αναγγελίας τους.

Β) Στάδιο αυθεντικοποίησης (authentication)

Στο στάδιο αυτό ο χρήστης επιβεβαιώνει ότι είναι αυτός που ισχυρίστηκε στο στάδιο της αυθεντικοποίησης. Η επιβεβαίωση αυτή μπορεί να πραγματοποιηθεί με την χρήση ενός τεκμηρίου (token) από την πλευρά του χρήστη, το οποίο πρέπει πάλι να είναι γνωστό από πριν στο σύστημα, αλλά σε αντίθεση με το προηγούμενο στάδιο πρέπει να τηρείται μυστικό από τρίτες οντότητες και να τυγχάνει ιδιαίτερης προστασίας. Το τεκμήριο αυτό μπορεί να είναι:

- Κάτι που γνωρίζει ο χρήστης (ένα συνθηματικό (password), δηλαδή μια συμβολοσειρά χαρακτήρων η οποία μεταδίδεται κρυπτογραφημένη στο σύστημα)
- Κάτι που κατέχει ο χρήστης (μία smart card)
- Κάτι που χαρακτηρίζει τον χρήστη (ένα βιομετρικό χαρακτηριστικό του π.χ, δακτυλικά αποτυπώματα, χρώμα ίριδας κλπ)

Γ) Στάδιο εξουσιοδότησης (authorization)

Στο στάδιο αυτό, το οποίο αποτελεί και το αντικείμενο μελέτης της παρούσας διατριβής, αφού έχουν αναγνωρισθεί θετικά τα δύο επικοινωνούντα μέρη, ελέγχονται διεξοδικά οι επιμέρους όροι της συνεργασίας (π.χ. δικαιώματα χρήσης αντικειμένων συστήματος, πρόσβασης σε αρχεία κλπ) με την βοήθεια ειδικών μηχανισμών ελέγχου πρόσβασης. Η φιλοσοφία της λειτουργίας τους στηρίζεται στην αντιστοίχιση

λογαριασμών χρηστών και πόρων του συστήματος, ανάλογα με τα συγκεκριμένα δικαιώματα πρόσβασης του κάθε χρήστη ή ομάδας χρηστών για κάθε πόρο ή ομάδα πόρων.

1.1.3 Ιδιωτικότητα

Ο σχεδιασμός ενός επιχειρησιακού συστήματος ή υπηρεσίας δεν μπορεί να θεωρηθεί ως μία καθαρά τεχνική δραστηριότητα, καθώς σαφώς έχει σημαντικό κοινωνικό αντίκτυπο από την άποψη των συνεπειών για την προστασία των προσωπικών δεδομένων και το δικαίωμα στην ιδιωτικότητα. Επιπλέον, η δημόσια πολιτική και οι κανονιστικές απαιτήσεις επηρεάζουν σημαντικά τις τεχνικές απαιτήσεις ενός τέτοιου συστήματος. Ως εκ τούτου, η παροχή της συνολικής εικόνας των βασικών αρχών κρίνεται απαραίτητη.

Από φιλοσοφική άποψη, η έννοια της ιδιωτικότητας διαθέτει ευρείες ιστορικές ρίζες, για παράδειγμα, σκεφτείτε τη διάκριση του Αριστοτέλη ανάμεσα στον δημόσιο τομέα της πολιτικής δραστηριότητας και του ιδιωτικού τομέα που σχετίζεται με την οικογενειακή ζωή, ή ο Όρκος του Ιπποκράτη, το δοκίμιο σχετικά με την ηθική της ιατρικής πρακτικής που περιλαμβάνει ρητά την προστασία της ιδιωτικής ζωής μεταξύ των ιατρικών ηθών.

Σήμερα, η προστασία της ιδιωτικότητας είναι αναγνωρισμένη ως θεμελιώδες ανθρώπινο δικαίωμα από την Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων των Ηνωμένων Εθνών (United Nations, 1948) και προστατεύεται από τη σχετική νομοθεσία σε όλες τις δημοκρατικές χώρες του κόσμου. Υποστηρίζει την ανθρώπινη αξιοπρέπεια και άλλες αξίες όπως η ελευθερία του συνεταιρίζεσθαι και της ελευθερίας του λόγου. Έχει γίνει ένα από τα σημαντικότερα δικαιώματα του ανθρώπου της σύγχρονης εποχής. Από όλα τα ανθρώπινα δικαιώματα στο διεθνή κατάλογο, η προστασία της ιδιωτικής ζωής είναι ίσως το πιο δύσκολο να προσδιοριστεί. Πιο συγκεκριμένα, στο άρθρο 12 αναφέρεται ότι «*κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του*». Το άρθρο καταλήγει τονίζοντας την αναγκαιότητα θέσπισης των σχετικών νόμων προστασίας αναφέροντας ότι «*καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους*».

Ταυτόχρονα η ιδιωτικότητα προστατεύεται ως αγαθό σε μια σειρά από σημαίνουσες συνθήκες για τα ανθρώπινα δικαιώματα ανά τον κόσμο με σπουδαιότερες όλων την Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (European Convention on Human Rights) (Συμβούλιο της Ευρώπης, 1950) και το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα (International Covenant on Civil and Political Rights) (Ηνωμένα Έθνη, 1966).

Η Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου και των Θεμελιωδών Ελευθεριών συντάχθηκε στις τάξεις του Συμβουλίου της Ευρώπης το 1950 με σκοπό την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών του ατόμου. Στο άρθρο 8 της σύμβασης αναφέρεται ότι *«κάθε πρόσωπο δικαιούται σεβασμό της ιδιωτικής και οικογενειακής του ζωής, της κατοικίας του και της αλληλογραφίας του»*. Το άρθρο συμπληρώνει ότι «*δεν επιτρέπεται η επέμβαση δημοσίας αρχής κατά την άσκηση του παραπάνω δικαιώματος, εκτός εάν η επέμβαση αύτη προβλέπεται από τον νόμο και αποτελεί μέτρο το οποίο, στα πλαίσια μιας δημοκρατικής κοινωνίας, κρίνεται αναγκαίο για την εθνική και δημόσια ασφάλεια, την οικονομική ευημερία της χώρας, την προάσπιση της τάξης και την πρόληψη ποινικών παραβάσεων, την προστασία της υγείας ή της ηθικής, ή την προστασία των δικαιωμάτων και άλλων ελευθεριών»*.

Το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα αποτελεί μια πολυμερή συμφωνία μεταξύ των μελών της Γενικής Συνέλευσης του Ο.Η.Ε που υιοθετήθηκε το 1966 και βρίσκεται σε ισχύ από το 1976. Το σύμφωνο επιβάλει στα υπογράφοντα μέλη τον σεβασμό των ατομικών και πολιτικών δικαιωμάτων των πολιτών ενώ μαζί με την Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα και το Διεθνές Σύμφωνο για τα Οικονομικά, Κοινωνικά και Πολιτιστικά/Μορφωτικά Δικαιώματα (International Covenant on Economic, Social and Cultural Rights) συναπαρτίζουν τον Διεθνή Χάρτη των Ανθρωπίνων Δικαιωμάτων (International Bill of Human Rights). Το άρθρο 17 του συμφώνου αποτελεί ουσιαστικά μια αναδιατύπωση του άρθρου 12 της Οικουμενικής Διακήρυξης των Δικαιωμάτων του Ανθρώπου περί σεβασμού της ιδιωτικής ζωής του ατόμου και της προστασίας του από τον νόμο.

Οι ορισμοί της ιδιωτικότητας ποικίλλουν ευρέως ανάλογα με το πλαίσιο και το περιβάλλον. Σε πολλές χώρες, η έννοια έχει τηχθεί με την προστασία των δεδομένων, η οποία ερμηνεύει την προστασία της ιδιωτικότητας όσον αφορά τη διαχείριση των προσωπικών πληροφοριών. Έξω από αυτό το μάλλον αυστηρό πλαίσιο, η προστασία της ιδιωτικότητας συχνά θεωρείται ως ένας τρόπος για να γίνει ο διαχωρισμός κατά πόσο η κοινωνία μπορεί να αναμειγνύεται στις υποθέσεις ενός ατόμου. Η έλλειψη ενός ενιαίου ορισμού δεν πρέπει να σημαίνει ότι το θέμα δεν έχει σημασία. Όπως μπορεί να παρατηρηθεί, "κατά μία έννοια, όλα τα ανθρώπινα δικαιώματα αποτελούν πτυχές του δικαιώματος στην ιδιωτικότητα".

1.1.4 Ορισμοί Οντολογιών

Ο όρος οντολογία (ontology) προέρχεται από τη φιλοσοφία και έχει εισαχθεί στο πεδίο της μηχανικής γνώσης ως ένα μέσο αναπαράστασης της γνώσης. Οι οντολογίες ως τυπικά εννοιολογικά μοντέλα αναπαράστασης μιας περιοχής γνώσης χρησιμοποιούνται για την επαναχρησιμοποίηση και το διαμοιρασμό αυτής της γνώσης. Από φιλοσοφικής πλευράς, η οντολογία ορίζεται ως η επιστήμη που μελετά την ύπαρξη, τη φύση και τις σχέσεις των όντων (Αριστοτέλης).

Πρόσφατα, οι οντολογίες έχουν εφαρμοστεί σε πολλά επιστημονικά πεδία, οπότε ο ορισμός τους εξελίσσεται επηρεαζόμενος από την εφαρμογή τους σε αυτά. Στη διεθνή βιβλιογραφία είναι δυνατό να εντοπιστούν πολλοί ορισμοί για το τι είναι η οντολογία. Ένας από τους πρώτους ορισμούς είναι ο παρακάτω. «*Μια οντολογία ορίζει τους βασικούς όρους και τις σχέσεις που αποτελούν το λεξικό μιας περιοχής ενδιαφέροντος καθώς και τους κανόνες για το συνδυασμό των όρων και των σχέσεων με σκοπό την επέκταση του λεξικού*» (Neches et al., 1991). Ο ορισμός αυτός αναγνωρίζει τους βασικούς όρους και τις σχέσεις μεταξύ των όρων, τους κανόνες που συνδυάζουν τους όρους και παρέχει τους ορισμούς των όρων και των σχέσεων. Από αυτό τον ορισμό, προκύπτει ότι μια οντολογία δεν περιλαμβάνει μόνο τους όρους που ορίζονται με σαφήνεια, αλλά και τη γνώση που εξάγεται με βάση τους κανόνες που περικλείονται στην οντολογία.

Στην επιστήμη και την τεχνητή νοημοσύνη, μια οντολογία αποτελείται από τις ρητές προδιαγραφές της αντίληψης για τον κόσμο (Gruber, 1993) "*an explicit specification of conceptualization*" ή ορίζεται ως η τυπική προδιαγραφή μίας κοινής

αντίληψης για τον κόσμο (Borst, 1997) "*a formal specification of a shared conceptualization*". Ο Fensel (2001), επιχειρώντας να αναλύσει τους σύνθετους εννοιολογικά αυτούς ορισμούς, αναγνωρίζει τις βασικές έννοιες που εμπεριέχονται σε αυτούς. Την "εννοιολογική αναπαράσταση", που αναφέρεται σε ένα αφηρημένο μοντέλο ενός φαινομένου, τον όρο «τυπική», που υποδηλώνει μια ακριβή μαθηματικά περιγραφή, τον όρο «σαφής», που εκφράζει την ακρίβεια των εννοιών και των εμφανώς ορισμένων σχέσεών τους και τον όρο «διαμοιρασμένη», που υποδηλώνει την ύπαρξη μιας συμφωνίας μεταξύ εκείνων που χρησιμοποιούν τις οντολογίες. Με αυτή την εξήγηση, περιγράφει πώς η φιλοσοφική φύση των οντολογιών ενσωματώνεται στις άλλες επιστήμες. Ο Guarino Guarino (1998) ορίζει την οντολογία ως «*μια λογική θεωρία που προτίθεται να ερμηνεύσει το νόημα ενός τυπικού λεξιλογίου*», εισάγοντας την έννοια της σημασιολογίας στον ορισμό της οντολογίας, ενώ οι Jasper και Uschold (1999) ορίζουν ότι μια οντολογία μπορεί να πάρει διάφορες μορφές, αλλά περιέχει απαραίτητα ένα λεξιλόγιο όρων και τον προσδιορισμό της σημασίας αυτών. Επίσης η οντολογία περιλαμβάνει ορισμούς και σχέσεις που συνδέουν τις έννοιες μεταξύ τους. Έτσι επιβάλλουν μια δομή για μια περιοχή ενδιαφέροντος περιορίζοντας τις πιθανές ερμηνείες των όρων που περιέχονται στην οντολογία. Αυτός ο ορισμός προσδιορίζει τις λειτουργίες των οντολογιών καθώς και την τεχνική προσέγγιση κατασκευής τους.

Για τους ανθρώπους, οι οντολογίες καθιστούν ικανή την καλύτερη πρόσβαση στην πληροφορία και επιδιώκουν κοινή κατανόηση, ενώ για τους υπολογιστές, οι οντολογίες διευκολύνουν την κατανόηση της πληροφορίας και την πιο διεξοδική επεξεργασία. Διευκολύνουν το διαμοιρασμό και την επαναχρησιμοποίηση της γνώσης, ώστε να υπάρχει η δυνατότητα επικοινωνίας μεταξύ ετερογενών και διανεμημένων συστημάτων εφαρμογών. Αποτελούν λοιπόν, ένα από τα βασικότερα εργαλεία σημασιολογικής διαλειτουργικότητας (semantic interoperability) γιατί προσφέρουν λεξιλόγια για την περιγραφή των εννοιών και των σχέσεών τους και λειτουργούν ως εργαλεία αυτόματης "διερμηνείας" και συσχέτισης των μετά-δεδομένων που χρησιμοποιούνται από διάφορες εφαρμογές και υπηρεσίες πληροφόρησης. Γενικά, οι οντολογίες προσθέτουν νόημα στην πληροφορία για να παρέχεται "*η σωστή πληροφορία στο σωστό άτομο τη σωστή στιγμή και με το σωστό τρόπο*". Η ανάγκη ύπαρξης, κατασκευής και διάδοσης των οντολογιών, στην

επιστήμη των υπολογιστών προέκυψε εξαιτίας της αύξησης της ψηφιακής πληροφορίας, της δύσκολης πρόσβασης, εύρεσης και σύνοψης της πληροφορίας, του μεγάλου κενού μεταξύ της σημασίας της πληροφορίας και της καταχωρημένης πληροφορίας που υπάρχει, της δύσκολης ενοποίησης της πληροφορίας και της δυσκολίας που αφορά στη διαμοίραση και διαχείριση της γνώσης.

1.2 Διάρθρωση Διατριβής

Η παρούσα διατριβή ακολουθεί την παρακάτω δομή: Στην πρώτη ενότητα παρουσιάζεται το πλαίσιο της διατριβής, κάποιες εισαγωγικές έννοιες και η δομή της.

Στη συνέχεια προχωρώντας στη δεύτερη ενότητα καθορίζεται η έννοια του ελέγχου πρόσβασης, παρουσιάζονται οι παραδοσιακές προσεγγίσεις ελέγχου πρόσβασης με έμφαση στο μοντέλο ελέγχου πρόσβασης βασισμένο σε ρόλους (Role-Based Access Control - RBAC). Επίσης, περιγράφεται η έννοια της ιδιωτικότητας και γίνεται αναφορά στο νομικό και κανονιστικό πλαίσιο που τη διέπει, στις απαιτήσεις που προκύπτουν για τον έλεγχο πρόσβασης από τα παραπάνω και στους περιορισμούς του RBAC όσον αφορά στην ιδιωτικότητα. Συνεχίζοντας παρουσιάζονται τυπικοί μηχανισμοί εξουσιοδοτήσεων τους οποίους χρησιμοποιεί η προτεινόμενη πλατφόρμα εξουσιοδοτήσεων η οποία περιγράφεται στην εργασία. Ακόμη, διασαφηνίζεται η έννοια της επίγνωσης πλαισίου και των σχετικών παραμέτρων του, περιγράφονται γενικά χαρακτηριστικά πλαισίου ελέγχου πρόσβασης καθώς και χαρακτηριστικά πλαισίου ιδιωτικότητας. Η ενότητα καταλήγει με την περιγραφή των σημασιολογικών τεχνολογιών που χρησιμοποιούνται για την αναπαράσταση και επεξεργασία των πληροφοριών ελέγχου πρόσβασης. Δίνεται ο ορισμός, τα πλεονεκτήματα και τα βασικά στοιχεία μιας οντολογίας και παρουσιάζονται κάποιες βασικές υπάρχουσες οντολογίες ιδιωτικότητας.

Στην τρίτη ενότητα γίνεται μία συγκριτική μελέτη μοντέλων ελέγχου πρόσβασης τα οποία έχουν επίγνωση πλαισίου και ιδιωτικότητας και χρησιμοποιούν τεχνολογίες σημασιολογικού ιστού. Περιγράφονται βασικά μοντέλα ελέγχου πρόσβασης της βιβλιογραφίας τα οποία ενσωματώνουν τα παραπάνω χαρακτηριστικά. Μέσω της μελέτης αυτής εξάγονται χρήσιμα συμπεράσματα για τα πλεονεκτήματα και τους περιορισμούς των μοντέλων αυτών.

Με την τέταρτη ενότητα ξεκινάει η περιγραφή της προτεινόμενης λύσης. Είναι αφιερωμένη στις βασικές αρχές της λύσης οι οποίες αφορούν στο προτεινόμενο σημασιολογικό μοντέλο και πιο συγκεκριμένα στις συσχετίσεις μεταξύ των συνόλων, στους κανόνες πρόσβασης και στην μοντελοποίηση των πληροφοριών πλαισίου.

Η προτεινόμενη οντολογία παρουσιάζεται λεπτομερώς στην πέμπτη ενότητα. Περιγράφονται όλες οι σχετικές κλάσεις και οι μεταξύ τους σχέσεις δίνοντας συγκεκριμένα παραδείγματα.

Η έκτη ενότητα περιγράφει την αρχιτεκτονική δομή της λύσης και επικεντρώνεται στην εξαγωγή πολιτικών πρόσβασης, την παραγωγή συλλογισμών, στις οντότητες που συμμετέχουν στη διαδικασία ελέγχου πρόσβασης και λήψης απόφασης και περιγράφεται βήμα προς βήμα η διαδικασία αυθεντικοποίησης και εξουσιοδότησης που εκτελείται στο σύστημα.

Στην έβδομη ενότητα δίνεται ένα βασικό σενάριο κανόνα έλεγχου πρόσβασης το οποίο ενσωματώνει όλες τις έννοιες και τους περιορισμούς που έχουν περιγραφεί και λαμβάνει χώρα σε περιβάλλον εφαρμογής παρακολούθησης δικτύου μέσα από το οποίο αξιολογείται και το προτεινόμενο σημασιολογικό μοντέλο.

Τέλος η τελευταία ενότητα παρουσιάζει τα συμπεράσματα και τη μελλοντική ερευνητική δραστηριότητα που αφορούν στην προτεινόμενη λύση.

Κεφάλαιο 2

Τεχνολογίες και απαιτήσεις ελέγχου πρόσβασης

Εξ' ορισμού, ο έλεγχος πρόσβασης είναι η διαδικασία της διαμεσολάβησης μεταξύ κάθε αιτήματος για πόρους και των δεδομένων που διατηρούνται από το σύστημα, καθορίζοντας αν το αίτημα θα πρέπει να εκπληρωθεί ή να απορριφτεί (Samarati, 2001). Από τυπικής πλευράς, τα αντικείμενα αντιπροσωπεύουν τους πόρους που προστατεύονται από το σύστημα, τα υποκείμενα αποτελούν, για παράδειγμα, οι χρήστες ή οι διεργασίες που εκτελούν ενέργειες σε ένα αντικείμενο, και οι πράξεις αντιπροσωπεύουν όλες τις δράσεις τις οποίες τα υποκείμενα μπορούν να εκτελέσουν στα αντικείμενα. Τα ευαίσθητα από πλευράς ασφαλείας περιβάλλοντα θα πρέπει να προστατεύουν τους πόρους τους από μη εξουσιοδοτημένη χρήση με την επιβολή μηχανισμών ελέγχου πρόσβασης οι οποίοι καθοδηγούνται από τις πολιτικές ελέγχου πρόσβασης.

2.1 Παραδοσιακές λύσεις ελέγχου πρόσβασης

Τα παραδοσιακά συστήματα ελέγχου πρόσβασης, είναι γενικά ταξινομημένα ως Προαιρετικός Έλεγχος πρόσβασης (Discretionary Access Control (DAC)) ή μη Προαιρετικός έλεγχος πρόσβασης (Non-Discretionary Access Control (NDAC)). Σε μια DAC προσέγγιση, ο ιδιοκτήτης του αντικειμένου ή οποιοσδήποτε άλλος που έχει λάβει άδεια για τον έλεγχο της πρόσβασης του αντικειμένου καθορίζει ποιος έχει πρόσβαση στο αντικείμενο μέσω της διατύπωσης των πολιτικών ελέγχου πρόσβασης. Για παράδειγμα, οι προσεγγίσεις Πίνακας Ελέγχου Πρόσβασης (Access Control Matrix (Lampson, 1974), οι Λίστες Ελέγχου Πρόσβασης (Access Control Lists)(Samarati, 2001), και Capability-Based Access Control (Levy, 1984) αποτελούν ευρέως γνωστές λύσεις της DAC.

Όλες οι υπόλοιπες προσεγγίσεις ελέγχου πρόσβασης, εκτός από τη DAC προσέγγιση κατηγοριοποιούνται ως NDAC. Στις NDAC προσεγγίσεις, οι πολιτικές είναι κανόνες που δεν είναι καθορισμένοι κατά την κρίση των χρηστών. Στην ομάδα αυτή, ξεχωρίζουν ο Υποχρεωτικός Έλεγχος Πρόσβασης (Mandatory Access Control (MAC)) (TCSEC 1985), ο Έλεγχος Πρόσβασης Βασισμένος σε Ρόλους (Role-Based

Access Control (RBAC)) (Ferraiolo, 1992), (Sandhu, 1996), και ο Έλεγχος Πρόσβασης Βασισμένος σε Ιδιότητες (Attribute-based Access Control (ABAC)) (Priebe, 2004), οι οποίοι εφαρμόζονται σε μεγάλο βαθμό από τα συμβατικά συστήματα ηλεκτρονικών υπολογιστών για την προστασία των ψηφιακών πόρων.

Στην πραγματικότητα, υπάρχουν και άλλοι τύποι κατηγοριοποίησης για τις προσεγγίσεις ελέγχου πρόσβασης, όπως αυτές που έχουν ως βάση τον τύπο των πληροφοριών που χρησιμοποιούνται για τον έλεγχο ταυτότητας των χρηστών (π.χ., βασισμένες στην ταυτότητα (identity-based), βασισμένες στην ομάδα (group-based)), βασισμένες στο περιεχόμενο των προστατευόμενων αντικειμένων (έλεγχος πρόσβασης με βάση το περιεχόμενο - content-based access control), στη σχέση εμπιστοσύνης μεταξύ του ιδιοκτήτη των πόρων και του αιτούντος των πόρων (ελέγχου πρόσβασης που βασίζεται στην εμπιστοσύνη - trust-based access control), στις κοινωνικές σχέσεις του χρήστη (κοινωνικός έλεγχος πρόσβασης- social based access control), και οι πλαίσιο-κεντρικές (context-centric) λύσεις. Οι πιο συνήθεις MAC λύσεις είναι η πολυεπίπεδη ασφάλεια (multilevel security - MLS) (Bell, 1973), το μοντέλο Ken Biba (Biba, 1977), και το μοντέλο Chinese Wall (Brewer, 1989).

Ταξινομούμε ως παραδοσιακά μοντέλα την υφιστάμενη λύση για τον έλεγχο της πρόσβασης των συμβατικών πηγών, όπως τα έγγραφα και οι υπηρεσίες των εταιρικών ή διοικητικών οργανισμών. Κανονικά, η ταυτότητα των χρηστών χρησιμοποιείται για να ελεγχθεί εάν επιτρέπεται ή όχι η πρόσβαση σε μια πηγή. Σας παρουσιάζουμε παρακάτω τα πιο σημαντικά και ευρέως εφαρμοζόμενα μοντέλα ελέγχου πρόσβασης από τα τρέχοντα λειτουργικά συστήματα και συστήματα διαχείρισης δεδομένων βάσης. Οι λύσεις αυτές βασίζονται στα μοντέλα DAC, MAC, και RBAC. Στη συνέχεια, θα επικεντρωθούμε στα υπάρχοντα RBAC-Extended μοντέλα, που περιγράφουν τις προτεινόμενες βελτιώσεις προκειμένου να ενισχυθούν δυναμικά οι πολιτικές ελέγχου πρόσβασης.

2.1.1 Προαιρετικός και Υποχρεωτικός έλεγχος πρόσβασης (DAC & MAC)

Η προσέγγιση DAC είναι ένα είδος ελέγχου πρόσβασης τεκμηριωμένο από τα Trusted Computer System Evaluation Criteria - TCSEC (TCSEC, 1985) "ως μέσο για τον περιορισμό της πρόσβασης σε αντικείμενα σχετικά με την ταυτότητα των ατόμων και/ή τις ομάδες στις οποίες ανήκουν". Οι έλεγχοι είναι προαιρετικοί, με την έννοια

ότι ένα υποκείμενο με μια συγκεκριμένη άδεια πρόσβασης είναι ικανό να μεταβιβάσει την άδεια σε κάποιο άλλο υποκείμενο.

Ο όρος Προαιρετικός χρησιμοποιείται συνήθως από τις λύσεις ελέγχου πρόσβασης που υποστηρίζουν ότι κάθε αντικείμενο έχει έναν ιδιοκτήτη που ελέγχει το δικαίωμα πρόσβασης του αντικειμένου του. Ωστόσο, ο ορισμός των TCSEC δεν περιγράφει τίποτα για τους ιδιοκτήτες των πόρων. Τεχνικά, ένα σύστημα ελέγχου πρόσβασης δεν οφείλει να υποστηρίζει της έννοια του ιδιοκτήτη για να καλύπτει τον ορισμό DAC των TCSEC. Ο Προαιρετικός έλεγχος πρόσβασης είναι συνήθως τεκμηριωμένος σε αναντιστοιχία με τον Υποχρεωτικό έλεγχο πρόσβασης, που μερικές φορές ονομάζεται μη Προαιρετικός έλεγχος πρόσβασης.

Έτσι, ένα σύστημα ελέγχου πρόσβασης είναι προαιρετικό ή καθαρά προαιρετικό ως ένας τρόπος επιβεβαίωσης ότι το σύστημα δεν έχει υποχρεωτικό έλεγχο πρόσβασης. Ωστόσο, τα συστήματα ελέγχου πρόσβασης μπορούν να εφαρμόσουν ταυτόχρονα και τις δύο αυτές προσεγγίσεις, όπου η DAC αναφέρεται στη δυνατότητα των ατόμων να μεταφέρουν την εξουσιοδότηση μεταξύ τους, και η MAC αναφέρεται στους επιβαλλόμενους περιορισμούς αυτού. Ως εκ τούτου, μία γνήσια DAC προσέγγιση είναι μία χρήστο-κεντρική προσέγγιση ελέγχου πρόσβασης που αποτρέπει την παράνομη πρόσβαση στους πόρους, προσφέροντας στους χρήστες όλα τα δικαιώματα σχετικά με τα αντικείμενα που δημιουργούν. Επιπλέον, οι χρήστες μπορούν να χορηγούν τα δικαιώματα που έχουν σε άλλους (αντιπροσωπεία) και μπορούν να αφαιρέσουν τα χορηγούμενα δικαιώματα προαίρεσης.

Το μεγάλο πλεονέκτημα του Προαιρετικού Ελέγχου Πρόσβασης είναι ότι είναι αρκετά ευέλικτος έτσι ώστε να μπορεί να χρησιμοποιηθεί από πολλά συστήματα. Ο διαχειριστής των συστημάτων, αν και του δίνεται η δυνατότητα να αλλάζει τα δικαιώματα πρόσβασης των αντικειμένων των χρηστών, δε χρειάζεται να ασχολείται με αυτά. Όμως, αυτό δεν είναι αρκετό για τα συστήματα υψηλής ασφάλειας (high assurance), καθώς ο προαιρετικός έλεγχος πρόσβασης δεν μπορεί να υποστηρίξει τις αυξημένες απαιτήσεις ασφαλείας των εμπορικών εφαρμογών (π.χ. η εφαρμογή που χειρίζεται την διανομή συγκεκριμένων εγγράφων σε μια εταιρία). Τέλος, ο εν λόγω έλεγχος πρόσβασης υποφέρει από το πρόβλημα του δούρειου ίππου (Trojan horse problem) που σημαίνει ότι αν ένας κακοπροαίρετος χρήστης αποκτήσει

ιδιοκτησία σε κάποιο αντικείμενο, μπορεί να μεταφέρει τα δικαιώματά του και σε άλλους κακοπροαίρετους χρήστες.

Ο αντίστροφος τρόπος για τον έλεγχο πρόσβασης είναι ο υποχρεωτικός έλεγχος πρόσβασης (Mandatory Access Control). Σε αυτό τον τρόπο, η πρόσβαση είναι τόσο βασισμένη σε κανόνες όσο και στην πληροφορία που συσχετίζει ένα αντικείμενο με τον χρήστη. Στα περισσότερα μοντέλα που ανήκουν στον υποχρεωτικό έλεγχο πρόσβασης, ο ιδιοκτήτης κάποιου αντικειμένου δεν έχει κάποιες ειδικές άδειες πάνω στο αντικείμενο αυτό. Η πληροφορία που συσχετίζει ένα χρήστη και ένα αντικείμενο συνήθως λέγεται «επίπεδο ασφαλείας» ή «επίπεδο ευαισθησίας» και συνήθως υλοποιείται ως ετικέτα στους χρήστες και τα αντικείμενα. Στον χρήστη δίνεται μια ετικέτα που αναπαριστά την άδεια ασφαλείας (security clearance) του χρήστη αυτού. Στο αντικείμενο δίνεται μια ετικέτα που αναπαριστά την ταξινόμηση ασφαλείας (security classification) του αντικειμένου αυτού. Οι ετικέτες των χρηστών και των αντικειμένων ανήκουν στο ίδιο σύνολο. Στο σύνολο αυτό υπάρχουν ετικέτες που μπορούν να συγκριθούν μεταξύ τους και άλλες που δεν μπορούν. Συνήθως αυτό που ισχύει είναι:

- Αν οι ετικέτες του χρήστη και του αντικειμένου δεν μπορούν να συγκριθούν, τότε απαγορεύεται η πρόσβαση σε αυτό το αντικείμενο.
- Αν οι ετικέτες του χρήστη και του αντικειμένου είναι συγκρίσιμες, τότε η πρόσβαση καθορίζεται από τους κανόνες που έχουν οριστεί για το μοντέλο αυτό.

Τα MAC συστήματα μπορούν να προστατεύσουν μόνο την εμπιστευτικότητα ή την ακεραιότητα των δεδομένων, αλλά ποτέ και τα δύο ταυτόχρονα. Η έννοια της εμπιστευτικότητας έχει οριστεί από τον Διεθνή Οργανισμό Τυποποίησης (ISO) στο πρότυπο ISO-17799, ως «διασφάλιση ότι οι πληροφορίες είναι προσβάσιμες μόνο σε εκείνους που έχουν εξουσιοδοτημένη πρόσβαση» και ακεραιότητα σημαίνει ότι «τα δεδομένα δεν μπορούν να τροποποιηθούν χωρίς άδεια εξουσιοδότησης». Επιπλέον, η έννοια του υποκειμένου που χρησιμοποιείται από το MAC σύστημα έχει διαφορετικό νόημα από αυτό της DAC λύσης. Τα υποκείμενα σε DAC λύση συνήθως αντιστοιχούν σε χρήστες ή ομάδες ενώ τα υποκείμενα στα MAC συστήματα αναφέρονται στις διαδικασίες (δηλαδή, τα προγράμματα σε εκτέλεση) που

λειτουργούν για λογαριασμό των χρηστών. Η διάκριση αυτή επιτρέπει στα MAC συστήματα να ελέγχουν τις έμμεσες προσβάσεις που προκαλούνται από την εκτέλεση των διεργασιών, το οποίο αποτελεί το βασικό πρόβλημα ασφαλείας των DAC λύσεων.

2.1.2 Έλεγχος πρόσβασης βάσει ρόλων (RBAC)

Ως εξέλιξη των ομάδων χρηστών είναι ο έλεγχος πρόσβασης που βασίζεται σε ρόλους. Η πρώτη αναφορά έγινε το 1992 από τους Ferraiolo και Kuhn ως μια λύση για τα πολύπλοκα προβλήματα ασφαλείας μεγάλων δικτύων και οργανισμών. Μέχρι σήμερα πάρα πολλές εταιρίες και οργανισμοί καθώς και καινούργιες εφαρμογές (π.χ. υπηρεσίες διαδικτυακών πυλών (portlets)) χρησιμοποιούν το μοντέλο ελέγχου πρόσβασης βασισμένο σε ρόλους (Role Based Access Control).

Η μεγάλη καινοτομία του μοντέλου ελέγχου πρόσβασης βασισμένο σε ρόλους σε σχέση με τις ομάδες χρηστών είναι ότι ένας χρήστης μπορεί να ανήκει σε πολλούς ρόλους (και ένας ρόλος μπορεί να έχει πολλούς χρήστες) ενώ ακόμη σε ένα ρόλο μπορεί να ανατεθούν αρκετές άδειες (permissions), κάτι που στις ομάδες χρηστών δεν ισχύει. Όποτε βλέπουμε ότι η πολιτική ελέγχου πρόσβασης είναι ενσωματωμένη με τις διάφορες συνιστώσες του μοντέλου αυτού όπως οι σχέσεις ρόλου – άδειας, χρήστη – ρόλου και ρόλου – ρόλου.

Σε αυτό το μοντέλο ένας ρόλος είναι υπεύθυνος για να εκτελέσει κάποια εργασία ή έχει τις απαραίτητες άδειες για να προσπελάσει κάποιο αντικείμενο και όχι οι χρήστες. Μάλιστα, η σχέση του χρήστη με τους ρόλους απεικονίζει την οργάνωση μιας εταιρίας ή ενός οργανισμού, αφού συνήθως και η οργάνωση και στελέχωση μιας εταιρίας ή ενός οργανισμού στηρίζεται συχνά στην ύπαρξη ρόλων (Εικόνα 2).

Εικόνα 2: Η λογική του ελέγχου πρόσβασης με βάση τους ρόλους

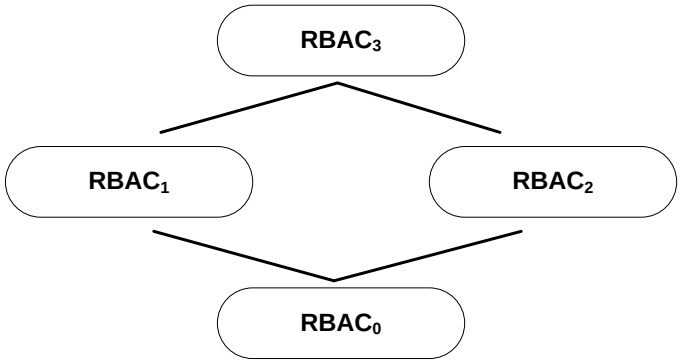
Με αυτόν τον τρόπο είναι αρκετά πιο εύκολη η διαχείριση ενός συστήματος μιας και ο διαχειριστής μπορεί εύκολα να αναθέσει ή να ανακαλέσει την συσχέτιση ενός χρήστη με κάποιους ρόλους. Βέβαια, κάτι τέτοιο δεν συμβαίνει και τόσο συχνά μέσα σε έναν οργανισμό (χρειάζεται να συμβεί μόνο όταν ένας εργαζόμενος αλλάζει τμήμα, ή παίρνει προαγωγή ή απολύεται). Ταυτόχρονα είναι το ίδιο εύκολη η προσθήκη ή η αφαίρεση αδειών από κάποιο ρόλο, πράγμα το οποίο και πάλι δεν είναι κάτι το σύνηθες να συμβεί (συμβαίνει μόνο όταν ένα καινούργιο έργο υπάρχει στον οργανισμό και χρειάζεται να ανατεθεί στους υπευθύνους και στους εργαζόμενους για την εκπόνησή του).

Ενώ το μοντέλο ελέγχου πρόσβασης βασισμένο σε ρόλους έχει ουδέτερη πολιτική (policy neutral), υποστηρίζει απευθείας τρεις αρκετά γνωστές αρχές ασφαλείας (security principles): των ελάχιστων προνομιών (least privilege), διαχωρισμό καθηκόντων (separation of duties) και αφαίρεση δεδομένων (data abstraction). Ελάχιστα προνόμια δίνονται στον χρήστη γιατί το μοντέλο αυτό είναι ρυθμισμένο να δίνει τα προνόμια που χρειάζονται στο ρόλο ώστε να εκτελέσει την εργασία που χρειάζεται. Διαχωρισμός καθηκόντων μπορεί να υπάρξει με το να χρησιμοποιηθούν αμοιβαίως αποκλειόμενοι ρόλοι σε μια ευαίσθητη εργασία. Αυτό μπορεί να υλοποιηθεί αν οι αμοιβαίως αποκλειόμενοι ρόλοι δεν έχουν κανένα κοινό χρήστη και για την σωστή εκτέλεση της εργασίας χρειάζονται και οι δυο ρόλοι.

Αφαίρεση δεδομένων υποστηρίζεται με την έννοια ότι σαν αφηρημένες άδειες μπορούν να δοθούν διαφορετικές άδειες που είναι πιο λειτουργικές για την εφαρμογή

και όχι οι άδειες ανάγνωσης, εγγραφής και εκτέλεσης που προσφέρονται από τα λειτουργικά συστήματα. Όμως, αν και οι αρχές αυτές υποστηρίζονται από το μοντέλο, πρέπει να γίνει και η αντίστοιχη σχεδίαση. Σε περίπτωση που η σχεδίαση δεν είναι σωστή, ενδέχεται οι αρχές αυτές να παραβιάζονται στην τελική υλοποίηση.

Για να γίνουν κατανοητές οι πολλαπλές διαστάσεις του ελέγχου πρόσβασης βασισμένο σε ρόλους (RBAC) θα ορίσουμε τέσσερα θεμελιώδη μοντέλα. Η σχέση των μοντέλων φαίνεται στην Εικόνα 3 ενώ τα επιμέρους χαρακτηριστικά φαίνονται στην Εικόνα 4 . Το $RBAC_0$ είναι το βασικό μοντέλο πού πρέπει να υλοποιεί κάθε σύστημα που υποστηρίζει το μοντέλο RBAC. Τα $RBAC_1$ και $RBAC_2$ εμπεριέχουν και τα δυο το μοντέλο $RBAC_0$ αλλά προσθέτουν σ' αυτό επιπλέον στοιχεία. Το $RBAC_1$ θέτει την αρχή της ιεραρχίας των ρόλων, δηλαδή τη δυνατότητα των ρόλων να κληρονομούν άδειες από άλλους ρόλους. Το $RBAC_2$ εισάγει την έννοια των περιορισμών (constraints) στο πώς μπορεί να οριστεί κάποιο συγκεκριμένο RBAC μοντέλο. Για παράδειγμα, οι περιορισμοί μπορεί να βοηθήσουν στην υλοποίηση των αμοιβαίως αποκλειόμενων ρόλων. Τέλος το $RBAC_3$ μοντέλο είναι ο συνδυασμός των $RBAC_1$ και $RBAC_2$, και εμμέσως του $RBAC_0$ μοντέλου.



Εικόνα 3: Οικογένεια RBAC

Ο ορισμός του $RBAC_0$ μοντέλου εμπεριέχει τα παρακάτω στοιχεία:

- U, R, P, and S (χρήστες (users), ρόλους (roles), άδειες (permissions) και συνεδρίες (sessions) αντίστοιχα),
- $PA \subseteq P \times R$, πολλαπλή (many-to-many) σχέση ανάθεσης αδειών (permission assignment) σε ρόλους,
- $UA \subseteq U \times R$, πολλαπλή (many-to-many) σχέση ανάθεσης χρηστών (user assignment) σε ρόλους,

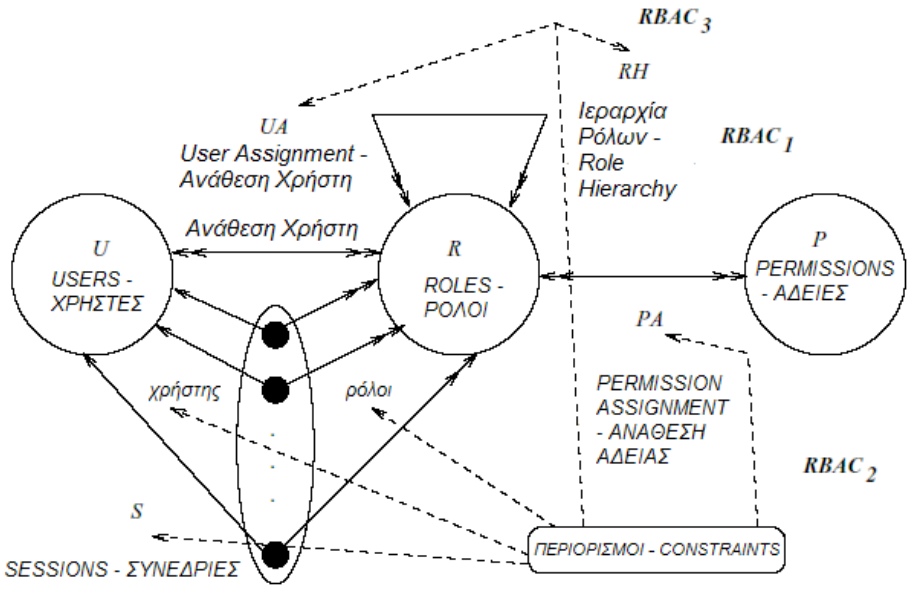
- user : S → U, μια συνάρτηση που αντιστοιχίζει κάθε συνεδρία s_i στον συγκεκριμένο χρήστη user(s_i) (σταθερό για την διάρκεια της συνεδρίας), και
- roles : S → 2R, μια συνάρτηση που αντιστοιχίζει κάθε συνεδρία s_i σε ένα σύνολο από ρόλους roles(s_i) ⊆ {r | (user(s_i), r) ∈ UA} (που μπορεί να αλλάζει με τον χρόνο) ενώ κάθε συνεδρία s_i έχει ένα σύνολο άδειων ∪ r∈ roles(s_i){p | (p, r) ∈ PA }

Στην απλή περίπτωση ένας χρήστης είναι ένας άνθρωπος, αλλά γενικότερα μπορεί να είναι ένα πρόγραμμα, ένας αυτόνομος πράκτορας, ένας υπολογιστής ακόμη και ένα δίκτυο από υπολογιστές. Η άδεια p_i είναι η αναπαράσταση μίας άδειας πρόσβασης σε κάποιο συγκεκριμένο αντικείμενο, που θα την αναγνωρίζει το σύστημα που χρησιμοποιεί το μοντέλο αυτό. Επίσης, μια συνεδρία s_i είναι η αντιστοίχιση του χρήστη με κάποιο σύνολο από ρόλους. Μια συνεδρία αρχικοποιείται όταν ο χρήστης ζητήσει ένα αντικείμενο και ορίσει και ένα υποσύνολο των ρόλων του. Τέλος, πολλές δημοσιεύσεις προτείνουν ένα επιπλέον χαρακτηριστικό ενός ρόλου: Το καθήκον (duty) του, δηλαδή το τι είναι υποχρεωμένος ο ρόλος να κάνει ώστε να μπορεί να λειτουργήσει φυσιολογικά κάποια συγκεκριμένη εργασία.

Στο $RBAC_1$ μοντέλο, εισάγεται η έννοια των ιεραρχιών. Οι ιεραρχίες ρόλων (role hierarchy) είναι μια φυσική μέθοδος δόμησης των ρόλων ώστε να αντανακλούν την οργάνωση ενός οργανισμού σε θέματα ευθύνης και εξουσίας. Τυπικά οι ιεραρχίες είναι μερικώς διατεταγμένες (partial ordering). Ο ορισμός για το $RBAC_1$ μοντέλο δίνεται ακολούθως:

- Τα σύνολα U, R, P, S, PA, UA και η συνάρτηση user() είναι ορισμένα όπως ακριβώς και στο $RBAC_0$ μοντέλο.
- RH ⊆ R × R, είναι η μερική διάταξη πάνω στο R και ονομάζεται ιεραρχία ρόλων ή σχέση κυριαρχίας ρόλων (role dominance relation), που επίσης μπορεί να αποδοθεί και ως ≥, και
- roles : S → 2R, έχει τροποποιηθεί από το $RBAC_0$ μοντέλο ώστε roles(s_i) ⊆ {r | (∃ r’ ≥ r)[(user(s_i), r’) ∈ UA]} (που μπορεί να αλλάζει με τον χρόνο) και κάθε συνεδρία s_i έχει άδειες ∪ r∈ roles(s_i){p | (∃ r’’ ≤ r) [(p, r’’) ∈ PA]}.

Το $RBAC_2$ μοντέλο είναι ίδιο με το $RBAC_0$ μοντέλο, προσφέροντας επιπλέον τη δυνατότητα να καθορίζουμε ένα σύνολο από περιορισμούς (constraints) που αφορούν στο ποιες από τις συσχετίσεις του $RBAC_0$ μοντέλου επιτρέπονται ή όχι. Με το μοντέλο αυτό μπορεί να οριστούν επιπλέον περιορισμοί, όπως αμοιβαίως αποκλειόμενοι ρόλοι και άλλα. Το $RBAC_3$ μοντέλο συνδυάζει τις ιεραρχίες του $RBAC_1$ μοντέλου μαζί με τους περιορισμούς του $RBAC_2$ μοντέλου. Θα μπορούσε να οριστεί η ιεραρχία ρόλων σαν περιορισμοί στο μοντέλο $RBAC_2$, αλλά το $RBAC_1$ μοντέλο θεωρείται αρκετά σημαντικό μοντέλο και από μόνο του. Από ότι φάνηκε παραπάνω, το RBAC μοντέλο μπορεί να αναπαραστήσει εύκολα την δομή ενός οργανισμού καθώς και να ορίσει αφηρημένες άδειες σε συγκεκριμένους ρόλους. Ταυτόχρονα ο διαχειριστής του συστήματος έχει να διαχειριστεί μόνο τους ρόλους και τις άδειες, παρά όλους τους χρήστες ξεχωριστά. Φυσικά το μοντέλο ελέγχου πρόσβασης δεν είναι πανάκεια για όλα τα θέματα που αφορούν στον έλεγχο πρόσβασης. Χρειάζονται πιο εξεζητημένα μοντέλα ελέγχου πρόσβασης σε περίπτωση που υπάρχει σειρά από διεργασίες που πρέπει να ελεγχθούν και να εκτελεστούν.



Εικόνα 4: Επιμέρους χαρακτηριστικά RBAC

2.2 Αξιοποιώντας τον έλεγχο πρόσβασης για την προστασία της ιδιωτικότητας

Στα πληροφοριακά συστήματα η ιδιωτικότητα παρουσιάζει άρρηκτους δεσμούς με την προστασία προσωπικών και ευαίσθητων δεδομένων. Υπό τη μορφή της πληροφοριακής ιδιωτικότητας, το δικαίωμα στην ιδιωτικότητα έχει καταγραφεί

σε μια σειρά από εθνικά συντάγματα παγκοσμίως. Η πρώτη πράξη της προστασίας των δεδομένων, που εγκρίθηκε το 1970 από το κρατίδιο της Έσσης στη Δυτική Γερμανία, έθεσε σε κίνηση μια τάση προς τη θέσπιση νομοθεσίας για την προστασία της ιδιωτικότητας.

2.2.1 Ιδιωτικότητα και νομοθεσία

Ένα σημαντικό ορόσημο στη βιβλιογραφία για την προστασία της ιδιωτικής ζωής αποτελεί η κωδικοποίηση των θεμελιωδών αρχών προστασίας της ιδιωτικότητας (Εικόνα 5) από τον Οργανισμό για την Οικονομική Συνεργασία και Ανάπτυξη (OECD), όπου αυτή η κωδικοποίηση θέτει τη βάση για την προστασία της ιδιωτικότητας.

Οι αρχές του OECD αντικατοπτρίζονται στην ευρωπαϊκή οδηγία 95/46/ΕΚ (European Parliament and Council, 1995), «*Για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών*». Η οδηγία 95/46/ΕΚ επιβάλλει ένα υψηλό επίπεδο προστασίας των δεδομένων και αποτελεί το μεγαλύτερο κομμάτι επιρροής για την ιδιωτικότητα σε παγκόσμιο επίπεδο νομοθεσίας, το οποίο επηρεάζει πολλές χώρες εκτός της Ευρώπης στη θέσπιση παρόμοιων νόμων.

Σύμφωνα με το άρθρο 2, της οδηγίας 95/46/ΕΚ τα προσωπικά δεδομένα ορίζονται ως «*κάθε πληροφορία που αναφέρεται σε κατονομαζόμενο ή αναγνωρίσιμο φυσικό πρόσωπο («υποκείμενο δεδομένων»). Ένα αναγνωρίσιμο πρόσωπο είναι εκείνο που μπορεί να προσδιοριστεί, άμεσα ή έμμεσα, ιδίως με αναφορά σε ένα αριθμό ταυτότητας ή βάσει ενός ή περισσότερων στοιχείων που αφορούν την φυσική, φυσιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική του ταυτότητα*». Ο ορισμός αυτός τονίζει τη ρητή αναφορά στην έμμεση αναγνώριση δεδομένων, πράγμα που σημαίνει ότι κάθε πληροφορία που μπορεί να οδηγήσει στην αυθεντικοποίηση του υποκειμένου των δεδομένων μέσω της σύνδεσης με άλλες διαθέσιμες πληροφορίες (άρα έμμεσα), μπορεί να πραγματοποιηθεί από οποιονδήποτε τρίτο.

Η οδηγία 95/46/ΕΚ εξειδικεύεται και συμπληρώνεται περαιτέρω από άλλες οδηγίες και αποφάσεις, για παράδειγμα, σε σχέση με τον τομέα ηλεκτρονικής

επικοινωνίας, η οδηγία 2002/58/ΕΚ (European Parliament and Council, 2002) επιβάλλει ρητές υποχρεώσεις και θέτει συγκεκριμένα όρια σχετικά με την επεξεργασία των προσωπικών δεδομένων των χρηστών από το δίκτυο και των παρόχων υπηρεσιών, με σκοπό την προστασία της ιδιωτικότητας των χρηστών των υπηρεσιών επικοινωνιών και δικτύων.

Στην Ελλάδα το δικαίωμα στην προστασία προσωπικών δεδομένων και στο απόρρητο των επικοινωνιών κατοχυρώνεται συνταγματικά. Πιο συγκεκριμένα, το Άρθρο 9Α του Συντάγματος της Ελλάδας (Ζ' Αναθεωρητική Βουλή των Ελλήνων, 2001) αναφέρει ότι «*καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων*», ενώ προβλέπει ότι η προστασία των προσωπικών δεδομένων διασφαλίζεται από κάποια ανεξάρτητη Αρχή.

Επιπλέον, το Άρθρο 19 ορίζει «*ως απόλυτα απαραβίαστο το απόρρητο των επικοινωνιών, προβλέποντας ωστόσο το νομοθετικό ορισμό εγγυήσεων υπό τις οποίες η δικαστική Αρχή δε δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Προβλέπει επίσης το νομοθετικό ορισμό των σχετικών με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης Αρχής που διασφαλίζει το απόρρητο*».

Υπό τη μορφή της προστασίας προσωπικών και ευαίσθητων δεδομένων το δικαίωμα στην πληροφοριακή ιδιωτικότητα στην Ελλάδα συναντάται ως επί το πλείστον στους Νόμους 2472/1997 (Βουλή των Ελλήνων, 1997), 3471/2006 (Βουλή των Ελλήνων, 2006) και 3917/2011 (Βουλή των Ελλήνων, 2011). Ο Νόμος 2472/1997 περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματεύεται τη «*θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής*» και αποτελεί υλοποίηση της Ευρωπαϊκής Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Αντίστοιχα, ο Νόμος 3471/2006 περί προστασίας δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών στόχο έχει αφενός την «*προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της*

ιδιωτικής ζωής και τη θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών» και αφετέρου την τροποποίηση του Νόμου 2472/1997. Ο Νόμος 3471/2006 αποτελεί υλοποίηση της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Τέλος, ο πρόσφατος Νόμος 3917/2011 σχετικά με τη «*διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις*» αντικατοπτρίζει την Ευρωπαϊκή Οδηγία 2006/24/ΕΚ (European Parliament and Council, 2006) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Πρέπει να σημειωθεί ότι από σχετικές διατάξεις Νόμων του Ελληνικού Συντάγματος προέκυψαν και δύο αρμόδιες ανεξάρτητες Αρχές, οι οποίες υλοποιούν, αντίστοιχα, τα Άρθρα 9Α και 19 του Συντάγματος: η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), η οποία ιδρύθηκε με το Νόμο 2472/1997, και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία συστάθηκε με το Νόμο 3115/2003 (Βουλή των Ελλήνων, 2003). Τέλος, καθώς τα σχετικά νομοσχέδια βασίζονται στο δικαίωμα στην πληροφοριακή ιδιωτικότητα ο ορισμός των προσωπικών και ευαίσθητων δεδομένων που αποτελούν αντικείμενο προστασίας αποκτά βαρύνουσα σημασία.

Σύμφωνα με το άρθρο 2α του Νόμου 2472/97 ως δεδομένα προσωπικού χαρακτήρα ή προσωπικά δεδομένα νοείται «*κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων*». Το άρθρο 2γ του ίδιου Νόμου ορίζει ως υποκείμενο των δεδομένων «*το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική*». Το άρθρο 2α καταλήγει εξαιρώντας από τον ορισμό των δεδομένων προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να

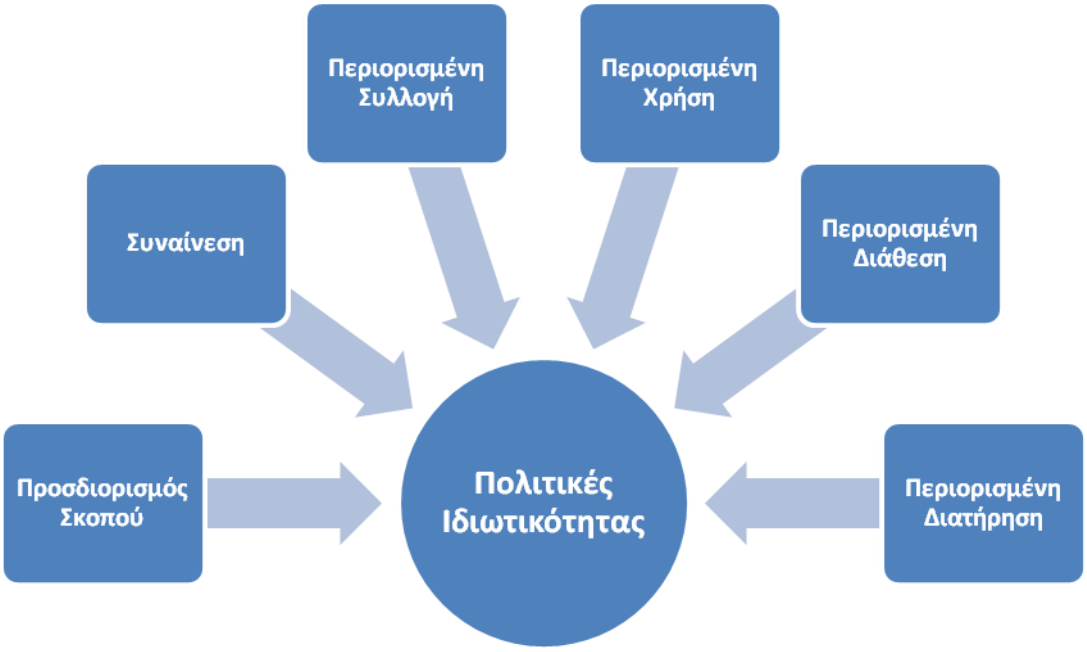
προσδιορισθούν τα υποκείμενα των δεδομένων. Ως ευαίσθητα προσδιορίζονται σαφώς στο άρθρο 2β του ίδιου Νόμου τα δεδομένα «*τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων*».

Πρέπει να σημειωθεί ότι σε αντίθεση με την Ευρωπαϊκή Ένωση, οι Ηνωμένες Πολιτείες της Αμερικής (ΗΠΑ) έχουν διατηρήσει μια λιγότερο ολιστική και διεπιστημονική προσέγγιση στο θέμα της νομοθεσίας περί ιδιωτικότητας, ενεργοποιώντας διαφορετικούς νόμους για διαφορετικά περιβάλλοντα (Solove, 2006). Ταυτόχρονα, ενώ η πλειοψηφία των ομοσπονδιακών νόμων για το προσωπικό απόρρητο βρίσκουν εφαρμογή κυρίως στους κυβερνητικούς φορείς ρυθμίζονται επιλεκτικά συγκεκριμένες περιοχές του ιδιωτικού τομέα επιτρέποντας με αυτόν τον τρόπο μια λιγότερο αυστηρή συγκριτικά με την Ε.Ε. προσέγγιση στο θέμα της προστασίας προσωπικών δεδομένων, ενώ χαρακτηριστική είναι η απουσία συγκεκριμένης σχετικής πρόβλεψης στο αμερικάνικο σύνταγμα (Ομοσπονδιακή Συνέλευση, 1787).

Σημαντική στιγμή αναφορικά με την προστασία της ιδιωτικότητας στις ΗΠΑ θεωρείται η θεσμοθέτηση της «Δράσης για την Ιδιωτικότητα» (Privacy Act) το 1974 (Act of Congress, 1974). Η «Δράση για την Ιδιωτικότητα» προδιέγραψε τις αρχές που πρέπει να διέπουν τη συλλογή, διατήρηση, χρήση και διακίνηση προσωπικών στοιχείων (Personally Identifiable Information) που βρίσκονται αποθηκευμένα σε αρχεία ομοσπονδιακών φορέων. Έκτοτε, μια σειρά από Νόμους με περιορισμένη και επιλεκτική εφαρμογή έχουν υιοθετηθεί προς ρύθμιση της προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων σε μια σειρά από συγκεκριμένους τομείς (United States Congress, 1996).

Στη συνέχεια, συνοψίζονται οι θεμελιώδες νομικές και ρυθμιστικές αρχές και απαιτήσεις. Το ενδιαφέρον επικεντρώνεται στη νομοθεσία της Ευρωπαϊκής Ένωσης, καθώς περιλαμβάνει τις πιο αντιπροσωπευτικές, με επιρροή και ώριμες προσεγγίσεις σε παγκόσμιο επίπεδο, που φαίνεται να κινητοποιεί ένα γενικό πλαίσιο και έχει χαρακτηριστεί ως «***μοχλός ενός παγκόσμιου καθεστώτος***»(Birnhack, 2008). Για

περαιτέρω προβληματισμό πάνω στα κανονιστικά και νομοθετικά πλαίσια των Η.Π.Α. και άλλων χωρών, ο αναγνώστης παραπέμπεται στο εξαιρετικό δοκίμιο του Solove (Solove, 2006).



Εικόνα 5: Οι βασικές Αρχές Ιδιωτικότητας

Οι νομικές και κανονιστικές απαιτήσεις (OECD, 1980), (European Parliament and Council, 1995), (European Parliament and Council, 2002), (Lioudakis et al., 2010) οι οποίες θα πρέπει να λαμβάνονται υπόψη στο πλαίσιο της προστασίας της ιδιωτικότητας στον τομέα των επιχειρήσεων μπορούν να συνοψιστούν ως εξής:

1. **Νομιμότητα της επεξεργασίας των δεδομένων:** Τα επιχειρησιακά συστήματα/υπηρεσίες θα πρέπει να είναι σε θέση να εξετάσουν κατά πόσον η επεξεργασία των δεδομένων είναι σύμφωνη με τους ισχύοντες νόμους και κανονισμούς.
2. **Οι σκοποί για τους οποίους διενεργείται επεξεργασία των δεδομένων:** Τα επιχειρησιακά συστήματα/υπηρεσίες θα πρέπει να παρέχουν τα μέσα για τον εντοπισμό των σκοπών επεξεργασίας των δεδομένων, οι οποίοι πρέπει να είναι νόμιμοι και να καταστούν σαφείς στο υποκείμενο των δεδομένων. Επιπλέον, θα πρέπει να είναι σε θέση να ελεγχθούν οι σκοποί αυτοί, έτσι ώστε να αποφευχθεί η περαιτέρω επεξεργασία των δεδομένων που έχουν

χρησιμοποιηθεί για κάποιο σκοπό, για σκοπούς που δεν συμβιβάζονται με αυτούς για τους οποίους τα δεδομένα έχουν συλλεχθεί.

3. **Η αναγκαιότητα, η επάρκεια και η αναλογικότητα της επεξεργασίας των δεδομένων:** Τα επιχειρησιακά συστήματα/υπηρεσίες πρέπει να είναι σε θέση να εγγυηθούν ότι μόνο τα δεδομένα που είναι λειτουργικά, απαραίτητα, συναφή, αναλογικά και όχι υπερπληθή σε σχέση με τον επιδιωκόμενο σκοπό επεξεργασίας υποβάλλονται σε επεξεργασία.
4. **Η ποιότητα των δεδομένων που επεξεργάζονται:** Τα επιχειρησιακά συστήματα/υπηρεσίες θα πρέπει να προβλέπουν ότι η επεξεργασία των δεδομένων είναι σωστή, ακριβής και ενημερωμένη. Ανακριβή δεδομένα πρέπει να διαγράφονται ή να διορθώνονται, παρωχημένα δεδομένα επίσης πρέπει να διαγραφούν ή να ενημερωθούν.
5. **Αναγνωρίσιμα δεδομένα:** Τα επιχειρησιακά συστήματα/υπηρεσίες θα πρέπει να παρέχουν τα μέσα για τη διατήρηση των δεδομένων που τυγχάνουν επεξεργασίας σε μία αναγνωρίσιμη μορφή μόνο για το χρονικό διάστημα που απαιτείται για την επίτευξη του επιδιωκόμενου σκοπού επεξεργασίας.
6. **Ειδοποίηση και άλλες εγκρίσεις από την αρμόδια Αρχή Προστασίας Προσωπικών Δεδομένων:** Τα επιχειρησιακά συστήματα/υπηρεσίες θα πρέπει να είναι σε θέση να παρακολουθούν τη συμμόρφωση με την υποχρέωση ειδοποίησης (π.χ., άρθρα 18-21, (Ευρωπαϊκό Κοινοβουλίου και του Συμβουλίου, 1995)) και με τις διατάξεις για τις εγκρίσεις των αρμόδιων Αρχών Προστασίας Προσωπικών Δεδομένων. Επιπλέον, τα συστήματα/υπηρεσίες θα πρέπει να προβλέπουν τα μέσα που επιτρέπουν την επικοινωνία μεταξύ των συστημάτων/υπηρεσιών και των αρμόδιων Αρχών Προστασίας Προσωπικών Δεδομένων.
7. **Πληροφόρηση των υποκείμενων των δεδομένων:** Τα επιχειρησιακά συστήματα/υπηρεσίες θα πρέπει να είναι σε θέση να παρέχουν πληροφορίες για την ενημέρωση του υποκειμένου των δεδομένων, ότι τα δεδομένα επεξεργάζονται σύμφωνα με την ισχύουσα νομοθεσία περί προστασίας των δεδομένων.
8. **Συγκατάθεση και άρση της συγκατάθεσης:** Τα επιχειρησιακά συστήματα/υπηρεσίες θα πρέπει να εγγυώνται ότι όταν ζητείται από την

ισχύουσα νομοθεσία για την προστασία των δεδομένων, η συγκατάθεση του υποκειμένου δεδομένων για την επεξεργασία αυτών είναι απαραίτητη, και ότι η επεξεργασία των δεδομένων γίνεται σύμφωνα με τις προτιμήσεις που εκφράζονται από το υποκείμενο των δεδομένων. Περαιτέρω, η ανάκληση της συναίνεσης και μια ένσταση για την επεξεργασία δεδομένων από το υποκείμενο των δεδομένων θα πρέπει να αντιμετωπίζονται κατάλληλα.

9. **Άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων:** Τα επιχειρησιακά συστήματα/υπηρεσίες θα πρέπει να επιτρέπουν στο υποκείμενο των δεδομένων να ασκεί τα δικαιώματα που αναγνωρίζονται από την ισχύουσα για την προστασία των δεδομένων νομοθεσία, σε σχέση με την παρέμβαση στην επεξεργασία δεδομένων (για παράδειγμα το δικαίωμα της πρόσβασης στα δεδομένα, να ζητά τη διόρθωση των δεδομένων, τη διαγραφή, το κλείδωμα, το δικαίωμα ένστασης κατά την επεξεργασία δεδομένων, κλπ.).
10. **Ασφάλεια δεδομένων και εμπιστευτικότητα:** Τα επιχειρησιακά συστήματα/υπηρεσίες θα πρέπει να είναι ασφαλή με σκοπό τη διασφάλιση του απορρήτου, της ακεραιότητας και της διαθεσιμότητας των δεδομένων προς επεξεργασία. Επιπλέον, τα συστήματα/υπηρεσίες θα πρέπει να προβλέπουν ότι η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης μπορεί να πραγματοποιηθούν μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων ή, όταν επιτρέπεται από την ισχύουσα νομοθεσία για σκοπούς κρατικού ενδιαφέροντος.
11. **Τα δεδομένα κίνησης και θέσης: ειδικές κατηγορίες δεδομένων:** Τα επιχειρησιακά συστήματα/υπηρεσίες θα πρέπει να είναι σε θέση να εξασφαλίσουν ότι η επεξεργασία των ειδικών κατηγοριών δεδομένων (για παράδειγμα, η κίνηση ή άλλα δεδομένα θέσης, ευαίσθητα δεδομένα) γίνεται σύμφωνα με τις ειδικές απαιτήσεις τις οποίες η ισχύουσα νομοθεσία περί προστασίας δεδομένων παραθέτει για τις προαναφερθέντες κατηγορίες δεδομένων.
12. **Περιορισμός πρόσβασης:** Τα επιχειρησιακά συστήματα/υπηρεσίες θα πρέπει να παρέχουν διαδικασίες χορήγησης εξουσιοδότησης που συνεπάγεται

διαφοροποιημένα επίπεδα πρόσβασης στα δεδομένα, αλλά και καταγραφή της πρόσβασης στα δεδομένα.

13. **Αποθήκευση δεδομένων:** Τα επιχειρησιακά συστήματα/υπηρεσίες θα πρέπει να είναι σε θέση να διαγράφουν αυτόματα (ή να κάνουν ανώνυμα) τα δεδομένα, όταν ο επιδιωκόμενος σκοπός επεξεργασίας επιτυγχάνεται ή σε περίπτωση παρόδου των περιόδων διατήρησης των δεδομένων που καθορίζονται σύμφωνα με την ισχύουσα νομοθεσία.
14. **Διάδοση των δεδομένων σε τρίτους:** Όταν τα στοιχεία των υπηρεσιών ανατεθούν σε τρίτους παρόχους και, σε αυτό το πλαίσιο, δεδομένα προσωπικού χαρακτήρα διατίθενται για επεξεργασία, τα συστήματα των επιχειρήσεων/υπηρεσίες πρέπει να είναι σε θέση να παρέχουν ορισμένες εγγυήσεις ότι η συνακόλουθη επεξεργασία των πληροφοριών είναι σύμφωνη με τις υποκείμενες θεμιτές πρακτικές δεδομένων και με τη σύμβαση με το υποκείμενο των δεδομένων.
15. **Μεταφορά των δεδομένων σε τρίτες χώρες:** Η αρχή που περιγράφει τη διάδοση των δεδομένων που περιγράφηκαν παραπάνω ισχύει κυρίως όταν τα δεδομένα μεταφερθούν σε τρίτες χώρες, ενδεχομένως με ουσιαστικά διαφορετική νομοθεσία σχετικά με την προσωπική συλλογή και επεξεργασία αυτών. Τα επιχειρησιακά συστήματα/υπηρεσίες θα πρέπει να είναι σε θέση να προβλέπουν την τήρηση των ειδικών διατάξεων για την απόφαση μεταφοράς των δεδομένων. Για παράδειγμα, σκεφτείτε τις Αρχές Ασφαλούς διακίνησης που διέπουν τη μεταφορά δεδομένων μεταξύ της Ευρωπαϊκής Ένωσης και των ΗΠΑ (Ευρωπαϊκή Επιτροπή, 2000).
16. **Εποπτεία και κυρώσεις:** Η αρμόδια Αρχή Προστασίας Προσωπικών Δεδομένων θα πρέπει να παρέχεται με τα μέσα για την εποπτεία και τον έλεγχο όλων των δράσεων της συλλογής και επεξεργασίας προσωπικών δεδομένων.
17. **Νόμιμη παρακολούθηση:** Η αρμόδια Αρχή Προστασίας Προσωπικών Δεδομένων θα πρέπει να παρέχεται με τα μέσα ώστε να εκτελεί παρακολούθηση μόνο όταν αυτό επιτρέπεται από την ισχύουσα νομοθεσία και τους κανονισμούς και σύμφωνα με τους όρους που εκτίθενται εκεί. Οι

αναγκαίες «συνδέσεις» για τη νόμιμη παρακολούθηση δε θα πρέπει σε καμία περίπτωση να είναι διαθέσιμες σε άλλους μη εξουσιοδοτημένους τρίτους.

Από τις κανονιστικές απαιτήσεις που παρουσιάστηκαν παραπάνω, εξάγονται τα ακόλουθα συμπεράσματα πάνω στα οποία βασίστηκε ο σχεδιασμός της προτεινόμενης λύσης:

Ο ρόλος των χρηστών: Οι χρήστες χορηγούνται ορισμένα δικαιώματα. Το δικαίωμα να ενημερώνονται σχετικά με τη συλλογή ή επεξεργασία δεδομένων προσωπικού χαρακτήρα, το δικαίωμα διάθεσης των δεδομένων μετά τη ρητή συγκατάθεσή τους, το δικαίωμα πρόσβασης στα δεδομένα τους. Επιπλέον, θα πρέπει να είναι σε θέση να καθορίσουν τις προτιμήσεις ιδιωτικότητάς τους και με αυτό τον τρόπο να επηρεάσουν τη διαδικασία παροχής υπηρεσιών, με σεβασμό στην ιδιωτικότητα.

Ο ρόλος των Αρχών: Η νομοθεσία εξουσιοδοτεί τις Αρχές Προστασίας Δεδομένων με ορισμένα δικαιώματα και αρμοδιότητες. Αυτές περιλαμβάνουν την ειδοποίηση της Αρχής, την εποπτεία των διαδικασιών και των μέσων για την εκτέλεση νόμιμης παρακολούθησης. Δηλαδή, η Αρχή πρέπει να είναι σε θέση να αλληλεπιδράσει με το σύστημα.

Ο ρόλος της σημασιολογίας: Η σημασιολογία παίζει πολύ σημαντικό ρόλο σε ό, τι μπορεί να χαρακτηριστεί ως «*το πλαίσιο προστασίας της ιδιωτικότητας*». Από τη μία πλευρά, κάθε στοιχείο δεδομένων θα πρέπει να αντιμετωπίζεται σύμφωνα με τον τύπο του. Από την άλλη πλευρά, πολύ σημαντικός είναι ο σκοπός για τον οποίο τα δεδομένα συλλέγονται και υποβάλλονται σε επεξεργασία.

Έλεγχος πρόσβασης: Η πρόσβαση στα δεδομένα θα πρέπει να ελέγχεται. Πέρα από τα παραδοσιακά μοντέλα ελέγχου πρόσβασης που βασίζονται σε ρόλους, οι αποφάσεις όσον αφορά την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα πρέπει να λαμβάνουν υπόψη τη σημασιολογία που χαρακτηρίζει κάθε συνεδρία ιδιωτικότητας. Στο πλαίσιο αυτό, εκτός από τις απαιτήσεις που αφορούν τον έλεγχο της πρόσβασης, οι σύγχρονοι κανονισμοί των εταιρειών και οι νόμοι προστασίας της ιδιωτικής ζωής επιβάλλουν συχνά απαιτήσεις τύπου υποχρέωσης, προσδιορίζοντας κάποιες άλλες ενέργειες που πρέπει να πραγματοποιηθούν κάποια στιγμή προκειμένου να επιτραπεί μία ενέργεια που θα εκτελεστεί άμεσα.

Συμπληρωματικές δράσεις: Η πρόσβαση στα δεδομένα πρέπει να συνοδεύεται από ορισμένους κανόνες συμπεριφοράς του συστήματος. Αυτοί περιλαμβάνουν τις πληροφορίες των χρηστών ή το αίτημα για τη ρητή συγκατάθεσή του, την ειδοποίηση των αρχών, την αυτόματη επιβολή των περιόδων διατήρησης των δεδομένων, καθώς και την προσαρμογή του επιπέδου λεπτομέρειας των δεδομένων.
Ασφάλεια: Φυσικά, προκειμένου να προστατευθούν τα δεδομένα προσωπικού χαρακτήρα, πρέπει να ληφθούν μέτρα για την εξασφάλιση της ασφαλούς μεταφοράς και αποθήκευσης τους. Η ασφάλεια αποτελεί πάντα την βάση για την προστασία της ιδιωτικής ζωής.

2.2.2 Ζητήματα και απαιτήσεις ελέγχου πρόσβασης για την εφαρμογή προστασίας της ιδιωτικότητας

Με βάση όλα τα παραπάνω, η εφαρμογή των πολιτικών προστασίας της ιδιωτικής ζωής που αφορά στα προσωπικά δεδομένα που αποθηκεύονται από τις επιχειρήσεις αποτελεί ένα βασικό ζήτημα. Η μοντελοποίηση των προσωπικών δεδομένων σε συνδυασμό με τον προσδιορισμό και την ανάπτυξη των πολιτικών προστασίας προσωπικών δεδομένων είναι στενά συνδεδεμένα με αυτό το θέμα. Όπως έχει ήδη αναφερθεί, οι ισχύοντες νόμοι προστασίας της ιδιωτικότητας διέπονται από τις παρακάτω αρχές:

- **Αρχή της περιορισμένης συλλογής**: Η συλλογή προσωπικών δεδομένων πρέπει να υπόκειται σε περιορισμούς με σύννομα και δίκαια μέσα και όταν είναι απαραίτητο μετά τη συγκατάθεση του υποκειμένου των δεδομένων.

- **Αρχή της ποιότητας των δεδομένων**: Τα προσωπικά δεδομένα πρέπει να σχετίζονται με τον σκοπό χρησιμοποίησής τους ενώ στα πλαίσια αυτού του σκοπού πρέπει να είναι ακριβή, πλήρη και ενημερωμένα.

- **Αρχή του καθορισμού του σκοπού και συναίνεση υποκειμένου**: Οι σκοποί συλλογής των προσωπικών δεδομένων πρέπει να καθορίζονται όχι αργότερα από τη στιγμή συλλογής τους ενώ η μετέπειτα χρήση τους πρέπει να περιορίζεται στα πλαίσια της επίτευξης των καθορισμένων σκοπών η άλλων σχετικών στόχων οι οποίοι είναι συμβατοί με τους δηλωμένους. Η συλλογή των προσωπικών δεδομένων θα πρέπει να βασίζεται σε μια νόμιμη βάση

επεξεργασίας (συναίνεση του υποκειμένου ή συγκεκριμένη διάταξη νόμου). Αν υπάρχουν περισσότεροι σκοποί επεξεργασίας τότε το υποκείμενο των δεδομένων θα πρέπει να παρέχει ξεχωριστή συγκατάθεση για καθένα από αυτούς.

- **Αρχή του περιορισμού της χρήσης**: Τα προσωπικά δεδομένα δεν πρέπει να αποκαλύπτονται, να γίνονται διαθέσιμα ή να χρησιμοποιούνται με οποιονδήποτε τρόπο προς επίτευξη σκοπού διαφορετικού από τους καθορισμένους σύμφωνα με την «*Αρχή του καθορισμού του σκοπού*», εκτός εάν υπάρχει συγκατάθεση του υποκειμένου των δεδομένων ή η σχετικές ενέργειες επιβάλλονται από τον Νόμο.

- **Αρχή των εγγυήσεων ασφάλειας:** Τα προσωπικά δεδομένα πρέπει να προστατεύονται από επαρκείς εγγυήσεις ασφάλειας έναντι κινδύνων όπως απώλεια ή μη εξουσιοδοτημένη πρόσβαση, καταστροφή, χρήση, αλλοίωση ή αποκάλυψη των δεδομένων.

- **Αρχή της διαφάνειας**: Υλοποιήσεις, πρακτικές και πολιτικές αναφορικά με προσωπικά δεδομένα πρέπει να διέπονται από την αρχή της διαφάνειας. Θα πρέπει να διατίθενται μηχανισμοί εξακρίβωσης της ύπαρξης και της φύσης των προσωπικών δεδομένων, των κύριων σκοπών χρήσης τους καθώς και της ταυτότητας και συνήθους κατοικίας του υπεύθυνου της επεξεργασίας τους.

- **Αρχή της ατομικής συμμετοχής**: Καθένας έχει το δικαίωμα

    - να ενημερώνεται από τον υπεύθυνο επεξεργασίας σχετικά με το αν βρίσκονται στην κατοχή του δεδομένα που τον αφορούν,

    - να λαμβάνει τα δεδομένα αυτά μέσα σε ένα εύλογο χρονικό διάστημα, με όχι υπερβολικά μεγάλο κόστος, με λογικά μέσα και σε κατανοητή μορφή,

    - να του αιτιολογείται πιθανή άρνηση άσκησης των παραπάνω δικαιωμάτων και να δύναται να προσβάλει αυτή την άρνηση και

  - να προσβάλει την ακρίβεια των δεδομένων και να διατηρεί το δικαίωμα διαγραφής, επανόρθωσης, τροποποίησης και ολοκλήρωσής τους.

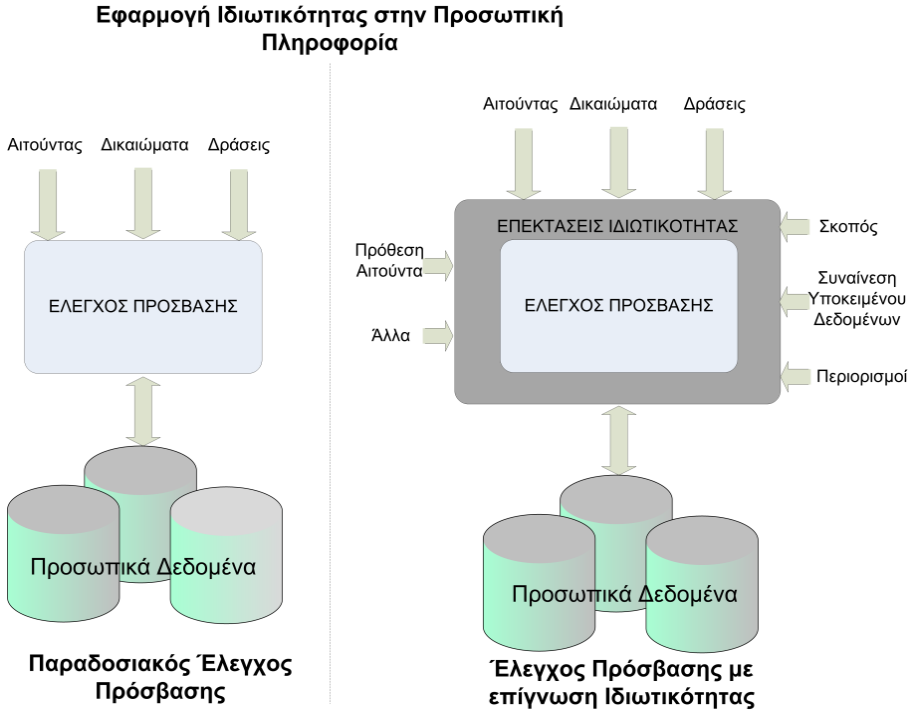
- **Αρχή της ευθύνης**: Ο υπεύθυνος της επεξεργασίας πρέπει να είναι υπεύθυνος για τη υιοθέτηση μέτρων που τον καθιστούν συμβατό με τις παραπάνω αρχές.

Κατά συνέπεια, οι πολιτικές προστασίας της ιδιωτικότητας πρέπει να είναι τόσο πολύπλοκες έτσι ώστε να επιβάλλουν διάφορους όρους και περιορισμούς, υπαγορευόμενους από τα υποκείμενα των δεδομένων και τη νομοθεσία, κατά τους οποίους τα δεδομένα προσωπικού χαρακτήρα μπορεί και πρέπει πραγματικά να είναι προσβάσιμα, δια μέσου συγκεκριμένου πλαισίου. Πρέπει να λαμβάνουν υπόψη πτυχές όπως τους συγκεκριμένους σκοπούς για τους οποίους τα δεδομένα αυτά έχουν συλλεχθεί, τη συναίνεση η οποία δίνεται από τα υποκείμενα των δεδομένων, ειδοποιήσεις, τις προθέσεις των αιτούντων καθώς και άλλες συμπληρωματικές ενέργειες.

Στις παραδοσιακές προσεγγίσεις για την επιβολή της ιδιωτικότητας, τροποποιημένα αιτήματα των δεδομένων που συμπεριλαμβάνουν περιορισμούς που βασίζονται στη συγκατάθεση των υποκειμένων των δεδομένων και το φιλτράρισμα των δεδομένων, μπορούσαν να ενσωματωθούν σε εφαρμογές και υπηρεσίες: η προσέγγιση αυτή θα μπορούσε όμως να λειτουργήσει σε περίπτωση μόνο στατικών περιβαλλόντων που δεν υπόκεινται σε αλλαγές. Ωστόσο, στον πραγματικό κόσμο η κατάσταση είναι πολύ πιο περίπλοκη, ιδιαίτερα για μεσαίες-μεγάλες επιχειρήσεις στις οποίες λειτουργούν και διατίθενται χιλιάδες εφαρμογές και υπηρεσίες, έχουν μεγάλο αριθμό πελατών και πρέπει να αντιμετωπίσουν τις συνεχώς μεταβαλλόμενες επιχειρησιακές και νομικές ανάγκες.

Η επιβολή των πολιτικών ιδιωτικότητας πρέπει να εξασφαλίζει ότι: η πρόθεση του αιτούντος είναι συμβατή με τον καθορισμένο σκοπό συλλογής των δεδομένων, η συγκατάθεση των υποκειμένων των δεδομένων λαμβάνεται υπόψη και εκτελείται σε συνδυασμό με τις σχετικές προτιμήσεις και τους περιορισμούς. Όλες αυτές οι πτυχές έχουν επιπτώσεις ελέγχου πρόσβασης.

Υποστηρίζουμε ότι τα παραδοσιακά συστήματα ελέγχου πρόσβασης είναι αναγκαία αλλά όχι ικανά για την επιβολή πολιτικών ιδιωτικότητας προσωπικών δεδομένων. Σημαντικό ζήτημα είναι ο τρόπος ο οποίος όλα αυτά τα πρόσθετα στοιχεία θα εξεταστούν έτσι ώστε να οικοδομηθούν "*επεκτάσεις ιδιωτικότητας*" των παραδοσιακών συστημάτων ελέγχου πρόσβασης έτσι ώστε τα μοντέλα ελέγχου πρόσβασης να έχουν επίγνωση πλαισίου ιδιωτικότητας (Εικόνα 6).



Εικόνα 6: Εφαρμογή Ιδιωτικότητας στον έλεγχο πρόσβασης

2.2.3 Μειονεκτήματα του μοντέλου RBAC όσον αφορά την ιδιωτικότητα

Αν και τα παραδοσιακό RBAC μοντέλο είναι πολύ αποτελεσματικό και δημοφιλές για τα παραδοσιακά και συνεργατικά συστήματα, το RBAC παρουσιάζει αρκετές αδυναμίες, δεν έχει σχεδιαστεί για την επιβολή πολιτικών προστασίας της ιδιωτικότητας και μόλις και μετά βίας ανταποκρίνεται στις απαιτήσεις προστασίας, που αφορούν στο σκοπό (δηλαδή τα δεδομένα που συλλέγονται για έναν σκοπό δεν πρέπει να χρησιμοποιούνται για άλλο σκοπό χωρίς τη συγκατάθεση του χρήστη), στις προϋποθέσεις και τις υποχρεώσεις. Η σημασία των σκοπών, των προϋποθέσεων οι οποίες περιγράφονται με τη βοήθεια των πληροφοριών πλαισίου προστασίας της ιδιωτικότητας, και των υποχρεώσεων, βρίσκεται στις κατευθυντήριες γραμμές του OECD για την προστασία της ιδιωτικής ζωής και τη διασυνοριακή ροή δεδομένων

προσωπικού χαρακτήρα, σε ισχύοντες νόμους προστασίας της ιδιωτικότητας σε πολλές χώρες, και στις δημόσιες πολιτικές απορρήτου γνωστών οργανισμών, όπως η Google, η IBM, και η Amazon.

Υπάρχουν πολλές περιπτώσεις στις οποίες η πρόσβαση σε ιδιωτικά δεδομένα επιβάλλει υποχρεώσεις, δηλαδή, δράσεις που πρέπει να πληρούνται σε κάποιο σημείο στο χρόνο, έτσι ώστε να εκτελεστεί μια ενέργεια σε αυτά τα δεδομένα. Για παράδειγμα, η αρχή της υπευθυνότητας του OEDC αναφέρει ότι «*Ένας ελεγκτής δεδομένων (data controller) θα πρέπει να είναι υπεύθυνος για τη συμμόρφωση με τα μέτρα που δίνουν ισχύ στις αρχές που αναφέρονται παραπάνω*». Μια κοινή προσέγγιση για την εφαρμογή αυτής της αρχής σε λειτουργικά συστήματα ή βάσεις δεδομένων είναι η καταγραφή κάθε πρόσβασης στα δεδομένα. Η καταγραφή των ενεργειών αποτελεί υποχρέωση που απαιτείται από την πλειοψηφία των πολιτικών απορρήτου.

Οι Προϋποθέσεις, δηλαδή, οι όροι που πρέπει να πληρούνται πριν από μια ενέργεια που πρόκειται να εκτελεστεί, είναι ζωτικής σημασίας σε ορισμένες περιπτώσεις. Μια τέτοια περίπτωση σχετίζεται με πληροφορίες που αφορούν παιδιά. Οι Κανόνες της δράσης Παιδικής Προστασίας Ηλεκτρονικού Απορρήτου (Children's Online Privacy Protection Act - COPPA) ισχύουν για την ηλεκτρονική συλλογή προσωπικών πληροφοριών από παιδιά κάτω των 13 ετών. Η πληροφορία που αναφέρεται στην παραδοχή «*η ηλικία της πηγής πληροφόρησης είναι κάτω των 13*» είναι μια κατάσταση που πρέπει να εκπληρωθεί πριν από την εφαρμογή των κανόνων COPPA.

Στο πλαίσιο αυτό, το παραδοσιακό RBAC στερείται τη δυνατότητα να καθορίσει ένα λεπτομερή έλεγχο για μεμονωμένους χρήστες με συγκεκριμένους ρόλους και σε επιμέρους στιγμιότυπα αντικειμένου. Για τα συνεργατικά περιβάλλοντα, είναι ανεπαρκές να υπάρχουν δικαιώματα ρόλου βάσει των τύπων αντικειμένων. Πιο συχνή είναι η περίπτωση που ένας χρήστης σε ένα στιγμιότυπο ρόλου μπορεί να χρειάζεται ειδική άδεια για ένα στιγμιότυπο ενός αντικειμένου. Ένα άλλο σημαντικό ζήτημα όσον αφορά την εφαρμογή του μοντέλου RBAC είναι η δύναμη της προδιαγραφής των περιορισμών. Οι περιορισμοί είναι μια σημαντική πτυχή του ελέγχου πρόσβασης που βασίζεται σε ρόλους και αποτελεί έναν ισχυρό μηχανισμό για τη διευθέτηση οργανωτικών πολιτικών υψηλότερου επιπέδου. Η

σημασία της ευελιξίας των περιορισμών για την υποστήριξη νέων εφαρμογών αποτελεί αντικείμενο ερευνητικής δραστηριότητας. Ωστόσο, ο προσδιορισμός των εν λόγω περιορισμών δεν έχει συζητηθεί στο RBAC μοντέλο.

Παρόλο όμως τους περιορισμούς της, η υπάρχουσα τεχνολογία ελέγχου πρόσβασης μπορεί να χρησιμοποιηθεί ως σημείο εκκίνησης για τη διαχείριση των προσωπικών αναγνωρίσιμων πληροφοριών. Επειδή γενικά οι πολιτικές ελέγχου πρόσβασης αλλά και οι πολιτικές ελέγχου πρόσβασης που σχετίζονται συγκεκριμένα με την ιδιωτικότητα συνήθως αναφέρονται στο ίδιο σύνολο δεδομένων, δεν θα πρέπει να συγκρούονται, η χρήση ενός ενιαίου μοντέλου και για τα δύο είδη των πολιτικών θα απλουστεύσει σημαντικά τη διαχείριση. Με την έννοια πολιτικές ελέγχου πρόσβασης με επίγνωση ιδιωτικότητας αναφερόμαστε στις πολιτικές ελέγχου πρόσβασης που ενσωματώνουν πρόσθετες πληροφορίες σχετικές με την ελεγχόμενη πρόσβαση σε ευαίσθητα δεδομένα.

2.3 Μηχανισμοί εξουσιοδοτήσεων

Η προστασία της ιδιωτικότητας και η ασφάλεια των πληροφοριών αποτελούν βασική λειτουργική απαίτηση οργανισμών παγκοσμίως, επιδρώντας ουσιαστικά στη διαμόρφωση και υλοποίηση σχετικών μέτρων προφύλαξης και εγκαθίδρυσης εμπιστοσύνης στις σχέσεις τους με αλληλεπιδρώντες φορείς. Οι μηχανισμοί διαχείρισης εξουσιοδοτήσεων εργάζονται προς αυτή την κατεύθυνση: την εξασφάλιση εξουσιοδοτημένης πρόσβασης σε υπηρεσίες και δεδομένα σε δυναμικά περιβάλλοντα. Ταυτόχρονα, παρέχουν τη δυνατότητα στους παρόχους υπηρεσιών και στα υποκείμενα των δεδομένων να οριοθετήσουν τις εξουσιοδοτήσεις ως προς τον υποκείμενο στόχο, χρόνο και τρόπο πρόσβασης. Επιπλέον αντιμετωπίζουν καίρια ζητήματα όπως είναι η πιστοποίηση των χρηστών (η διευκρίνηση δηλαδή της ταυτότητας και των γνωρισμάτων των χρηστών) και η απόδοση δικαιωμάτων και προνομίων πρόσβασης (ο καθορισμός δηλαδή του επιπέδου της πρόσβασης μιας πιστοποιημένης οντότητας) προσφέροντας με αυτόν τον τρόπο κάλυψη των βασικών αρχών ιδιωτικότητας και ασφάλειας, όπως αυτές παρουσιάστηκαν στην προηγούμενη ενότητα. Έτσι, στον πυρήνα συγκεκριμένων προσεγγίσεων εδράζονται μοντέλα ελέγχου πρόσβασης, μηχανισμοί αυθεντικοποίησης, κρυπτογραφικά εργαλεία και αλγόριθμοι συλλογιστικής ανάλυσης, η δυναμικότητα, η εκφραστικότητα και η

ευελιξία των οποίων καθορίζουν και τις δυνατότητες του εφαρμοζόμενου πλαισίου διαχείρισης εξουσιοδοτήσεων. Παρακάτω παρουσιάζονται μερικού θεμελιώδεις μηχανισμοί και διαδικασίες αυθεντικοποίησης χρηστών και διαχείρισης εξουσιοδοτήσεων.

2.3.1 Κρυπτογραφία

Η κρυπτογραφία αναφέρεται στη μελέτη, σχεδίαση και ανάπτυξη των μαθηματικών τεχνικών, εργαλείων και πρωτοκόλλων για την επίτευξη στόχων που άπτονται της ασφάλειας πληροφοριών όπως εμπιστευτικότητα, ακεραιότητα, αυθεντικοποίηση οντοτήτων και πιστοποίηση της προέλευσης των δεδομένων. Η κρυπτογραφία καθώς και τα κρυπτογραφικά συστήματα κατηγοριοποιούνται σε δύο ευρείς κατηγορίες: συστήματα συμμετρικής κρυπτογραφίας και συστήματα ασύμμετρης κρυπτογραφίας. Τα συστήματα συμμετρικής κρυπτογραφίας κάνουν χρήση ενός μοναδικού κλειδιού – μετασχηματισμού για την κρυπτογράφηση ενός μηνύματος. Ο αποστολέας αφού κωδικοποιήσει την πληροφορία με τη χρήση κάποιου μετασχηματισμού, πρέπει παράλληλα με την κωδικοποιημένη πληροφορία να κάνει γνωστό και τον μετασχηματισμό που αξιοποίησε στον παραλήπτη των δεδομένων. Ο τελευταίος, κάνοντας χρήση του κοινοποιηθέντα μετασχηματισμού, μπορεί να επαναφέρει την πληροφορία στην αρχική αποκωδικοποιημένη της μορφή.

Στα συστήματα ασύμμετρης κρυπτογραφίας, αξιοποιείται ένα ζεύγος κλειδιών κωδικοποίησης που αποτελείται από ένα δημόσιο κλειδί, η εμπιστευτικότητα του οποίου δεν συνεπάγεται κάτι για την ασφάλεια της κωδικοποιημένης πληροφορίας και ένα ιδιωτικό κλειδί, το οποίο δεν διαμοιράζεται και δεν κοινοποιείται σε καμία οντότητα εκτός από τον ιδιοκτήτη του κλειδιού. Ο αποστολέας κωδικοποιεί την πληροφορία με το δημόσιο κλειδί του παραλήπτη καθιστώντας τα εμπλεκόμενα δεδομένα μη αναγνώσιμα από οποιαδήποτε άλλη οντότητα εκτός από τον κάτοχο του ιδιωτικού κλειδιού, δηλαδή τον παραλήπτη.

2.3.2 Ψηφιακές υπογραφές και Ψηφιακά πιστοποιητικά

Ο μηχανισμός των ψηφιακών υπογραφών κατέχει επίσης σημαντική θέση στις διαδικασίες της αυθεντικοποίησης χρηστών και της διαχείρισης των εξουσιοδοτήσεων ενώ ταυτόχρονα αξιοποιείται συχνά σε συστήματα ασφάλειας προς

τήρηση της αρχή της μη-αποποίησης. Η υλοποίηση του μηχανισμού των ψηφιακών υπογραφών στηρίζεται στις τεχνικές κρυπτογράφησης δημόσιου κλειδιού. Ειδικότερα, ένας χρήστης προς επικύρωση της ταυτότητάς του ως αποστολέας μιας πληροφορίας κρυπτογραφεί μια σύνοψη της πληροφορίας (που έχει παραχθεί με την εφαρμογή μιας κοινά αποδεκτής μονόδρομης συνάρτησης σύνοψης) με χρήση του ιδιωτικού του κλειδιού παράγοντας ουσιαστικά την ψηφιακή του υπογραφή. Ο λήπτης της πληροφορίας είναι σε θέση να επικυρώσει την ορθότητα της ψηφιακής υπογραφής αποκρυπτογραφώντας τη με το δημόσιο κλειδί του αποστολέα και συγκρίνοντας την εξαχθείσα σύνοψη με μια σύνοψη του μηνύματος που ο ίδιος παράγει. Σε περίπτωση που οι δύο συνόψεις είναι ταυτόσημες, τότε η ψηφιακή υπογραφή είναι έγκυρη. Ο μηχανισμός των ψηφιακών υπογραφών επιτρέπει στη διαδικασία ανταλλαγής μηνυμάτων να είναι συμβατή με τις ακόλουθες αρχές της ασφάλειας πληροφοριών:

- **Ακεραιότητα**: Εφόσον η εξαχθείσα από την ψηφιακή υπογραφή σύνοψη είναι σωστή και ταυτόσημη με την παραχθείσα από το μήνυμα σύνοψη, η αρχική πληροφορία δεν είναι δυνατό να έχει τροποποιηθεί κατά τη μετάδοσή της.

- **Αυθεντικότητα**: Το μήνυμα έχει αποσταλεί από τη συγκεκριμένη οντότητα και μόνο αυτή, εφόσον μόνο αυτή έχει την κυριότητα του χρησιμοποιηθέντος ιδιωτικού κλειδιού.

- **Μη αποποίηση**: Ο αποστολέας δεν μπορεί να αρνηθεί την αποστολή του μηνύματος καθώς αποτελεί τη μοναδική οντότητα σε θέση να παράξει τη συγκεκριμένη υπογραφή.

- **Υπευθυνότητα**: Σε συνέχεια του προηγούμενου γνωρίσματος, ο αποστολέας καθίσταται υπεύθυνος για την αποστολή του μηνύματος και υπόλογος για τις όποιες ενέργειες άπτονται της αποστολής αυτής.

Η ασφαλής λειτουργία ενός κρυπτογραφικού συστήματος δημόσιου κλειδιού είναι σημαντικά εξαρτώμενη από την ισχύ και εγκυρότητα των εμπλεκόμενων δημόσιων κλειδιών και τη σύνδεση τους με τις ιδιοκτήτριες οντότητες. Προς τούτο, στην πράξη τα δημόσια κλειδιά οργανώνονται υπό τη μορφή ψηφιακών

πιστοποιητικών τα οποία συνιστούν και τον πλέον δημοφιλή τρόπο επικύρωσης της κατοχής ενός ασύμμετρου ζεύγους κλειδιών από μια οντότητα.

Ένα ψηφιακό πιστοποιητικό (συχνά συναντάται ο όρος πιστοποιητικό δημόσιου κλειδιού) συνιστά μια τεκμηριωμένη σύζευξη μεταξύ ενός δημόσιου κλειδιού και της ταυτότητας του κατόχου του. Στο πλαίσιο χρήσης των ψηφιακών πιστοποιητικών, η ταυτότητα μια οντότητας συναποτελείται από οποιοδήποτε σύνολο πληροφοριών που προσδιορίζει πλήρως την οντότητα που κατέχει και χρησιμοποιεί το αντίστοιχο με το δημόσιο ιδιωτικό κλειδί.

Επιπλέον, τα ψηφιακά πιστοποιητικά είναι δυνατόν να περιέχουν πλήθος άλλων πληροφοριών όπως είναι το χρονικό διάστημα ισχύος τους, οι χρησιμοποιούμενοι αλγόριθμοι κρυπτογράφησης και το μέγεθος των σχετικών κλειδιών. Προς επικύρωση της ισχύος τους, τα πιστοποιητικά δημόσιου κλειδιού υπογράφονται ψηφιακά από έμπιστες τρίτες οντότητες οι οποίες καλούνται Αρχές Πιστοποίησης (Certification Authority – CA). Οι Αρχές Πιστοποίησης επιτελούν μια σειρά από κρίσιμες λειτουργίες καθώς είναι υπεύθυνες για την έκδοση, τη διαχείριση, τη διανομή, την αποθήκευση και την ανάκληση των ψηφιακών πιστοποιητικών. Προφανώς, ο βαθμός εμπιστοσύνης που επιδεικνύει σε μια CA κάποιος χρήστης συνιστά και το επίπεδο εμπιστοσύνης που διατηρεί για τα εκδιδόμενα από εκείνη πιστοποιητικά.

Το πλέον διαδεδομένο και αναγνωρισμένο πρότυπο προδιαγραφής πιστοποιητικών δημόσιου κλειδιού παγκοσμίως εντοπίζεται στην έκδοση ITU-T X.509 (Telecommunication Standardization Sector of International Telecommunication Union, 2008) της Διεθνούς Ένωσης Τηλεπικοινωνιών (International Telecommunication Union – ITU). Σύμφωνα με το πρότυπο X.509 η δομή των ψηφιακών πιστοποιητικών αποτελείται από πεδία που υποδεικνύουν τις ακόλουθες τιμές: το δημόσιο κλειδί του κατόχου, ένα αναγνωριστικό του ασύμμετρου αλγορίθμου με τον οποίο θα αξιοποιηθεί το κλειδί, το όνομα του κατόχου του ζεύγους κλειδιών, το όνομα της Αρχής Πιστοποίησης που επικυρώνει την ιδιοκτησία αυτή, τον αριθμό της έκδοσης του προτύπου X.509 με το οποίο είναι συμβατό το πιστοποιητικό και μια σειρά από προαιρετικά πεδία που περιέχουν πληροφορίες σχετικά με τις πολιτικές πιστοποίησης της CA. Όπως προαναφέρθηκε, προς

επικύρωση της ισχύος του το πιστοποιητικό υπογράφεται κάνοντας χρήση του ιδιωτικού κλειδιού της CA. Η υπογραφή αυτή εκτός από την εγκυρότητα του πιστοποιητικού βεβαιώνει ταυτόχρονα ότι τυχόν τροποποιήσεις στο περιεχόμενο των πληροφοριών δεν μπορούν να πραγματοποιηθούν χωρίς ανίχνευση.

Μια οντότητα για να εξακριβώσει το αληθές και έγκυρο της ψηφιακής υπογραφής μιας CA σε κάποιο πιστοποιητικό πρέπει να έχει πρόσβαση στο δημόσιο κλειδί της. Καθώς το εν λόγω κλειδί είναι δυνατό να πιστοποιείται από μια άλλη, ανώτερη ιεραρχικά CA στη μορφή ψηφιακού πιστοποιητικού, εν τέλει η διαδικασία εξακρίβωσης της εγκυρότητας πιστοποιητικών δημόσιου κλειδιού μπορεί να εμπεριέχει μια αλυσίδα πιστοποιητικών και Αρχών Πιστοποίησης. Στο τέλος της αλυσίδας αυτής εντοπίζεται το πιστοποιητικό μιας CA, η οποία καλείται ρίζα αξιοπιστίας (root of trust). Τα δημόσια κλειδιά των συγκεκριμένων CA εκδίδονται και διαμοιράζονται υπό τη μορφή πιστοποιητικών που υπογράφονται από τις ίδιες (self-signed certificates) και υποδηλώνουν ότι οι ίδιες έχουν στην κατοχή τους τα συγκεκριμένα δημόσια κλειδιά. Ωστόσο, ενώ η υπογραφή των self-signed πιστοποιητικών επιτρέπει την εξακρίβωση της ακεραιότητας των περικλειόμενων πληροφοριών, δεν επιτρέπει την επαλήθευση της ακρίβειάς τους, καθώς η απουσία κάποιας πιστοποίησης από μια έμπιστη τρίτη οντότητα αφήνει ανοιχτό το ενδεχόμενο αναπαραγωγής λανθασμένων στοιχείων. Επομένως, στα κρυπτογραφικά συστήματα δημόσιου κλειδιού ιδιαίτερη προσοχή δίνεται στην ασφαλή και έγκυρη διανομή των δημόσιων κλειδών των Αρχών Πιστοποίησης ρίζας (root CA) έτσι ώστε να βεβαιώνεται ότι τα στοιχεία των εμπλεκόμενων πιστοποιητικών ανήκουν όντως στις σωστές οντότητες – CA. Απουσία ή απώλεια της βεβαιότητας αυτής θέτει σε κίνδυνο ολόκληρη την υποδομή καθώς ενεργοποιεί τη δυνατότητα επίτευξης μια επίθεσης πλαστοπροσωπίας (masquerade attack), όπου μια μη έμπιστη οντότητα μπορεί να υποδυθεί τον ρόλο μιας έμπιστης Αρχή Πιστοποίησης ρίζας.

2.3.4 Υποδομή Δημόσιου Κλειδιού και Υποδομή Διαχείρισης Δικαιωμάτων

Οι Υποδομές Δημόσιου Κλειδιού (Public Key Infrastructure – PKI) συνιστούν μια από τις πιο σημαντικές στιγμές της εφαρμογής της κρυπτογραφίας στα πληροφοριακά συστήματα. Στόχος των υποδομών PKI είναι η οργανωμένη έκδοση και διαχείριση πιστοποιητικών δημόσιου κλειδιού καθώς και η συντεταγμένη

διαχείριση των εμπλεκόμενων κλειδιών. Προς τούτο ενεργοποιούν Αρχές Πιστοποίησης, των οποίων ο ρόλος είναι κρίσιμος για την αποδοτικότητα μιας εγκατάστασης PKI καθώς αναπαριστούν το σημείο απόδοσης εμπιστοσύνης και άντλησης αξιοπιστίας χρηστών και λοιπών CA. Παραδοσιακά σχήματα PKI συνιστούν τα ακόλουθα:

- Αρχιτεκτονική μοναδικής CA: Όλες οι οντότητες του συστήματος αντιλαμβάνονται μια μοναδική CA ως έμπιστη οντότητα, η οποία είναι υπεύθυνη για τη διαχείριση όλων των εμπλεκόμενων πιστοποιητικών.

- Αρχιτεκτονική ιεραρχικά οργανωμένων CA: Οι CA του συστήματος είναι οργανωμένες και συνδεδεμένες ιεραρχικά, με την Αρχή Πιστοποίησης ρίζας να βρίσκεται υπεύθυνη για την πιστοποίηση των υπό αυτή CA και κάθε ενδιάμεση CA να είναι υπεύθυνη για την πιστοποίηση των κατωτέρων τους ιεραρχικά CA και των χρηστών της.

- Αρχιτεκτονική Πλέγματος (mesh architecture): Οι CA βρίσκονται συνδεδεμένες με σχέσεις ομοίου προς όμοιο καταργώντας τις ιεραρχίες του προηγούμενου τύπου αρχιτεκτονικής και καθιστώντας κάθε CA υπεύθυνη για την πιστοποίηση κατά κύριο λόγο των χρηστών της και κατά δεύτερο λόγο των συνδεδεμένων με αυτή CA.

Οι πρώτες εκδόσεις του προτύπου για τα ψηφιακά πιστοποιητικά X.509 (1988, 1993 και 1997) προδιέγραψαν τα βασικά δομικά και λειτουργικά στοιχεία των πιστοποιητικών δημόσιου κλειδιού και των Υποδομών Δημόσιου Κλειδιού. Οι αναθεωρημένη έκδοση του προτύπου το 2001 (όπως και οι επικαιροποιημένες εκδόσεις το 2005 και το 2008) εισήγαγαν σημαντικές επεκτάσεις και βελτιώσεις με κορυφαία όλων την περιγραφή των πιστοποιητικών ιδιοτήτων (attribute certificates) και του πλαισίου λειτουργίας των Υποδομών Διαχείρισης Δικαιωμάτων (Privilege Management Infrastructure – PMI). Οι Υποδομές Διαχείρισης Δικαιωμάτων διαχειρίζονται τα δικαιώματα χρηστών, παρέχουν υπηρεσίες εξουσιοδότησης οντοτήτων και λειτουργούν πανομοιότυπα αλλά συμπληρωματικά με τις Υποδομές Δημόσιου Κλειδιού που επικεντρώνονται στη διαχείριση της αυθεντικοποίησης χρηστών. Μάλιστα, η συνεργασία και η ολοκλήρωση συστημάτων PKI και PMI έχει

αποτελέσει αντικείμενο ανάλυσης και μελέτης του προτύπου X.509. Οι λειτουργίες και οι μηχανισμοί μιας υποδομής PMI επιτρέπουν τον ορισμό δικαιωμάτων σε χρήστες και την απεικόνισή τους σε πιστοποιητικά ιδιοτήτων εκδιδόμενα από μια Αρχή Εξουσιοδοτήσεων (Source of Authority – SoA) ή από εξουσιοδοτημένες προς τούτο Αρχές Ιδιοτήτων (Attribute Authority – AA). Τα πιστοποιητικά ιδιοτήτων επιτελούν στις υποδομές PMI τον σκοπό των ψηφιακών πιστοποιητικών στις υποδομές PKI, συνδέοντας και συσχετίζοντας δημόσια κλειδιά με ένα πλήθος γνωρισμάτων, χαρακτηριστικών και δικαιωμάτων χρηστών. Μάλιστα, πεδία των πιστοποιητικών ιδιοτήτων μπορούν να υποδεικνύουν τιμές βιομετρικών μεγεθών προς σύζευξη των φυσικών γνωρισμάτων ενός χρήστη με το δημόσιο κλειδί που έχει στην κατοχή του.

2.4 Επίγνωση πλαισίου στον έλεγχο πρόσβασης

Τι εννοούμε με τον όρο «επίγνωση πλαισίου»; Ετυμολογικά, με τον όρο πλαίσιο (context), αναφερόμαστε σε οτιδήποτε περιβάλλει και ορίζει κάτι άλλο. Ένας ορισμός για την έννοια του πλαισίου που βρίσκεται στο Collegiate λεξικό της Merriam-Webster είναι: *«(1) τα μέρη ενός λόγου που περιβάλλουν μια λέξη ή μια φράση και μπορούν να διαφωτίσουν το νόημά της (2) τις αλληλένδετες προϋποθέσεις υπό τις οποίες κάτι υπάρχει ή συμβαίνει»*. Εξειδικεύοντας τον όρο στον τομέα της πληροφορικής, αυτό το «κάτι άλλο» μπορεί να είναι μία υπόθεση, ένα άτομο, ένα υπολογιστικό σύστημα. Με το ρήμα «ορίζει» εννοούμε όλα εκείνα τα χαρακτηριστικά τα οποία δίνουν ξεχωριστή αξία στο αντικείμενο. Για παράδειγμα, αυτό το «κάτι», έστω ότι είναι ένας άνθρωπος, το «πλαίσιο» του οποίου αναφέρεται στην πληροφορία, στις ιδιότητες και στα χαρακτηριστικά του περιβάλλοντός του, όπως οι τοποθεσίες ατόμων που βρίσκονται γύρω του και τα αντίστοιχα προφίλ τους.

Πολλά παρόμοια παραδείγματα μπορούμε να σκεφτούμε στο ίδιο μοντέλο. Κοιτάζοντας τα προσεκτικά, θα βρούμε αρκετά σημεία κοινά, τα οποία θα μας βοηθήσουν στο να αναγνωρίσουμε κάποια συγκεκριμένα πρότυπα τα οποία ακολουθούνται. Σχεδόν πάντα θα αναγνωρίζουμε κάποιο στοιχείο και κάποια κατάσταση που ορίζεται. Έτσι οδηγούμαστε σε έναν πιο γενικό ορισμό που λέει ότι: Πλαίσιο είναι κάθε πληροφορία που μπορεί να χρησιμοποιηθεί για να χαρακτηρίσει την κατάσταση μίας οντότητας. Την προαναφερθείσα πληροφορία μπορούμε να την

χωρίσουμε σε δύο κατηγορίες με βάση την πολυπλοκότητά της: Σε στοιχειώδη πλαίσια (πχ. Χωρική τοποθεσία, Χρόνος, Κατάσταση εκτέλεσης μίας εφαρμογής, Πόροι συστήματος, Χωρητικότητα δικτύου, Κάποια δραστηριότητα, Τάσεις χρηστών, Συναισθηματικό προφίλ χρηστών, Θερμοκρασία) και σε μοντέλα πλαισίου (πχ. Χωρικά μοντέλα, Μοντέλα δραστηριοτήτων (δραστηριότητες ανθρώπων, τάσεις), Μοντέλο φυσικής κατάστασης (θερμοκρασία, καύσιμη ύλη, υγρασία, άνεμος και συναρτήσεις αυτών)).

Δεδομένου ότι η έννοια της επίγνωσης πλαισίου θεσπίστηκε με το Schilit, αρκετοί ορισμοί έχουν διατυπωθεί που περιγράφουν τα διαφορετικά επίπεδα διαδραστικότητας. Ο Cheverst για παράδειγμα, εξετάζει κατά πόσον οι πληροφορίες θα πρέπει να ωθούνται προς το χρήστη ή ο χρήστης θα πρέπει να αφεθεί να ανακτήσει τις πληροφορίες από μόνος τους, ενώ άλλοι ερευνητές θεωρούν ότι μόνο όταν οι εφαρμογές στις οποίες η πληροφορία καταχωρείται (και όχι να ανακτάται χειροκίνητα) πρέπει να ονομάζονται επίγνωσης πλαισίου. Ο ορισμός των Chen και Kotz αναγνωρίζει την ενεργητική και παθητική διαφοροποίηση στις εν λόγω εφαρμογές. Το ενεργό πλαίσιο επίγνωσης (Active context awareness) περιγράφει εφαρμογές που βασίζονται σε δεδομένα από αισθητήρες που αλλάζουν το περιεχόμενο των εφαρμογών αυτόματα, με βάση τα δεδομένα που ανακτώνται, ενώ στο παθητικό πλαίσιο επίγνωσης (Passive context awareness), απλώς υποβάλλονται αιτήσεις προς ενημέρωση του χρήστη και εκείνος προσδιορίζει κατά βούληση τον τρόπο με τον οποίο η εφαρμογή θα αλληλεπιδρά μαζί του.

Το πλαίσιο λοιπόν στον έλεγχο πρόσβασης περιλαμβάνει στατικά περιβαλλοντικά χαρακτηριστικά όπως η θέση ενός ατόμου σε έναν οργανισμό, καθώς και δυναμικά περιβαλλοντικά χαρακτηριστικά όπως ο χρόνος ενός αιτήματος δεδομένων, η τοποθεσία από όπου ένα αίτημα λαμβάνει χώρα, κλπ. Οι παράμετροι πλαισίου, που αφορούν το υποκείμενο, το αντικείμενο ή την ενέργεια του αιτήματος ελέγχου πρόσβασης, συνήθως επηρεάζουν την ενεργοποίηση ενός ρόλου, ή την επιβολή ενός κανόνα. Οι πιο σημαντικοί παράμετροι που αφορούν την επίγνωση πλαισίου στον έλεγχο πρόσβασης είναι οι χρονικοί, χωρικοί και οι ιστορικοί καθώς και ο συνδυασμός τους.

Συνεπώς, η προστασία των προσωπικών δεδομένων αποτελεί ένα σημαντικό παράγοντα για συστήματα επίγνωσης πλαισίου, επειδή κάθε είδους περιεχόμενο που σχετίζεται με ένα άτομο περιλαμβάνει ένα μεγάλο μέρος προσωπικών πληροφοριών. Τέλος, η σημασιολογική αναπαράσταση των πληροφοριών πλαισίου παρέχει τη δυνατότητα εξαγωγής γνώσης πέρα από την πραγματική αναπαράσταση και αποτελεί σημαντικό αντικείμενο μελέτης.

2.4.1 Παράμετροι επίγνωσης πλαισίου

Χρονικοί περιορισμοί πλαισίου

Χρησιμοποιώντας τις χρονικού τύπου πληροφορίες πλαισίου, είναι δυνατόν να εκφραστεί ότι μια ενέργεια που πραγματοποιεί ο χρήστης σε ένα συγκεκριμένο αντικείμενο επιτρέπεται μόνον σε μια δεδομένη χρονική στιγμή ή κατά τη διάρκεια συγκεκριμένου χρονικού διαστήματος. Το χρονικού τύπου πλαίσιο εκφράζεται μέσω των χρονικών περιορισμών, οι οποίοι αποτελούν δηλώσεις των πολιτικών ελέγχου πρόσβασης που περιλαμβάνουν περιορισμούς βασισμένους στο χρόνο όσον αφορά στην πρόσβαση στους πόρους.

Οι χρονικοί περιορισμοί μπορεί επίσης να απαιτούνται για τον περιορισμό της χρήσης των πόρων ή για τον έλεγχο χρόνο-ευαίσθητων δραστηριοτήτων. Αυτοί οι περιορισμοί πρέπει να αξιολογηθούν δυναμικά για να παρθεί η απόφαση εξουσιοδότησης. Οι χρονικοί περιορισμοί μπορεί επίσης να απαιτηθούν σε στατικά περιβάλλοντα. Για παράδειγμα, είναι δυνατόν να υπάρχουν χρονικοί περιορισμοί που περιορίζουν την ανάθεση και ενεργοποίηση του ρόλου μόνο σε συγκεκριμένα χρονικά διαστήματα. Χρησιμοποιώντας τις βασικές χρονικές πληροφορίες πλαισίου, είναι δυνατόν να οριστούν πιο περίπλοκα χρονικά πλαίσια.

Χωρικοί περιορισμοί πλαισίου

Επιπλέον, η τοποθεσία από όπου ο χρήστης κάνει την αίτηση μπορεί να είναι χρήσιμη, προκειμένου να καθοριστεί η πολιτική ελέγχου πρόσβασης. Για παράδειγμα ένας CEO (Chief Executive Officer) μπορεί να κατέχει το δικαίωμα ανάγνωσης των μισθών όλων των εργαζομένων μόνο αν βρίσκεται σε δικό του γραφείο στο εσωτερικό του οργανισμού. Το χωρικού τύπου πλαίσιο χρησιμοποιείται για να εκφράσει αυτές τις συνθήκες και θα μπορούσε να διακρίνεται σε δύο διαφορετικούς

τύπους: το φυσικό και το λογικό χωρικό πλαίσιο. Το πρώτο αντιστοιχεί στην φυσική τοποθεσία του χρήστη, δηλαδή το γραφείο του ή ένα συγκεκριμένο κτίριο, κλπ. Το τελευταίο αντιστοιχεί σε μία "λογική θέση" αναφερόμενο για παράδειγμα στον υπολογιστή ή το δίκτυο, κλπ.

Σε ορισμένες περιπτώσεις, το φυσικό και το λογικό χωρικό πλαίσιο σχετίζονται σε μεγάλο βαθμό. Για παράδειγμα, η δικτυακή διεύθυνση IP του χρήστη πιθανώς σχετίζεται με ένα συγκεκριμένο φυσικό χώρο όπως ένα τμήμα μέσα σε έναν οργανισμό. Πρέπει να σημειωθεί επίσης ότι, λόγω της εξάπλωσης της χρήσης του παγκόσμιου συστήματος προσδιορισμού θέσης (GPS), θα μπορούσε ένας χρήστης ή ένα τερματικό να εντοπιστεί, ανεξάρτητα από το δίκτυο. Εάν ένας οργανισμός επιτρέπει στους υπαλλήλους του τη χρήση του Mobile IP, είναι απαραίτητο να ληφθεί υπόψη το δίκτυο από το οποίο εκπέμπεται το αίτημα. Ένας χρήστης θα πάρει κατά πάσα πιθανότητα μειωμένα δικαιώματα, εάν αυτός είναι συνδεδεμένος από το γραφείο ενός πελάτη.

Επιπλέον, η ανάπτυξη των ασύρματων τεχνολογιών, όπως το Wi-Fi παρακινεί αυτό το έργο. Η πολιτική ασφάλειας πρέπει να μπορεί να λαμβάνει υπόψη το γεγονός ότι ο χρήστης είναι συνδεδεμένος μέσω δικτύου καλωδίων, μέσω ασύρματου δικτύου, ή σε ποιο Wi-Fi σημείο πρόσβασης είναι συνδεδεμένος.

Ιστορικοί περιορισμοί πλαισίου

Από την άλλη πλευρά, οι ιστορικού τύπου πληροφορίες πλαισίου εξαρτώνται από τις προηγούμενες ενέργειες που το υποκείμενο έχει εκτελέσει στο σύστημα. Με βάση αυτό, κάποιες πολιτικές ελέγχου πρόσβασης που σχετίζονται με χρονικούς περιορισμούς αποτελούν τις πολιτικές ελέγχου πρόσβασης που βασίζονται στην ιστορία. Σε αυτές τις πολιτικές, προηγούμενα γεγονότα πρόσβασης χρησιμοποιούνται ως παράγοντες απόφασης για την επόμενη εξουσιοδότηση πρόσβασης. Αυτό δημιουργεί την απαίτηση ύπαρξης ενός ιστορικού συστήματος ελέγχου κατάστασης για τον εντοπισμό και τη διατήρηση των παρελθοντικών γεγονότων.

2.4.2 Περιορισμοί πλαισίου που στοχεύουν στην προστασία της ιδιωτικότητας

Η έννοια του σκοπού

Μια πολύ σημαντική απαίτηση που προέρχεται από τις θεμελιώδεις αρχές προστασίας της ιδιωτικότητας είναι η προδιαγραφή και δέσμευση του σκοπού που ορίζει ότι, οποιαδήποτε συλλογή και/ή επεξεργασία των δεδομένων θα πρέπει να πραγματοποιηθεί για ένα καλά καθορισμένο σκοπό, ρητά κοινοποιημένο στο υποκείμενο των δεδομένων, ενώ τα προσωπικά δεδομένα που συλλέγονται για κάποιους συγκεκριμένους και νόμιμους σκοπούς, δεν πρέπει να χρησιμοποιηθούν για άλλους σκοπούς, οι οποίοι δε συμβιβάζονται με αυτούς για τους οποίους έχουν αρχικά συλλεχθεί.

Η έννοια του σκοπού είναι παρούσα σε προσεγγίσεις προδιαγραφής πολιτικών για την προστασία της ιδιωτικής ζωής , όπως η Platform for Privacy Preferences (P3P) (P3P) (World Wide Web Consortium, 2006), και αποτελεί τον κοινό παρονομαστή όλων των μοντέλων ελέγχου πρόσβασης με επίγνωση πλαισίου ιδιωτικότητας. Στην πραγματικότητα, η ενσωμάτωση του σκοπού στην διαδικασία απόφασης ελέγχου πρόσβασης στις Ιπποκρατικές βάσεις δεδομένων (Agrawal et al, 2002, Lefevre et al, 2004) ανάδειξε την εμφάνιση των τεχνολογιών ελέγχου πρόσβασης με επίγνωση ιδιωτικότητας.

Υποχρεώσεις

Σε αρκετές περιπτώσεις, η πρόσβαση στα δεδομένα πρέπει συμπληρώνεται από την εκτέλεση ορισμένων ενεργειών, που συχνά αναφέρονται στη βιβλιογραφία ως υποχρεώσεις "obligations" (Hilty, Basin & Pretschner, 2005). Για παράδειγμα, η νομοθεσία καθορίζει τις αλληλεπιδράσεις με το υποκείμενο των δεδομένων (π.χ., πληροφορίες ή παροχή συναίνεσης) και τις Αρχές Προστασίας Προσωπικών Δεδομένων, κλπ. Ως εκ τούτου, τα συστήματα ελέγχου πρόσβασης συχνά εμπλουτίζονται και ενσωματώνουν λειτουργίες που επιτρέπουν την εκτέλεση των υποχρεώσεων.

Ιδιαίτερα όσον αφορά στην ιδιωτικότητα, ο όρος «υποχρεώσεις ιδιωτικότητας» (Casassa Mont, 2004) έχει προκύψει και χαρακτηρίζει μια ποικιλία μοντέλων. Μερικές υποχρεώσεις πρέπει να πληρούνται σε ένα συγκεκριμένο χρονικό διάστημα. Στο πλαίσιο αυτό, χωρίζονται σε δύο κατηγορίες: η προ-υποχρεώσεις (pro-obligations) που αφορούν δράσεις που πρέπει να πληρούνται πριν από την άδεια πρόσβασης και μετά-υποχρεώσεις (post-obligations) που αναφέρονται σε

συμπληρωματικές ενέργειες που θα πρέπει να ολοκληρωθούν αφού επιτραπεί η πρόσβαση, προκειμένου να εκπληρωθεί το αίτημα.

Επιπλέον, υπάρχουν περιπτώσεις όπου η υποχρέωση είναι περιστασιακή, ανάλογα με περιορισμούς, ή για την εκτέλεση άλλων υποχρεώσεων. Στην πραγματικότητα, κάτι που δεν πρέπει να παραμεληθεί είναι ότι οι υποχρεώσεις είναι δράσεις και, ως εκ τούτου, για να εκπληρωθεί μια υποχρέωση απαιτούνται επιπρόσθετα κάποια προνόμια. Εάν τα προνόμια που απαιτούνται δεν είναι διαθέσιμα, μια τέτοια υποχρέωση είναι ανεκπλήρωτη.

Το πρόβλημα μπορεί να γίνει πιο περίπλοκο διότι οι πολιτικές που σχετίζονται με αυτά τα προνόμια μπορεί να απαιτούν περαιτέρω εκτέλεση κάποιων άλλων υποχρεώσεων. Ως εκ τούτου, οι τεχνικές που χρησιμοποιούνται για την ανάλυση των αλληλεπιδράσεων μεταξύ των υποχρεώσεων και των πολιτικών πρέπει να σχεδιασθούν έτσι ώστε να ανιχνεύουν άκυρες πολιτικές λόγω ανεκπλήρωτων υποχρεώσεων.

Διαχωρισμός καθηκόντων

Ο Διαχωρισμός καθηκόντων (SoD) αποτελεί μία σημαντική αρχή ασφάλειας που χρησιμοποιείται για την πρόληψη της απάτης και λαθών. Χρησιμοποιείται για να περιγράψει και να επιβάλει τη σύγκρουση συμφερόντων των πολιτικών, που απαιτούν ότι δύο ή περισσότεροι διαφορετικοί χρήστες είναι υπεύθυνοι για την ολοκλήρωση μιας εργασίας ή σχετικών εργασιών. Ο σκοπός της SoD στο RBAC είναι «*Να διασφαλιστεί ότι οι αποτυχίες της παράλειψης ή της αξίωσης στα πλαίσια ενός οργανισμού προκαλούνται μόνο ως αποτέλεσμα συμπαιγνίας μεταξύ των ατόμων*».

Η απλούστερη μορφή της αρχής SoD δηλώνει ότι, αν μία ευαίσθητη εργασία αποτελείται από δύο βήματα, τότε διαφορετικοί χρήστες θα πρέπει να εκτελέσουν τις επιμέρους ενέργειες. Σε γενικές γραμμές, όταν μία ευαίσθητη εργασία αποτελείται από j βήματα, μια πολιτική SoD απαιτεί τη συνεργασία τουλάχιστον i (για κάποιο $i \leq j$) διαφορετικών χρηστών για την ολοκλήρωσή της. Μια πολιτική SoD μπορεί να επιβληθεί είτε στατικά ή δυναμικά. Σε στατική επιβολή, καθορίζονται οι στατικές SoD (SSoD) πολιτικές. Η SSoD επιβάλλει περιορισμούς στη μεταβίβαση των χρηστών σε ρόλους. Κάθε πολιτική SSoD δηλώνει ότι k - 1 χρήστες δεν μπορούν να

έχουν ταυτόχρονα όλα τα δικαιώματα για την ολοκλήρωση μίας ευαίσθητης εργασίας. Φαίνεται ότι, αν μια SSoD πολιτική ικανοποιείται, τότε η αντίστοιχη πολιτική SoD ικανοποιείται επίσης. Η δυναμική SoD (DSoD) επιτρέπει σε ένα χρήστη να έχει δύο ή περισσότερους ρόλους που δεν δημιουργούν σύγκρουση συμφερόντων όταν ενεργούν ανεξάρτητα, αλλά παράγουν ανησυχίες όσον αφορά στην ιδιωτικότητα όταν ενεργοποιούνται ταυτόχρονα. Οι DSoD σχέσεις, όπως και οι SSoD σχέσεις, έχουν ως σκοπό να περιορίσουν τα δικαιώματα που είναι στη διάθεση του χρήστη.

Διαχείριση συγκρούσεων

Μια κρίσιμη πτυχή της προδιαγραφής πολιτικών όσον αφορά τον έλεγχο πρόσβασης είναι να εξασφαλιστεί ότι μια πολιτική δεν είναι σε σύγκρουση με άλλες υφιστάμενες πολιτικές. Μια προσέγγιση επικύρωσης θα πρέπει να χρησιμοποιείται για την ανίχνευση των συγκρούσεων μεταξύ των πολιτικών ασφάλειας (Charalambides et al., 2006). Πιθανές καταστάσεις συγκρούσεων σε ένα μοντέλο ελέγχου πρόσβασης προκαλούνται, για παράδειγμα λόγω της συμπερίληψης ενός συγκεκριμένο συνόλου οντοτήτων πολιτικής (υποκείμενο, δράση, αντικείμενο) σε περισσότερες από μια οντότητες ή σε περιπτώσεις που υπάρχουν αντικρουόμενες σχέσεις μεταξύ των κανόνων εξουσιοδότησης, καθώς και ασυνέπειες μεταξύ σκοπών, περιορισμών πλαισίου ή/και υποχρεώσεων.

Για παράδειγμα, ένας κανόνας μπορεί να «*επιτρέψει σε ένα υποκείμενο (s) την πρόσβαση σε ένα αντικείμενο (o), ενώ ένας δεύτερος κανόνας μπορεί να απαγορέψει στην ομάδα (g), εκ των οποίων το υποκείμενο s είναι μέλος, την πρόσβαση στο αντικείμενο o*». Επειδή όμως δεν είναι δυνατόν να ανιχνεύονται όλες οι καταστάσεις των συστημάτων, δεν υπάρχει καμία εγγύηση για την ανίχνευση όλων των συγκρούσεων των πολιτικών.

Ως εκ τούτου, ένας μηχανισμός επίλυσης συγκρούσεων απαιτείται για την συστηματική επίλυση του εντοπιζόμενων συγκρούσεων. Σε γενικές γραμμές, η μέθοδος επίλυσης της σύγκρουσης είναι ο αλγόριθμος που ένα σύστημα ελέγχου πρόσβασης χρησιμοποιεί για τον προσδιορισμό του ποιος κανόνας, από ένα σύνολο κανόνων σε σύγκρουση, θα λάβει προτεραιότητα έναντι των άλλων.

Ιεραρχίες

Οι ιεραρχίες έχουν χρησιμοποιηθεί για τη διάδοση της απόφασης εξουσιοδότησης στην πλειοψηφία των μοντέλων ελέγχου πρόσβασης και αποτελούν μια σημαντική πτυχή στα μοντέλα προστασίας της ιδιωτικότητας. Στο πλαίσιο αυτό καθορίζονται συνήθως ιεραρχίες ρόλου, δεδομένων, σκοπού και ιεραρχίες περιορισμών.

Οι ιεραρχίες ρόλου χρησιμοποιούνται για την αναπαράσταση της δομής των ρόλων στις γραμμές εξουσίας και καθηκόντων ενός οργανισμού. Επιτρέπουν την ανάθεση ρόλων σε μεμονωμένους οργανισμούς, η οποία επιτρέπει προσαρμογή των ρόλων για την εκπλήρωση των αναγκών του κάθε οργανισμού. Για να εξασφαλιστεί το υψηλότερο επίπεδο ασφάλειας, οι εξουσιοδοτημένοι διαχειριστές μπορούν να μεταβιβάζουν την πρόσβαση μόνο σε προνόμια που τους έχουν χορηγηθεί. Η κορυφή προς βάση (top-down) ιεραρχία δημιουργεί ένα ασφαλές, αποτελεσματικό μοντέλο για τους οργανισμούς για την τροποποίηση των ρόλων με σκοπό την κάλυψη των αναγκών τους χωρίς να παρακάμπτουν τους περιορισμούς της πρόσβασης τους.

Από την άλλη πλευρά, οι σκοποί που αναφέρονται στις πολιτικές προστασίας της ιδιωτικής ζωής αποτελούν συχνά υψηλού επιπέδου επιχειρηματικές υπηρεσίες, π.χ. "Μέτρηση του δικτύου". Αυτό δημιουργεί την προϋπόθεση ότι πιο συγκεκριμένα δικαιώματα προστασίας της ιδιωτικότητας μπορεί να σχετίζονται με πιο συγκεκριμένους σκοπούς που εμπίπτουν στον τομέα του σκοπού υψηλού επιπέδου. Εν προκειμένω, στα συνήθη περιβάλλοντα των επιχειρήσεων, οι σκοποί όπως είναι φυσικό θα πρέπει να έχουν κάποια ιεραρχική σχέση μεταξύ τους, δηλαδή, σχέσεις γενίκευσης και σχέσεις εξειδίκευσης, προκειμένου να απλουστευθεί η διαχείρισή τους. Συνήθως αναπαρίστανται ως γράφοι δέντρου. Ένας κόμβος γονέας αντιπροσωπεύει ένα γενικότερο σκοπό από αυτούς που εκπροσωπούνται από τα παιδιά κόμβους, ομαδοποιώντας τους ειδικότερους σκοπούς σε πιο γενικούς.

Από την άλλη πλευρά, τα δεδομένα των αντικειμένων που αναφέρονται στα δικαιώματα ιδιωτικότητας είναι συχνά υψηλού επιπέδου ταξινομήσεις των δεδομένων, όπως τα στοιχεία επικοινωνίας των πελατών. Αυτά τα αντικείμενα δεδομένων χρησιμοποιούνται για τη διάκριση της ταξινόμησης των συλλεγόμενων στοιχείων που πρέπει να αντιμετωπίζονται με διαφορετικό τρόπο από την άποψη της

προστασίας της ιδιωτικότητας. Οργανώνοντας τα υψηλού επιπέδου δεδομένα σύμφωνα με μια ιεραρχία, συνήθως σε μια δενδροειδή δομή, όχι μόνο βελτιώνει άμεσα τα μοντέλα οργάνωσης δεδομένων των οργανισμών, αλλά επίσης, βελτιώνει και την εκφραστικότητα των δικαιωμάτων. Για παράδειγμα, μια άδεια που αναφέρεται σε ένα υψηλού επιπέδου δεδομένο εφαρμόζεται σε όλα τα μέρη του, μειώνοντας έτσι το συνολικό αριθμό των δικαιωμάτων.

Τέλος, για τους ίδιους λόγους οι ιεραρχίες είναι σημαντικές στον τομέα των πληροφοριών πλαισίου. Από την άποψη αυτή, πολλά μοντέλα ελέγχου πρόσβασης υιοθετούν αυτήν την προσέγγιση και το σύνολο των διαφόρων περιορισμών πλαισίου που σχετίζονται με το χρόνο, το χώρο καθώς και την ιστορία μπορεί να οργανώνονται σε ιεραρχίες, προκειμένου οι σύνθετες πολιτικές ελέγχου πρόσβασης να εκτελεστούν και να διαχειριστούν με αποτελεσματικό και ευέλικτο τρόπο.

Το σύνολο των χαρακτηριστικών επίγνωσης πλαισίου και πλαισίου ιδιωτικότητας αντικατοπτρίζονται στις Εικόνες 7 και 8 αντιστοίχως.

Εικόνα 7: Πληροφορίες Επίγνωσης Πλαισίου

Εικόνα 8: Πλαίσιο Ιδιωτικότητας

2.5 Σημασιολογικές τεχνολογίες στον έλεγχο πρόσβασης με επίγνωση πλαισίου και επίγνωση ιδιωτικότητας

Ο συγκεκριμένος τύπος που χαρακτηρίζει κάθε αντικείμενο δεδομένου αποτελεί μια πολύ σημαντική παράμετρο για τον καθορισμό των διαδικασιών οι οποίες ορίζουν ποιο θα είναι το υποκείμενο των δεδομένων και, κατά συνέπεια, για την προσαρμογή της επιχειρησιακής διαδικασίας ή τη συμπεριφορά των υπηρεσιών, όπως επίσης γίνεται σαφές από τις αρχές προστασίας της ιδιωτικότητας.

Η σημασιολογία των επιχειρησιακών διεργασιών ή υπηρεσιών, οι υποκείμενοι σκοποί συλλογής και επεξεργασίας, καθώς και οι εμπλεκόμενοι φορείς, είναι ίσης σπουδαιότητας και συνολικά είναι μέρος αυτού που θα μπορούσε να χαρακτηριστεί ως «*Πλαίσιο Ιδιωτικότητας*». Με βάση τα παραπάνω, ένα μεγάλο ερευνητικό θέμα σήμερα αποτελούν οι προκλήσεις που αντιμετωπίζονται στην αναπαράσταση αυτής της πληροφορίας. Για παράδειγμα, αξίζει να αναφέρουμε ότι σήμερα πιστεύεται πως για τον σχεδιασμό συστημάτων επίγνωσης πλαισίου, οι οντολογίες αποτελούν ένα από τα καλύτερα μέσα αναπαράστασης γνώσης. Αυτό συμβαίνει για τους εξής λόγους:

- Με μία κοινή οντολογία διευκολύνεται ο διαμοιρασμός γνώσης σε ανοιχτά και δυναμικά κατανεμημένα συστήματα

- Οντολογίες με καλώς ορισμένη δηλωτική σημασιολογία παρέχουν ένα μέσο σε έξυπνους πράκτορες να βγάλουν συμπεράσματα για την πληροφορία πλαισίου (contextual information).
- Με οντολογίες μπορούν οι συσκευές και οι πράκτορες να μπορούν να συνομιλούν χωρίς να είναι απαραίτητα σχεδιασμένα για να μπορούν να επικοινωνούν μεταξύ τους.

Συνεπώς, η ανακάλυψη και η διαλειτουργικότητα μεταξύ των διαφορετικών πηγών πληροφόρησης των οργανισμών, καθώς και η αναπαράστασή τους σε δυναμικά, ανοικτά και ετερογενή περιβάλλοντα μπορεί να βελτιωθεί με τις τεχνολογίες του Σημασιολογικού Ιστού και τις οντολογίες οι οποίες εκφράζονται στη γλώσσα Οντολογίας του Παγκοσμίου Ιστού (OWL) (World Wide Web Consortium, 2004). Οι οντολογίες OWL παρέχουν πλούσια εκφραστικότητα, καθώς και προηγμένες δυνατότητες συλλογιστικής και αποτελούν ένα ενδιαφέρον εργαλείο για τη σημασιολογική εκπροσώπηση σε συστήματα ελέγχου πρόσβασης, η οποία έχει υιοθετηθεί από ορισμένα μοντέλα.

2.5.1 Δομικά στοιχεία οντολογιών

Η γνώση στις οντολογίες τυποποιείται χρησιμοποιώντας πέντε κατηγορίες συστατικών (Uschold & Cruninger, 1996):

- Κλάσεις (classes): Οι κλάσεις αναπαριστώνται με τις έννοιες (concepts). Μια έννοια μπορεί να είναι οτιδήποτε για το οποίο μπορεί να ειπωθεί κάτι και μπορεί να είναι η περιγραφή μιας εργασίας, μιας λειτουργίας, μιας ενέργειας, μιας ιδέας, κλπ. Οι έννοιες είναι δυνατό να διαιρεθούν σε δύο βασικές κατηγορίες: τις πρωταρχικές έννοιες (primitive concepts) οι οποίες έχουν μόνο απαραίτητες συνθήκες (ως προς τις ιδιότητές τους), για να είναι μέλος μιας κλάσης και τις έννοιες εξ ορισμού (defined concepts) των οποίων η περιγραφή είναι ικανή και αναγκαία συνθήκη για να είναι ένα αντικείμενο μέλος της κλάσης.
- Σχέσεις (properties): Οι σχέσεις εκφράζουν ένα είδος αλληλεπίδρασης μεταξύ των εννοιών ενός πεδίου ενδιαφέροντος, για παράδειγμα subclass-of, is-a, κλπ.

- Συναρτήσεις (functions): Οι συναρτήσεις εκπροσωπούν μια ειδική περίπτωση σχέσης. Για παράδειγμα, η τιμή-μεταχειρισμένου-αυτοκινήτου μπορεί να προσδιορίζεται ως συνάρτηση της αρχικής τιμής του αντίστοιχου καινούργιου αυτοκινήτου, του μοντέλου και των χαρακτηριστικών του αυτοκινήτου, των χιλιομέτρων που έχει διανύσει κλπ.
- Αξιώματα (axioms): Τα αξιώματα περιγράφουν προτάσεις που είναι πάντοτε αληθείς. Για παράδειγμα, αν ο Χ είναι δευτεροετής φοιτητής τότε μπορεί να παρακολουθήσει το μάθημα Υ.
- Στιγμιότυπα (instances): Τα στιγμιότυπα αναπαριστούν συγκεκριμένα στοιχεία. Για παράδειγμα, ο φοιτητής με το όνομα "Γιάννης" είναι στοιχείο της κλάσης "Φοιτητής".

2.5.2 Οντολογίες σχετικές με την ιδιωτικότητα

Στο σημείο αυτό θα αναφέρουμε κάποιες ήδη υπάρχουσες οντολογίες που προσεγγίζουν το πρόβλημα της ιδιωτικότητας και αφορούν σε ζητήματα ασφάλειας (security) και εμπιστοσύνης (trust). Πριν περιγράψουμε τις παραπάνω οντολογίες, είναι σημαντικό να δώσουμε περαιτέρω έμφαση στον ορισμό της έννοιας της πολιτικής (policy) καθώς η έννοια αυτή παίζει σημαντικό ρόλο στην προστασία των πόρων ενός συστήματος.

Η πολιτική είναι μια τεχνική που προκύπτει για τον έλεγχο και τη ρύθμιση της συμπεριφοράς χαμηλού επιπέδου του συστήματος καθορίζοντας υψηλού επιπέδου κανόνες του συστήματος. Η χρήση της πολιτικής είναι συνηθισμένη σε υπολογιστικά συστήματα που έχουν σαν γνώρισμα την ασφάλεια ή την προστασία της ιδιωτικότητας. Οι γλώσσες καθορισμού μιας πολιτικής, οι οποίες αναπαριστώνται μέσω των γλωσσών του σημασιολογικού ιστού (π.χ. RDFS, DAML+OIL και OWL) ορίζονται συνήθως σε όρους οντολογιών.

KAoS Policy Ontology

Η KAoS (Uszok et al., 2004) είναι από τις πρώτες προσπάθειες για την αναπαράσταση μιας πολιτικής χρησιμοποιώντας την γλώσσα OWL. Ξεκίνησε από τα μέσα της δεκαετίας του '90 σαν ένα σύνολο υπηρεσιών ανεξαρτήτως πλατφόρμας (platform-independent) που επιτρέπει στους ανθρώπους να ορίσουν πολιτικές που

εξασφαλίζουν επαρκή προβλεψιμότητα και ελεγξιμότητα τόσο σε συστήματα πρακτόρων όσο και σε κλασσικά κατανεμημένα συστήματα. Οι υπηρεσίες και τα εργαλεία που προσφέρει η KAoS, επιτρέπουν τον προσδιορισμό, τη διαχείριση και την επίλυση αντιθέσεων, και την εκτέλεση των πολιτικών στα ειδικά πλαίσια που καθορίζονται από το πεδίο της οντολογίας. Χρησιμοποιεί έννοιες (concepts) οντολογιών (κωδικοποιημένες σε OWL) για να χτίσει πολιτικές.

Η τωρινή έκδοση του πυρήνα των οντολογιών της KAoS (Uszok et al., 2004) ορίζει βασικές έννοιες για τους δράστες (actors), τις ενέργειες (actions), τις ομάδες (groups), τις τοποθεσίες και διάφορες οντότητες που σχετίζονται με τις δράσεις. Περιλαμβάνει περισσότερες από 100 κλάσεις και 60 ιδιότητες. Η οντολογία *actor* περιέχει κλάσεις για ανθρώπους και μέρη λογισμικού τα οποία μπορεί να είναι το αντικείμενο μιας πολιτικής. Οι ομάδες δραστών ή άλλων οντοτήτων μπορούν να διαχωριστούν ανάλογα με το αν το σύνολο των μελών ορίζεται εκτατικά (π.χ. μέσω απαρίθμησης σε κάποια καταχώρηση) ή εκούσια (π.χ. βάσει ενός συγκεκριμένου μέρους όπου διάφορες οντότητες βρίσκονται αυτή τη στιγμή). Η οντολογία *action* ορίζει διάφορους τύπους βασικών ενεργειών όπως η πρόσβαση, η επικοινωνία, η κίνηση κλπ. Ο οντολογικός ορισμός μιας ενέργειας συνδέει την ενέργεια με μια λίστα ιδιοτήτων που περιγράφουν το περιεχόμενο της πράξης αυτής. Παραδείγματα ιδιοτήτων των κλάσεων των ενεργειών είναι: ο προορισμός της επικοινωνίας, το είδος κρυπτογράφησης, ο χρόνος, προηγούμενο ιστορικό κλπ. Κάθε ιδιότητα συνδέεται με εύρος τιμών που θα μπορούσε να έχει στην κλάση των ενεργειών. Ένα συγκεκριμένο στιγμιότυπο της κλάσης των ενεργειών μπορεί να πάρει τιμές για μια συγκεκριμένη ενέργεια μόνο μέσα από αυτό το εύρος. Για μια συγκεκριμένη εφαρμογή, οι οντολογίες του πυρήνα της KAoS συνήθως επεκτείνονται με επιπρόσθετες κλάσεις, στιγμιότυπα και κανόνες, που χρησιμοποιούν τις έννοιες των οντολογιών του πυρήνα σαν υπερσύνολα. Αυτό επιτρέπει στο πλαίσιο της KAoS (δημιουργία, διαχείριση, εξαγωγή συμπερασμάτων μέσω οντολογιών) να βρίσκει εξειδικευμένες έννοιες. Στην KAoS οι πολιτικές μπορεί να εκφράζουν εξουσιοδότηση (περιορισμοί που επιτρέπουν ή απαγορεύουν μια ενέργεια) ή υποχρέωση (περιορισμοί που απαιτούν μια ενέργεια για να εκτελεστούν) για κάποιο είδος ενέργειας που πραγματοποιείται από έναν ή περισσότερους δράστες, ενώ επιπλέον βοηθητικές πληροφορίες μπορούν να

συνδέονται με μια πολιτική όπως π.χ. η ύπαρξη κάποιας ποινής για την παραβίαση μιας συγκεκριμένης πολιτικής.

Η πολιτική επομένως στην KAoS αναπαριστάται σαν ένα στιγμιότυπο μιας εκ των τεσσάρων κλάσεων: *positive* ή *negative authorization*, και *positive* ή *negative obligation*. Το στιγμιότυπο κατέχει τιμές για διάφορες ιδιότητες που σχετίζονται με τη διαχείριση (π.χ. προτεραιότητα, time stamp) που προσδιορίζουν πώς μια δεδομένη πολιτική χειρίζεται μέσα στο σύστημα. Η σημαντικότερη ιδιότητα είναι το όνομα της κλάσης της ενέργειας, όπου χρησιμοποιείται για να προσδιορίσει την πραγματική σημασία της πολιτικής. Οι πολιτικές εξουσιοδότησης χρησιμοποιούν την παραπάνω ιδιότητα για να προσδιορίσουν την πράξη που επιτρέπεται ή απαγορεύεται. Οι πολιτικές υποχρέωσης την χρησιμοποιούν για τον προσδιορισμό της πράξης που επιβάλλεται ή απαλλάσσεται. Οι ιδιότητες που αφορούν την ποινή μιας πολιτικής περιέχουν μια τιμή που αντιστοιχεί σε μια κλάση ενεργειών που πρέπει να γίνουν αφού παραβιαστεί μια πολιτική.

Από τα παραπάνω φαίνεται ότι η έννοια της ενέργειας παίζει κεντρικό ρόλο στον ορισμό μιας KAoS πολιτικής. Συνήθως κάθε ενέργεια που απαιτείται για την υποστήριξη μιας νέας πολιτικής παράγεται αυτόματα όταν ο χρήστης ορίζει μια νέα πολιτική μέσω του εργαλείου KPAT (KAoS Policy Administration Tool) που προσφέρει η KAoS. Μέσω διαφόρων περιορισμών ιδιοτήτων, ένα δεδομένο αντικείμενο μιας πράξης μπορεί να μελετηθεί με διάφορους τρόπους, για παράδειγμα, είτε με επιμέρους πράκτορες, με πράκτορες μιας συγκεκριμένης κλάσης κλπ. Το συγκεκριμένο πλαίσιο μέσα στο οποίο ο περιορισμός μιας πολιτικής εφαρμόζεται μπορεί να περιγραφεί επακριβώς με τον περιορισμό των τιμών των ιδιοτήτων της συγκεκριμένης ενέργειας.

Rei Policy Ontology

Η Rei (Rei Ontology Specifications) είναι μια γλώσσα καθορισμού πολιτικών που χρησιμοποιεί την γλώσσα OWL και επιτρέπει στους χρήστες να αναπτύσσουν πολιτικές που αφορούν οντολογίες πεδίου ενδιαφέροντος. Χρησιμοποιείται για να περιγράψει θετικές και αρνητικές παραχωρήσεις αλλά και υποχρεώσεις. Καθώς η Rei στρέφεται προς κατανεμημένα περιβάλλοντα, περιλαμβάνει και προδιαγραφές

επίλυσης συγκρούσεων όπως για παράδειγμα ανάθεση προτεραιότητας μεταξύ πολιτικών ή μεταξύ των επιμέρους κανόνων μιας πολιτικής.

Η Rei αποτελείται από διάφορες οντολογίες: *ReiPolicy*, *ReiMetaPolicy*, *ReiEntity*, *ReiDeontic*, *ReiConstraint*, *ReiAnalysis*, και *ReiAction*. Κάθε οντολογία περιγράφει τις κλάσεις και τις ιδιότητες που σχετίζονται με το πεδίο αυτό. Παρακάτω περιγράφονται οι οντολογίες αυτές :

Policy: Οι πολιτικές χρησιμοποιούνται για να οδηγήσουν τη συμπεριφορά των οντοτήτων μέσα στο πεδίο. Μια πολιτική κυρίως περιέχει μια λίστα κανόνων και το πλαίσιο που χρησιμοποιήθηκε για τον ορισμό του πεδίου της πολιτικής. Θα μπορούσε επίσης να περιλαμβάνει επίσης μια λίστα προεπιλογών που χρησιμοποιήθηκαν για την ερμηνεία της πολιτικής καθώς επίσης και ένα σύνολο προδιαγραφών για την επίλυση συγκρούσεων.

Deontic Object: Η κλάση αυτή χρησιμοποιείται για τη δημιουργία παραχωρήσεων, απαγορεύσεων, υποχρεώσεων και απαλλαγών (δεοντικά αντικείμενα) για τις διάφορες οντότητες του πεδίου της πολιτικής. Περιλαμβάνει δομές που περιγράφουν πάνω σε ποιές ενέργειες το ένα δεοντικό αντικείμενο περιγράφεται, ποιος είναι ο δράστης μιας ενέργειας, καθώς και κάτω από ποιές συνθήκες εφαρμόζεται το δεοντικό αντικείμενο.

Action: Η οντολογία αυτή είναι από τις πιο σημαντικές στις προδιαγραφές της Rei καθώς οι πολιτικές περιγράφονται πάνω σε πιθανές ενέργειες στο πεδίο. Η κλάση αυτή περιλαμβάνει ιδιότητες που απαιτούνται για όλες τις ενέργειες. Η Rei περιλαμβάνει ακόμα μια αναπαράσταση των ενεργειών που επιτρέπει την λήψη περισσότερων χρήσιμων πληροφοριών, κάνοντας έτσι ευκολότερη την κατανόηση της ενέργειας και των παραμέτρων της. Τέλος, επιτρέπει πληροφορίες εξαρτώμενες από το πεδίο για ενέργειες που πρόκειται να προστεθούν.

Constraint: Η κλάση αυτή περιλαμβάνει τους περιορισμούς, ορίζοντας ένα σύνολο αντικειμένων, ένα σύνολο ενεργειών και ένα σύνολο χρηστών. Υπάρχουν δύο είδη περιορισμών, *SimpleConstraint* και *BooleanConstraint*. Στην πρώτη περίπτωση οι περιορισμοί μοντελοποιούνται σαν μια τριάδα που αποτελείται από το υποκείμενο (subject), το κατηγόρημα (predicate) και το αντικείμενο (object). Οι περιορισμοί

(απλοί και λογικοί) μπορούν να συνδυαστούν σαν ζευγάρια χρησιμοποιώντας τους λογικούς τελεστές and, or και not. Κάθε λογικός τελεστής είναι υποκλάση της κλάσης *BooleanConstraint*.

Entity: Κάθε χρήστης, πράκτορας ή πόρος υλικού περιγράφεται σαν μία οντότητα. Προς το παρόν η κλάση *Entity* έχει μόνο μία ιδιότητα, την *affiliation*, που περιγράφει τον οργανισμό στον οποίο ανήκει μία οντότητα. Η κλάση Entity χωρίζεται στις υποκλάσεις *Agent*, *Object* και *Variable* που προσδιορίζουν αν μια οντότητα είναι πράκτορας, κάποιος πόρος υλικού ή μια μεταβλητή για την περιγραφή των περιορισμών.

MetaPolicy: Οι προδιαγραφές της Rei περιλαμβάνουν δομές μεταπολιτικών (metapolicies) για το πώς ερμηνεύονται οι πολιτικές και το πώς μπορούν να επιλυθούν οι συγκρούσεις. Η Rei μοντελοποιεί δύο βασικούς τύπους μεταπολιτικών, έναν για τις προεπιλογές και έναν για την επίλυση συγκρούσεων, για τον χειρισμό διαφορετικών απαιτήσεων των πολιτικών.

Analysis: Για να είναι δυνατή η ανάπτυξη συνεκτικών και έγκυρων πολιτικών, η Rei παρέχει δύο καθορισμούς. Τη διαχείριση μέσω περιπτώσεων χρήσης (use-cases) και ανάλυση what-if. Στην πρώτη περίπτωση, ένα σύνολο περιπτώσεων χρήσης μπορεί να περιγραφεί σαν το σύνολο το οποίο μπορεί να επαληθεύεται συνεχώς με βάση μια σειρά πολιτικών. Η ανάλυση what-if χρησιμοποιείται για τον προσδιορισμό προσωρινών αλλαγών στην πολιτική ή στις οντότητες με σκοπό να εξεταστούν τα αποτελέσματά τους πριν από την ολοκλήρωσή τους.

Rein Ontology

Η Rein οντολογία (Kagal, 2006) είναι ένα πλαίσιο που στηρίζεται στον Ιστό (web-based) για την αναπαράσταση και εξαγωγή συμπερασμάτων πάνω σε πολιτικές σε πεδία που χρησιμοποιούν διαφορετικές γλώσσες αναπαράστασης πολιτικών. Το σύνολο των πόρων (resources) του συστήματος, οι πολιτικές τους καθώς και οι σχέσεις μεταξύ τους σχηματίζουν δίκτυα (Rein Policy Networks). Η Rein επιτρέπει στις οντότητες των δικτύων αυτών να εντοπιστούν τοπικά ή απομακρυσμένα. Η Rein δεν προτείνει μια απλή γλώσσα για να περιγράψει πολιτικές. Επιτρέπει σε κάθε χρήστη να έχει πιθανώς τη δικιά του γλώσσα πολιτικής ή την επαναχρησιμοποίηση

μιας ήδη υπάρχουσας γλώσσας και αν είναι απαραίτητο, μια μεταπολιτική. Το πλαίσιο αυτό λοιπόν αποτελείται από δύο κυρίως μέρη, (i) ένα σύνολο οντολογιών που περιγράφουν τα δίκτυα πολιτικών της Rein καθώς και τις αιτήσεις για πρόσβαση σε κάποιο πόρο, και (ii) μια μηχανή εξαγωγής συμπερασμάτων που δέχεται τις αιτήσεις αυτές και αποφασίζει εάν είναι έγκυρες. Περιλαμβάνει την οντολογία Rein Policy network και την οντολογία Rein Request.

Η οντολογία Rein Policy network είναι κατασκευασμένη από τρείς βασικές ιδιότητες που χρησιμοποιούνται για να συνδέσουν τις οντότητες του δικτύου των πολιτικών (policy network entities) οι οποίες βρίσκονται τοπικά ή φιλοξενούνται μέσω HTTP. Η ιδιότητα policy χρησιμοποιείται για να αντιστοιχήσει τους πόρους με τις αντίστοιχες πολιτικές που έχουν οι μηχανισμοί εισόδων των πόρων αυτών. Η ιδιότητα policylanguage χρησιμοποιείται από μια πολιτική για να αναφερθεί στη γλώσσα που χρησιμοποιεί η πολιτική αυτή και η ιδιότητα meta-policy χρησιμοποιείται από μια γλώσσα και αναφέρεται στους κανόνες που μπορούν να χρησιμοποιηθούν για περαιτέρω εξαγωγή συμπερασμάτων. Μια γλώσσα πολιτικής αναπαριστάται σαν μια RDF-S ή OWL οντολογία. Μια πολιτική μπορεί να είναι ένα σύνολο από στιγμιότυπα RDF-S ή OWL ή ακόμα και ένα σύνολο κανόνων σε κάποια από τις γλώσσες αναπαράστασης πολιτικών που υποστηρίζονται από την Rein.

Τέλος, η κλάση Request είναι ένας τρόπος για να τίθενται ερωτήματα στο δίκτυο της Rein. Η κλάση αυτή έχει τέσσερις ιδιότητες – η requester ορίζει ποιά οντότητα πραγματοποιεί την αίτηση, resource είναι ο εκάστοτε πόρος, υπηρεσία ή πράξη που ζητείται, η access είναι ένας όρος (κλάση ή ιδιότητα) που ορίζεται στην γλώσσα αναπαράστασης της πολιτικής για τον μηχανισμό πρόσβασης, και answer είναι η απάντηση της μηχανής. Συνήθως η ιδιότητα resource είναι το URI (Unique Resource Identifier) του πόρου που ζητείται, ενώ η ιδιότητα requester είναι ένα σύνολο ιδιοτήτων ή πιστοποιητικών του αιτούντος, γιατί η ταυτότητά του μπορεί να μην έχει πάντα κάποιο νόημα σε ένα ανοιχτό περιβάλλον όπως ο Ιστός.

Τέλος, η μηχανή εξαγωγής συμπερασμάτων της Rein μπορεί εύκολα να τροποποιηθεί ώστε να χειρίζεται επιπλέον ιδιότητες για ένα αίτημα, συμπεριλαμβανομένων περιβαλλοντικών συνθηκών και ιδιοτήτων των πόρων.

P3P

Η P3P (Platform for Privacy Preferences) είναι μια γλώσσα περιγραφής πολιτικών που έχει υλοποιηθεί από την W3C. Επιτρέπει στις ιστοσελίδες να εκφράσουν τις διάφορες πρακτικές ιδιωτικότητάς τους σε ένα συγκεκριμένο τύπο (format) έτσι ώστε να μπορούν να ανακτηθούν αυτόματα και να ερμηνευτούν εύκολα από τους πράκτορες χρηστών (user agents). Οι πράκτορες θα επιτρέπουν στους χρήστες να ενημερώνονται για τις πρακτικές της συγκεκριμένης σελίδας (σε μορφή κατανοητή τόσο από τη μηχανή όσο και από τους ανθρώπους) και να αυτοματοποιούν τη λήψη αποφάσεων βασιζόμενοι στις πρακτικές αυτές, όπου χρειάζεται. Οι χρήστες δε χρειάζεται να διαβάζουν τις πολιτικές ιδιωτικότητας κάθε φορά που επισκέπτονται την σελίδα. Επιπλέον γνωρίζοντας ο χρήστης αυτές τις πληροφορίες (συνήθως μέσω έξυπνων διεπαφών), μπορεί να πάρει συνειδητές αποφάσεις για το αν θα υποβάλει ή όχι προσωπικές πληροφορίες σε μια συγκεκριμένη υπηρεσία.

Παρότι η P3P παρέχει ένα τεχνικό μηχανισμό για να εξασφαλίσει ότι οι χρήστες μπορούν να είναι ενημερωμένοι σχετικά με τις πολιτικές ιδιωτικότητας πριν ανακοινώσουν προσωπικές τους πληροφορίες, δεν παρέχει ένα μηχανισμό για να εξασφαλίσει ότι οι ιστοσελίδες συμπεριφέρονται σύμφωνα με τις πολιτικές τους. Παρόλα αυτά η P3P είναι συμπληρωματική σε κανονισμούς και αυτορυθμιζόμενα προγράμματα που παρέχουν μηχανισμούς επιβολής. Οι πολιτικές ιδιωτικότητας προορίζονται για να περιγράψουν τις πρακτικές μιας εταιρίας όσο αφορά τα δεδομένα, δηλαδή τι κάνουν με τις πληροφορίες που συλλέγουν από τα άτομα (συνήθως πελάτες αλλά μερικές φορές εργαζόμενους και άλλους).

Οι προδιαγραφές της P3P περιλαμβάνουν ένα τυποποιημένο λεξιλόγιο για την περιγραφή των πρακτικών αυτών και ένα σχήμα βάσης δεδομένων για να περιγράψουν το είδος των πληροφοριών που συλλέγονται. Μια πολιτική P3P είναι μια συλλογή στοιχείων λεξιλογίου και δεδομένων που περιγράφουν τις παραπάνω πρακτικές μιας συγκεκριμένης ιστοσελίδας. Μια P3P πολιτική αποτελείται ουσιαστικά από τις απαντήσεις σε μια σειρά πολλαπλών ερωτήσεων και επομένως δεν περιέχει πάντα τόσο λεπτομερείς πληροφορίες όσο μια πολιτική ιδιωτικότητας

που είναι αναγνώσιμη από τους ανθρώπους. Η τυποποιημένη μορφή μιας P3P πολιτικής της επιτρέπει την αυτόματη επεξεργασία.

Οι προδιαγραφές της P3P περιλαμβάνουν ακόμα ένα πρωτόκολλο για την αίτηση και μετάδοση πολιτικών. Το πρωτόκολλο αυτό είναι χτισμένο στο ίδιο πρωτόκολλο μεταφοράς υπερκειμένου (HTTP protocol) (Krishnamurthy, 2001), το οποίο χρησιμοποιούν οι περιηγητές για την επικοινωνία με τους εξυπηρετητές. Οι πράκτορες χρησιμοποιούν τυποποιημένα HTTP αιτήματα ενός αρχείου αναφοράς πολιτικών (policy reference file) από μια γνωστή τοποθεσία της ιστοσελίδας στην οποία ο χρήστης κάνει το αίτημα. Το αρχείο αναφοράς της πολιτικής προσδιορίζει την τοποθεσία του αρχείου της πολιτικής που εφαρμόζεται σε κάθε κομμάτι της ιστοσελίδας. Μπορεί να υπάρχει μια πολιτική για ολόκληρη την ιστοσελίδα, ή διάφορες πολιτικές που καλύπτουν ένα διαφορετικό κομμάτι της σελίδας. Ο πράκτορας τότε μπορεί να βρει την κατάλληλη πολιτική, να την αναλύσει και στη συνέχεια να δράσει ανάλογα με τις προτιμήσεις του χρήστη.

Η P3P επίσης επιτρέπει στις ιστοσελίδες να τοποθετούν τα αρχεία αναφοράς των πολιτικών σε άλλες τοποθεσίες πέρα των γνωστών. Σε αυτές τις περιπτώσεις η ιστοσελίδα πρέπει να υποδεικνύει την τοποθεσία αυτή χρησιμοποιώντας μια ειδική HTTP επικεφαλίδα. Οι ειδικές επικεφαλίδες επιπλέον χρησιμοποιούνται ώστε να μεταφέρουν μια προαιρετική συνοπτική πολιτική. Οι πολιτικές αυτές αποτελούν περιλήψεις ολόκληρων των P3P πολιτικών και περιγράφουν μόνο τις πρακτικές όσο αφορά τα δεδομένα, χωρίς να έχουν τις πλήρεις δυνατότητες έκφρασης των P3P πολιτικών.

2.5.3 Σύγκριση και παρατηρήσεις

Παρακάτω, βλέπουμε ένα συγκριτικό πίνακα με βάση κάποια τεχνικά χαρακτηριστικά μεταξύ των οντολογιών που παρουσιάστηκαν οι οποίες αποτελούν τις βασικότερες οντολογίες που σχετίζονται με τις πολιτικές ιδιωτικότητας και της προτεινόμενης οντολογίας.

	KAoS	**Rei**	**Rein**	**Προτεινόμενη**
Γλώσσα Προσδιορισμού	OWL	RDF-S	RDF-S ή OWL	OWL

Σπονδυλωτή Σκοπός	ΟΧΙ Προσδιορισμός Πολιτικών	ΝΑΙ Προσδιορισμός Πολιτικών	ΝΑΙ Προσδιορισμός Πολιτικών	ΟΧΙ Μοντελοποίηση πληροφοριών ελέγχου πρόσβασης και προσδιορισμός πολιτικών
Ενσωματωμένοι Κανόνες	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΝΑΙ

Πίνακας 1: Σύγκριση Οντολογιών Ιδιωτικότητας

Παρατηρούμε λοιπόν τα εξής :

Όλες οι παραπάνω οντολογίες αποτελούνται από επιμέρους οντολογίες (εκτός από την KAoS και την προτεινόμενη), κάθε μία από τις οποίες εξυπηρετεί και διαφορετικό σκοπό.

Από τις οντολογίες που παρουσιάστηκαν οι Rei και P3P αποτελούν από μόνες τους γλώσσες προσδιορισμού πολιτικών. Ειδικότερα η P3P αποτελεί το τρέχον πρότυπο για την προστασία της ιδιωτικότητας στον Ιστό. Η προτεινόμενη οντολογία δεν εστιάζει αποκλειστικά στον προσδιορισμό πολιτικής (όπως η Rei και η P3P), αντίθετα χρησιμοποιείται ως μια βασική έννοια για την προστασία της ιδιωτικότητας σε οποιοδήποτε πληροφοριακό σύστημα. Η προτεινόμενη οντολογία, η οποία είναι ενιαία, μπορεί να υποστηρίξει τις ιδιωτικές δραστηριότητες του χρήστη καθώς συμπεριλαμβάνονται μηχανισμοί ασφαλείας όπως ο έλεγχος πρόσβασης. Ακόμα, ένα από τα χαρακτηριστικά της οντολογίας που παρουσιάζεται είναι η προσέγγιση όλων των ενεργειών με όρους δεδομένων και επεξεργασίας αυτών. Με αυτό τον τρόπο γίνεται καλύτερα αντιληπτή η έννοια της προστασίας της ιδιωτικότητας, αφού ουσιαστικά προστατεύονται τα δεδομένα και ως συνέπεια όλες οι δραστηριότητες.

Σκοπός της προτεινόμενης οντολογίας είναι να δοθεί μια γενική περιγραφή της έννοιας της ιδιωτικότητας σε ένα πληροφοριακό σύστημα, δημιουργώντας από την αρχή μια νέα οντολογία. Στην πορεία της διατριβής θα γίνει προσπάθεια να δοθούν με κάθε λεπτομέρεια τα μέρη που συμμετέχουν σε ένα τέτοιο περιβάλλον, όπως είναι οι διάφορες οντότητες καθώς και τις σχέσεις μεταξύ τους. Επιπλέον

γίνεται περιγραφή όλων εκείνων των ενεργειών μέσα στο πλαίσιο όπως αυτό δόθηκε σε προηγούμενες ενότητες και αφορούν κυρίως την συλλογή και επεξεργασία των δεδομένων. Για το λόγο αυτό θα επαναχρησιμοποιηθούν κάποιες από τις έννοιες που είδαμε στις υπάρχουσες οντολογίες που περιγράφηκαν παραπάνω. Μερικές από αυτές είναι: η οντότητα, οι υπηρεσίες που παρέχονται, οι χρήστες, τα δεδομένα κλπ. Παράλληλα με την λεπτομερή περιγραφή όλων των παραπάνω, στην παρούσα οντολογία, αναπτύσσεται η έννοια της πολιτικής. Παρόλα αυτά δεν αποτελεί γλώσσα καθορισμού πολιτικών όπως κάποιες από τις οντολογίες που είδαμε παραπάνω. Περιγράφεται τι ρόλο παίζει η πολιτική σε ένα πληροφοριακό σύστημα, τι ιδιότητες έχει καθώς επίσης και τους μηχανισμούς που απαιτεί μια πολιτική για να υλοποιηθεί.

Σε αντίθεση λοιπόν με τις οντολογίες που υπάρχουν και παρουσιάστηκαν παραπάνω, η παρούσα οντολογία δε θα αποτελείται από επιμέρους οντολογίες και θα δίνει μια λεπτομερή περιγραφή του πλαισίου μέσα στο οποίο θα χρησιμοποιηθεί. Η συγκεκριμένη διατριβή δεν ασχολείται με το πώς κάθε πόρος σε ένα πληροφοριακό σύστημα μπορεί να πραγματοποιήσει μηχανισμούς που σχετίζονται με την ιδιωτικότητα. Αντίθετα, στόχος είναι η μοντελοποίηση των πολιτικών ιδιωτικότητας η οποία θα έχει σαν κέντρο αναφοράς τους ρόλους και τους σκοπούς του κάθε χρήστη, θα είναι ανεξάρτητη από τους πόρους που θα συμμετέχουν και θα μπορεί να υλοποιηθεί για οποιαδήποτε σφαίρα δραστηριοτήτων σε οποιοδήποτε περιβάλλον ελέγχου πρόσβασης.

Κεφάλαιο 3

Συγκριτική μελέτη και εξαγωγή απαιτήσεων μοντέλων ελέγχου πρόσβασης

Αυτή η ενότητα παρέχει μια επισκόπηση των μοντέλων ελέγχου πρόσβασης τα οποία μελετήθηκαν διεξοδικά στα πλαίσια της παρούσας διατριβής. Παρουσιάζονται τα χαρακτηριστικά του κάθε μοντέλου που αφορούν σε πτυχές προσανατολισμένες στην προστασία της ιδιωτικότητα, καθώς και τα σημαντικότερα μη επουσιώδη χαρακτηριστικά που συναντώνται στα υπο μελέτη μοντέλα ελέγχου πρόσβασης της βιβλιογραφίας. Κάθε ένα από τα μοντέλα που περιγράφονται παρακάτω βασίζεται στο μοντέλο RBAC και παρέχει καλά καθορισμένους μηχανισμούς ελέγχου πρόσβασης και διαφύλαξης της ιδιωτικότητας. Ωστόσο, όλες αυτές οι προσεγγίσεις στην προοπτική τους να καλύψουν συγκεκριμένα επιστημονικά κενά παρουσιάζουν κάποια ισχυρά σημεία, καθώς και ορισμένους περιορισμούς. Σε αυτό το πλαίσιο, διεξάχθηκε και παρέχεται μια συγκριτική μελέτη μεταξύ των μοντέλων όσον αφορά τα χαρακτηριστικά τους και τη σημασία της συμβολής τους στον τομέα του ελέγχου πρόσβασης με επίγνωση προστασίας της ιδιωτικότητας, ως σημείο αναφοράς για περαιτέρω διερεύνηση και έρευνα, έτσι ώστε να καθοριστούν καλύτερα και λεπτομερέστερα οι απαιτήσεις που πρέπει να πληρεί ένα μοντέλο ελέγχου πρόσβασης με επίγνωση πλαισίου και ιδιωτικότητας. Έχοντας ως βάση τη μελέτη αυτή καθορίστηκαν οι αρχές και η σχεδίαση του προτεινόμενου μοντέλου.

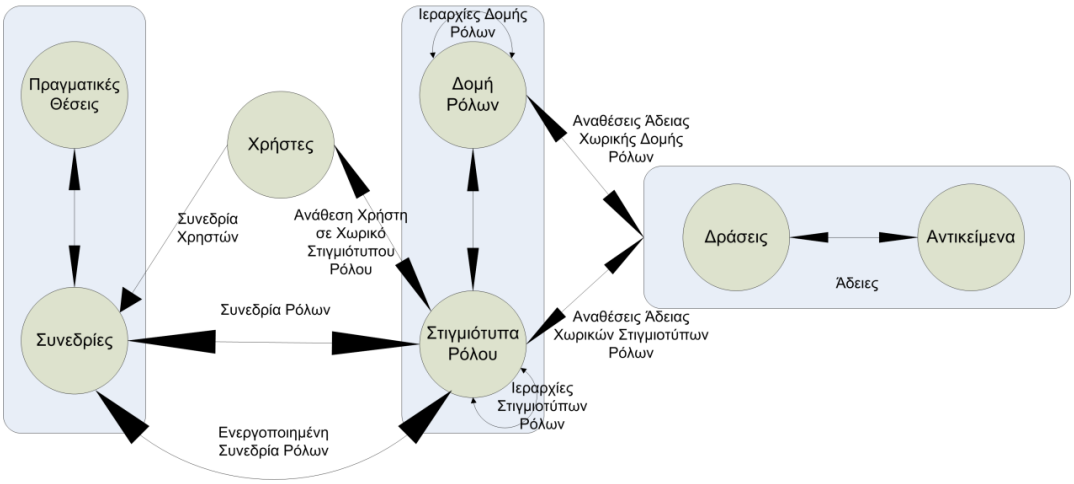
3.1 Μοντέλα ελέγχου πρόσβασης με επίγνωση πλαισίου

Έλεγχος Πρόσβασης Βάσει Ρόλων με Επίγνωση Χωρικών Δεδομένων (Spatially Aware RBAC - GEO-RBAC)

Το μοντέλο GEO-RBAC (Bertino et al., 2005) (Εικόνα 9) επεκτείνει το RBAC μοντέλο με πλήρεις προδιαγραφές των χωρικών περιορισμών. Χρησιμοποιείται ένα γεωμετρικό μοντέλο για την αναπαράσταση των αντικειμένων, των θέσεων των χρηστών και της ανάθεσης των ρόλων. Οι γεωμετρίες στο μοντέλο σχετίζονται με τους διαφορετικούς τύπους των τοπολογικών σχέσεων οι οποίες μπορεί να είναι δυαδικές και να αλληλοαναιρούνται. Οι έννοιες των χωρικών αντικειμένων, ρόλων

και δικαιωμάτων επεκτείνονται από χαρακτηριστικά κληρονομικότητας εκφρασμένα από σχέσεις μερικής διάταξης (partial order).

Όσον αφορά την τοποθεσία, ενσωματώνονται οι προδιαγραφές τόσο για πραγματικές αλλά και για λογικές θέσεις. Οι λογικές θέσεις μοντελοποιούνται ως σταθερές και υπολογίζονται από τις πραγματικές θέσεις μέσα από συγκεκριμένες συναρτήσεις χαρτογράφησης. Όσον αφορά στην ιδιωτικότητα, εισάγεται η έννοια μίας χονδρικής μορφής τοποθεσίας έτσι ώστε η πραγματική τοποθεσία του χρήστη να μην είναι εμφανής.



Εικόνα 9: Το μοντέλο GEO-RBAC

Γενικευμένος Έλεγχος Πρόσβασης Βάσει Ρόλων με Επίγνωση Χρονικών Δεδομένων (Generalized Temporal Role Based Access Control - GTRBAC)

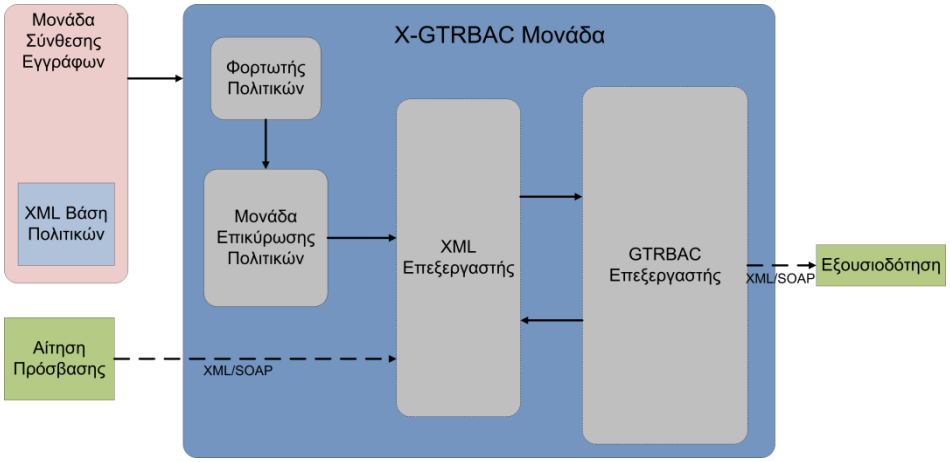
Το μοντέλο GTRBAC (Joshi et al., 2005) περιλαμβάνει σημαντικά χαρακτηριστικά που σχετίζονται με πτυχές προστασίας της ιδιωτικότητας. Το μοντέλο αποτελεί επέκταση του RBAC και υποστηρίζει χρονικές εξουσιοδοτήσεις με αποτελεσματικό και ολοκληρωμένο τρόπο. Περιλαμβάνει επίσης τις έννοιες DSoD και SSoD καθώς και περιορισμούς που σχετίζονται με το χωρικό πλαίσιο. Το κύριο χαρακτηριστικό του μοντέλου είναι η διάκριση μεταξύ των εννοιών ανάθεσης και ενεργοποίησης του ρόλου προσδιορίζοντας την κατάσταση ενός ρόλου. Οι Χρονικοί περιορισμοί χωρίζονται σε έξι κατηγορίες, προκειμένου το μοντέλο να λάβει υπόψη όλες τις σχετικές πιθανές καταστάσεις και τις απαιτήσεις των επιχειρήσεων για ένα δυναμικό μοντέλο ελέγχου πρόσβασης επίγνωσης πλαισίου.

Ειδικότερα, το μοντέλο μπορεί να εκφράσει περιοδικότητα, καθώς και διάρκεια, περιορισμούς σχετικά με την ανάθεση και την ενεργοποίηση του ρόλου και αναθέσεις ρόλου-εξουσιοδότησης. Σε ένα χρονικό διάστημα, η ενεργοποίηση ενός ρόλου μπορεί να περιοριστεί εκτενέστερα, ως αποτέλεσμα των πολυάριθμων περιορισμών ενεργοποίησης, συμπεριλαμβανομένων και των περιορισμών πληθικότητας και περιορισμούς μέγιστης διάρκειας ενεργοποίησης. Υποστηρίζει, επίσης, γεγονότα πραγματικού χρόνου εκτέλεσης , εκφράσεις ενεργοποίησης και ιεραρχίες ρόλων. Επιπλέον, το μοντέλο παρέχει μηχανισμούς επίλυσης συγκρούσεων που αφορούν όλες τις πιθανές ανιχνεύσιμες μορφές συγκρούσεων.

Προδιαγραφή Πολιτικών και Αρχιτεκτονική για Έλεγχο Πρόσβασης σε Επιχειρήσεις Βάσει της Γλώσσας Σήμανσης XML (An XML-Based Policy Specification Framework and Architecture for Enterprise-Wide Access Control - X-GTRBAC)

Το X-GTRBAC σύστημα (Bhatti et al., 2005) (Εικόνα 10) βασίζεται στο GTRBAC μοντέλο και ενσωματώνει όλα τα χαρακτηριστικά του εμπλουτισμένα από μία γλώσσα αναπαράστασης πολιτικών βασισμένη στην XML (World Wide Web Consortium, 2006). Αποτελεί ένα ολοκληρωμένο πλαίσιο υλοποιημένο στη γλώσσα προγραμματισμού Java . Το σύστημα υποστηρίζει όλες τις απαιτήσεις ενός δυναμικού μοντέλου ελέγχου πρόσβασης επίγνωσης πλαισίου ενός σύγχρονου επιχειρηματικού περιβάλλοντος και ο κινητήριος μοχλός για την ανάπτυξη του οφείλεται στην ετερογένεια των συνεργαζόμενων οντοτήτων που ανήκουν σε ένα κατανεμημένο επιχειρησιακό περιβάλλον.

Από την άποψη αυτή, η χρήση της XML παρέχει την απαραίτητη ευελιξία και τα χαρακτηριστικά της διαλειτουργικότητας όσον αφορά την επιβολή μηχανισμού ελέγχου πρόσβασης σε τέτοιου είδους περιβάλλοντα λόγω της ευκολίας της σύνταξης της και της σημασιολογικής επέκτασης της. Ως εκ τούτου, παρέχει όλες τις πτυχές υλοποίησης σχετικά με τους χρονικούς περιορισμούς του GTRBAC μοντέλου εμπλουτισμένες από ένα πλαίσιο προσδιορισμού περιορισμών και πιστοποίησης βασισμένο σε ιδιοχαρακτηριστικά. Ο όρος πιστοποίηση βασισμένη σε ιδιοχαρακτηριστικά αναφέρεται στην ομαδοποίηση των χρηστών με βάση τα διαπιστευτήριά τους και την εφαρμογή ενός κοινού συνόλου ζεύγους τιμών ιδιοχαρακτηριστικών για κάθε ομάδα. Οι πληροφορίες που σχετίζονται με τα διαπιστευτήρια αφορούν στην ανάθεση ρόλου για κάθε ομάδα χρηστών.



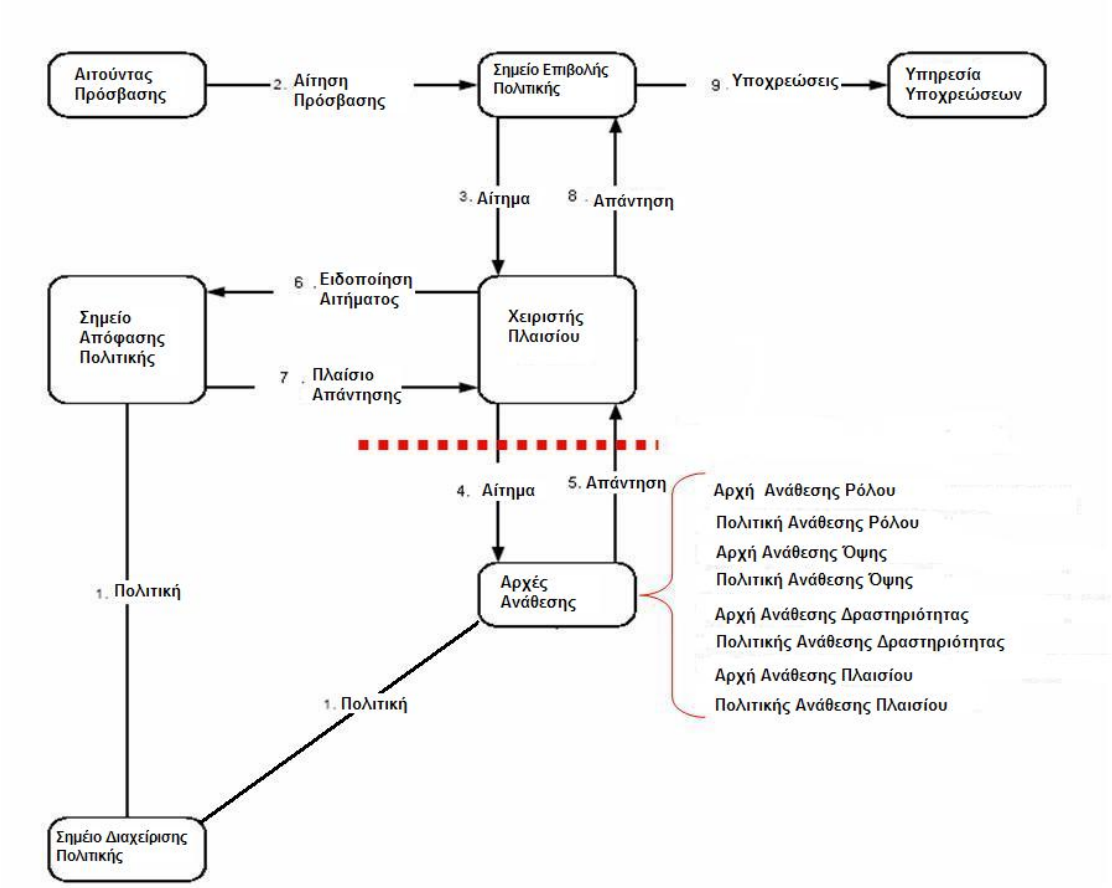
Εικόνα 10: Το σύστημα X-GTRBAC

Εκτεταμένο Προφίλ Ελέγχου Πρόσβασης Βάσει Ρόλων για τη Γλώσσα Σήμανσης XACML (Extended RBAC Profile of XACML)

Αυτό το προφίλ επέκτασης (Haidar et al., 2006) (Εικόνα 11) έχει ως βάση το RBAC και μπορεί να ενσωματωθεί εύκολα σε άλλα μοντέλα ελέγχου πρόσβασης εξαιτίας του γεγονότος ότι ενσωματώνει όλη την εκφραστική δύναμη της γλώσσας XACML μαζί με πρόσθετα χαρακτηριστικά που σχετίζονται με πτυχές επίγνωσης πλαισίου. Σε αντίθεση με την κοινή προσέγγιση συσχετισμού του πλαισίου με τους ρόλους που υιοθετεί η πλειοψηφία των προτεινόμενων μοντέλων ελέγχου πρόσβασης, το μοντέλο αυτό σχετίζει όλες τις πληροφορίες πλαισίου με τους κανόνες ασφαλείας.

Όσον αφορά την προδιαγραφή των πληροφοριών πλαισίου, το μοντέλο υιοθετεί την προσέγγιση του μοντέλου OrBAC, που παρουσιάζεται σε ενότητα που ακολουθεί, και είναι σε θέση να εκφράσει όλα τα είδη πληροφοριών πλαισίου (χρονικά, χωρικά και ιστορικά). Συνεπώς, το προφίλ επεκτείνει το πλαίσιο XACML με την έννοια της Αρχής Ανάθεσης (Enablement Authority) η οποία αναφέρεται στην πολιτική ανάθεσης όσον αφορά το ρόλο, την όψη, τη δραστηριότητα και τις πολιτικές εκχώρησης πλαισίου. Κάθε αρχή ανάθεσης αξιολογεί το ερώτημα για να καθορίσει την τιμή της οντότητας που έχει την ευθύνη (ρόλος, δραστηριότητα, όψη και τιμή πλαισίου) και η οποία ταιριάζει με τις οντότητες (υποκείμενο, δράση και αντικείμενο). Η απάντηση της αξιολόγησης μπορεί να είναι «Επιτρέπεται», «Απορρίπτεται», «Μη Εφαρμόσιμο» ή «Απροσδιόριστο» για κάθε αίτημα. Η απάντηση «Επιτρέπεται» σημαίνει ότι η αντίστοιχη τιμή εκχωρείται. Μετά την παραλαβή των τιμών ανάθεσης (αυτές για τις οποίες η XACML απάντηση είναι

«Επιτρέπεται»), οι αρχές ανάθεσης θα επαναλάβουν την αξιολόγηση για κάθε τιμή που βρέθηκε, για να βεβαιωθούν ότι δεν υπάρχουν επιπλέον κατώτερες τιμές ανάθεσης. Τέλος, το πλαίσιο παρέχει τα μέσα για μεταβίβαση δικαιωμάτων σχετικά με τους ρόλους, τις όψεις, τις δραστηριότητες και το πλαίσιο μέσω προδιαγεγραμμένων ιεραρχιών μεταξύ αυτών των εννοιών. Οι περιορισμοί υποχρεώσεων υποστηρίζονται επίσης με τον ίδιο μηχανισμό της XACML.



Εικόνα 11: Προφίλ επέκτασης RBAC για XACML

Μοντέλο ενσωμάτωσης των GSTRBAC χωρικών περιορισμών στο X-GTRBAC (Integrating GSTRBAC Spatial Constraints in X-GTRBAC - GSTRBAC+X-GTRBAC)

Το πλαίσιο GSTRBAC + X-GTRBAC (Haseeb et al, 2009), (Samuel, Ghafoor and Bertino, 2008) επεκτείνει το X-GTRBAC μοντέλο υιοθετώντας όλα τα συγκεκριμένα χαρακτηριστικά που αφορούν τους περιορισμούς πλαισίου, ενσωματώνοντας την λεπτομερή προδιαγραφή των χωρικών περιορισμών του GSTRBAC μοντέλου το οποίο αποτελεί μια κρίσιμη πτυχή σχετικά με την αποτελεσματική ασφάλεια των πληροφοριών.

Πιο αναλυτικά, το σύστημα εισάγει τις έννοιες της ανάθεσης ρόλου, της χωρικής ενεργοποίησης του ρόλου, της χωρικής ανάθεσης ρόλου σε χρήστη και της χωρικής εκχώρησης δικαιωμάτων σε ρόλο, σε συνδυασμό με τους χρονικούς περιορισμούς που προδιαγράφει το GTRBAC μοντέλο. Το μοντέλο θα μπορούσε να επεκταθεί προκειμένου να υποστηριχθεί το χαρακτηριστικό χωρικής SoD καθώς και χωρικές ιεραρχίες ρόλου.

3.2 Μοντέλα ελέγχου πρόσβασης με επίγνωση ιδιωτικότητας και επίγνωση πλαισίου

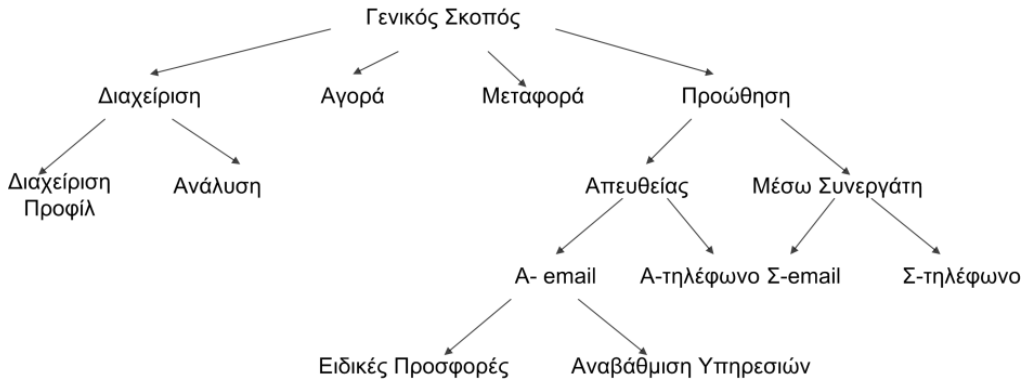
Έλεγχος Πρόσβασης Βάσει Σκοπού (Purpose Based Access Control - Pu-BAC)

Όπως έχει ήδη αναφερθεί ο σκοπός αποτελεί μία από τις βασικές έννοιες στις οποίες στηρίζονται οι αποφάσεις πρόσβασης με επίγνωση ιδιωτικότητας. Στο Pu-BAC μοντέλο (Byun, Bertino and Li, 2005) οι σκοποί οργανώνονται σε μια ιεραρχική δομή που βασίζεται σε σχέσεις is-a που δηλώνουν τις έννοιες της εξειδίκευσης/γενίκευσης οι οποίες χρησιμοποιούνται ευρέως στα επιχειρησιακά περιβάλλοντα. Οι πολιτικές ιδιωτικότητας επιτρέπουν την πρόσβαση σε συγκεκριμένα αντικείμενα δεδομένου μόνον αν ο σκοπός επιτρέπει την πρόσβαση σε αυτά τα δεδομένα. Από αυτή την άποψη, οι σκοποί συνδέονται με τα δεδομένα και αναφέρονται ως σκοποί πρόθεσης (intended purposes) δηλώνοντας, για ποιους σκοπούς τα δεδομένα είναι προσβάσιμα. Ο όρος σκοπός πρόσβασης εισάγεται επίσης και ελέγχεται έναντι του σκοπού πρόθεσης όσον αφορά τα δεδομένα που ζητούνται. Οι σκοποί σε αυτό το μοντέλο υποστηρίζουν τόσο θετικές όσο και αρνητικές πολιτικές ιδιωτικότητας για την παροχή μεγαλύτερης ευελιξίας. Σε περίπτωση αντικρουόμενων σκοπών, οι σκοποί πρόθεσης με αρνητική έκβαση υπερισχύουν των θετικών. Η εξουσιοδότηση για κάθε χρήστη παρέχεται για ένα σύνολο σκοπών πρόσβασης και η σχετική άδεια επιτρέπει στους χρήστες να έχουν πρόσβαση σε δεδομένα σχετικά με ένα συγκεκριμένο σκοπό. Οι άδειες χορηγούνται μέσω των ρόλων των χρηστών. Η έννοια του ρόλου σε αυτό το μοντέλο είναι βασισμένη σε ιδιοχαρακτηριστικά σχετικά με τους ρόλους και είναι οργανωμένη σε μια ιεραρχική δομή που επιτρέπει την κληρονομικότητα των ιδιοχαρακτηριστικών.

Στο πλαίσιο αυτό, εισάγεται η έννοια του υπό όρους ρόλου η οποία βασίζεται στο ρόλο και στα χαρακτηριστικά του συστήματος, προκειμένου να περιοριστεί η

πρόσβαση σε οντότητες. Τα ιδιοχαρακτηριστικά ρόλου μπορεί να θεωρηθούν ως προσωρινά αποθηκευμένες πληροφορίες χρήστη που είναι σχετικές με τους συγκεκριμένους ρόλους, και οι τιμές ιδιοχαρακτηριστικών ρόλου ενός χρήστη ενημερώνονται, εάν οι πληροφορίες των χρηστών αλλάξουν. Τα ιδιοχαρακτηριστικά του συστήματος αφορούν τους όρους που σχετίζονται με τις καταστάσεις του συστήματος, όπου οι εξουσιοδοτήσεις θα πρέπει να τεθούν σε ισχύ (ή όχι). Οι προϋποθέσεις αυτές αναφέρονται σε χρονικές καθώς και χωρικές πληροφορίες πλαισίου. Για την επιβολή του ελέγχου πρόσβασης κάθε δεδομένο λαμβάνει μία ετικέτα σκοπού πρόθεσης. Τα δεδομένα είναι επίσης ιεραρχικά οργανωμένα με σχέσεις “instance-of”, “sub element-of” και “reference-of”. Για να παρέχει μεγαλύτερη αποτελεσματικότητα το μοντέλο εκμεταλλεύεται τις ιεραρχίες όπως φαίνεται στην Εικόνα 12 και εισάγει την έννοια του έμμεσου σκοπού πρόθεσης διασφαλίζοντας ότι όλα τα στιγμιότυπα ενός αντικειμένου δεδομένων (και όλων των επιμέρους στοιχείων του) θα διέπονται από τον σκοπό πρόθεσης.

Για επίλυση των συγκρούσεων μεταξύ των σκοπών πρόθεσης το μοντέλου ορίζει τις έννοιες των ισχυρών και αδύναμων σκοπών πρόθεσης. Οι ισχυροί σκοποί πρόθεσης δεν είναι δυνατόν να παρακαμφθούν από σκοπούς πρόθεσης που σχετίζονται με στιγμιότυπα ενός τύπου (ή επιμέρους στοιχεία του αντικειμένου), ενώ ένας αδύναμος σκοπός πρόθεσης μπορεί να ανατραπεί. Κατά συνέπεια το Pu-BAC μοντέλο προτείνει μια μέθοδο για τον προσδιορισμό των σκοπών πρόσβασης, με αποτελεσματικό τρόπο, αλλά δεν ασχολείται με σημαντικά χαρακτηριστικά όπως οι υποχρεώσεις και ο ορισμός πολύπλοκων περιορισμών.



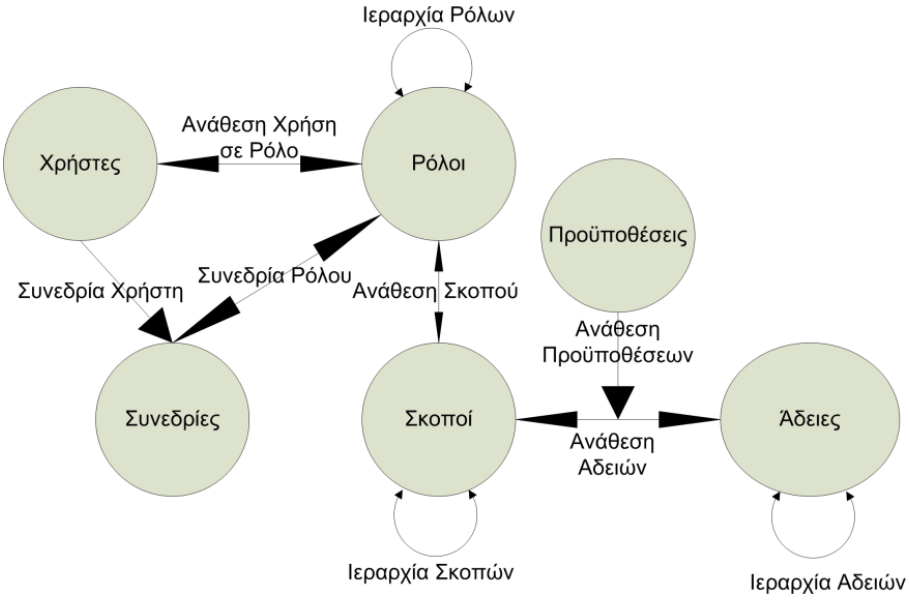
Εικόνα 12: Ιεραρχία Σκοπών στο μοντέλο Pu-BAC

Έλεγχος Πρόσβασης Βάσει Ρόλων με Επίγνωση του Σκοπού (Purpose-Aware Role-Based Access Control - PuRBAC)

Το εκτεταμένο μοντέλο RBAC αναφέρεται ως PuRBAC (Masoumzadeh and Joshi, 2008) (Εικόνα 13) και ορίζει την έννοια του σκοπού της ως ενδιάμεσο φορέα μεταξύ του ρόλου και της άδειας για την εκτέλεση αποφάσεων ελέγχου πρόσβασης με επίγνωση ιδιωτικότητας. Αυτό το μοντέλο περιλαμβάνει επίσης τα χαρακτηριστικά περιορισμών και υποχρεώσεων για την εκχώρηση της εξουσιοδότησης. Με τον όρο ανάθεση αναφέρεται στις σχέσεις των οντοτήτων. Σε αυτό το πλαίσιο, ένα σκοπός εκχωρείται σε κατάλληλους ρόλους και ως συνέπεια ένα υποκείμενο θα πρέπει ειδικά να δηλώσει το σκοπό της πρόσβασης σε δεδομένα στην αίτησή του για πρόσβαση ενός μέρος των δεδομένων. Επιπλέον, το μοντέλο καθορίζει τους όρους για τη διαδικασία επικύρωσης ανάθεσης. Η ανάθεση ισχύει σε μια κατάσταση αν και μόνο αν οι όροι της είναι ικανοποιημένοι. Οι όροι είναι δυαδικά (Boolean) κατηγορήματα και σε περίπτωση που υπάρχουν πολλαπλές εφαρμόσιμες υπό όρους αναθέσεις όλα αυτά θα πρέπει να συγκεντρώνονται για να εκτελεστεί η ανάθεση.

Οι ιεραρχίες αποτελούν επίσης μια σημαντική συμβολή του PuRBAC μοντέλου. Οι ιεραρχίες ρόλων, σκοπών, και δικαιωμάτων (μέσω της ιεραρχίας δεδομένων) ορίζονται ως ιεραρχίες μερικής διάταξης. Οι προϋποθέσεις συμπληρώνονται με την προδιαγραφή των εννοιών όπως χρονικό πλαίσιο, προ και μετά υποχρεώσεις καθώς και με περιορισμούς που σχετίζονται με τη συναίνεση του χρήστη, τη διατήρηση των δεδομένων, τη χρήση των δεδομένων και την καταγραφή των δράσεων. Καθώς οι όροι περιλαμβάνουν υποχρεώσεις πέραν των περιορισμών, το ενοποιημένο σύνολο των προϋποθέσεων αυτών μπορεί να οδηγήσει σε αντιφάσεις ή συγκρούσεις μεταξύ των υποχρεώσεων για την ολοκλήρωση της πρόσβασης.

Επιπλέον, η επιβολή των επιμέρους υποχρεώσεων μπορεί να έχει αντιφάσεις ή συγκρούσεις με τις τρέχουσες υποχρεώσεις στο σύστημα. Στην περίπτωση δύο ασυνεπών υποχρεώσεων, η ασυνέπεια μπορεί να επιλυθεί με την παράκαμψη αυτής που μπορεί να εντάξει την άλλη. Αλλά στην περίπτωση της σύγκρουσης, όπου καμία από τις υποχρεώσεις δε μπορεί να εντάξει την άλλη, το σύστημα χρειάζεται μια μετά-πολιτική σύμφωνα με την οποία μπορεί να καθορίσει ποια υποχρέωση θα πρέπει να παρακαμφθεί, ή, ενδεχομένως, η πρόσβαση να μη γίνεται δεκτή εφόσον καμία επίλυση δεν είναι δυνατή.



Εικόνα 13: Το μοντέλο PuRBAC

Έλεγχος Πρόσβασης Βάσει Οργανισμού (Organization Based Access Control - OrBAC)

Το Organization Based Access Control (OrBAC) πλαίσιο (Cuppens and Cuppens-Boulahia, 2008) παρέχει τα μέσα για τον προσδιορισμό των δυναμικών, ευέλικτων πολιτικών ελέγχου πρόσβασης με επίγνωση ιδιωτικότητας. Το OrBAC μοντέλο επικεντρώνεται γύρω από την έννοια του Οργανισμού, δηλαδή, του φορέα που είναι υπεύθυνος για τη διαχείριση μιας πολιτικής ασφάλειας. Οι OrBAC πολιτικές μοντελοποιούνται σε επίπεδο οργανισμού, ακολουθώντας ένα τρόπο ανεξάρτητο της υλοποίησης. Αντί η μοντελοποίηση της πολιτικής να γίνει βάσει συγκεκριμένων και εξαρτημένων από την υλοποίηση εννοιών του υποκειμένου, της δράσης και του αντικειμένου, το μοντέλο προτείνει ένα σκεπτικό με βάση το ρόλο που τα υποκείμενα, οι δράσεις και τα αντικείμενα παίζουν σε έναν οργανισμό. Ο ρόλος του υποκειμένου καλείται απλά ως ρόλος όπως και στο μοντέλο RBAC, ο ρόλος μιας δράσης ονομάζεται μια δραστηριότητα ενώ ο ρόλος ενός αντικειμένου ονομάζεται όψη (Εικόνα 14).

Οι OrBAC πολιτικές καθορίζουν τα δικαιώματα, τις απαγορεύσεις, τις υποχρεώσεις και τις κατ 'εξαίρεση άδειες που ισχύουν σε έναν οργανισμό για τον έλεγχο των δραστηριοτήτων που εκτελούνται από τους ρόλους των όψεων. Οι κανόνες που ορίζονται είναι δυναμικοί και ενσωματώνουν την έννοια του πλαισίου,

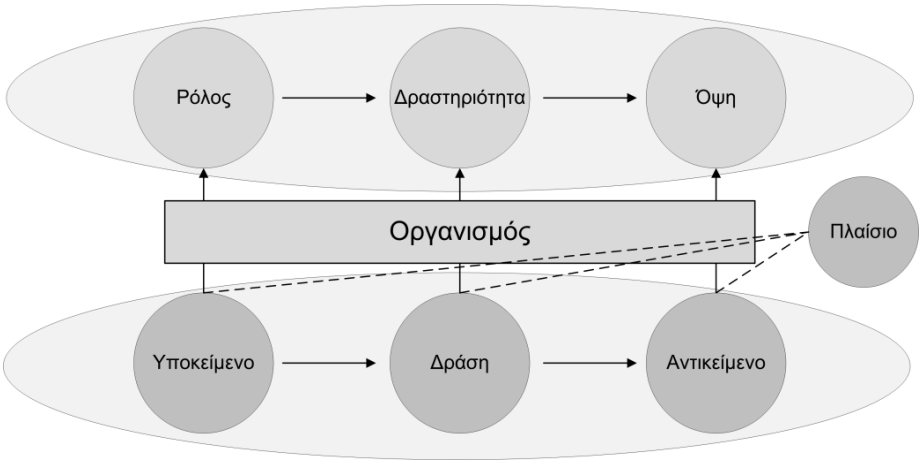
εννοώντας όλες τις πρόσθετες προϋποθέσεις που πρέπει να ικανοποιούνται για την ενεργοποίηση του κανόνα. Οι ρόλοι, οι όψεις, οι δραστηριότητες, το πλαίσιο και οι οργανισμοί είναι δομημένα σε ιεραρχίες και οι κανόνες κληρονομούνται μέσω αυτών των ιεραρχιών, παρέχοντας ένα ευέλικτο τρόπο προδιαγραφής για τις πολιτικές. Δεδομένου ότι ενδέχεται να προκύψουν συγκρούσεις μεταξύ θετικών και αρνητικών εξουσιοδοτήσεων, το OrBAC παρέχει στρατηγικές διαχείρισης συγκρούσεων για την ανίχνευση και την επίλυση αυτών των δυνητικών συγκρούσεων (Cuppens et al., 2007).

Επιπλέον, διατάξεις SoD μεταξύ ρόλων μέσα στον ίδιο ή σε διαφορετικούς οργανισμούς μπορούν να εκφραστούν. Το πλαίσιο αποτελεί μία πολύ σημαντική και καλά μελετημένη έννοια στο μοντέλο OrBAC. Οι προϋποθέσεις περιλαμβάνουν διάφορους τύπους πλαισίου, όπως χρονικές, χωρικές, προαπαιτούμενες, που δηλώνονται από το χρήστη, συναίνεσης και προσωρινές προϋποθέσεις. Μπορούν να συνδυαστούν με σκοπό το σχηματισμό σύνθετων προϋποθέσεων με συνδετικές, διαζευκτικές και αρνητικές σχέσεις. Το μοντέλο επίσης, καθορίζει την έννοια των ολικών περιορισμών, δηλαδή, των συνθηκών που σχετίζονται με την πολιτική ασφάλειας. Εάν ένας ολικός περιορισμός δεν ικανοποιείται, τότε αυτό σημαίνει ότι αυτή η πολιτική ασφάλειας δεν είναι συνεπής.

Ιστορικά στοιχεία που σχετίζονται με τις πολιτικές ελέγχου πρόσβασης μπορούν επίσης να εκφραστούν μέσω του προσωρινού πλαισίου, καθώς και χαρακτηριστικά προ και μετά υποχρεώσεων. Οι διατάξεις που στοχεύουν ειδικά στην προστασία της ιδιωτικότητας είναι ως επί το πλείστον υλοποιημένες χρησιμοποιώντας την έννοια του πλαισίου (Ajam et al., 2010). Η έννοια του σκοπού μοντελοποιείται ως μία έννοια πλαισίου δηλωμένη από το χρήστη, η οποία δηλώνεται από τον αιτούντα πριν από κάθε διάθεση δεδομένου, ενώ υπάρχουν προκαθορισμένες αντιστοιχίσεις μεταξύ των σκοπών και των ρόλων που μπορούν να τους δηλώσουν. Οι προδιαγραφές του πλαισίου συναίνεσης επιτρέπουν την ειδοποίηση του υποκειμένου των δεδομένων όταν τα προσωπικά στοιχεία του είναι προσβάσιμα.

Συνεπώς, με την αρχή του περιορισμού της συλλογής, το OrBAC επιτρέπει προσεχτική πρόσβαση στα δεδομένα, ανάλογα με το σκοπό και με το υποκείμενο, με άλλα λόγια, το OrBAC εκμεταλλεύεται την έννοια των διαφορετικών επιπέδων της

ακρίβειας των δεδομένων κατά την πραγματοποίηση του ελέγχου της πρόσβασης, ενώ το χαρακτηριστικό της ακρίβειας εισάγεται μέσω της ιεράρχησης των όψεων. Τέλος, το προσωρινό πλαίσιο επιτρέπει την πραγματοποίηση του ελέγχου της χρήσης των δεδομένων που συλλέγονται κατά τη διάρκεια της ζωής τους.



Εικόνα 14: Το μοντέλο OrBAC

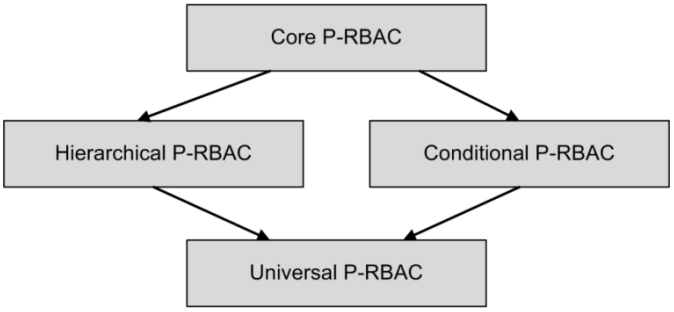
Έλεγχος Πρόσβασης Βάσει Ρόλων με Επίγνωση της Ιδιωτικότητας (Privacy-Aware Role Based Access Control - P-RBAC)

Το P-RBAC μοντέλο (Ni et al., 2010) ασχολείται με τα πλέον σημαντικά χαρακτηριστικά που σχετίζονται με την τον έλεγχο πρόσβασης με επίγνωση ιδιωτικότητας, όπως οι σκοποί, οι υποχρεώσεις και οι προϋποθέσεις που διατυπώνονται με ολοκληρωμένο τρόπο. Αυτά τα χαρακτηριστικά καθορίζονται μέσα από το συνδυασμό τεσσάρων προηγμένων μοντέλων που έχουν διαφορετικές ικανότητες μοντελοποίησης, το κύριο P-RBAC, το ιεραρχικό P-RBAC, το υπό όρους P-RBAC και το Οικουμενικό P-RBAC (Εικόνα 15). Το P-RBAC ενσωματώνει, δεδομένα, δράση, σκοπό, προϋπόθεση, και υποχρέωση ως εξουσιοδότηση για δεδομένα με βάση την ιδιωτικότητα.

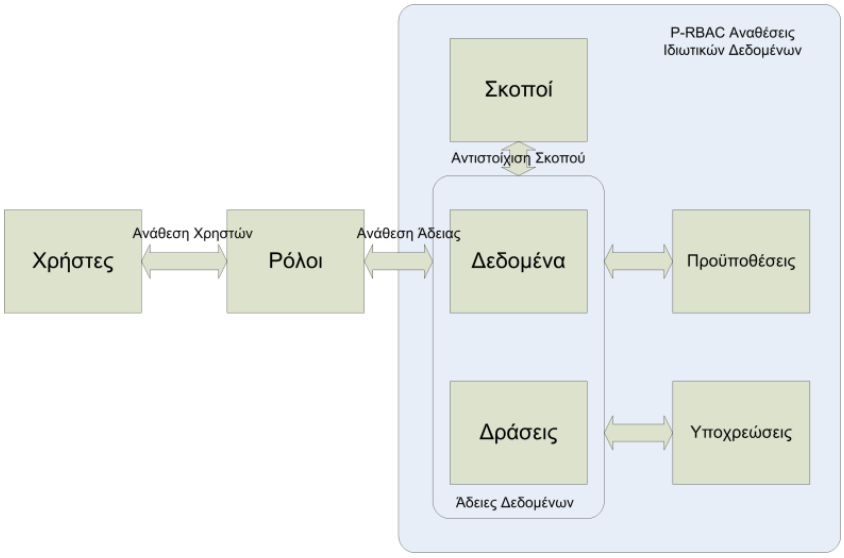
Το κύριο P-RBAC βασίζεται στο RBAC μοντέλο και χρησιμοποιείται για να εκφράσει τις πολιτικές ιδιωτικότητας. Το Ιεραρχικό P-RBAC εισάγει τις έννοιες της ιεραρχίας Ρόλου, Αντικείμενου και Σκοπού υποστηρίζοντας σχέσεις μερικής διάταξης μεταξύ των αντικειμένων και των σκοπών. Η ιεραρχία των ρόλων βασίζεται στις σχετικές προδιαγραφές του RBAC μοντέλου. Το υπό όρους P-RBAC εισάγει τις έννοιες των συνόλων αδειών ανάθεσης και σύνθετη λογική έκφραση προκειμένου να

εκφράσει πολύπλοκες συνθήκες και να προσδιορίσει σχέσεις διάζευξης και σύζευξης μεταξύ διαφορετικών αναθέσεων αδείας. Το Οικουμενικό P-RBAC παρέχει εκτός από τα προαναφερθέντα, χαρακτηριστικά, τα αρνητικά δικαιώματα, τον έλεγχο της ροής της εκτέλεσης υποχρέωσης και τις αρχές συνδυασμού άδειας για την αντιμετώπιση πιθανών ασυνεπειών. Επιπλέον, η οικογένεια του P-RBAC μοντέλου χρησιμοποιεί μία απλή πρακτική γλώσσα που αναφέρεται ως LC_0, προκειμένου να εκφράσει τις προϋποθέσεις, χρησιμοποιώντας μεταβλητές πλαισίου. Επίσης, καθορίζει την έννοια του χρονικού περιορισμού που αντιπροσωπεύει μία ακολουθία από χρονικά διαστήματα.

Συνεπώς, το μοντέλο υποστηρίζει τις έννοιες του SoD, προ και μετά υποχρεώσεων συμπεριλαμβανομένων των χαρακτηριστικών όπως η χρήση των δεδομένων και η διάθεσή τους καθώς και συναίνεση του χρήστη. Τέλος, το μοντέλο ενσωματώνει μηχανισμό επίλυσης σύγκρουσης μεταξύ δύο αντικρουόμενων αναθέσεων άδειας. Η λογική του ελέγχου πρόσβασης του μοντέλου φαίνεται στην Εικόνα 16.



Εικόνα 15: Οικογένεια μοντέλου P-RBAC



Εικόνα 16: Εξουσιοδότηση στο P-RBAC

3.3 Σημασιολογικά μοντέλα ελέγχου πρόσβασης με επίγνωση πλαισίου

Σημασιολογικό Χρονικό Μοντέλο Ελέγχου Πρόσβασης (Temporal Semantic-Based Access Control Model - TSBAC)

Το TSBAC μοντέλο (Ravari et al., 2008) ενσωματώνει τα ίδια χαρακτηριστικά με το μοντέλο GTHBAC μέσω της αξιοποίησης των πλεονεκτημάτων του Σημασιολογικού Ιστού που αντιπροσωπεύουν όλες τις βασικές οντότητες σε Οντολογίες OWL. Το μοντέλο εισάγει το ακόλουθο σύνολο οντολογιών: Οντολογία - Υποκειμένων, Οντολογία - Αντικειμένων και Οντολογία - Ενεργειών. Η αναπαράσταση των βασικών τομέων ελέγχου πρόσβασης χρησιμοποιώντας οντολογίες στοχεύει στην εξέταση σημασιολογικών σχέσεων σε διάφορα επίπεδα της οντολογίας έτσι ώστε να τεκμηριώσει τη λήψη αποφάσεων σχετικά με μια αίτηση πρόσβασης. Το μοντέλο επιχειρεί να μειώσει τις σημασιολογικές σχέσεις σε περιληπτικές σχέσεις και να τις χρησιμοποιήσει κατά τη διαδικασία ελέγχου πρόσβασης. Με βάση αυτό ο προσδιορισμός και ο χειρισμός πολύπλοκων πολιτικών και εκφράσεων είναι εφικτός με εύκολο τρόπο.

Υποστηρίζοντας το RBAC χρησιμοποιώντας τις τεχνολογίες XACML + OWL (Supporting RBAC with XACML+OWL)

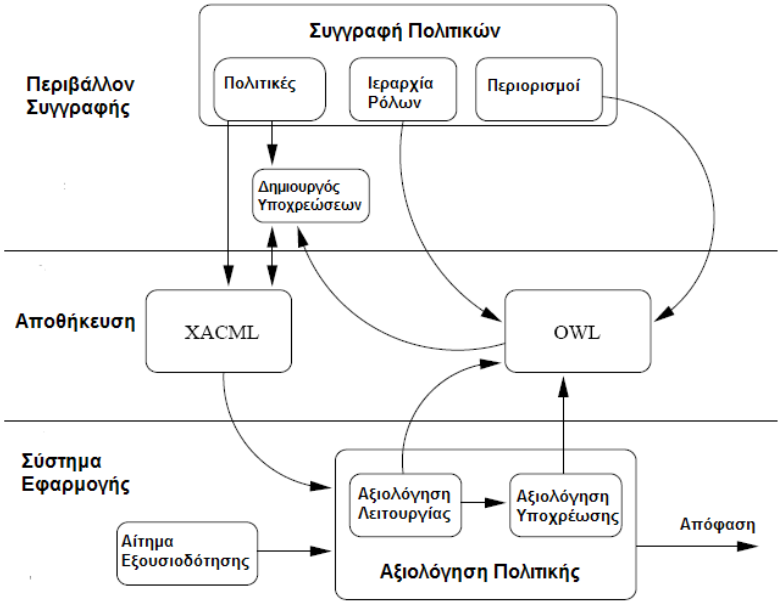
Το πλαίσιο RBAC with XACML+OWL αποτελεί ένα μοντέλο (Ferrini and Bertino, 2009) που ενσωματώνει Οντολογίες OWL και XACML πολιτικές προκειμένου να υποστηρίξει το RBAC μοντέλο. Η XACML είναι μια ευρέως

χρησιμοποιούμενη γλώσσα για τις διαδικασίες ελέγχου πρόσβασης, έκφρασης και προδιαγραφής πολιτικών.

Επιπλέον, λόγω του γεγονότος ότι είναι μία εύκολα επεκτάσιμη και ευέλικτη γλώσσα πολιτικών, μπορεί να υιοθετηθεί από πολλά μοντέλα ελέγχου πρόσβασης. Σε αυτό το μοντέλο η επέκταση XACML παρέχει τη δυνατότητα έκφρασης πολλών σημαντικών χαρακτηριστικών του RBAC, όπως τα SSoD/DSoD, οι ιεραρχίες ρόλων, οι ιεραρχίες όσον αφορά την διάδοση των εξουσιοδοτήσεων, μαζί με ιεραρχίες κληρονομικότητας ρόλου. Η ευελιξία του πλαισίου βασίζεται στο γεγονός ότι η αναπαράσταση των περιορισμών καθώς και των σχετικών ιεραρχιών του RBAC είναι αποσυνδεδεμένη από τις προδιαγραφές και την εκτέλεση των XACML πολιτικών. Η συνεργασία μεταξύ των XACML πολιτικών και της οντολογίας OWL επιτυγχάνεται μέσω ειδικών σημασιολογικών συναρτήσεων που προβλέπει το μοντέλο.

Πιο αναλυτικά, οι σχετικές ιδιότητες OWL που αντιπροσωπεύουν ιεραρχίες ρόλου, μαζί με τις κατάλληλες σημασιολογικές συναρτήσεις είναι ενσωματωμένες στο εσωτερικό των κανόνων των XACML πολιτικών, ώστε οι σχετικές πληροφορίες να ανακτηθούν και να συνδυαστούν για την αξιολόγηση του κανόνα. Μετά τη διαδικασία αξιολόγησης, οι αναγκαίες αλληλεπιδράσεις με την οντολογία λαμβάνουν χώρα προκειμένου να εκπληρωθούν οι υποχρεώσεις και άλλοι περιορισμοί που καθορίζονται στην πολιτική.

Το μοντέλο δεν παρέχει ειδική αναπαράσταση των πληροφοριών πλαισίου που σχετίζονται με το χρόνο, την τοποθεσία ή την ιστορία των προσβάσεων, αλλά όλα τα σχετικά χαρακτηριστικά του μηχανισμού XACML θα μπορούσαν πιθανώς να αναπτυχθούν (Εικόνα 17).



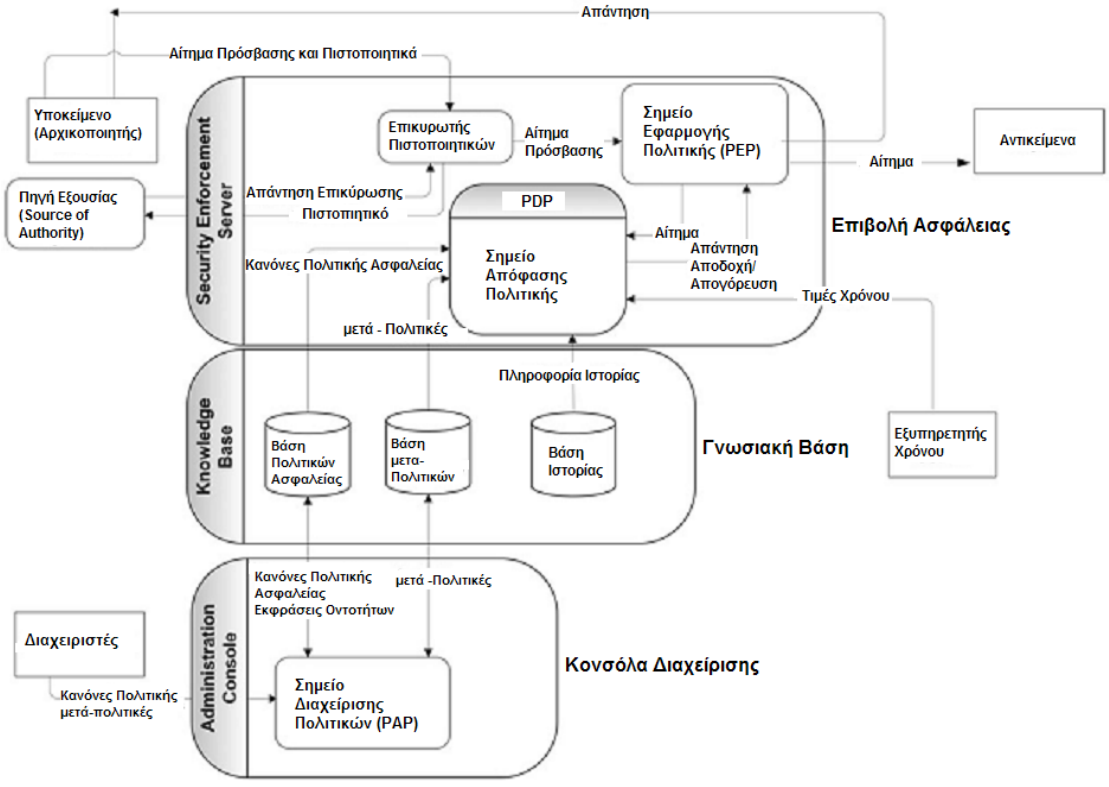
Εικόνα 17: Το πλαίσιο RBAC with XACML+OWL

Γενικευμένο Χρονικό Μοντέλο Ελέγχου Πρόσβασης με Επίγνωση Ιστορικών Δεδομένων (Generalized Temporal History Based Access Control Model - GTHBAC)

Το GTHBAC (Ravari et al., 2010) αποτελεί μοντέλο ελέγχου πρόσβασης που δεν είναι ρολο-κεντρικό μοντέλο, παρά το γεγονός ότι οι ρόλοι μπορούν να εκφραστούν ως ιδιοχαρακτηριστικά στο εσωτερικό των κανόνων αδειοδότησης. Ως εκ τούτου, το μοντέλο χρησιμοποιεί τη γενική διατύπωση του υποκειμένου, της δράσης και του αντικείμενου ως κεντρικούς φορείς των κανόνων της πολιτικής ελέγχου πρόσβασης. Ωστόσο, παρέχει έναν ολοκληρωμένο μηχανισμό έκφρασης και επιβολής των περιορισμών του ιστορικού πλαισίου. Σε γενικές γραμμές, η απόφαση εξουσιοδότησης λαμβάνεται μετά την αξιολόγηση των σχετικών κανόνων αδειοδότησης μαζί με τους χρονικούς περιορισμούς που σχετίζονται με την ιστορία των προσβάσεων. Οι χρονικοί περιορισμοί αναφέρονται και στις δύο έννοιες του πραγματικού και λογικού χρόνου που σχετίζονται ο ένας με τον άλλον μέσα από λογικούς τελεστές. Οι χρονικοί κανόνες παροχής εξουσιοδότησης αναπαρίστανται από τριάδες οι οποίες περιλαμβάνουν το έγκυρο χρονικό διάστημα εξουσιοδότησης μαζί με το αναφερόμενο σύνολο υποκειμένου, δράσης, αντικείμενου και τη διαδικασία ορισμού του χρονικού περιορισμού.

Η διαδικασία αξιολόγησης μπορεί να επιτευχθεί με τον έλεγχο των σχετικών διαπιστευτηρίων που διατίθενται από το υποκείμενο με τη μορφή X.509 Πιστοποιητικών Ιδιοτήτων (X.509 Attribute Certificates) (International Telecommunication Union, 2005) μαζί με τις σχετικές πληροφορίες που αποθηκεύονται σε μια βάση ιστορίας. Επιπλέον, το μοντέλο παρέχει μηχανισμούς για την επίλυση διάφορων ειδών συγκρούσεων μέσω των ακόλουθων τεσσάρων διαφορετικών στρατηγικών: ο αρνητικός κανόνα εξουσιοδότησης έχει προτεραιότητα (negative authorization rule takes precedence-NTP), ο θετικός κανόνας εξουσιοδότησης κανόνας έχει προτεραιότητα (positive authorization rule takes precedence - PTP), ο πιο συγκεκριμένος κανόνας έχει προτεραιότητα, και ο νεότερος κανόνας υπερισχύει του παλαιότερου κανόνα.

Τέλος, το μοντέλο θεωρείται ως ένα πολύ εφαρμόσιμο μοντέλο εξαιτίας του γεγονότος ότι ενσωματώνει τους χρονικούς περιορισμούς στην ιστορία των προσβάσεων σε ένα γενικό μοντέλο ελέγχου πρόσβασης που μπορεί εύκολα να αντικατασταθεί από άλλα μοντέλα ελέγχου πρόσβασης (Εικόνα 18).



Εικόνα 18: Το σύστημα GTHBAC

3.4 Σύνοψη χαρακτηριστικών μοντέλων ελέγχου πρόσβασης επίγνωσης πλαισίου και ιδιωτικότητας

Ο πίνακας που ακολουθεί συνοψίζει τα συγκεκριμένα χαρακτηριστικά που σχετίζονται με την επίγνωση πλαισίου σε συνδυασμό με το πλαίσιο ιδιωτικότητας των υπό μελέτη μοντέλων.

Όλες οι παραπάνω προσεγγίσεις ασχολούνται με την πλειοψηφία των εννοιών που περιγράφονται στις προηγούμενες ενότητες, με ένα διαφορετικό τρόπο, αξιοποιώντας διάφορες τεχνολογίες και μέσα, παρέχοντας σημαντική συμβολή στον τομέα της προστασίας της ιδιωτικότητας και του ελέγχου της πρόσβασης σε επιχειρησιακά περιβάλλοντα.

Μοντέλα με επίγνωση Ιδιωτικό-τητας	Επίγνωση Πλαισίου			Υποχρεώσεις	Διαχωρισμός Καθηκόντων		Ιεραρχίες				Επίλυση Συγκρούσεων	Βασισμένα σε Οντολογίες	Βασισμένα σε Πιστοποιητικά
	Χρονικά	Χωρικά	Ιστορικά		Στατικός	Δυναμικός	Ρόλος	Σκοπός	Δεδομένα	Πλαίσιο			
Μοντέλα ελέγχου πρόσβασης με επίγνωση Πλαισίου (με χαρακτηριστικά πλαισίου ιδιωτικότητας)													
GEO-RBAC	×	✓	×	×	✓	×	✓	×	✓	×	×	×	×
GTRBAC	✓	×	×	×	✓	✓	×	×	×	×	✓	×	×
X-GTRBAC	✓	×	×	×	✓	✓	×	×	×	✓	✓	×	×
RBAC for XACML	✓	✓	✓	✓	✓	✓	✓	×	✓	×	×	×	×
GSTRBAC+ X-GTRBAC	✓	✓	×	×	✓	✓	×	×	×	✓	✓	×	×
Σημασιολογικά μοντέλα ελέγχου πρόσβασης (με χαρακτηριστικά πλαισίου ιδιωτικότητας)													
ROWLBAC	✓	✓	✓	×	✓	✓	✓	×	×	✓	×	✓	×
TSBAC	✓	×	✓	×	✓	×	✓	×	✓	✓	✓	✓	×
XACML+ OWL	✓	×	×	✓	✓	✓	✓	×	×	✓	✓	✓	×
GTHBAC	✓	×	✓	×	✓	×	×	×	×	✓	✓	✓	✓
Μοντέλα ελέγχου πρόσβασης με επίγνωση Ιδιωτικότητας (επίγνωση πλαισίου και/ή χρήση Οντολογιών)													
Pu-BAC	✓	✓	×	×	✓	×	✓	✓	✓	✓	✓	×	×
PuRBAC	✓	×	×	✓	×	×	✓	✓	✓	×	✓	×	×
OrBAC	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	×	×
P-RBAC	✓	×	×	✓	✓	✓	✓	✓	✓	✓	✓	×	×

Πίνακας 2: Συγκριτική μελέτη των μοντέλων ελέγχου πρόσβασης

3.4.1 Ενσωμάτωση του πλαισίου ιδιωτικότητας

Η έννοια του «σκοπού» εισάγεται σε τέσσερα από τα προαναφερθέντα μοντέλα. Το P-RBAC, το Pu-BAC, το PuRBAC και το OrBAC ορίζουν το σκοπό ως ένα βασικό στοιχείο των πολιτικών προστασίας της ιδιωτικότητας που υποδεικνύει το λόγο και τις συνθήκες υπό τις οποίες τα δεδομένα πρέπει να συλλέγονται και να χρησιμοποιούνται. Οι σκοποί σε αυτά τα μοντέλα είναι δομημένοι σε ιεραρχίες που υποστηρίζουν σχέσεις κληρονομικότητας.

Το χαρακτηριστικό των υποχρεώσεων αποτελεί επίσης μία πολύ σημαντική πτυχή προστασίας ιδιωτικότητας στον έλεγχο πρόσβασης. Ως εκ τούτου, αρκετά από τα μοντέλα ενσωματώνουν αυτό το χαρακτηριστικό. Το P-RBAC, PuRBAC και OrBAC, καθορίζουν το χαρακτηριστικό των προ και μετά υποχρεώσεων, συμπεριλαμβανομένων χαρακτηριστικών ιδιωτικότητας όπως η χρήση των δεδομένων και η διάθεσή τους, καθώς και η συγκατάθεση του χρήστη. Στο RBAC προφίλ για XACML, οι υποχρεώσεις υποστηρίζονται από τον ίδιο μηχανισμό με το σύστημα XACML. Η ίδια προσέγγιση υιοθετείται από το XACML + OWL πλαίσιο με την κύρια διαφορά ότι κατά την εκπλήρωση υποχρεώσεων λαμβάνουν χώρα οι απαραίτητες αλληλεπιδράσεις με την οντολογία, προκειμένου η πληροφορία που περιέχεται σε αυτήν να ενημερώνεται.

Σχετικά με το χαρακτηριστικό SoD παρατηρείται ότι η πλειοψηφία των μοντέλων υποστηρίζουν το SSoD χαρακτηριστικό εκτός από την PuRBAC προσέγγιση. Από την άλλη πλευρά, η έννοια του DSoD δεν είναι τόσο ευρέως εισηγμένη στα μοντέλα. Πιο συγκεκριμένα, τα πλαίσια που υποστηρίζουν το DSoD χαρακτηριστικό είναι κυρίως η GTRBAC οικογένεια μοντέλων, το P-RBAC καθώς και οι προσεγγίσεις που εκμεταλλεύονται την εκφραστική δύναμη της XACML και της OWL. Όσον αφορά στις ιεραρχίες, αξίζει να σημειωθεί ότι τρία από τα μοντέλα, το P-RBAC, το Pu-BAC και το OrBAC, στηρίζουν κληρονομικότητα των χαρακτηριστικών σε όλες τις βασικές οντότητες προδιαγραφής του μοντέλου ελέγχου πρόσβασής. Θα πρέπει επίσης να σημειωθεί ότι τα μοντέλα PuRBAC και TSBAC καθορίζουν ιεραρχικές σχέσεις σχετικά με τους ρόλους, τους σκοπούς και τα δεδομένα στη μία περίπτωση και τους ρόλους, τα δεδομένα και το πλαίσιο στην άλλη.

Τα μοντέλα επίσης παρουσιάζουν αρκετούς μηχανισμούς και αλγορίθμους επίλυσης συγκρούσεων και σχετικά με αντικρουόμενες καταστάσεις στις αναθέσεις εξουσιοδότησης.

Η P-RBAC προσέγγιση παρέχει μία λεπτομερή προδιαγραφή των πιθανών αντιφατικών καταστάσεων σχετικά με τη σύγκρουση μεταξύ των συνθηκών καθώς και λόγω των ιεραρχιών. Όσον αφορά το Pu-BAC μοντέλο, ορίζονται μηχανισμοί εντοπισμού και επίλυσης συγκρούσεων προλαμβάνοντας συγκρούσεις μεταξύ απαγορευμένων και επιτρεπόμενων σκοπών. Από την άλλη πλευρά, το GTRBAC καθώς και το PuRBAC μοντέλο παρουσιάζουν τέτοιου είδους μηχανισμούς σχετικά με τη σύγκρουση που προκαλείται από την επιβολή διαφορετικών περιορισμών. Στην πρώτη περίπτωση, το μοντέλο ορίζει για το σκοπό αυτό κατώτερους και ανώτερους κανόνες προτεραιότητας. Όσον αφορά το PuRBAC, στην περίπτωση δύο ασυνεπών υποχρεώσεων, η ασυνέπεια μπορεί να επιλυθεί με την παράβλεψη ενός κανόνα ο οποίος μπορεί να υποτάξει τον άλλο. Τα μοντέλα GTHBAC και TSBAC καθορίσουν στρατηγικές για την επίλυση των συγκρούσεων στις περιπτώσεις που υπάρχει να ενσωμάτωση ενός ειδικού συνόλου οντότητας σε περισσότερα από ένα σύνολα οντοτήτων, καθώς και σε καταστάσεις που υπάρχουν αντικρουόμενες σχέσεις υπο-διαστημάτων μεταξύ των κανόνων αδειοδότησης. Όσον αφορά το XACML + OWL μοντέλο, ο εντοπισμός των συγκρούσεων που αφορούν τους περιορισμούς και τις υποχρεώσεις υποστηρίζεται μέσα από τον έλεγχο αντιφάσεων στην οντολογία. Σε μία τέτοια περίπτωση, η εξουσιοδότηση δεν επιτρέπεται και η οντολογία ενημερώνεται αυτόματα με τις σχετικές πληροφορίες.

3.4.2 Πλεονεκτήματα και Περιορισμοί

Τα υπό μελέτη μοντέλα προσπαθούν να επεκτείνουν το RBAC μοντέλο για την αντιμετώπιση της πλειοψηφίας των προαναφερθέντων ως χαρακτηριστικά «Πλαισίου ιδιωτικότητας». Παρ' όλα αυτά, μερικά από τα μοντέλα παρουσιάζουν ορισμένα πλεονεκτήματα καθώς και περιορισμούς έναντι των άλλων, από την άποψη της εφαρμογής, της χρηστικότητας και της πληρότητας. Πιο συγκεκριμένα, μερικές από αυτές τις προσεγγίσεις, όπως η GEO-RBAC, η GTRBAC, η X-GTRBAC, η GSTRBAC + X-GTRBAC και η Pu-BAC, προτείνουν, συνδυάζοντας την έννοια του ρόλου με χωρικούς ή/και χρονικούς περιορισμούς πλαισίου για την δημιουργία ρόλων-πλαισίου. Υποστηρίζουμε ότι το πλαίσιο δεν θα πρέπει να συνδέεται με το ρόλο, αλλά με τους κανόνες ασφαλείας, λόγω του γεγονότος ότι η έννοια του ρόλου-πλαισίου γενικά αντιστοιχεί σε τεχνητούς και μερικές φορές σε διφορούμενους ρόλους. Για παράδειγμα, αν ο διαχειριστής είναι ένας ρόλος και O1 είναι ένας οργανισμός, ένας "συνδυαστικός" ρόλος

όπως ο O1 γιατρός είναι αμφίσημος δεδομένου ότι μπορεί να ερμηνευθεί ως ρόλος-πλαισίου (που αντιστοιχεί με το διαχειριστή που βρίσκεται στον οργανισμό O1) ή "Οργανωτικό" ρόλο (που αντιστοιχεί με το διαχειριστή που δουλεύει για τον οργανισμό O1).

Όσον αφορά την επίγνωση πλαισίου αρκετά από τα μοντέλα ενσωματώνουν χαρακτηριστικά που αφορούν τα τρία σημαντικά χαρακτηριστικά πλαισίου (χρονικά, χωρικά και βασισμένα στην ιστορία). Ωστόσο, μόνο η χρονική πληροφορία πλαισίου διερευνάται από την πλειοψηφία των μοντέλων. Πιο αναλυτικά, όλα τα προαναφερθέντα μοντέλα, εκτός από το GEO-RBAC που έχει ως βάση το πλαίσιο χώρου, ασχολούνται με χρονικούς περιορισμούς. Από την άλλη πλευρά, η συνδυασμένη επίδραση της θέσης και του χρόνου κατά τη λήψη της πρόσβασης λαμβάνεται υπόψη μόνο στις προσεγγίσεις Pu-BAC, OrBAC, και GSTRBAC + X-GTRBAC. Αυτές οι πληροφορίες μπορούν επίσης εύκολα να εισαχθούν στα πιο γενικευμένα και βασισμένα σε πρότυπα μοντέλα, όπως το XACML για RBAC και ROWLBAC, γεγονός που οφείλεται στο ότι αυτά τα μοντέλα είναι εύκολα επεκτάσιμα. Από την άλλη πλευρά, το ιστορικό χαρακτηριστικό πλαισίου εισάγεται και ορίζεται στην μειονότητα των παραπάνω μοντέλων, όπως το OrBAC, το GTHBAC, το TSBAC, και, ενδεχομένως, το XACML για RBAC και ROWLBAC. Με βάση τα παραπάνω, πρέπει να σημειωθεί ότι σύμφωνα με το μοντέλο GSTRBAC, όλα τα δικαιώματα διατίθενται σε ένα ρόλο που μπορεί να εκτελεστεί όπου και όποτε αυτός ο ρόλος είναι ενεργοποιημένος. Ωστόσο, το μοντέλο αγνοεί τη χωρο-χρονική φύση εξουσιοδοτήσεων του RBAC. Για παράδειγμα, ο βασικός ρόλος του υπαλλήλου μπορεί να επικαλεστεί ένα πρόσωπο που εργάζεται σε έναν οργανισμό στην πρωινή συνεδρίαση καθώς και στην απογευματινή συνεδρίαση, παρόλο που στο μοντέλο, η συμμετοχή σε απευθείας σύνδεση επιτρέπεται μέσω του ρόλου του υπαλλήλου μόνο κατά την πρωινή συνεδρίαση.

Σε σχέση με την ικανότητα έκφρασης των πολύπλοκων περιορισμών, αξίζει να σημειωθεί ότι τα μοντέλα OrBAC, GSTRBAC + X-GTRBAC, RBAC προφίλ για XACML, ROWLBAC, XACML + OWL είναι σε θέση να εκφράσουν όλα τα είδη των συνθηκών κατά τρόπο αποτελεσματικό και ολοκληρωμένο. Επιπλέον, ένα υψηλό επίπεδο αφαιρετικότητας, σχετικά με τη σημασιολογική αναπαράσταση των οντοτήτων του μοντέλου αποτελεί σημαντικό πλεονέκτημα λόγω του ότι στο πλαίσιο αυτό το μοντέλο

μπορεί να εκφράσει και άλλα μοντέλα ελέγχου πρόσβασης και καθιστά ευκολότερη την ενημέρωση και διαχείριση των κανόνων πρόσβασης. Το RBAC προφίλ του XACML, το ROWLBAC, το XACML + OWL, το TSBAC και το GTHBAC είναι γενικού χαρακτήρα μοντέλα και προσαρμόσιμα ώστε να εκφράσουν, επιπρόσθετα του RBAC, τις ανάγκες του κάθε μοντέλου βασισμένα στην ιδέα των κλάσεων, όψεων, και δραστηριοτήτων.

Τέλος, λαμβάνοντας υπόψη τα μοντέλα ελέγχου πρόσβασης που βασίζονται στην έννοια του σκοπού, θα πρέπει να σημειωθεί ότι το P-RBAC αν και είναι αρκετά ισχυρό, υποστηρίζουμε ότι κινείται μακριά από το πνεύμα απλότητας διαχείρισης της πολιτικής του RBAC. Το P-RBAC συμπυκνώνει τα δεδομένα, τη δράση, το σκοπό, την κατάσταση, και την υποχρέωση ως άδεια για δεδομένα με επίγνωση ιδιωτικότητας. Ωστόσο, με τη χρήση των ρόλων, ως φορείς που μεσολαβούν μεταξύ των χρηστών και των δικαιωμάτων, το RBAC μετατοπίζεται από παράδειγμα απλής αναπαράστασης αλλά δύσκολης διαχείρισης που αποτελείται μόνο από κανόνες αδειοδότησης, σε μία πιο εύχρηστη και διαχειρίσιμη προσέγγιση χρήστη-ρόλου και ανάθεσης άδειας-ρόλου. Ωστόσο, η άδεια δεδομένων με προστασία ιδιωτικότητας στο P-RBAC δεν λαμβάνει υπόψη αυτό το χαρακτηριστικό, και με την παρουσία ιεραρχιών των δεδομένων και των σκοπών, η διαχείριση των πολιτικών γίνεται πολύπλοκη. Από την άλλη πλευρά, τα μοντέλα PuRBAC και Pu-BAC θεωρούν το σκοπό ως οντότητα ενδιάμεση μεταξύ του ρόλου και των οντοτήτων παραχώρησης δικαιωμάτων.

Με βάση όλα τα παραπάνω είναι φανερό ότι κανένα από τα παραπάνω μοντέλα δεν ενσωματώνει όλα τα χαρακτηριστικά ελέγχου πρόσβασης που σχετίζονται με την προστασία της ιδιωτικότητας και την επίγνωση πλαισίου. Στόχος λοιπόν της παρούσας διατριβής είναι η ενσωμάτωση όλων των παραπάνω χαρακτηριστικών και απαιτήσεων στο προτεινόμενο μοντέλο ελέγχου πρόσβασης.

Κεφάλαιο 4

Μοντέλο ελέγχου πρόσβασης

Η χρήση των σημασιολογικών τεχνολογιών παρέχει ένα υψηλό επίπεδο αφαίρεσης, το οποίο κάνει εύκολη την ενημέρωση και διαχείριση των κανόνων και καθιστά το προτεινόμενο μοντέλο απλούστερα επεκτάσιμο και γενικευμένο, γεγονός το οποίο στοχεύει στην διαχειρίσιμη ενσωμάτωση και υιοθέτησή του από άλλα μοντέλα.

Το σημασιολογικό μοντέλο που θα παρουσιαστεί και αποτελεί τη βάση της προτεινόμενης λύσης στοχεύει στην εκπλήρωση των κανονιστικών απαιτήσεων όσον αφορά στην προστασία της ιδιωτικότητας στον έλεγχο πρόσβασης δεδομένων. Το μοντέλο επιχειρεί να ενσωματώσει όλα τα βασικά χαρακτηριστικά για το σκοπό αυτό και να συμβάλει στην αντιμετώπιση των περιορισμών των προαναφερθέντων μοντέλων οι οποίοι παρουσιάστηκαν στην ενότητα 3.4.2. Θεμελιώδες χαρακτηριστικό αποτελεί το γεγονός ότι η διαδικασία ελέγχου πρόσβασης βασίζεται στην έννοια του «σκοπού» για τον οποίο τα δεδομένα συλλέγονται και χρησιμοποιούνται, όπως ορίζουν οι βασικές αρχές προστασίας της ιδιωτικότητας. Οι σκοποί είναι οργανωμένοι σε δομημένες ιεραρχίες που ορίζονται από σχέσεις κληρονομικότητας.

Επιπρόσθετα, υποστηρίζει την έννοια των προ- και μετά-υποχρεώσεων ως προϋποθέσεις ή συμπληρωματικές ενέργειες αντίστοιχα που θα πρέπει να εκτελούνται μαζί με την επιβολή ενός κανόνα.

Η προτεινόμενη προσέγγιση προβλέπει και αποτρέπει αντικρουόμενες καταστάσεις, μέσω του ορισμού των ειδικών ιδιοτήτων επισημείωσης (annotation properties) της οντολογίας, οι οποίες είναι συναφείς με κάθε κανόνα, που αφορούν ιεραρχικές σχέσεις, αμοιβαία αποκλειόμενους συνδυασμούς τύπων δεδομένων, κλπ.

Η επίγνωση πλαισίου ενσωματώνει πληροφορίες που αφορούν όλα τα σημαντικά χαρακτηριστικά τα οποία αναφέρονται στην ενότητα 2.4 και έχει επίσης τη δυνατότητα να εκφράσει σύνθετους περιορισμούς πλαισίου με αποδοτικό και ολοκληρωμένο τρόπο.

4.1 Βασικές αρχές της προτεινόμενης λύσης

Η παρούσα διατριβή προτείνει μια νέα προσέγγιση ελέγχου πρόσβασης για την προστασία της ιδιωτικότητας και είναι σε θέση να εξυπηρετήσει τις ανάγκες εφαρμογών σε πραγματικό και μη πραγματικό χρόνο. Παρέχει ένα γενικευμένο μοντέλο ελέγχου πρόσβασης με επίγνωση πλαισίου και ιδιωτικότητας βασισμένο σε ρόλους.

Η προσέγγιση βασίζεται σε πολιτικές που αξιολογούνται και εκτελούνται από το σύστημα, προκειμένου να ληφθεί η απόφαση πρόσβασης. Οι διαδικασίες εξουσιοδότησης επιτυγχάνονται με ανταλλαγή διαπιστευτηρίων μεταξύ των σχετικών φορέων όπως θα αναλυθεί στο κεφάλαιο 6. Τα βασικά στοιχεία που συνθέτουν το πλαίσιο των πολιτικών είναι τα σύνολα των τύπων προσωπικών δεδομένων, των σκοπών, των ρόλων, των δράσεων, των δραστών, των κανόνων, των συνθηκών και των υποχρεώσεων.

- Το σύνολο των τύπων προσωπικών δεδομένων (personal data types (*DT*)) αντιπροσωπεύει τους διάφορους τύπους δεδομένων που συλλέγονται στο πλαίσιο της εκάστοτε εφαρμογής. (πχ., για εφαρμογή παρακολούθησης δικτύων, έναν τύπο δεδομένου αποτελεί η IP διεύθυνση).

- Το σύνολο των σκοπών (purposes (*Pu*)) αναπαριστά κυρίως τις διαφορετικές πιθανές υπηρεσίες σε μία λεπτομερή και καλά δομημένη ταξινόμηση η οποία περιλαμβάνει πρωταρχικές ατομικές εργασίες καθώς και σύνθετες.

- Το σύνολο των ρόλων (roles (*R*)) αντιπροσωπεύει – παρόμοια με όλες τις προσεγγίσεις που βασίζονται σε ρόλους – τους λειτουργικούς ρόλους μέσα σε έναν οργανισμό, πχ. Διαχειριστής συστήματος.

- Το σύνολο των δραστών (actors (*Ac*)) αντιστοιχεί σε ανθρώπινες οντότητες, τους χρήστες του συστήματος στους οποίους ανατίθενται ένας ή και περισσότεροι ρόλοι.

- Το σύνολο των δράσεων (actions (*A*)) αναπαριστά τους τύπους πρόσβασης που ένας δράστης μέσω ενός ρόλου για ένα συγκεκριμένο σκοπό μπορεί να έχει σε ένα σύνολο προσωπικών δεδομένων

- Το σύνολο των κανόνων (rules (*Ru*)) αναπαριστά τους κανόνες ελέγχου πρόσβασης (δικαιώματα και απαγορεύσεις).

- Το σύνολο των συνθηκών (Conditions (*C*)) αντικατοπτρίζει τις πληροφορίες πλαισίου και θέτει τους περιορισμούς πραγματικού χρόνου στην εφαρμογή των κανόνων.

- Το σύνολο των υποχρεώσεων (Obligations (*O*)) αντικατοπτρίζει πράξεις οι οποίες πρέπει να εκπληρωθούν πριν ή και μετά την εφαρμογή των κανόνων (πχ. ειδοποίηση υποκειμένου για τη διάθεση των δεδομένων).

Τα τελευταία τρία σύνολα λοιπόν, εκπροσωπούν, αντίστοιχα, τους κανόνες ελέγχου πρόσβασης, δηλαδή τα δικαιώματα και τις απαγορεύσεις, και τους περιορισμούς που υφίσταται η εφαρμογή των κανόνων σε πραγματικό χρόνο.

Το σύνολο των προσωπικών δεδομένων χαρακτηρίζεται από τρεις σχέσεις που αντικατοπτρίζουν, αντίστοιχα, τα χαρακτηριστικά κληρονομικότητας, το επίπεδο λεπτομέρειας της ίδιας έννοιας και τη συμπερίληψη ενός τύπου δεδομένου σε έναν άλλο. Παρόμοιου τύπου σχέσεις (δέντρα λογικού *AND* και *OR*) ορίζονται για τους σκοπούς, τις δράσεις και τους ρόλους.

Οι κανόνες ελέγχου πρόσβασης, από τους οποίους προκύπτουν οι αποφάσεις εξουσιοδότησης, είναι πάντα συνδεδεμένοι με μια τετράδα {τύποι προσωπικών δεδομένων, σκοπός, δράση, ρόλος}. Οι κανόνες ελέγχου πρόσβασης μπορεί να είναι είτε θετικοί είτε αρνητικοί, με αποτέλεσμα θετική ή αρνητική εξουσιοδότηση, αντίστοιχα, αφού έχει ληφθεί υπόψη η υποκείμενη δράση.

4.2 Συσχετίσεις μεταξύ των συνόλων

Η χρησιμότητα των παραπάνω συνόλων αναδεικνύεται μέσω της προδιαγραφής των κατάλληλων σχέσεων γενίκευσης και ειδίκευσης για την παραγωγή πιο σύνθετων και ολοκληρωμένων εννοιών. Στοχεύοντας στο φορμαλισμό των ιδιοτήτων της κληρονομικότητας χαρακτηριστικών μεταξύ των στοιχείων των συνόλων και της «εννοιολογικής συμπερίληψης» ενός στοιχείου από ένα άλλο του ίδιου συνόλου, προδιαγράφηκαν και τα αντίστοιχα είδη συσχετίσεων. Οι συγκεκριμένες ιδιότητες αποσκοπούν στην αποφυγή της επανάληψης ορισμού κοινών χαρακτηρισμών και μεθόδων και εν τέλει στη μεγαλύτερη κλιμακοθετησιμότητα της προδιαγραφής κανόνων. Οι εν λόγω σχέσεις δημιουργούν επιμέρους σύνολα μερικής διάταξης (partially ordered sets), ενώ είναι μεταβατικές (transitive) και αντί-συμμετρικές (anti-symmetric).

Πιο συγκεκριμένα, οι ρόλοι ανατίθενται στους φορείς του συστήματος γεγονός το οποίο δημιουργεί το σύνολο αναθέσεων ρόλου (Role Assignments (*RA*)). Επιπλέον, οι σκοποί έχουν εκχωρηθεί σε ρόλους σαν δικαιώματα, δεδομένου ότι δεν είναι όλοι οι τύποι των ρόλων που επιτρέπεται να ενεργούν (δηλαδή, να εκτελούν μια λειτουργία) όσον αφορά στην εξυπηρέτηση όλων των πιθανών σκοπών. Αυτό δημιουργεί ένα σύνολο συσχετισμού σκοπού-προς-ρόλο (*PR*). Ο συσχετισμός των προσωπικών δεδομένων με το σύνολο *PR* δημιουργεί την έννοια των επιτρεπόμενων τύπων δεδομένων που αντανακλούν θετική εξουσιοδότηση για κάποια συγκεκριμένη ενέργεια σε δεδομένα.

Επιπλέον, το μοντέλο ορίζει αμοιβαίως αποκλειόμενα σύνολα για τύπους δεδομένων. Αυτά τα σύνολα είναι σχετικά με την ύπαρξη «απαγορευμένων» συνδυασμών δεδομένων.

Για την προδιαγραφή του ελέγχου πρόσβασης, η προσέγγιση που υιοθετήθηκε είναι η έκφραση όλων των τύπων των πληροφοριών που περιγράφονται με τη βοήθεια μιας οντολογίας, υλοποιημένη σε OWL. Αυτό αφορά όχι μόνο τα προσωπικά δεδομένα, τους σκοπούς, τις δράσεις και τους ρόλους, αλλά και τους κανόνες, τους περιορισμούς πλαισίου, των υποχρεώσεων και όλων των σχετικών πληροφοριών.

Κάθε περιορισμός σχετίζεται με έναν ή περισσότερους κανόνες, είτε επειδή είναι άμεσα συνδεδεμένοι, είτε ως μέρος της δομής και της κληρονομικότητας μεταξύ των περιορισμών. Οι καθορισμένες δομές των περιορισμών αφορούν χρονικούς, χωρικούς και βασισμένους σε συμβάντα περιορισμούς πλαισίου.

Ένα πρόσθετο χαρακτηριστικό που προσφέρει το σημασιολογικό μοντέλο είναι η υποστήριξη των προ και μετά υποχρεώσεων που θα πρέπει να εκτελούνται μαζί με την επιβολή ενός κανόνα. Κάθε υποχρέωση ακολουθεί ένα μοτίβο που χαρακτηρίζεται από ιδιότητες οι οποίες κατηγοριοποιούν την υποχρέωση σε προ-ενεργή ή μετά-ενεργή του κανόνα. Το μοτίβο της υποχρέωσης αφορά, για παράδειγμα, την ενημέρωση του υποκειμένου των δεδομένων ή ακόμη και την αίτηση για ρητή συναίνεση σε πραγματικό χρόνο, κ.α.

Όπως γενικευμένα περιγράφηκε παραπάνω, το σύνολο των τύπων προσωπικών δεδομένων (*DT*) χαρακτηρίζεται από τρεις σχέσεις οι οποίες αποτελούν μερικές διατάξεις των δεδομένων (partial orders). Πιο συγκεκριμένα:

- Δηλώνουμε ότι ένας τύπος δεδομένου dt_i *inherits from* dt_j (σημειώνοντας ως $dt_i \blacktriangleleft dt_j$) όταν τα χαρακτηριστικά του dt_j κληρονομούνται από τον dt_i, αναφερόμενοι σε όποιους κανόνες ρυθμίζουν τη συλλογή και την επεξεργασία των δεδομένων αυτού του τύπου.

- Δηλώνουμε ότι ένας τύπος δεδομένου dt_i *is less detailed than* dt_j (σημειώνοντας ως $dt_i < dt_j$) όταν ο τύπος δεδομένου dt_j περιγράφει την ίδια έννοια με τον dt_i, αλλά με μεγαλύτερη ακρίβεια.

- Δηλώνουμε ότι ένας τύπος δεδομένου dt_i *is contained to type* dt_j (σημειώνοντας ως $dt_i \angle dt_j$) όταν ο τύπος δεδομένου dt_i αποτελεί μέρος του dt_j.

Οι τελευταίες δύο σχέσεις υπονοούν την πρώτη ως εξής:

- $dt_i < dt_j \Rightarrow dt_i \blacktriangleleft dt_j$, για θετικές εξουσιοδοτήσεις

- $dt_i < dt_j \Rightarrow dt_j \blacktriangleleft dt_i$, για αρνητικές εξουσιοδοτήσεις

- $dt_i \angle dt_j \Rightarrow dt_i \blacktriangleleft dt_j$, για θετικές εξουσιοδοτήσεις

- $dt_i \angle dt_j \Rightarrow dt_j \blacktriangleleft di_j$, για αρνητικές εξουσιοδοτήσεις

Στην πραγματικότητα, οι δύο πρώτες σχέσεις δημιουργούν ιεραρχίες δέντρων λογικού *OR* των τύπων προσωπικών δεδομένων, ενώ η τρίτη σχέση αποτελεί ιεραρχία *AND* δέντρου. Οι σχέσεις αυτές είναι μεταβατικές (transitive) και αντι-συμμετρικές (anti-symmetric). Το σύνολο των σκοπών (*Pu*) χαρακτηρίζεται από δύο σχέσεις, επίσης μεταβατικές και αντι-συμμετρικές, δημιουργώντας ιεραρχίες δέντρων *AND* και *OR*, αντίστοιχα. Η κληρονομικότητα των χαρακτηριστικών ενός σκοπού pu_i από ένα σκοπό pu_j σημειώνεται ως $pu_i \blacktriangleleft pu_j$, ενώ η *AND*-αποσύνθεση ενός σκοπού pu_j (π.χ., σε υποσκοπούς που πρέπει να εκπληρωθούν) σημειώνεται ως $pu_i < pu_j$, εννοώντας ότι ο σκοπός pu_j περιλαμβάνει τον pu_i.

Παρομοίως, δύο σχέσεις καθορίζονται και για το σύνολο των ρόλων (*R*):

- Δηλώνουμε ότι ένα ρόλος r_i *inherits from* r_j (σημειώνοντας ως $r_i \blacktriangleleft r_j$) όταν τα χαρακτηριστικά του r_j κληρονομούνται από τον r_i, αναφερόμενοι σε οποιαδήποτε ιδιότητα ρόλου και εξουσιοδότηση.

– Δηλώνουμε ότι ένα ρόλος r_i *is part of* r_j (σημειώνοντας ως $r_i \angle r_j$) όταν ο ρόλος r_i αποτελεί μέρος του r_j.

Η πρώτη σχέση δηλώνει ιεραρχία *OR* δέντρου ενώ η τελευταία δηλώνει ιεραρχία *AND* δέντρου και αντικατοπτρίζει την ιδιότητα συνεργασίας ενός ρόλου με έναν άλλο, εννοώντας την ανάγκη αλληλεπίδρασης μεταξύ των ρόλων-συνεργατών έτσι ώστε να εκτελεστεί μία εργασία. Και οι δύο σχέσεις είναι μεταβατικές και αντι-συμμετρικές,

Οι ρόλοι ανατίθενται σε δράστες – χρήστες του συστήματος, γεγονός το οποίο δημιουργεί το σύνολο:

– Αναθέσεις ρόλων (Role Assignments (*RA*)): $RA \subseteq Ac \times R$; το οποίο αντικατοπτρίζει μία σχέση πολλών-σε-πολλούς (many-to-many), αναθέτοντας ρόλους σε χρήστες.

Επιπρόσθετα, οι σκοποί ανατίθενται σε ρόλους σαν αδειοδοτήσεις με συγκεκριμένα προνόμια πρόσβασης, εφόσον, προφανώς, δεν μπορούν να δράσουν όλοι οι ρόλοι για την εξυπηρέτηση όλων των σκοπών. Για παράδειγμα, οι αρμοδιότητες ενός διαχειριστή ασφάλειας δικτύου διαφέρει αισθητά από τις αρμοδιότητες ενός διαχειριστή λογιστηρίου. Έτσι δημιουργείται το σύνολο:

– Συσχετισμός σκοπός-ρόλου-δράσης (Purpose-to-Role-to-Action (*PRA*)): $PRA \subseteq P \times R \times A$, ο οποίος αντικατοπτρίζει μία σχέση πολλών-σε-πολλούς (many-to-many), αναθέτοντας ρόλους κατάλληλους για δράση όσον αφορά σε συγκεκριμένους σκοπούς με συγκεκριμένα προνόμια πρόσβασης.

4.3 Κανόνες ελέγχου πρόσβασης

Οι κανόνες ελέγχου πρόσβασης από τους οποίους εξάγονται οι αποφάσεις εξουσιοδότησης, είναι πάντα συνδεδεμένοι με την τετράδα {τύποι προσωπικών δεδομένων, σκοπός, δράση, ρόλος}. Τα τέσσερα αυτά αντίστοιχα σύνολα αποτελούν το πεδίο ορισμού του κανόνα, ενώ μία πέμπτη παράμετρος αντιπροσωπεύει τις συνθήκες ή περιορισμούς, εάν υπάρχουν: dom $Ru = DT^n \times Pu \times R \times A \times C$. Οι κανόνες ελέγχου πρόσβασης μπορεί να είναι είτε θετικοί είτε αρνητικοί, έχοντας ως αποτέλεσμα θετικές ή αρνητικές εξουσιοδοτήσεις, αντίστοιχα, λαμβάνοντας πάντα υπόψη την υποκείμενη πράξη. Τα δικαιώματα πρόσβασης καθορίζονται από τις δράσεις και μπορεί, για παράδειγμα, να αφορούν προνόμια ανάγνωσης (read) και τροποποίησης (write). Εκφραζόμενοι ως λογικά

κατηγορήματα (predicates), οι διαφορετικοί κανόνες ελέγχου πρόσβασης που αφορούν στα παραπάνω προνόμια είναι οι παρακάτω:

- readAccessPermission(⟨*DT*⟩, *Pu*, *R*, *C*)
- writeAccessPermission(⟨*DT*⟩, *Pu*, *R*, *C*)
- readAccessProhibition(⟨*DT*⟩, *Pu*, *R*, *C*)
- writeAccessProhibition(⟨*DT*⟩, *Pu*, *R*, *C*)

Συνεπώς, $\forall\ dt_i \in DT^n$, $pu_j \in Pu$, $r_k \in R$, $c_l \in C$:

- readAccessProhibition(dt_i, pu_j, r_k, c_l) $\rightarrow \neg$ readAccessPermission(dt_i, pu_j, r_k, c_l)
- writeAccessProhibition(dt_i, pu_j, r_k, c_l) $\rightarrow \neg$ writeAccessPermission(dt_i, pu_j, r_k, c_l)

Όπως αναφέρθηκε προηγουμένως, οι ρόλοι ανατίθενται σε δράστες και στους ρόλους εκχωρείται το δικαίωμα της δράσης για την εκπλήρωση ενός σκοπού. Το μόνο που απομένει είναι ο συσχετισμός των τύπων προσωπικών δεδομένων με το ζεύγος σκοπού-ρόλου το οποίο σημαίνει τα στοιχεία του *PR*. Ιδιαίτερη σημασία δίνεται στις θετικές εξουσιοδοτήσεις οι οποίες εκχωρούν δικαιώματα στους συσχετισμένους ρόλους και δράστες με την ανάλογη δράση. Τα παραπάνω δημιουργούν την έννοια των επιτρεπόμενων τύπων δεδομένων *permitted data types* αναπαριστώντας τις θετικές εξουσιοδοτήσεις που αφορούν τα δεδομένα: δηλώνουμε ότι ένα σύνολο δεδομένων ⟨dt_1, dt_2, …, dt_m⟩ είναι επιτρεπόμενο για ένα συσχετισμό σκοπού-ρόλου-δράσης *(is permitted)* apr_{xzy}, όταν όλοι οι τύποι προσωπικών δεδομένων που αποτελούν το σύνολο είναι απαραίτητοι έτσι ώστε ένας δράστης με ρόλο r_y, να εκπληρώσει το σκοπό pu_z, όπου $pr_{zy} = \langle pu_z, r_y \rangle$ για τη δράση α_x. Έτσι δημιουργείται το ακόλουθο σύνολο:

- Permitted data types (*PDT*): $PDT \subseteq DT^n \times APR$.

4.4 Πληροφορίες πλαισίου

Οι γενικές πληροφορίες πλαισίου που λαμβάνονται υπόψη σε πραγματικό χρόνο της αξιολόγησης και της εφαρμογής των κανόνων ελέγχου πρόσβασης χωρίζονται σε δύο πιθανές κατηγορίες: από τη μία πλευρά, υπάρχουν οι προϋποθέσεις που καθορίζονται έναντι των κανόνων ελέγχου πρόσβασης, ενώ, από την άλλη πλευρά, υπάρχουν οι υποχρεώσεις και οι αμοιβαίοι αποκλεισμοί που ορίζονται μεταξύ των τύπων των δεδομένων.

Όσον αφορά τους αμοιβαίους αποκλεισμούς, υιοθετήθηκε μια απλή προσέγγιση. Το μοντέλο καθορίζει σύνολα τύπων δεδομένων που χαρακτηρίζονται ως αμοιβαίως αποκλειόμενα, $MED \subseteq DT^n$. Αυτά τα σύνολα αφορούν «απαγορευμένους» συνδυασμούς των δεδομένων μέσα στο σύνολο *PDT* και, με βάση τα αποτελέσματα, οι τύποι δεδομένων που περιλαμβάνει το *PDT* μπορούν να διατεθούν στο σύνολό τους ή μερικοί να αποκλειστούν. Ένα θέμα σχετικό με τους αμοιβαίως αποκλειόμενους συνδυασμούς αφορά τον ενδεχόμενο έμμεσο αποκλεισμό που προκύπτει ως αποτέλεσμα της κληρονομικότητας. Για παράδειγμα, σε μία εφαρμογή παρακολούθησης δικτύου, εάν ο τύπος δεδομένου `IPv4SourceAddress` αποκλείεται λόγω του εκ των προτέρων αποκλεισμού ενός αντικρουόμενου τύπου δεδομένων, κάθε τύπος δεδομένων που περιέχει τον `IPv4SourceAddress` (π.χ., ο `IPv4ProtocolHeader`) αποκλείεται επίσης. Αυτό συνεπάγεται συλλογιστική πραγματικού χρόνου στην οντολογία η οποία, καθώς η οντολογία μεγαλώνει, μπορεί να γίνει η αιτία για δυσχερή απόδοση. Από την άποψη αυτή και λαμβάνοντας υπόψη τη στατική φύση των ιδίων των αποκλεισμών (αν και η αξιολόγησή τους είναι ιδιαίτερα δυναμική), η συλλογιστική αυτή εκτελείται "offline", δημιουργώντας έναν κατάλογο αποκλειόμενων συνδυασμών, ο οποίος χρησιμοποιείται αποδοτικά σε πραγματικό χρόνο.

Οι υποχρεώσεις που περιλαμβάνονται στο σύνολο *O* αποτελούν μεμονωμένες ή σύνθετες ενέργειες, οι οποίες πρέπει να εκτελεστούν πριν η μετά την εφαρμογή του κανόνα για να πραγματοποιηθεί η αντίστοιχη ενέργεια πρόσβασης. Ακολουθούν ένα μοτίβο και αφορούν, π.χ., σε καταστάσεις που απαιτείται η συναίνεση ενός ρόλου για την τελική επιβολή του κανόνα και διάθεση ή επεξεργασία των δεδομένων ή στην ειδοποίηση ενός ρόλου μετά τη διάθεση ή την επεξεργασία κάποιων δεδομένων, κ.α. Ως εκ τούτου, οι υποχρεώσεις είναι άμεσα συνδεδεμένες με το σύνολο των κανόνων του μοντέλου.

Το προτεινόμενο μοντέλο περιλαμβάνει επίσης ένα σύνολο συνθηκών (*C*). Κάθε συνθήκη αντικατοπτρίζει μια λογική έκφραση και ορίζουμε ότι σχετίζεται με έναν ή περισσότερους κανόνες, είτε με το να είναι άμεσα συνδεδεμένη, ή ως μέρος μιας δομής. Για την τελική επιβολή των κανόνων, αξιολογείται πρώτα η αλήθεια των συνθηκών εφόσον υπάρχουν.

Οι δομή των συνθηκών ορίζεται με τη χρήση διαφορετικών σχέσεων μέσω λογικών, αριθμητικών ή συγκριτικών τελεστών. Πράγματι, μια συνθήκη μπορεί να αντανακλά την ανάγκη για ταυτόχρονη εφαρμογή ενός συνόλου διαφορετικών περιορισμών, ενώ αρκετές

διαφορετικές συνθήκες μπορεί να συνεπάγονται ανεξάρτητα και να ενεργοποιούν κάποια άλλη συνθήκη. Με βάση αυτό, μια συνθήκη $c_k \in C$ μπορεί να εκφραστεί, για παράδειγμα, ως το λογικό *AND/OR* ενός επιμέρους συνόλου συνθηκών, αντίστοιχα, δηλαδή, $c_k = (c_{k1} \wedge c_{k2} \wedge \ldots \wedge c_{kn})$ ή $c_k = (c_{k1} \vee c_{k2} \vee \ldots \vee c_{kn})$.

Αρνητικές συνθήκες είναι επίσης πιθανές. Δηλαδή, μια συνθήκη μπορεί να λάβει τη μορφή $c_k = (c_{k1} \wedge \neg\, c_{k2})$. Οι συνθήκες που αποτελούν συνδυασμούς επιμέρους συνθηκών ονομάζονται σύνθετες συνθήκες, σε αντίθεση με τις ατομικές συνθήκες.

Όσον αφορά το είδος μίας συνθήκης, το σύνολο των τύπων πλαισίου (*CT*), ορίζεται ως εξής: κάθε ατομική συνθήκη αντιστοιχίζεται σε έναν τύπο πλαισίου, το οποίο για να εκφραστεί διατυπώνεται το κατηγόρημα hasContextValue(c_i, ct_j), όπου $c_i \in C$ και $ct_j \in CT$. Στο προτεινόμενο μοντέλο, το σύνολο *CT* ορίζεται ως *CT* = {χρονικό, χωρικό, βασισμένο σε συμβάντα}. Πιο συγκεκριμένα, οι τύποι πλαισίου αντιστοιχούν σε χρονικές, χωρικές και βασισμένες σε συμβάντα παραμέτρους, ενώ το μοντέλο έχει δημιουργηθεί με σκοπό να είναι γενικευμένο και, κατά συνέπεια, να είναι δυνατό να προστεθούν και άλλοι τύποι πλαισίου.

Κεφάλαιο 5

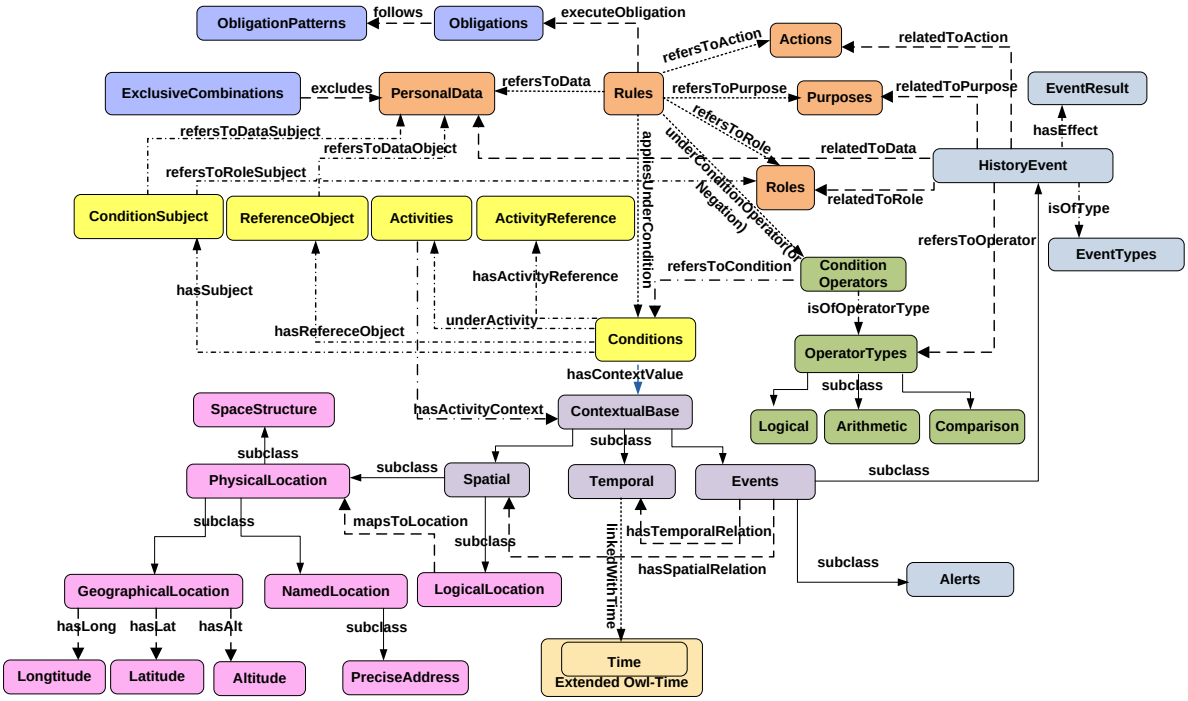
Οντολογία ελέγχου πρόσβασης

Δεδομένης της σπουδαιότητας της σημασιολογίας στην προστασία των προσωπικών δεδομένων (Lioudakis et al., 2010), για την εφαρμογή του πλαισίου ελέγχου πρόσβασης, χρησιμοποιείται ένα σημασιολογικό μοντέλο πληροφοριών κατά το οποίο συνδέονται τα δεδομένα προσωπικού χαρακτήρα, οι σκοποί, οι δράσεις και οι ρόλοι με σαφώς καθορισμένους κανόνες πρόσβασης. Η βάση γνώσεων του συστήματος από την άποψη των κανόνων ελέγχου πρόσβασης, όπως έχει ήδη αναφερθεί, εκφράζεται με μια οντολογία, η οποία υλοποιείται με την W3C Web Ontology Language (OWL). Η οντολογία είναι όσο το δυνατόν λεπτομερέστερη από την άποψη των διαφόρων τύπων των προσωπικών δεδομένων, των σκοπών, των δράσεων και των ρόλων, έτσι ώστε το ευρύτερο φάσμα των υπηρεσιών και των περιπτώσεων όταν πρόκειται για προσωπικά δεδομένα να μπορούν να καλυφθούν.

Στο πλαίσιο αυτό, η οντολογία είναι δομημένη με ιεραρχικό τρόπο και υλοποιημένη με υπογράφους, τους οποίους διέπουν σαφώς καθορισμένοι κανόνες κληρονομικότητας, και επιτρέπει στο σύστημα να συνδέσει όλες τις αποφάσεις με σημασιολογικά προσδιορισμένες έννοιες. Οι υπογράφοι των προσωπικών δεδομένων, των σκοπών, των δράσεων και των ρόλων αποτελούν τη βάση του σημασιολογικού μοντέλου και είναι ο τομέας προσδιορισμού των κανόνων.

Το σημασιολογικό μοντέλο ελέγχου πρόσβασης σε πληροφορίες ολοκληρώνεται με τις προδιαγραφές συμπληρωματικών οντολογικών κλάσεων που αφορούν την επίγνωση πλαισίου και προστασία της ιδιωτικότητας. Οι σχέσεις μεταξύ των στιγμιότυπων των κλάσεων, ορίζονται με τη χρήση των OWL ιδιοτήτων αντικειμένου (object properties). Στην Εικόνα 19, παρέχεται μία γραφική αναπαράσταση της οντολογίας σε επίπεδο κλάσεων, η οποία συνοψίζει τις έννοιες που θα περιγραφούν στις ακόλουθες παραγράφους.

Η προτεινόμενη οντολογία έχει αξιολογηθεί σε περιβάλλοντα παρακολούθησης δικτύου. Το παράδειγμα χρήσης αυτό παρουσιάζεται στο Κεφάλαιο 7 της εργασίας.



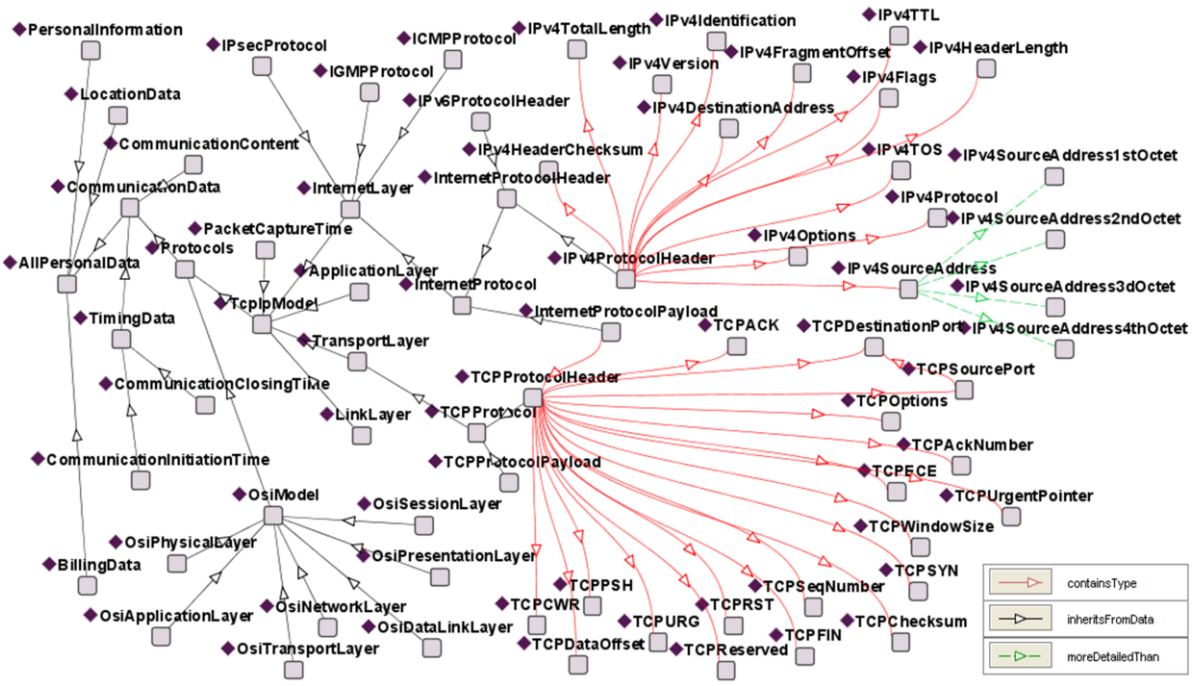
Εικόνα 19: Το προτεινόμενο σημασιολογικό μοντέλο

5.1 Βασικές Κλάσεις Οντολογίας ελέγχου πρόσβασης

5.1.1 Η κλάση PersonalData

Η `PersonalData` OWL κλάση περιλαμβάνει τους τύπους των δεδομένων με τα οποία ασχολείται το σύστημα. Τα δεδομένα αυτά ορίζονται ως στιγμιότυπα αυτής της κλάσης της οντολογίας. Οι σχέσεις και κυρίως οι ιεραρχίες κληρονομικότητας μεταξύ των τύπων δεδομένων ορίζονται ως OWL ιδιότητες και οργανώνονται χρησιμοποιώντας την κληρονομικότητα των χαρακτηριστικών, το επίπεδο λεπτομέρειας των δεδομένων και τη σύνθεση των σύνθετων τύπων δεδομένων από απλούστερους. Στο πλαίσιο αυτό, οι ιδιότητες που χρησιμοποιούνται είναι αντίστοιχα οι `inheritsFromData` και `inheritsDataTo`, `lessDetailedThan` και `moreDetailedThan`, `containsType` και `isContainedToType` ιδιότητες αντικειμένου OWL. Για παράδειγμα, η ρίζα του υπογράφου τύπων δεδομένων είναι ο τύπος `AllPersonalData`, από τον οποίο κληρονομούν όλα τα άλλα είδη, ενώ τα στιγμιότυπα `PersonalInformation`, `LocationData`, `CommunicationData`, κλπ., αποτελούν «πρώτο επίπεδο» απογόνων του τύπου `AllPersonalData`. Οι τύποι αυτοί αποτελούν γενικούς τύπους δεδομένων, στην ουσία κατηγορίες τύπων δεδομένων. Αυτή η ιεραρχία

υλοποιείται μέσω της σχέσης `inheritsFromData`. Παράδειγμα του γράφου δεδομένων παρουσιάζεται στην Εικόνα 20.



Εικόνα 20: Ο γράφος δεδομένων

5.1.2 Η κλάση Purposes

Η μοντελοποίηση των σκοπών αποτελείται από τους τύπους των διαφόρων υπηρεσιών που είναι οργανωμένες ως μια ιεραρχία που ορίζει κληρονομικότητα των χαρακτηριστικών. Όλοι οι σκοποί αποτελούν στιγμιότυπα της OWL κλάσης `Purposes`. Οι προδιαγραφές των υπηρεσιών εξαρτώνται βασικά από τους διάφορους σκοπούς για τους οποίους ο χρήστης που έχει υποβάλει αίτημα για πρόσβαση σε τύπους δεδομένων σκοπεύει να ολοκληρώσει. Οι σχέσεις κληρονομικότητας μεταξύ των τύπων υπηρεσιών ορίζονται επίσης από OWL ιδιότητες. Η ρίζα του υπογράφου των σκοπών είναι ο τύπος `AllPurposes`, από τον οποίο κληρονομούν οι τύποι όλων των άλλων σκοπών. Οι σχέσεις ιεραρχίας υλοποιούνται μέσω των OWL σχέσεων `inheritsFromPurpose` και `inheritsPurposeTo`. Σημειώνεται ότι η πολλαπλή κληρονομικότητα είναι δυνατή. Μια δεύτερη ιεραρχία έχει οριστεί για τον υπογράφο των σκοπών η οποία αποτελεί AND δέντρο ιεραρχίας, που χαρακτηρίζει την αποσύνθεση μιας υπηρεσίας σε υπο-υπηρεσίες. Αυτή εφαρμόζεται με τη βοήθεια των OWL σχέσεων `consistsOf` και `isConsistedIn`.

5.1.3 Η κλάση Roles

Η μοντελοποίηση των ρόλων ορίζει τους ρόλους οι οποίοι εκχωρούνται οι δράστες (actors) του συστήματος. Οι ρόλοι αυτοί βρίσκουν τη σημασιολογική αναπαράστασή τους ως στιγμιότυπα της OWL κλάσης `Roles`. Οι ρόλοι αντιπροσωπεύουν μια ρεαλιστική ιεραρχική δομή των μελών ενός οργανισμού. Για παράδειγμα, ως στιγμιότυπα ρόλων είναι οι τύποι `InternalUser`, `ThirdPartyUsers`, `Subcontractors` και `Customer`. Όλοι αυτοί οι τύποι ρόλων αποτελούν πρώτο επίπεδο απογόνων του στιγμιότυπου ρίζα `AllRoles`. Ο υπογράφος αυτός χαρακτηρίζεται από δύο είδη ιεραρχίες. Η πρώτη ιεραρχία είναι ένα OR-δέντρο το οποίο χρησιμεύει ως μέσο για τον καθορισμό της κληρονομικότητας των χαρακτηριστικών μεταξύ των μελών του υπογράφου και υλοποιείται από την OWL σχέση `inheritsFromRole` και την αντίστροφή της.

Τέτοιες ιεραρχίες είναι αρκετά τυπικές σε μοντέλα που βασίζονται στο ρόλο και είναι βασισμένες στην ιδέα ότι τα υψηλότερα επίπεδα του υπογράφου αποτελούν τους πιο γενικούς ρόλους μέσα σε έναν οργανισμό, π.χ. «υπάλληλος». Από την άλλη πλευρά, το καινοτόμο χαρακτηριστικό του μοντέλου είναι η προδιαγραφή μιας ιεραρχίας AND δέντρου για τους ρόλους. Αυτή η ιεραρχία καθορίζει τη ρητή συμμετοχή των ρόλων σε άλλους. Για παράδειγμα, ο λογικός ρόλος `BoardOfExecutives` αποτελείται από ρόλους, όπως ο `ChiefExecutiveOfficer`, ο `ChiefTechnologyOfficer` και το `BoardMember` όπου για να παρθεί μία τελική απόφαση που αφορά στον οργανισμό πρέπει όλοι οι παραπάνω ρόλοι να δώσουν τη συγκατάθεσή τους και να αλληλεπιδράσουν. Αυτή η ιεραρχία υλοποιείται με τη βοήθεια του OWL σχέσης `isPartOfRole`.

5.1.4 Η κλάση Actions

Οι διάφορες ενέργειες πρόσβασης (π.χ. ανάγνωση, εγγραφή, διαγραφή, ενημέρωση, κλπ.) στα προσωπικά δεδομένα αντιπροσωπεύονται από τις δράσεις, οι οποίες είναι όλες στιγμιότυπα της κλάσης `Actions`. Το σύνολο των δράσεων χαρακτηρίζεται επίσης από OR και AND ιεραρχίες, εκφράζοντας αντίστοιχα την κληρονομικότητα των χαρακτηριστικών και της αποσύνθεσης μιας δράσης σε επιμέρους δράσεις που υλοποιούνται μέσω των `inheritsFromAction` και `isComposedOf` OWL σχέσεων. Για παράδειγμα η δράση «επεξεργασία» μπορεί να αποτελείται από τις δράσεις «διαγραφή» και «ενημέρωση».

5.2 Η κλάση Rules

Οι κανόνες ελέγχου πρόσβασης ορίζονται ως στιγμιότυπα της OWL κλάσης `Rules` της οντολογίας. Κάθε στιγμιότυπο της κλάσης αυτής αντιστοιχεί σε μια τετράδα, η οποία συνίσταται σε ένα ρόλο, σε μία δράση, σε κάποια δεδομένα και σε ένα σκοπό, στιγμιότυπα των κλάσεων `Roles`, `Actions`, `PersonalData`, και `Purposes` αντίστοιχα, χρησιμοποιώντας τις αντίστοιχες OWL σχέσεις `refersToRole`, `refersToAction`, `refersToData`, και `refersToPurpose`. Η προδιαγραφή των κανόνων βασίζεται στις επιτρεπόμενες καθώς και στις ενέργειες που απαγορεύονται από ένα συγκεκριμένο ρόλο να εκτελέσει. Οι ενέργειες αυτές αφορούν σε υπηρεσίες και προκειμένου να εφαρμοστούν, έχουν συνδεθεί, με συγκεκριμένα δεδομένα.

Επιπλέον, η κληρονομικότητα των κανόνων καθώς και η διευθέτηση των συγκρούσεων μεταξύ αντιφατικών κανόνων υλοποιείται με συγκεκριμένες ιδιότητες. Για παράδειγμα, η `appliesToPersonalDataDescendants` αποτελεί δυαδική ιδιότητα και καθορίζει αν ο κανόνας κληρονομείται στους απογόνους του συγκεκριμένου τύπου δεδομένων σε σχέση με τις σχέσεις κληρονομικότητας του αντίστοιχου υπογράφου της οντολογίας. Η `appliesToPurposeDescendants` καθορίζει την κληρονομικότητα του κανόνα στους απογόνους του τύπου της υπηρεσίας. Η `appliesToRoleDescendants` αναφέρεται στην κληρονομικότητα του κανόνα στους απογόνους του τύπου ρόλου και η `appliesToActionDescendants` που αναφέρεται στην κληρονομικότητα του κανόνα στους απογόνους του τύπου δράση.

Επιπλέον η `OverrideDataSubjectPreferences` χρησιμεύει για να καθορίσει ποιος κανόνας κυριαρχεί πάνω στον άλλο όσον αφορά τις προτιμήσεις του υποκειμένου δεδομένων. Σε αυτό το σημείο πρέπει να τονιστεί ότι η ιδιότητα αυτή απλά ορίζεται στο μοντέλο της παρούσας διατριβής καθώς δεν έχει υλοποιηθεί μηχανισμός Preferences. Επιπλέον, η `OverrideExclusions` καθορίζει το κατά πόσον οι πιθανοί περιορισμοί που καθορίζονται στην κλάση `ExclusiveCombinations` για τον τύπο δεδομένων υπό εξέταση πρέπει να αγνοηθούν στο πλαίσιο της εφαρμογής αυτού του κανόνα. Κάθε στιγμιότυπο της κλάσης `Rules` χαρακτηρίζεται προαιρετικά από μια περιγραφή κειμένου. Με βάση αυτό, χρησιμοποιείται η ιδιότητα rdfs:comment, όπως ορίζεται στο W3C RDF Schema (World Wide Web Consortium, 2004). Η OWL σχέση `appliesUnderCondition` συνδέει τον κανόνα με τις συνθήκες της κλάσης

Conditions (εάν υπάρχουν) που πρέπει να πληρούνται, προκειμένου ο κανόνας να εφαρμοστεί. Τέλος, η κλάση Rules συνδέεται με την κλάση Obligations (εάν υπάρχουν) μέσω της σχέσης executeObligation.

5.3 Βοηθητικές Κλάσεις

5.3.1 Η κλάση ExclusiveCombinations

Η κλάση ExclusiveCombinations αντιπροσωπεύει τον τρόπο με τον οποίο ορισμένοι τύποι δεδομένων είναι αμοιβαίως αποκλειόμενοι όσον αφορά τη διάθεσή τους. Ως παράδειγμα, καθένα από τα τέσσερα octets μιας διεύθυνσης IP από μόνο του είναι συνήθως αβλαβές από άποψη προστασίας της ιδιωτικότητας. Ωστόσο, στην κατάσταση της σύνθεσής τους, συνιστούν την πλήρη διεύθυνση IP, η οποία είναι ενίοτε προσωπικό δεδομένο και, ως εκ τούτου, η διάθεση και των τεσσάρων από αυτά, στην ίδια οντότητα με τρόπο που να είναι σε θέση να ανασυνθέσει τη διεύθυνση IP πρέπει να αποτραπεί. Από την άποψη αυτή, η κλάση ExclusiveCombinations βασίζεται στην ιδέα ότι κάθε στιγμιότυπο σχετίζεται μέσω της OWL σχέσης excludes με τα διάφορα είδη δεδομένων που αποτελούν έναν αποκλειόμενο συνδυασμό.

5.3.2 Η κλάση Obligations

Σε αρκετές περιπτώσεις, η επιβολή ενός κανόνα πρέπει να συμπληρώνεται από την εκτέλεση ορισμένων δράσεων, οι οποίες αναφέρονται συχνά στη βιβλιογραφία ως «υποχρεώσεις» (Hilty and Pretschner, 2005). Οι υποχρεώσεις χωρίζονται σε δύο κατηγορίες: στις προ-υποχρεώσεις, που αφορούν τις δράσεις που θα πρέπει να πληρούνται πριν από την απόφαση της πρόσβασης, και στις μετα-υποχρεώσεις, που αναφέρονται σε συμπληρωματικές δράσεις που θα πρέπει να εκτελεστούν μετά την επιβολή του κανόνα προκειμένου να εκπληρωθεί το αίτημα.

Η έννοια των υποχρεώσεων υλοποιείται σημασιολογικά μέσω της κλάσης Obligations. Η σχέση executeObligation συνδέει τους κανόνες με τις υποχρεώσεις. Κάθε υποχρέωση ακολουθεί ένα μοτίβο, που αντιπροσωπεύεται από ένα στιγμιότυπο της κλάσης ObligationPatterns, η οποία ορίζει τα σχετικά αρχέτυπα. Κάθε πρότυπο υποχρέωσης χαρακτηρίζεται από ιδιότητες, οι οποίες ορίζουν ορισμένες πτυχές των υποχρεώσεων μετά από αυτό.

Μία βασική ιδιότητα είναι το κατά πόσον οι υποχρεώσεις θα είναι προ-ενεργές ή μετά-ενεργές, το οποίο καθορίζεται από την αντίστοιχη Boolean ιδιότητα `isProActive`. Κάθε πρότυπο υποχρέωσης (ή υποχρέωση), έχει επιπλέον χαρακτηριστικά σύμφωνα με την ειδική φύση της υποχρέωσης. Το μοτίβο `dataRetention`, για παράδειγμα, καθώς και οι υποχρεώσεις που το ακολουθούν, έχουν την ιδιότητα `retentionDuration` για την προδιαγραφή της απαιτούμενης περιόδου διατήρησης των δεδομένων.

5.3.3 Η κλάση Conditions και συμπληρωματικές κλάσεις πλαισίου

Η έννοια του πλαισίου (context), όπως έχει ήδη περιγραφεί μπορεί να αναφέρεται σε όλα τα είδη των πληροφοριών που περιγράφουν μια συγκεκριμένη κατάσταση. Περιλαμβάνει δυναμικά χαρακτηριστικά, όπως τη χρονική στιγμή του αιτήματος για πρόσβαση των δεδομένων, την τοποθεσία από την οποία το αίτημα λαμβάνει χώρα, κλπ., τα οποία επηρεάζουν συνήθως στο προτεινόμενο μοντέλο την επιβολή ενός κανόνα.

Αυτές οι παράμετροι υλοποιούνται μέσω της κλάσης `Conditions`. Η κλάση αυτή προσδιορίζει και ενσωματώνει εύκολα τους περιοριστικούς παράγοντες που είναι υπεύθυνοι για την ρύθμιση των δικαιωμάτων του χρήστη, σχετικά με τους επιτρεπόμενους τύπους δεδομένων, προκαλώντας διαφορετικά δικαιώματα πρόσβασης με βάση τις πληροφορίες πλαισίου του χρήστη. Από την άποψη αυτή, ορίζονται κανόνες πρόσβασης που προσδιορίζουν και επικαιροποιούν το δικαίωμα πρόσβασης ενός χρήστη σε αιτήματα πραγματικού χρόνου με ορισμένες άδειες (περιορισμοί) βασισμένες στην τρέχουσα κατάσταση του χρήστη. Κάθε στιγμιότυπο αυτής της κλάσης αντανακλά μια λογική έκφραση, η οποία σχετίζεται με έναν ή περισσότερους κανόνες και έχει ένα τύπο πλαισίου, ένα υποκείμενο, ένα αντικείμενο αναφοράς, μια δραστηριότητα, μια αναφορά δραστηριότητας και μια τιμή. Οι τύποι πλαισίου οι οποίοι εξετάζονται στην παρούσα διατριβή αντιστοιχούν σε χρονικούς, χωρικούς καθώς και βασισμένους σε συμβάντα τύπους, οι τελευταίοι από τους οποίους αναφέρονται κυρίως σε παρελθοντικά γεγονότα και γεγονότα συναγερμών.

Το υποκείμενο κάθε συνθήκης αντιπροσωπεύει την έννοια στην οποία αναφέρεται η συνθήκη και περιγράφεται μέσω της κλάσης `ConditionSubject`. Για παράδειγμα, όσον αφορά σε παραμέτρους θέσης, ο κανόνας «*επιτρέπεται η ανάγνωση κάποιων δεδομένων μόνο αν ο χρήστης βρίσκεται στο Κτίριο Α*» είναι διαφορετικός από τον κανόνα «*επιτρέπεται*

η ανάγνωση αυτών των δεδομένων μόνο αν τα δεδομένα είναι αποθηκευμένα στη βάση δεδομένων που βρίσκεται στο κτίριο A». Στο πλαίσιο αυτό, το υποκείμενο της συνθήκης μπορεί να αναφέρεται σε δεδομένα, καθώς και σε ένα χρήστη μέσω του ρόλου του. Όταν το υποκείμενο της συνθήκης είναι ένα σύνολο δεδομένων, τα στιγμιότυπα της κλάσης αυτής δείχνουν σε αυτά τα δεδομένα μέσω της σχέσης `refersToDataSubject`. Από την άλλη πλευρά, αν το αντικείμενο της συνθήκης αναφέρεται σε ένα χρήστη ο οποίος έχει ένα συγκεκριμένο ρόλο, χρησιμοποιείται η σχέση `refersToRoleSubject`. Η `hasSubject` σχέση συνδέει την κλάση `ConditionSubject` με την `Conditions`.

Το αντικείμενο αναφοράς αποτελεί το σύνολο δεδομένων που επηρεάζονται από την εφαρμογή της εκάστοτε συνθήκης. Για παράδειγμα, ένας κανόνας που χορηγεί δικαίωμα επεξεργασίας στο σύνολο των δεδομένων {*source IP address, source port, destination IP address, destination port, protocol*} ισχύει υπό τη συνθήκη η οποία αποκλείει μόνο τα δεδομένα *source IP address* και *destination IP address* από διαγραφή.

Συνεπώς έτσι ορίζεται η βοηθητική κλάση `ReferenceObject`. Τα στιγμιότυπα της κλάσης αυτής (μέσω της σχέσης `refersToObject`) δείχνουν προς τους τύπους δεδομένων που επηρεάζονται από την συνθήκη, ενώ οι ίδιοι σημειώνονται από τις συνθήκες μέσω της σχέσης `hasReferenceObject`.

Η έννοια της δραστηριότητας εισάγεται μέσω της κλάσης `Activity` προκειμένου να προσδιοριστεί η ενέργεια στην οποία αναφέρεται η συνθήκη. Για παράδειγμα, μια συνθήκη που δηλώνει «*επιτρέπεται η ανάγνωση των καταγεγραμμένων αρχείων ανίχνευσης εισβολής μόνο εάν τα αρχεία καταγραφής είναι αποθηκευμένα σε μια βάση δεδομένων στο εσωτερικό του οργανισμού*» συνεπάγεται ως αντικείμενο αναφοράς αλλά και ως υποκείμενο τα καταγεγραμμένα δεδομένα ανίχνευσης εισβολής, και ως δραστηριότητα την ενέργεια «είναι αποθηκευμένα σε».

Επιπρόσθετες έννοιες που κάνουν αυτή την ιδέα πιο σαφή είναι το αντικείμενο της δραστηριότητας μέσω της κλάσης `ActivityReference` και το πλαίσιο δράσης που αντικατοπτρίζει το είδος των συνθηκών υπό τις οποίες η δραστηριότητα πρέπει να πραγματοποιηθεί μέσω της κλάσης `ContextualBase`. Στο προαναφερθέν παράδειγμα, η βάση δεδομένων αποτελεί την αναφορά δραστηριότητας «αποθηκευμένα σε» και το εσωτερικό του οργανισμού αντιπροσωπεύει το χωρικό πλαίσιο της δραστηριότητας. Από

την άποψη αυτή, τα στιγμιότυπα της κλάσης Activities καθώς και τα στιγμιότυπα της κλάσης ActivityReference συνδέονται επίσης με τα στιγμιότυπα της κλάσης Conditions μέσω των σχέσεων underActivity και hasActivityReference αντίστοιχα. Επιπλέον, η σχέση hasActivityContext συνδέει τα στιγμιότυπα της κλάσης Activities με την κλάση ContextualBase.

Τέλος, μια συνθήκη μπορεί να αναφέρεται στην ταυτόχρονη εφαρμογή ενός συνόλου διαφορετικών περιορισμών. Στο πλαίσιο αυτό, οι δομές των συνθηκών ορίζονται μέσω τελεστών, οι οποίοι αποτελούν στιγμιότυπα της κλάσης ConditionOperators. Κάθε στιγμιότυπο αυτής της κλάσης έχει έναν τύπο που αντιπροσωπεύεται από τη σχέση isOfOperatorType και αναφέρεται σε ένα συγκεκριμένο στιγμιότυπο της κλάσης Conditions μέσω της σχέσης refersToCondition. Η πρώτη από αυτές τις σχέσεις δείχνει στην κλάση OperatorTypes και αποτελεί την υπερκλάση των Logical, Arithmetic και Comparison υποκλάσεων. Οι υποκλάσεις αυτές αφορούν σε τρείς διαφορετικούς τύπους τελεστών, τους λογικούς, τους αριθμητικούς και του τελεστές σύγκρισης αντιστοίχως. Συνοψίζοντας, και με βάση όλα τα παραπάνω, για τη σύνδεση των συνθηκών με τους κανόνες, χρησιμοποιούνται οι σχέσεις appliesUnderCondition, underConditionOperator και underNegativeConditionOperator.

5.3.4 Η κλάση ContextualBase

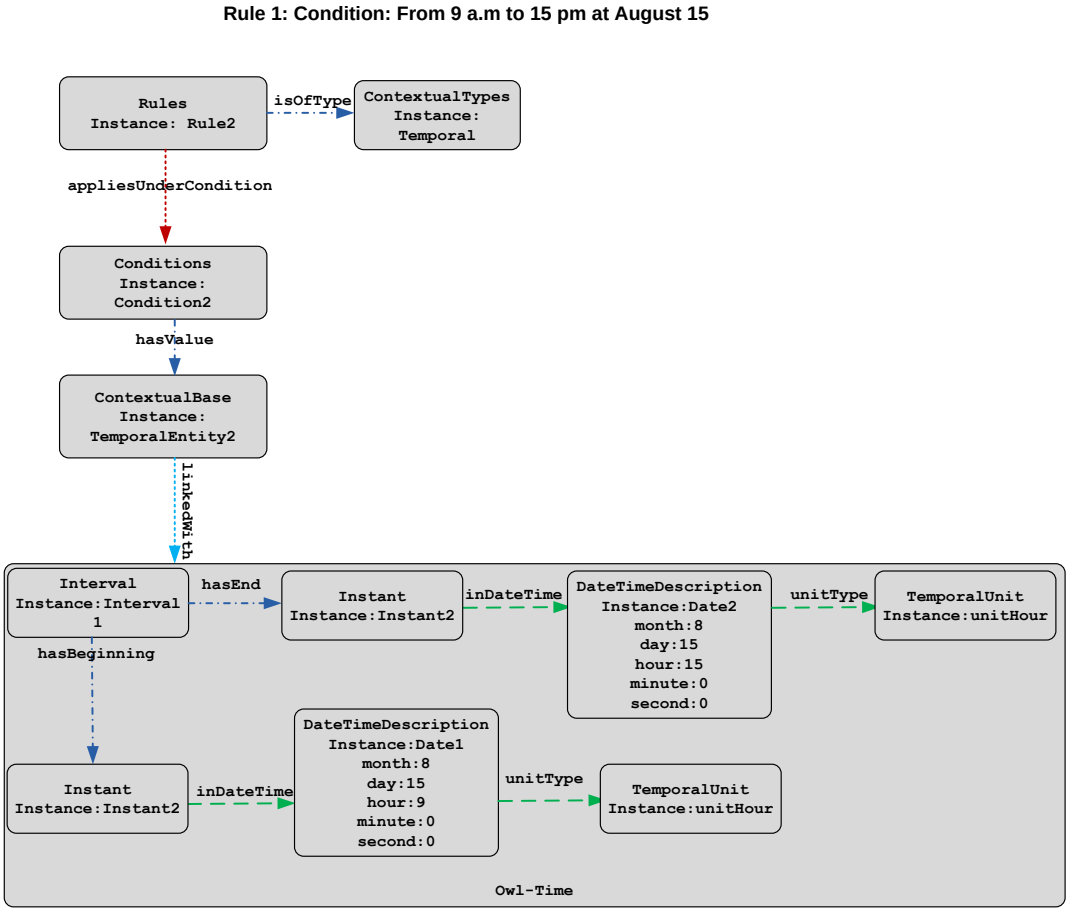
Η τιμή της συνθήκης υλοποιείται σημασιολογικά χρησιμοποιώντας την οντολογική κλάση ContextualBase. Η κλάση αυτή περιλαμβάνει μια υποκλάση για κάθε τύπο πλαισίου. Με βάση αυτό, οι τρεις υποκλάσεις που θεωρήθηκαν στη διατριβή είναι οι Temporal, Spatial και Events, ενώ επιπλέον κλάσεις μπορούν να προστεθούν.

Όσον αφορά την κλάση Temporal που αναφέρεται σε χρονικού τύπου πλαίσιο, κάθε στιγμιότυπο αυτής συνδέεται με ένα στιγμιότυπο της κλάσης που καθορίζεται από την οντολογία OWL-Time (Hobbs and Pan, 2006) με τη βοήθεια της σχέσης linkedwithTime προκειμένου να εκφραστούν λεπτομερώς όλες οι δυνατές περιπτώσεις χρονικού πλαισίου.

Παραδείγματα υλοποίησης συνθηκών χρονικού τύπου πλαισίου χρησιμοποιώντας την οντολογία OWL-Time παρουσιάζονται στις Εικόνες 21, 22.

Το χωρικό πλαίσιο αντιπροσωπεύεται από την SpatialBase υπερκλάση και τις υποκλάσεις LogicalLocation και PhysicalLocation. Περαιτέρω ταξινόμηση αυτών των υποκλάσεων απεικονίζεται στην Εικόνα 23.

Η υπερκλάση Events περιέχει τις υποκλάσεις HistoryEvent και Alert. Το πλαίσιο το οποίο σχετίζεται με παρελθοντικά γεγονότα σχετίζεται με προηγούμενες δράσεις τις οποίες ένα υποκείμενο έχει εκτελέσει στο σύστημα και οποίες χρησιμοποιούνται ως ένας από τους παράγοντες απόφασης για την επόμενη εξουσιοδότηση πρόσβασης. Αυτό το είδος των πολιτικών σχετίζεται επίσης με χρονικούς περιορισμούς.

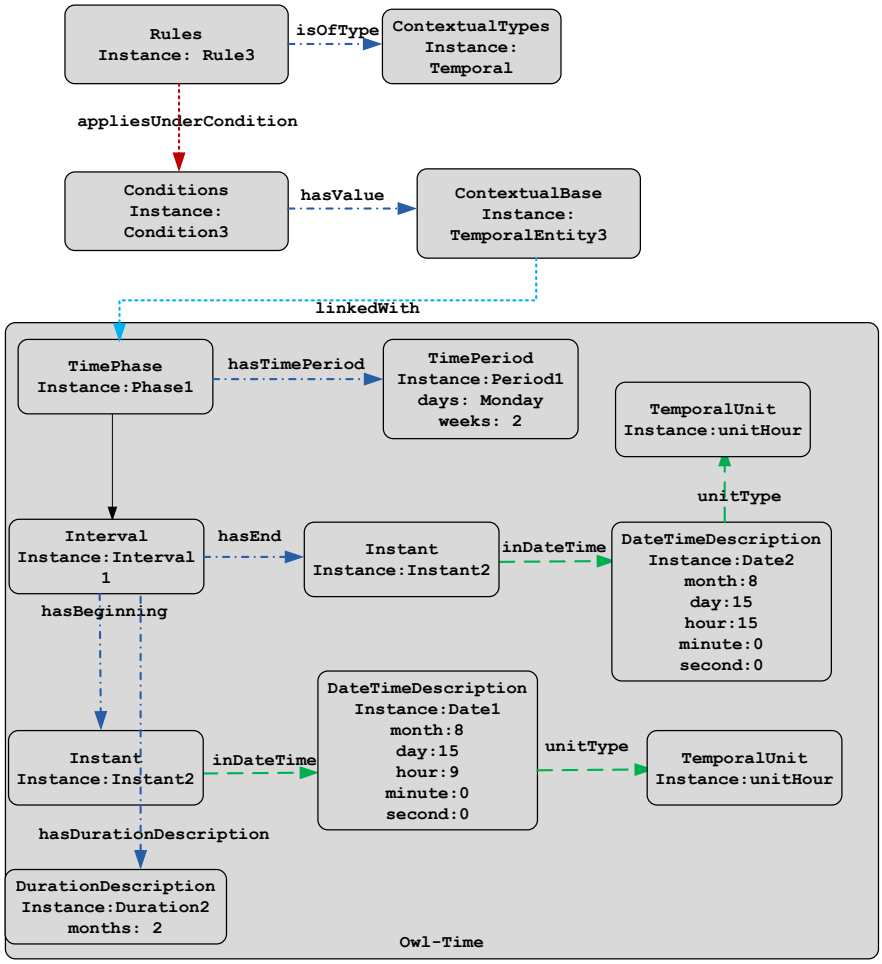


Εικόνα 21: Παράδειγμα συνθήκης χρονικού τύπου πλαισίου

Για παράδειγμα, ένα HistoryEvent το οποίο αναφέρει ότι: «*ένας μηχανικός διάβασε τον τύπο δεδομένου IPAddress για το σκοπό NetworkTroubleshooting περισσότερο από 5 φορές μεταξύ της χρονοθυρίδας 9πμ-5μμ*». Από αυτή την άποψη, το γεγονός είναι τύπου «πρόσβασης» που εφαρμόζεται από την τάξη EventTypes μέσω της σχέσης isOfType και συνδέεται με τα στιγμιότυπα Engineer, IPAddress,

NetworkTroubleshooting και read με τη βοήθεια των σχέσεων relatedToRole, relatedToData, relatedToPurpose και relatedToAction αντίστοιχα. Επιπλέον, το αποτέλεσμα του παρελθοντικού γεγονότος όπου το HistoryEvent στο παράδειγμα αναφέρεται είναι το permittedAccess μέσω της σχέσης hasEffect. Επιπλέον, το στιγμιότυπο HistoryEvent δείχνει στον Comparison τελεστή OperatorType "greaterThan" με τιμή "5" με τη βοήθεια της σχέσης refersToOperator. Τέλος, το στιγμιότυπο της κλάσης Events δείχνει στο στιγμιότυπο που αφορά στο χρονικό διάστημα 5μμ-9μμ της κλάσης Temporal μέσα από την σχέση hasTemporalRelation.

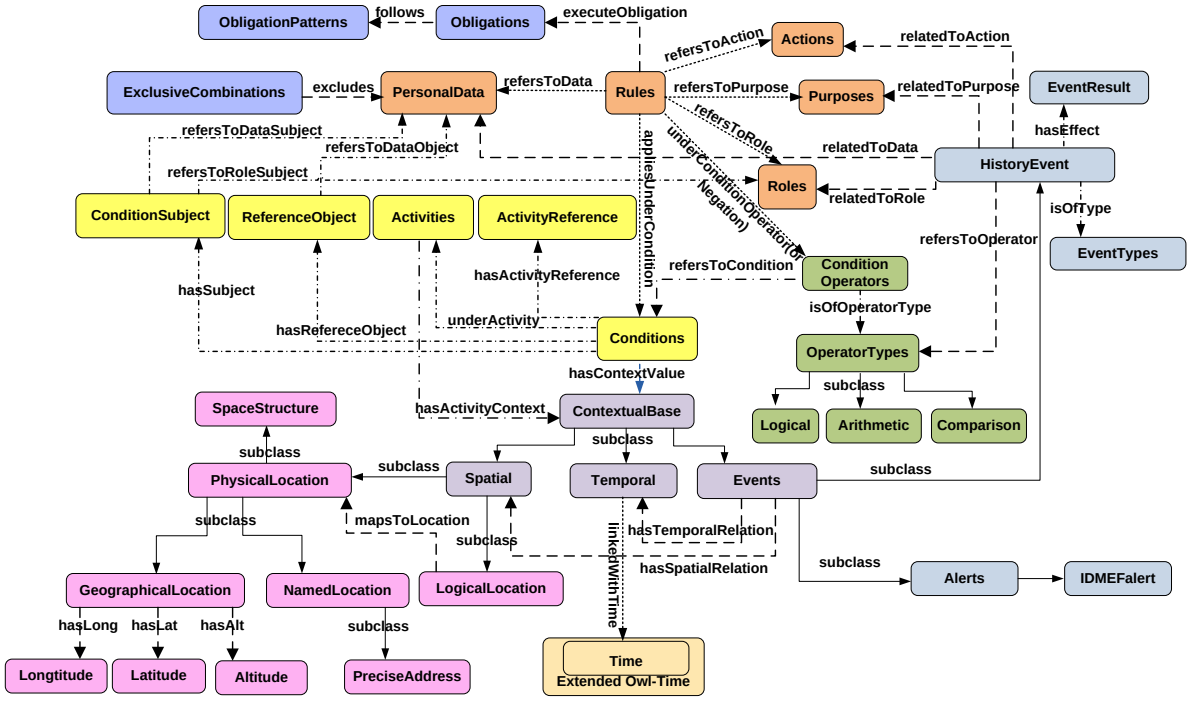
Rule 3: Condition: Every other Monday From 9 a.m to 15 pm starting at August 15 for 2 months



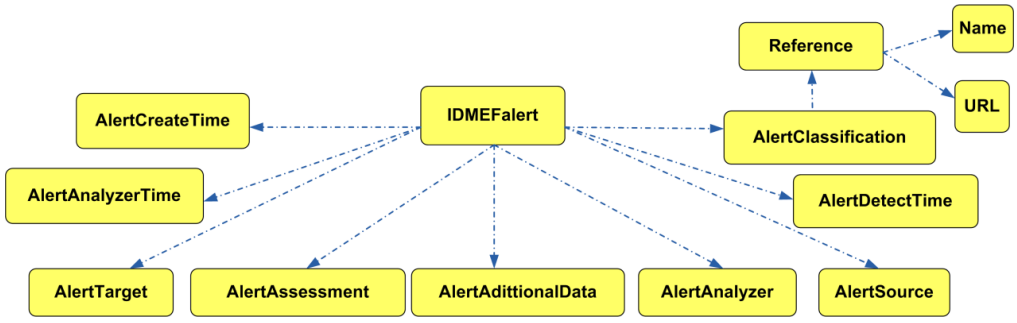
Εικόνα 22: Παράδειγμα συνθήκης χρονικού τύπου πλαισίου

. Η προτεινόμενη οντολογία ενσωματώνει επιπρόσθετα πληροφορίες απαραίτητες για τον έλεγχο πρόσβασης οι οποίες αφορούν σε συμβάντα ειδοποίησης παραβίασης

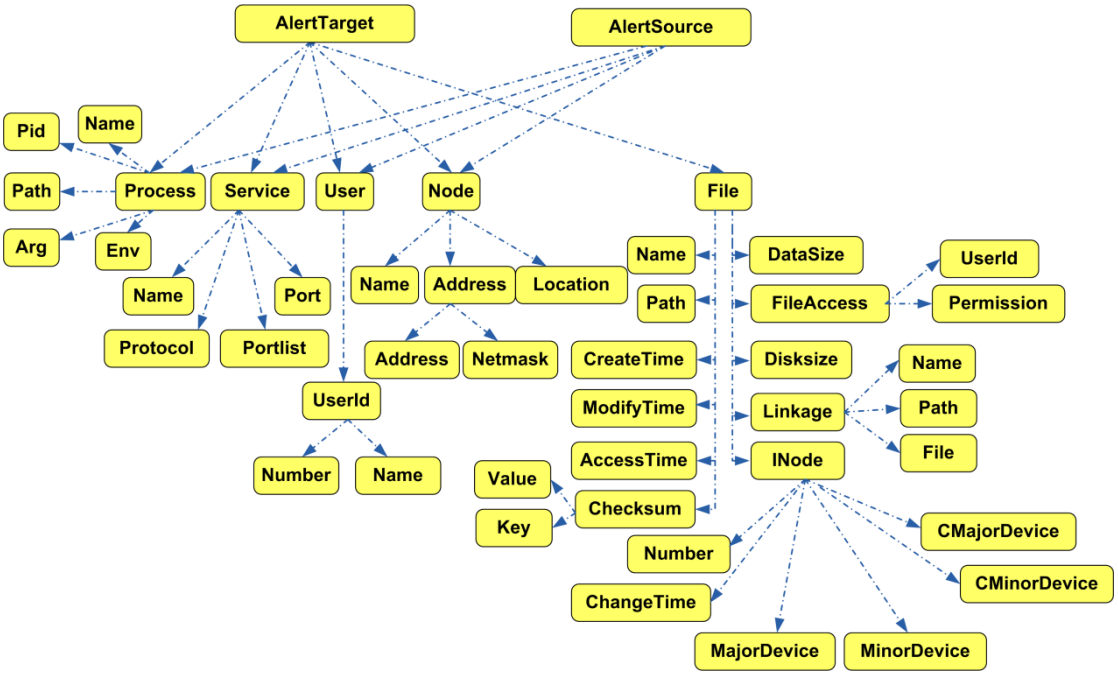
ασφαλείας πληροφοριακών συστημάτων. Οι πληροφορίες αυτές προδιαγράφονται μέσω της κλάσης `Alerts` η οποία συγκεκριμενοποιείται με την υποκλάση `IDMEFalert` που αφορά σε έναν ειδικό τύπο γεγονότων όπως φαίνεται στην Εικόνα 23. Η κλάση αυτή αναφέρεται στην ταξινόμηση μηνυμάτων τύπου συναγερμού που ορίζεται από τη μορφή ανταλλαγής μηνυμάτων ανίχνευσης εισβολών, όπως καθορίζεται στο πρότυπο (Bebar, Curry και Feinstein, 2007) και αποτελεί μια ειδική κατηγορία του μοντέλου, λόγω της ευρείας χρήσης και της σημασίας των μηνυμάτων ειδοποίησης για την εκπλήρωση των καθηκόντων παρακολούθησης της ασφάλειας του δικτύου (π.χ Morin and Debar, 2005). Ο λεπτομερής προσδιορισμός της κλάσης αυτής παρουσιάζεται στις Εικόνες 24 και 25 καθώς επίσης στον Πινάκα 4 καταγράφονται οι οντολογικές ιδιότητες οι οποίες συνδέουν τις βασικές κλάσεις.



Εικόνα 23: Εκτεταμένο σχήμα της Οντολογίας



Εικόνα 24: Η κλάση IDMEFalert



Εικόνα 25: Οι κλάσεις AlertTarget και AlertSource

Ιδιότητα	*Πεδίο Ορισμού*	*Πεδίο Τιμών*
hasAlertCreateTime	IDMEFalert	AlertCreateTime
hasAlertAnalyzerTime	IDMEFalert	AlertAnalyzerTime
hasAlertClassification	IDMEFalert	AlertClassification
hasAlertDetectTime	IDMEFalert	AlertDetectTime
hasAlertSource	IDMEFalert	AlertSource
hasAlertAnalyzer	IDMEFalert	AlertAnalyzer
hasAlertAssesment	IDMEFalert	AlertAssesment
hasAlertAdditionalData	IDMEFalert	AlertAdditionalData
hasAlertTarget	IDMEFalert	AlertTarget
hasReference	AlertClassification	Reference
hasReferenceName	Reference	Name

hasReferenceURL	Reference	URL
hasTargetNode	AlertTarget	Node
hasTargetUser	AlertTarget	User
hasTargetService	AlertTarget	Service
hasTargetProcess	AlertTarget	Process
hasTargetFile	AlertTarget	File
hasSourceProcess	AlertSource	Process
hasSourceNode	AlertSource	Node
hasSourceUser	AlertSource	User
hasSourceService	AlertSource	Service

Πίνακας 3: Οι OWL ιδιότητες της κλάσης Alerts

Συνολικά, οι OWL ιδιότητες, αντικειμενικές και επισημείωσης, που αξιοποιήθηκαν για τη σύνθεση νοημάτων στην Οντολογία απαριθμούνται στον Πίνακα 4.

Ιδιότητα	***Πεδίο Ορισμού***	***Πεδίο Τιμών***
refersToData	Rules	Data
refersToPurpose	Rules	Purposes
refersToRole	Rules	Roles
referesToAction	Rules	Actions
executeObligation	Rules	Obligations
appliesUnderCondition	Rules	Conditions
refersToRule	Rules	Rules
Follows	Obligations	ObligationPatterns
Excludes	ExclusiveCombinations	Data

hasSubject	Conditions	ConditionSubject
hasReferenceObject	Conditions	ReferenceObject
underActivity	Conditions	Activities
has ActivityReference	Conditions	ActiityReference
hasActivityContect	Activities	ContextualBase
underConditionOperator	Conditions	ConditionOperators
underNegativeConditionOperator	Conditions	ConditionOperators
refersToCondition	ConditionOperators	Conditions
isOfOperatorType	ConditionOperators	OperatorTypes
refersToOperator	HistoryEvent	OperatorTypes
isOfType	HistoryEvent	EventTypes
hasEffect	HistoryEvent	EventResult
relatedToData	HistoryEvent	Data
relatedToRole	HistoryEvent	Roles
relatedToPurpose	HistoryEvent	Purposes
relatedToAction	HistoryEvent	Actions
refersToDataSubject	ConditionSubject	Data
refersToDataObject	ConditionObject	Data
refersToRoleSubject	ConditionSubject	Roles
hasContextValue	Conditions	ContexualBase
hasTemporalRelation	Events	Temporal
hasSpatialRelaton	Events	Spatial

linkedWithTime	Temporal	Time
mapsToLocation	LogicalLocation	PhysicalLocation
hasLong	GeographicalLocation	Longtitude
hasAlt	GeographicalLocation	Altitude
hasLat	GeographicalLocation	Latitude
inheritsFromRole	Roles	Roles
isPartOfRole	Roles	Roles
inheritsFromPurpose	Purposes	Purposes
consistOf	Purposes	Purposes
inheritsFromAction	Actions	Actions
isComposedOf	Actions	Actions
inheritsFromData	Data	Data
containsType	Data	Data
moreDetailedThan	Data	Data
appliesToDataDescendants	Rules	-
appliesToPurposeDescendants	Rules	-
appliesToRoleDescendants	Rules	-
appliesToActionDescendants	Rules	
overrideDataubjectPreferences	Rules	-

Πίνακας 4: Οι OWL ιδιότητες της Οντολογίας

Κεφάλαιο 6

Αρχιτεκτονική προτεινόμενης λύσης

Σε αυτό το κεφάλαιο παρουσιάζεται η αρχιτεκτονική του συστήματος το οποίο υλοποιήθηκε και αξιολογήθηκε στο πλαίσιο της παρούσας διατριβής. Μέσω της περιγραφής της αποσαφηνίζονται οι βασικές αρχές και έννοιες που παρουσιάστηκαν στο κεφάλαιο 4 και επιπρόσθετα η χρηστικότητα της προτεινόμενης οντολογίας όσον αφορά στον έλεγχο πρόσβασης με επίγνωση ιδιωτικότητας στα σύγχρονα πληροφοριακά συστήματα.

Η αρχιτεκτονική του συστήματος καθορίζει ένα σύστημα ελέγχου πρόσβασης σύμφωνα με το προσδιορισμένο σημασιολογικό μοντέλο. Αυτό το σύστημα ελέγχου πρόσβασης εγγυάται την εφαρμογή των πολιτικών που παράγονται σύμφωνα με τις απαιτήσεις της ασφάλειας και της ιδιωτικής ζωής που ορίζονται στην Ενότητα 2.2.

Μια απλοϊκή προσέγγιση στο σχεδιασμό αυτού του συστήματος ελέγχου πρόσβασης, κατά την οποία μία υπερ-οντότητα θα συγκεντρώνει όλες τις αποφάσεις ελέγχου πρόσβασης θα ήταν μη ρεαλιστική. Ένα τέτοιο σύστημα δε θα μπορούσε να εφαρμοστεί στον πραγματικό κόσμο, λαμβάνοντας υπόψη τους τεχνικούς και κοινωνικούς διαχωρισμούς μεταξύ διοικητικών τομέων. Για τους λόγους αυτούς, στο σύστημα υιοθετήθηκε μια αποκεντρωμένη και κατανεμημένη προσέγγιση.

Στο πλαίσιο αυτό και προκειμένου να καταστεί δυνατή η ευελιξία της αρχιτεκτονικής είναι απαραίτητη μια προκαταρκτική διαδικασία ελέγχου ταυτότητας και εξουσιοδότησης. Για να επιτευχθεί αυτό, το σύστημα εκμεταλλεύεται το παράδειγμα των Υποδομών Διαχείρισης Δικαιωμάτων (***Privilege Management Infrastructures*** (PMIs)). Πράγματι, ο στόχος του συστήματος είναι να εγγυάται ότι μόνον οντότητες με δεδομένο επίπεδο προνομίων, εξαρτώμενων από τον σκοπό και το πλαίσιο, μπορούν να έχουν τελικά πρόσβαση σε κάποιους από τους πόρους του συστήματος. Οι πόροι μπορεί να αποτελούν αποθηκευμένα δεδομένα, μετά-δεδομένα κτλ. Ενώ μερικές αποφάσεις πρόσβασης βασίζονται σε ad hoc πληροφορία η οποία αποτελεί δυναμικό χαρακτηριστικό και, ως εκ τούτου, πρέπει να αξιολογείται σε πραγματικό χρόνο από τους μηχανισμούς της πολιτικής που βασίζεται, υπάρχουν περιπτώσεις όπου η πρόσβαση εξαρτάται, ή επηρεάζεται από χαρακτηριστικά πλαισίου τα οποία παραμένουν σταθερά για μια συγκεκριμένη χρονική

περίοδο (π.χ., ένας ρόλος). Αυτή η πληροφορία μπορεί να εκτιμηθεί «off-line», και αυτό μπορεί να εκφράζεται μέσω των πιστοποιητικών PMI, με αποτέλεσμα τη μείωση της προσπάθειας που απαιτείται για την «on-line» επεξεργασία και αξιολόγηση.

Όπως προαναφέρθηκε στο Κεφάλαιο 2 οι PMIs επικεντρώνονται σε μια οντότητα που είναι γνωστή ως η Αρχή Εξουσιοδότησης (Source of Authority - SoA), η οποία παράγει και διαχειρίζεται προφίλ εξουσιοδότησης, δικαιώματα και πολιτικές. Οι υπηρεσίες αυτές παρέχονται «off-line», έτσι ώστε οι φορείς που χρησιμοποιούν την υποδομή μπορούν ανεξάρτητα να επαληθεύσουν τα δικαιώματα εξουσιοδότησης, χωρίς την ανάγκη να αλληλεπιδρούν με τη SoA. Με άλλα λόγια, οι PMIs αποτελούν για την εξουσιοδότηση ότι οι Υποδομές Δημοσίου Κλειδιού (Public Key Infrastructures (PKIs)) για τον έλεγχο ταυτότητας. Οι PMIs χρησιμοποιούν πιστοποιητικά ιδιοτήτων (Attribute Certificates -ACs) για να διατηρήσουν τα προνόμια των χρηστών, με τη μορφή των ιδιοτήτων, αντί για τα πιστοποιητικά δημόσιου κλειδιού (Public Key Certificates - PKCs) τα οποία κατέχουν δημόσια κλειδιά. Οι PMIs έχουν τις Αρχές Εξουσιοδότησης (SoAs) και τις Αρχές Ιδιοτήτων (Attribute Authorities - AAs) οι οποίες εκδίδουν πιστοποιητικά ιδιοτήτων αντί για τις Αρχές Πιστοποίησης (Certification Authorities – CAs) οι οποίες εκδίδουν PKCs στους χρήστες. Η SoA είναι συνεπώς ανάλογη με την CA, η οποία δεν έχει ρόλο στο χρόνο εκτέλεσης της λειτουργίας της υποδομής.

Στο προτεινόμενο σύστημα, η SoA ονομάζεται Ελεγκτής Διασφάλισης Ιδιωτικότητας (ΕΔΙ). Παρέχει ταυτοποιήσεις και εξουσιοδοτήσεις, με τη μορφή X.509 πιστοποιητικών, μέσω offline "συμβάσεων" με τις διάφορες οντότητες του συστήματος, σε συμμόρφωση με το σημασιολογικό μοντέλο. Επιπρόσθετα, εφόσον το σημασιολογικό μοντέλο έχει σχεδιαστεί σύμφωνα με τις νομικές και κανονιστικές απαιτήσεις, το σύστημα είναι σύμφωνο με το νομικό και κανονιστικό περιβάλλον στο οποίο αναπτύσσεται. Το ολοκληρωμένο σύστημα ελέγχου πρόσβασης συμπληρώνει αυτό το PMI μοντέλο με την αξιολόγηση κατά το χρόνο εκτέλεσης των αιτήσεων πρόσβασης, ανάλογα με το ρόλο του φορέα που έχει πρόσβαση και της εφαρμογής, καθώς και του πλαισίου στο οποίο εντάσσεται το αίτημα πρόσβασης.

6.1 Εξαγωγή πολιτικών πρόσβασης

Από την οπτική γωνία του ελέγχου πρόσβασης και της εξουσιοδότησης, η διαδικασία μπορεί γενικά να συνοψιστεί ως εξής: ένας δράστης εκτελεί μια εφαρμογή ενός

πληροφοριακού συστήματος έτσι ώστε να εξυπηρετήσει ένα σκοπό και, κατά συνέπεια, ζητάει κάποια δεδομένα τα οποία σχετίζονται με την εφαρμογή. Λόγω του γεγονότος ότι το είδος των δεδομένων μπορεί να αποτελεί ευαίσθητη πληροφορία (π.χ., εφαρμογές τομέα υγείας ή εφαρμογές παρακολούθησης δικτύων) όσον αφορά την ιδιωτικότητα, η εφαρμογή των πολιτικών ιδιωτικότητας αποτελεί βασικό ζήτημα.

Ως εκ τούτου, όπως αναφέρθηκε στο προηγούμενο κεφάλαιο τα θεμέλια της οντολογίας είναι η ίδια η πληροφορία, οργανωμένη με τρόπο που να αντανακλά τις πραγματικές ταξινομήσεις των σχετικών τύπων δεδομένων, τους σκοπούς που αναφέρονται στις υπηρεσίες για τους οποίους τα δεδομένα έχουν συλλεχθεί, τους διαφορετικούς ρόλους των δραστών, τη συναίνεση που δίδεται από τα υποκείμενα των δεδομένων, τις ειδοποιήσεις και άλλες συμπληρωματικές έννοιες, καθώς και τις πολιτικές που διέπουν τη λειτουργία ενός συστήματος όσον αφορά την επιβολή ελέγχου πρόσβασης.

Αυτό σημαίνει ότι οι πολιτικές ιδιωτικότητας θα πρέπει να είναι αρκετά περίπλοκες για να επιβάλλουν διάφορους όρους και περιορισμούς, οι οποίοι συχνά αναφέρονται στη βιβλιογραφία ως «υποχρεώσεις ιδιωτικότητας» (privacy obligations) (Casassa Mont, 2004).

Οι πολιτικές απεικονίζονται μέσα από την Οντολογία χρησιμοποιώντας την κλάση των κανόνων και των στιγμιότυπών της, τα οποία παρέχουν τα μέσα για το συνδυασμό όλων των εννοιών που είναι σχετικές με την πολιτική (δηλαδή τους ρόλους, τις υπηρεσίες, τις δράσεις, τα δεδομένα, τις προϋποθέσεις και τις υποχρεώσεις). Οι κανόνες καθώς και το υπόλοιπο σημασιολογικό μοντέλο αρχικοποιείται από το Διαχειριστή Πολιτικής (Policy Administrator) του συστήματος, ώστε να αντανακλούν τις ειδικές ανάγκες και απαιτήσεις της επιχείρησης.

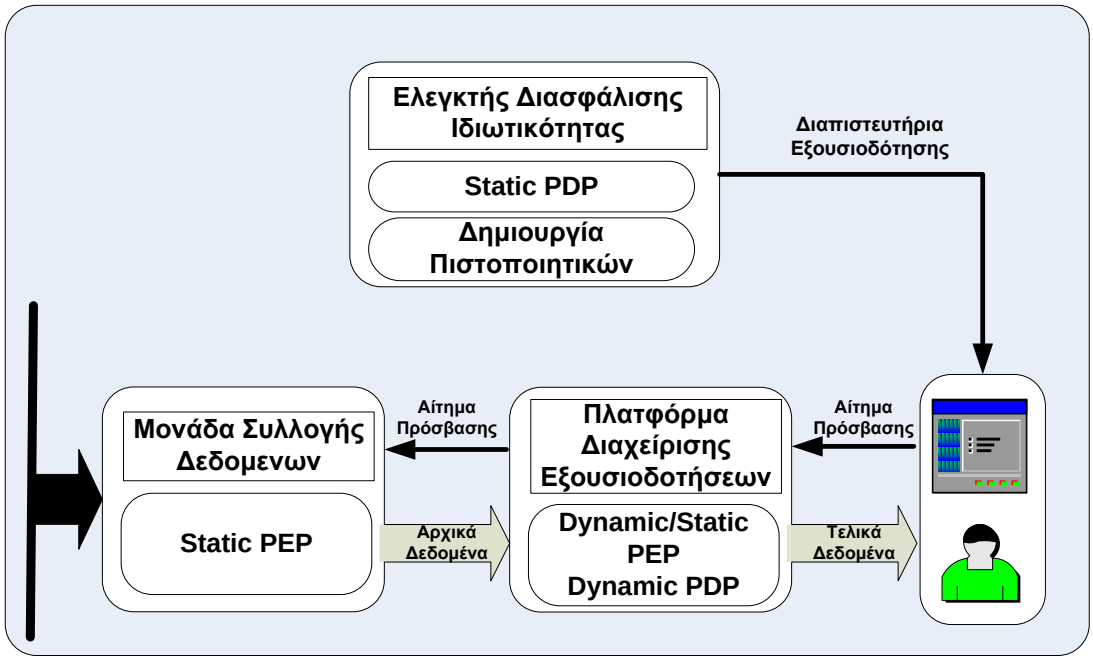
Ωστόσο, ένας ορισμός κανόνα ελέγχου πρόσβασης δεν μπορεί και δεν πρέπει να οδηγήσει σε συγκεκριμένες αποφάσεις για τη χορήγηση άδειας. Πιο συγκεκριμένα, η εφαρμογή ενός κανόνα εξαρτάται από έναν αριθμό σχετικών παραγόντων που όλοι πρέπει να ληφθούν υπόψη πριν από την οριστικοποίηση σε ένα στέρεο τελικό σύνολο κανόνων. Αυτή η αυστηρή διαδικασία η οποία πραγματοποιείται με διαφάνεια από το διαχειριστή πολιτικών περιλαμβάνει μηχανισμούς διάσχισης της Οντολογίας και αλγορίθμους συλλογιστικής και λαμβάνει υπόψη ανάλυση συγκρούσεων, τους αποκλειόμενους συνδυασμούς και τις σημασιολογικές ιεραρχίες πριν παραχθεί το επιθυμητό τελικό σύνολο των κανόνων που ισχύουν.

Παρά την ύπαρξη ενός αριθμού ευρέως γνωστών εργαλείων συλλογιστικής, όπως το εργαλείο Pellet (Sirin et. al, 2007) υλοποιήθηκε ένα προσαρμοσμένο OWL DL εργαλείο γραμμένο σε Java για την παροχή υπηρεσιών συλλογιστικής σε οντολογίες OWL βασισμένο στο Jena API (Jena, 2013), στοχευόμενο στις ανάγκες του προτεινόμενου σημασιολογικού μοντέλου.

6.2 Περιγραφή του συστήματος

Βασιζόμενο σε όλα τα παραπάνω το προτεινόμενο σύστημα αποτελείται από στοιχεία που ενσωματώνουν τη λογική για την λήψη αποφάσεων και την πρόσβαση σε πληροφορίες, ενώ παράλληλα ενεργεί ως ενδιάμεση οντότητα διασφάλισης της ιδιωτικότητας των χρηστών που έχουν ανάγκη από κάποιες υπηρεσίες.

Σε γενικές γραμμές, εάν εξετάσουμε το σύστημα από τη σκοπιά των συστημάτων βασισμένων σε πολιτικές (policy-based systems) (Westerinen et al., 2001), θεωρείται ένα σύστημα απόφασης και εκτέλεσης δύο φάσεων το οποίο αποτελείται από διακριτές οντότητες όπως φαίνεται και στην Εικόνα 26.



Εικόνα 26: Αρχιτεκτονική του συστήματος

Το Σημείο Επιβολής Πολιτικής (Policy Enforcement Point - PEP), το οποίο αποτελεί τον πυρήνα της επιχειρησιακής λογικής και ενσωματώνει λειτουργίες για την εξυπηρέτηση των αιτημάτων των χρηστών. Το Σημείο Επιβολής Πολιτικής διαχωρίζεται μεταξύ δύο οντοτήτων, της Πλατφόρμας Διαχείρισης Εξουσιοδοτήσεων (ΠΔΕ) η οποία αποτελεί το

δυναμικό σημείο και της Μονάδας Συλλογής Δεδομένων (ΜΣΔ) που αποτελεί το στατικό σημείο. Η πρώτη εφαρμόζει πολιτικές που αφορούν την εμπιστοσύνη και τον έλεγχο πρόσβασης μεταξύ αυτής και της Μονάδας Συλλογής Δεδομένων και η δεύτερη εφαρμόζει τον έλεγχο πρόσβασης μεταξύ του χρήστη που αιτείται τα δεδομένα και της Πλατφόρμας Διαχείρισης Εξουσιοδοτήσεων, υλοποιώντας έτσι την έννοια των τελικών επιτρεπόμενων τύπων δεδομένων (*permitted data types PDT*) και όποιων επιπρόσθετων δυναμικών παραμέτρων.

Το Σημείο Απόφασης Πολιτικής (Policy Decision Point - PDP) χρησιμοποιείται για τη λήψη απόφασης εξουσιοδότησης, στο πλαίσιο της παροχής των υπηρεσιών που ζητούνται και αποτελείται από δύο επιμέρους οντότητες: το Στατικό Σημείο Απόφασης Πολιτικής (Static Policy Decision Point (S-PDP)) το οποίο αποτελεί μέρος του Ελεγκτή Διασφάλισης Ιδιωτικότητας και το Δυναμικό Σημείο Απόφασης Πολιτικής (Dynamic Policy Decision Point (D-PDP)) το οποίο αποτελεί μέρος της Πλατφόρμας Διαχείρισης Εξουσιοδοτήσεων.

Το Σημείο Διαχείρισης Πολιτικής (Policy Administration Point - PAP) επονομαζόμενο ως Ελεγκτής Διασφάλισης Ιδιωτικότητας ενσωματώνει λειτουργίες διαχείρισης για τις πολιτικές ασφάλειας που πρέπει να εφαρμόζονται. Αποτελεί επίσης το Στατικό Σημείο Απόφασης Πολιτικής και την οντότητα η οποία καθορίζει και διατηρεί την Οντολογία και λειτουργεί επίσης ως Αρχή Εξουσιοδότησης (Source of Authority (SoA)) κατέχοντας έτσι ένα ζωτικό ρόλο στη υποδομή εξουσιοδότησης. Έχοντας το ρόλο της Αρχής Εξουσιοδότησης, το Σημείο Διαχείρισης Πολιτικής, , αποτελεί την οντότητα εκείνη η οποία θεωρείται απόλυτης εμπιστοσύνης από έναν επαληθευτή εκχωρούμενων δικαιωμάτων και επίσης κατέχει την απόλυτη ευθύνη για την ανάθεση και πιστοποίηση ενός συνόλου ιδιοτήτων.

Τέλος βασική οντότητα του συστήματος αποτελούν οι χρήστες ή οι εφαρμογές μέσω των οποίων τα δεδομένα αιτούνται από το σύστημα.

6.3 Διαδικασία συλλογιστικής

Η διαδικασία της εξαγωγής συμπερασμάτων και συλλογιστικής στη βάση ενός συνόλου κανόνων εξουσιοδότησης, αποτελεί τον πυρήνα της επιχειρησιακής λογικής της προτεινόμενης λύσης. Με στόχο την αύξηση της κλιμακοθετησιμότητας του συστήματος οι συγκεκριμένες λειτουργικότητες στο πλαίσιο της λειτουργίας του συστήματος

πραγματοποιούνται στη λογική του σαφούς διαχωρισμού τους σε διαδικασίες «στατικής» και «δυναμικής» συλλογιστικής.

6.3.1 Στατική συλλογιστική

Πιο λεπτομερώς, ένα βασικό συμπέρασμα που μπορεί να εξαχθεί σε σχέση με το υιοθετημένο μοντέλο πληροφοριών και των ακολουθούμενων κανόνων συλλογιστικής, αφορά το γεγονός ότι η αποσαφήνιση των ισχυουσών εξουσιοδοτήσεων μπορεί να πραγματοποιηθεί πριν καν την καταχώρηση σχετικών αιτημάτων για εξουσιοδότηση, τουλάχιστον σε σχέση με τα θεμελιώδη συστατικά τους (τύπος δεδομένων, ρόλος, δράση και σκοπός πρόσβασης). Έτσι, ο όρος της στατικής συλλογιστικής εισήχθηκε για να περιγράψει τις διαδικασίες εκτίμησης του συνόλου των εξουσιοδοτήσεων βάσει παραμέτρων που παραμένουν σταθερές για το χρονικό διάστημα κατά το οποίο η οντολογία δε μεταβάλλεται και περιγράφουν μια *a priori* θεώρηση του συστήματος (π.χ. οι συσχετίσεις μεταξύ ρόλων, δράσεων και σκοπών πρόσβασης, δηλαδή τα στιγμιότυπα του συνόλου *PAR*, ορίζονται άπαξ πριν την εκκίνηση της λειτουργίας του συστήματος).

Στόχος των διαδικασιών στατικής συλλογιστικής αποτελεί η αποσαφήνιση του συνόλου των ισχυουσών εξουσιοδοτήσεων στη βάση των κανόνων που έχουν δημιουργηθεί από τις οντότητες του συστήματος. Πιο συγκεκριμένα, σε αυτή τη φάση της διαδικασίας συλλογισμού εξετάζονται όλες οι πιθανές σημασιολογικές δηλώσεις όπως αυτές προκύπτουν από την Οντολογία και υπό το πρίσμα των προαναφερθέντων κανόνων συμπερασμού, με στόχο την καταγραφή όλων εκείνων των συνδυασμών στιγμιότυπων που περιγράφουν θετικές εξουσιοδοτήσεις. Οι εξουσιοδοτήσεις-αποτελέσματα των διαδικασιών στατικής συλλογιστικής συνιστούν στοιχεία του συνόλου *PDT*, συσχετισμένα με σύνολα ρόλων, δράσεων και σκοπών πρόσβασης, καθώς και δηλώσεις των απαραίτητων συνθηκών που καθορίζουν την ισχύ της εξουσιοδότησης και των υποχρεώσεων που απορρέουν από την εφαρμογή της. Σημειώνεται ότι στοιχεία του συνόλου *PDT* δύναται φυσικά να προέρχονται από ευθείς εξουσιοδοτήσεις αλλά και από σχετικές πολιτικές μεταφοράς δικαιωμάτων.

Σε αυτό το σημείο αξίζει να σημειωθεί ότι δόθηκε έμφαση στη διατήρηση της ποιότητας της μη μονοτονικότητας κατά την παραγωγή εξουσιοδοτήσεων. Αν και προφανής στόχος των λειτουργιών στατικής συλλογιστικής είναι η εξακρίβωση των θετικών εξουσιοδοτήσεων, η δυνατότητα προδιαγραφής αρνητικών πολιτικών εξουσιοδότησης επιτρέπει στο σύστημα να διαχειρίζεται τις δηλώσεις εξουσιοδότησης με μη μονοτονικό

τρόπο, καθώς η προδιαγραφή προστιθέμενων κανόνων δεν ισοδυναμεί αυστηρά με την προσθήκη περισσότερων εξουσιοδοτήσεων.

Όπως προαναφέρθηκε, για τη διεκπεραίωση των λειτουργιών στατικής συλλογιστικής υιοθετήθηκαν δυο διαφορετικές προσεγγίσεις. Η πρώτη περιλαμβάνει το ευρέως διαδεδομένο εργαλείο λογισμικού Pellet (Sirin et al., 2007) που παρέχει υπηρεσίες συλλογιστικής για οντολογίες σχεδιασμένες στη γλώσσα OWL. Η δεύτερη μέθοδος αντιστοιχεί στην αξιοποίηση ενός τυπικού λογισμικού παραγωγής συμπερασμάτων που υλοποιήθηκε στο πλαίσιο της εκπόνησης της παρούσας διατριβής, προσαρμοσμένο ακριβώς στις ανάγκες εξαγωγής συμπερασμάτων του σχήματος της Οντολογίας. Το εργαλείο αναπτύχθηκε στη γλώσσα προγραμματισμού Java, ενώ εκμεταλλεύεται της δυνατότητες υποβολής ερωτημάτων σε οντολογίες της βιβλιοθήκης Jena (2013). Πέραν της περιγραφής της λειτουργίας των δύο εργαλείων λογισμικού συλλογιστικής, στη συνέχεια πραγματοποιείται μια συνοπτική σύγκριση της απόδοσής τους όπως αυτή αξιολογήθηκε μέσω μιας σειράς διαφορετικών πειραμάτων λειτουργίας με εικονικές Οντολογίες. Οι εικονικές εκδόσεις της Οντολογίας δημιουργήθηκαν με στόχο την εκτίμηση της χρονικής διάρκειας των διαδικασιών συλλογιστικής ανάλογα με το συνολικό μέγεθος της οντολογίας δείγματος, σε ότι αφορά το σύνολο των αντικειμένων της. Ο Πίνακας 5 απεικονίζει τις διαφορετικές εκδόσεις της Οντολογίας, συνοδευόμενες από το μέγεθός τους. Σημειώνεται, ότι οι εκδόσεις των εικονικών οντολογιών δημιουργήθηκαν αυτόματα από κατάλληλα σχεδιασμένο λογισμικό και επομένως χαρακτηρίζονται από μεγάλο βαθμό τυχαιότητας σε ότι αφορά την πολυπλοκότητα των αντικειμενικών OWL ιδιοτήτων. Το γεγονός αυτό επιτρέπει την εξαγωγή κυρίως γενικών συμπερασμάτων για τις διαδικασίες στατικής συλλογιστικής και τις επιδόσεις τους.

Έκδοση	***Αντικείμενα Data***	***Αντικείμενα Purposes***	***Αντικείμενα Roles***	***Αντικείμενα Rules***	***Συνολικά Αντικείμενα***
A	500	750	100	300	1650
B	1000	750	100	300	2150
C	500	1500	200	300	2500
D	500	750	100	300	1650
E	500	750	100	600	1950
F	1500	750	100	300	2650
G	2000	750	100	300	3150

H	500	2250	100	300	3150
I	500	3000	100	300	3900
J	500	750	300	300	1850
K	500	750	400	300	1950
L	500	750	100	900	2250
M	500	750	100	1200	2550
N	1000	1500	200	600	3300
O	1500	2250	300	900	4950
P	2000	3000	400	1200	6600

Πίνακας 5: Διαφορετικές εκδόσεις εικονικών Οντολογιών Εξουσιοδότησης

Παραγωγή Συμπερασμάτων με Χρήση του Pellet

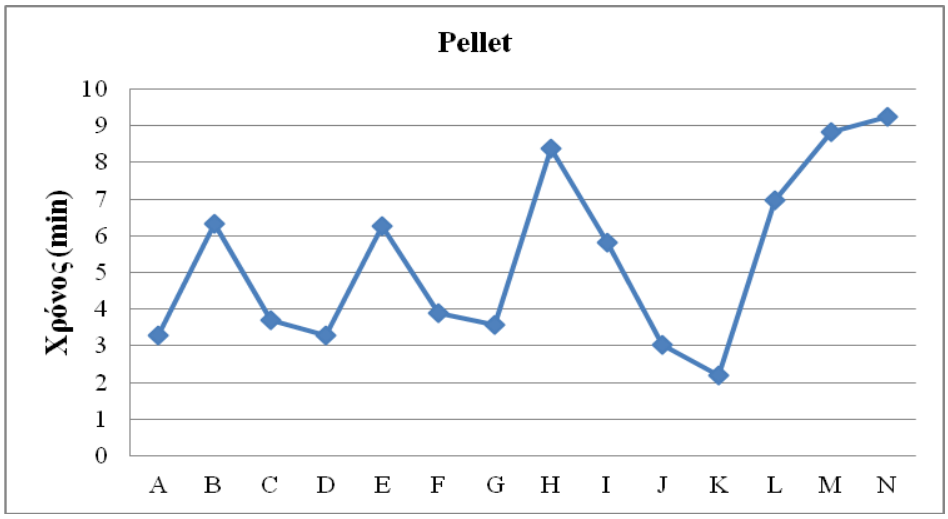
Το λογισμικό Pellet αποτελεί ένα διαδεδομένο εργαλείο λογισμικού ανοιχτού κώδικα για την παραγωγή συμπερασμάτων σε οντολογίες OWL. Ως ολοκληρωμένο εργαλείο προσφέρει μια πλούσια ποικιλία υπηρεσιών συλλογιστικής όπως, ολοκλήρωση με τις βιβλιοθήκες Jena και OWL, αξιοποίηση κανόνων συλλογιστικής της γλώσσας Semantic Web Rule Language (SWRL) και έλεγχο συνοχής οντολογιών μεταξύ άλλων. Για τις ανάγκες της διατριβής, το εργαλείο χρησιμοποιήθηκε σε συνδυασμό με την προδιαγραφή συγκεκριμένων κανόνων συμπερασμού στη γλώσσα SWRL. Οι κανόνες καταγράφονται στη μορφή επαγωγής μεταξύ μιας υπόθεσης και ενός συμπεράσματος και μπορούν να ερμηνευτούν ως εξής: *όταν οι συνθήκες της υπόθεσης ισχύουν τότε ισχύουν και οι συνθήκες του συμπεράσματος*. Για παράδειγμα, η μεταφερσιμότητα των κανόνων ελέγχου πρόσβασης μεταξύ δύο τύπων δεδομένων που συνδέονται με την OWL ιδιότητα *inheritsFromData*, συμβατή με τη σύνταξη της γλώσσας SWRL, παρουσιάζεται στην Εικόνα 27.

Η Εικόνα 28 συνοψίζει την επίδοση του εργαλείου Pellet σε ότι αφορά τον συνολικό χρόνο εκτέλεσής του για την εξαγωγή όλων των στιγμιότυπων *PDT* στη βάση των διαφορετικών εκδόσεων της Οντολογίας. Αποδεικνύεται, ότι οι χρόνοι λειτουργίας του εργαλείου επηρεάζονται μερικώς από τον συνολικό αριθμό αντικειμένων της οντολογίας, όσο αυτός διατηρείται εντός κάποιου ορίου (οντολογίες A, D, J, K και E). Ωστόσο, καθώς ο αριθμός των στιγμιότυπων των οντολογικών κλάσεων αυξάνεται, οι μετρήσεις αποδεικνύουν μια πιο άμεση επίδραση στον χρόνο εκτέλεσης, αρχικά μικρή και τελικά απαγορευτική, σε σημείο που το λογισμικό δεν ολοκληρώνει επιτυχημένα την εκτέλεσή του (οντολογίες O και P). Τέλος, απεικονίζεται εμφανώς η επιρροή του μεγέθους του συνόλου

των κανόνων εξουσιοδότησης στον συνολικό χρόνο εκτέλεσης, σε μια σχεδόν γραμμική σχέση (οντολογίες A, E, L και M).

```
<swrl:Imp rdf:about="OntRule1">
	<swrl:head rdf:parseType="Collection">
		<swrl:IndividualPropertyAtom>
		<swrl:propertyPredicate rdf:resource="#refersToData" />
			<swrl:argument1 rdf:resource="#x" />
			<swrl:argument2 rdf:resource="#z" />
		</swrl:IndividualPropertyAtom>
	</swrl:head>
	<swrl:body rdf:parseType="Collection">
		<swrl:ClassAtom>
			<swrl:classPredicate rdf:resource="#Rules" />
			<swrl:argument1 rdf:resource="#x" />
		</swrl:ClassAtom>
		<swrl:IndividualPropertyAtom>
			<swrl:propertyPredicate rdf:resource="#refersToData"
/>
			<swrl:argument1 rdf:resource="#x" />
			<swrl:argument2 rdf:resource="#y" />
		</swrl:IndividualPropertyAtom>
		<swrl:IndividualPropertyAtom>
		<swrl:propertyPredicate rdf:resource="#inheritsFromData" />
			<swrl:argument1 rdf:resource="#z" />
			<swrl:argument2 rdf:resource="#y" />
		</swrl:IndividualPropertyAtom>
	</swrl:body>
</swrl:Imp>
```

Εικόνα 27: Ενδεικτικός κανόνας SWRL



Εικόνα 28: Χρόνος εκτέλεσης λογισμικού Pellet

Παραγωγή Συμπερασμάτων με Χρήση του Προσαρμοσμένου Λογισμικού

Το λογισμικό παραγωγής συμπερασμάτων που υλοποιήθηκε στο πλαίσιο της εκπόνησης της παρούσας διατριβής βασίστηκε στις δυνατότητες υποβολής οντολογικών ερωτημάτων (ontology queries) της βιβλιοθήκης Jena και στην εφαρμογή ενός αλγορίθμου διάσχισης της Οντολογίας. Ο εν λόγω αλγόριθμος αποτελεί ένα σχήμα διάσχισης γράφων

οριζόντιας διερεύνησης (Breadth First Search – BFS), όπου κάθε στιγμιότυπο της κλάσης *Roles* αντιστοιχίζεται στιγμιότυπα της κλάσης *Purposes* και τελικά με Επιτρεπτούς Τύπους Δεδομένων *PDTs*. Οι ίδιοι κανόνες συλλογιστικής που εφαρμόστηκαν στην περίπτωση του εργαλείου Pellet προδιαγράφηκαν και εφαρμόστηκαν και στην περίπτωση του προσαρμοσμένου λογισμικού με χρήση της βιβλιοθήκης Jena.

Ο αλγόριθμος υπολογισμού των αντικειμένων του συνόλου *PDT*, σύμφωνα με τους κανόνες ελέγχου πρόσβασης παρουσιάζεται στην Εικόνα 29. Πανομοιότυπος αλγόριθμος, αξιοποιείται και για την εξαγωγή των *PDT* αντικειμένων, όπως αυτά προκύπτουν από κανόνες μεταφοράς δικαιωμάτων και προώθησης δεδομένων.

Επιπλέον των μετρήσεων σχετικά με τον χρόνο εκτέλεσης του λογισμικού στη βάση των διαφορετικών εκδόσεων της Οντολογίας, πραγματοποιήθηκαν μετρήσεις του χρόνου εξαγωγής καθενός διακριτού αντικειμένου του συνόλου *PDT* με στόχο την αναγνώριση των μέσων χρόνων απόκρισης του λογισμικού σε μοναδικά οντολογικά ερωτήματα (Πίνακας 6).

```
PDTAlg ()
{
for each (instance of the Roles class)
{
       for each (instance of the Rules class that has refersToRole property
       referring to the Role instance under investigation)
       {
       associate Role instance to Rule instance in a "Role to
       Rules" map;
       }
}
for each (Role entry of the "Role to Rules" map)
{
       for each (Rule entry)
       {
              if (appliesToRoleDescendants property is YES)
              {
              for each (instance of the Roles class that is linked
              with the Role entry under investigation via an
              inheritsFromRole property)
                     {
                     add association of Role instance to the Rule entry
                     under investigation in the "Role to Rules" map;
                     }
                     for each (instance of the Roles class that is linked
                     with the Role entry under investigation via an
                     isPartOfRole property)
                     {
                     if (DisclosureOfData property is YES)
                     add association of Role instance to the Rule
                     entry under investigation in the "Role to
                     Rules" map;
                     }
                     for each (instance of the Roles class that is linked
                     with the Role entry under investigation via an
                     containsRole property)
                     {
```

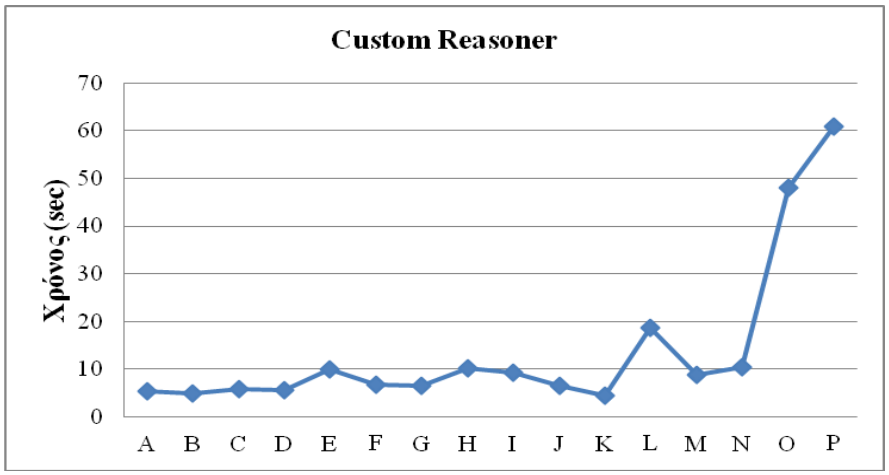
```
                        if ((DisclosureOfData property is YES)&&(all
                        similarly linked instances of the Roles class
                        have the same Rule applied with the same
                        values))
                        add association of Role instance to the Rule
                        entry under investigation in the "Role to
                        Rules" map;
                        if (DisclosureOfData property is NO)
                        add association of Role instance to the Rule
                        entry under investigation in the "Role to
                        Rules" map;
                    }
                }
        }
}

for each (instance of the Purposes class)
{
for each (instance of the Rules class that has refersToPurpose property referring
to the Purpose instance under investigation)
        {
        associate Purpose instance to Rule instance in a "Purpose to
        Rules" map;
        }
}
for each (Purpose entry of the "Purpose to Rules" map)
{
        for each (Rule entry)
        {
        if (appliesToPurposeDescendants property is YES)
                {
                for each (instance of the Purposes class linked
                with the Purpose entry under investigation via an
                inheritsFromPurpose property)
                        {
                        add association of Purpose instance to the Rule entry
                        under investigation in the "Purpose to Rules" map;
                        }

                        for each (instance of the Purposes class linked
                        with the Purpose entry under investigation via an
                        isPartOfPurpose property)
                        {
                        if (DisclosureOfData property is YES)
                        add association of Purpose instance to the Rule
                        entry  under investigation in the "Purpose to
                        Rules" map;
                        }
                        for each (instance of the Purposes class linked
                        with the Purpose entry under investigation via an
                        containsOfPurpose property)
                        {
                        if ((DisclosureOfData property is YES)&&(all
                        similarly linked instances of Purposes  have
                        the sane Rule applied with the same values))
                        add association of Purpose instance to the Rule
                        entry under investigation in the "Purpose to
                        Rules" map;
                                if (DisclosureOfData property is NO)
                                add association of Purpose instance to the Rule
                                entry under investigation in the "Purpose to
                                Rules" map;
                        }
                }
        }
```

```
}

for each (instance of the Data class)
{
       for each (instance of the Rules class that has refersToData property
       referring to the Data instance under investigation)
       {
       associate Data instance to Rule instance in a
       "Data to Rules" map;
       }
}
for each (Data entry of the "Data to Rules" map)
{
       for each (Rule entry)
       {
              if (appliesToDataDescendants property is YES)
              {
              for each (instance of the Data class that is
              linked with the Data entry under investigation
              via an inheritsFromData property)
                     {
                     add association of Data instance to the Rule
                     entry under investigation in the "Data to
                     Rules" map;
                     }
                     for each (instance of the Data class that is
                     linked with the Data entry under investigation
                     via an isPartOfData property)
                     {
                            if (DisclosureOfData property is YES)
                            add association of Data instance to the
                            Rule entry under investigation in the
                            "Data to Rules" map;
                     }
                     for each (instance of the Data class that is
                     linked with the Data entry under investigation
                     via a containsData property)
                     {
                            if ((DisclosureOfData property is YES)&&(all
                                   similarly linked instances of the Data
                            class have the same Rule applied with the same
                            values))
                            add association of Data instance to the
                                   Rule entry under investigation in the
                            "Data to Rules" map;
                            if (DisclosureOfData property is NO)
                            add association of Data instance to the
                            Rule entry under investigation in the
                            "Data to Rules" map;
                     }
              }
       }
}

for each (instance of the Rules class)
{
       find intersection between "Roles to Rules", "Purposes to Rules" and
       "Data to Rules" maps;
       add Role, Purpose, Data triples into PDT set;
}
for each (instance of the created PDT set)
{
       if ((multiple Rules apply to the PDT instance)&&(these Rules have
       different values in their DisclosureOfData property))
```

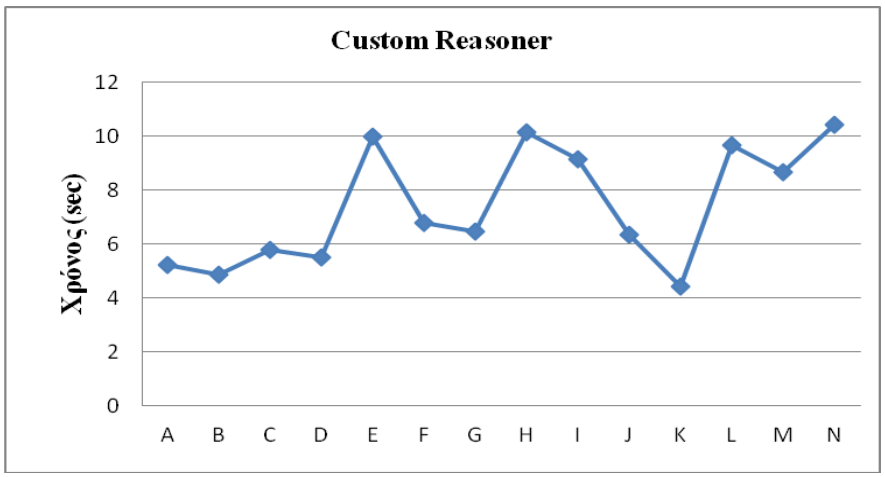
```
        apply the Rule originally applied to the "closest" Role, Purpose or
        Data instance;
}
return (PDT set);
}
```

Εικόνα 29: Αλγόριθμος υπολογισμού των αντικειμένων του συνόλου *PDT*

Τα διεξαχθέντα πειράματα ανέδειξαν μια κοινή συμπεριφορά του προσαρμοσμένου λογισμικού με αυτή του εργαλείου Pellet σε ότι αφορά την επίδραση των διαφορετικών εκδόσεων της Οντολογίας στον συνολικό χρόνο εκτέλεσης του αλγορίθμου συλλογισμού, καθώς και τα δύο παρουσιάζουν παρόμοια «ευαισθησία» στην αύξηση του αριθμού των κανόνων εξουσιοδότησης (Εικόνα 30). Η ομοιότητα αυτή αποσαφηνίζεται από μια παραλλαγή της γραφικής παράστασης, όπου παραλείπονται τα σημεία στα οποία το εργαλείο Pellet δεν ολοκλήρωσε την εκτέλεσή του (Εικόνα 31).



Εικόνα 30: Χρόνος εκτέλεσης λογισμικού παραγωγής συμπερασμάτων (1)



Εικόνα 31: Χρόνος εκτέλεσης λογισμικού παραγωγής συμπερασμάτων (2)

Έκδοση Οντολογίας	Χρόνος εξαγωγής μοναδικού αντικειμένου	Max/Min χρόνος (nsec)
A	32182766	*Max*
	23067	*Min*
B	24787451	*Max*
	22757	*Min*
C	2472278	*Max*
	35779	*Min*
D	5378962	*Max*
	22671	*Min*
E	27663464	*Max*
	38441	*Min*
F	118927123	*Max*
	22590	*Min*
G	1060466	*Max*
	34927	*Min*
H	33868376	*Max*
	37207	*Min*
I	28045845	*Max*
	35237	*Min*
J	25306220	*Max*
	35372	*Min*
K	1087368	*Max*
	35904	*Min*
L	20509455	*Max*
	39127	*Min*
M	5669407	*Max*
	34597	*Min*
N	711351213	*Max*
	35177	*Min*
O	750146683	*Max*
	38335	*Min*
P	987565990	*Max*
	35543	*Min*

Πίνακας 6: Χρόνος εξαγωγής μοναδικών αντικειμένων του συνόλου *PDT*

Αποκρυπτογραφώντας τα παραπάνω διαγράμματα, γίνεται εμφανές ότι η διαδικασία παραγωγής συλλογισμών δεν είναι κατάλληλη για διεξαγωγή σε πραγματικό χρόνο κατά τη διάρκεια λειτουργίας της πλατφόρμας. Ακόμα και στην περίπτωση μοναδικών ερωτημάτων στις οντολογίες προκύπτει ότι η εξαγωγή απόφασης μπορεί να διαρκέσει έως 1 sec.

Ωστόσο, οι συγκεκριμένες χρονικές απαιτήσεις δεν είναι απόλυτες, καθώς για να θεωρηθεί η εξαχθείσα απόφαση τελική είναι απαραίτητη η διεξαγωγή πολλαπλών ακόμα αιτημάτων στις οντολογίες για την εύρεση κανόνων που είναι δυνατόν να επηρεάζουν την αρχική απόφαση. Επιπλέον, δεδομένης της καταχώρησης πολλαπλών διαφορετικών ταυτόχρονων ερωτημάτων σε πραγματικές συνθήκες, η διαχείριση των διαδικασιών στατικής συλλογιστικής σε πραγματικό χρόνο κρίνεται υπολογιστικά ασύμφορη. Επομένως στο πλαίσιο της λειτουργίας της πλατφόρμας οι εργασίες στατικής συλλογιστικής πραγματοποιούνται πριν την εκκίνηση του συστήματος κατά τη φάση διαμόρφωσης της υποδομής, όπως θα περιγραφεί σε επόμενη ενότητα.

Παράλληλα, είναι προφανής η βελτίωση του χρόνου απόκρισης του προσαρμοσμένου λογισμικού έναντι των επιδόσεων του εργαλείου Pellet. Εν μέρει, η σημαντική διαφορά στους χρόνους οφείλεται στην ποικιλία των περιφερειακών ενεργειών που εφαρμόζει το Pellet, όπως είναι ο έλεγχος της συνοχής της οντολογίας και των εμπλεκόμενων δηλώσεων. Αντίθετα, η λογική του προσαρμοσμένου λογισμικού είναι επικεντρωμένη αποκλειστικά στην εξαγωγή των αποτελεσμάτων εξουσιοδότησης, δουλεύοντας στην υπόθεση της δεδομένης συνοχής της οντολογίας.

Επιπρόσθετα, το προσαρμοσμένο εργαλείο εργάζεται οικονομώντας χρόνο απόκρισης σε ερωτήματα καθώς συμβουλεύεται μια κατάλληλα σχεδιασμένη γνωσιακή βάση, που δημιουργείται σε προκαταρκτικό επίπεδο. Τέλος, οι επιπτώσεις της διεύρυνσης των οντολογιών από άποψη στιγμιότυπων είναι περισσότερο εμφανείς στην περίπτωση του Pellet, το οποίο μάλιστα ολοκληρώνει εσφαλμένα την εκτέλεσή του όταν λειτουργεί στη βάση των δύο ογκωδέστερων οντολογιών (οντολογίες O και P). Η επίδοση του προσαρμοσμένου λογισμικού επηρεάζεται επίσης αλλά με πιο ανεκτό υπολογιστικά τρόπο.

6.3.2 Δυναμική συλλογιστική

Η δυναμική συλλογιστική αντιστοιχεί στην εκτίμηση δυναμικών παραμέτρων που αποκτούν υπόσταση μόνο σε πραγματικό χρόνο (π.χ. η εξακρίβωση της τρέχουσας ώρας κατά την καταχώρηση αιτήματος δεν μπορεί παρά να ελεγχθεί σε πραγματικό χρόνο). Με αυτόν τον τρόπο, οι διαδικασίες δυναμικής συλλογιστικής παρέχουν τη δυνατότητα στο σύστημα να διατηρεί χαρακτηριστικά «αυτό-προσαρμοστικότητας» σε σχέση με δυναμικές μεταβολές παραμέτρων του περιβάλλοντος λειτουργίας.

Ως εκ τούτου, η δυναμική συλλογιστική διαδικασία αναλαμβάνει τον έλεγχο του συνόλου των δεδομένων που θα παραδοθεί τελικά στην αιτούσα οντότητα, μετά την εξαγωγή των στατικών πολιτικών που βασίζεται στους κανόνες, και με βάση τις γενικές πληροφορίες, έχοντας ως αφετηρία το σύνολο *PDT* συνοδευμένο από συγκεκριμένα στιγμιότυπα συνθηκών και υποχρεώσεων.

Για παράδειγμα, ένας χρήστης έχοντας ένα συγκεκριμένο ρόλο που ορίζεται από το πιστοποιητικό ιδιοτήτων του, όπως θα δούμε και στη συνέχεια, κάνει αίτηση για τη λήψη δεδομένων, προκειμένου να επιτευχθεί ένας συγκεκριμένος σκοπός. Από τη δυναμική συλλογιστική άποψη, πρέπει να πληρούνται ειδικές προϋποθέσεις κατά την ενεργοποίηση των δικαιωμάτων του ρόλου προκειμένου να επιτευχθεί ο σκοπός, αλλιώς η πρόσβαση στα δεδομένα περιορίζεται περαιτέρω. Με άλλα λόγια, οι περιορισμοί αυτοί επιβάλλουν περαιτέρω περιορισμούς για το σύνολο των δεδομένων που τελικά θα παραδοθεί στο χρήστη έχοντας ως αφετηρία το αντίστοιχο σύνολο δεδομένων (ένα υποσύνολο των *PDT*), που αποτελεί το προϊόν της στατικής συλλογιστικής, αλλά μπορεί να επίσης να οδηγήσει σε περιορισμό ολόκληρου του συνόλου των προνομίων του χρήστη.

Συνεπώς, η διαδικασία δυναμικής συλλογιστικής είναι επιφορτισμένη με τον έλεγχο εκείνων των δυναμικών παραμέτρων που καθορίζουν την ισχύ των συνθηκών που με τη σειρά τους ορίζουν την ισχύ του κανόνα εξουσιοδότησης και την εφαρμογή των κατάλληλων περιορισμών/υποχρεώσεων. Πιο συγκεκριμένα, εξετάζεται η ισχύς των χωρικών, χρονικών και των βασισμένων σε συμβάντα συνθηκών, καθώς και η ύπαρξη αμοιβαίως αποκλειόμενων συνδυασμών τύπων δεδομένων και εξουσιοδοτήσεων. Στις περιπτώσεις εξακρίβωσης των συνθηκών σε κανόνες μεταφοράς δικαιωμάτων, το δυναμικό τμήμα της συλλογιστικής διαδικασίας είναι αρμόδιο να εξετάσει επιπρόσθετα την ισχύ των συνθηκών του κανόνα ελέγχου πρόσβασης. Έτσι, εξασφαλίζεται ότι οι ενέργειες μεταφοράς δικαιωμάτων δε θα διεξαχθούν έχοντας ως αντικείμενό τους δικαιώματα και εξουσιοδοτήσεις που δεν υφίστανται κατά τη χρονική στιγμή του ελέγχου.

Σε ό,τι αφορά την πιθανότητα ύπαρξης πολλαπλών κανόνων εξουσιοδότησης για το ίδιο σύνολο (dt_i, pu_j, a_l, r_k) από διαφορετικούς χρήστες του συστήματος, αναγνωρίζονται δύο περιπτώσεις:

1. Πολλαπλές θετικές εξουσιοδοτήσεις, οπότε το δυναμικό τμήμα της συλλογιστικής διαδικασίας είναι υπεύθυνο για τον έλεγχο του συνόλου των συνθηκών, αλλά και για την εφαρμογή του συνόλου των υποδεικνυόμενων υποχρεώσεων.

2. Αντικρουόμενοι κανόνες (ύπαρξη τόσο θετικής όσο και αρνητικής εξουσιοδότησης), όπου αποδίδεται απόλυτη προτεραιότητα στις προτιμήσεις των υποκείμενων των δεδομένων για τα οποία προέκυψαν οι αντικρουόμενοι κανόνες. Στο ενδεχόμενο που μια οντότητα, παρά την απόλυτη προτεραιότητα που της αναγνωρίζεται, είναι διατεθειμένη να αποδεχτεί τις προτιμήσεις κάποιας άλλης οντότητας που έχει προδιαγράψει συγγενή κανόνα (ορίζοντας αρνητικά την OWL σημαία *overrideDataSubjectPreferences*), η δυναμική συλλογιστική αποδίδει αυτόματα προτεραιότητα στους κανόνες αυτής. Η ίδια λογική υιοθετείται και στις περιπτώσεις που προκύπτουν αντιφάσεις μεταξύ των συνθέσεων των συνθηκών (που αναφέρονται στο ίδιο υποκείμενο και αντικείμενο) θετικών εξουσιοδοτήσεων. Πρέπει να σημειωθεί πως ο εν λόγω μηχανισμός παρότι περιγράφεται στην παρούσα διατριβή η υλοποίηση του αποτελεί αντικείμενο μελλοντικής εργασίας.

Σε ό,τι αφορά την εξακρίβωση του συνόλου των αμοιβαίως αποκλειόμενων συνδυασμών τύπων δεδομένων κατά τη διενέργεια της δυναμικής συλλογιστικής, οι ακόλουθοι κανόνες συλλογιστικής εφαρμόζονται:

$\forall\ (dt_i, dt_j, exc_k)$,

- $inheritsFrom(dt_i, dt_j) \wedge excludes(exc_k, dt_i) \rightarrow excludes(exc_k, dt_j)$
- $isPartOf(dt_i, dt_j) \wedge excludes(exc_k, dt_i) \rightarrow excludes(exc_k, dt_j)$

, όπου exc_k *ένα* στιγμιότυπο της κλάσης *ExclusiveCombinations* και το κατηγόρημα $excludes(exc_k, dt_i)$ η δήλωση της συμμετοχής του dt_i στο στιγμιότυπο exc_k.

Η εξακρίβωση των αμοιβαίως αποκλειόμενων συνδυασμών εξουσιοδοτήσεων συνιστά πιο άμεση διαδικασία καθώς οι κανόνες εξουσιοδότησης (στιγμιότυπα της κλάσης Rules) δε διατηρούν σχέσεις κληρονομικότητας μεταξύ τους και, επομένως, δε συνεπάγεται την εφαρμογή εξειδικευμένων κανόνων συλλογιστικής.

Μια ενδιαφέρουσα πτυχή που πρέπει να επισημανθεί εδώ αφορά το διαχωρισμό πληροφοριών πλαισίου μεταξύ του πλαισίου του ρόλου και του πλαισίου κάθε χρήστη. Για

παράδειγμα, ένας περιορισμός μπορεί να ισχυρίζεται ότι "ένας ρόλος *r* μπορεί να διαβάσει τα δεδομένα dt_j μόνο κατά τη διάρκεια των ωρών εργασίας του". Παρ 'όλα αυτά, οι ώρες εργασίας δεν μπορεί να είναι εξειδικευμένες για το ρόλο αυτό, αλλά εξαρτώνται από κάθε χρήστη. Για να ξεπεραστεί αυτό, η προσέγγιση που ακολουθείται αντιστοιχίζει τις τιμές αυτές σε κάθε χρήστη και καταχωρεί τις σχετικές σημασιολογικές τιμές σε ένα πιστοποιητικό ιδιοτήτων όπως θα περιγραφεί στην ενότητα 6.4.

6.4 Ψηφιακά Πιστοποιητικά: Δομή και Διαχείριση

Αυτή η ενότητα παρέχει μια λεπτομερή περιγραφή της δομής και διαχείρισης των πιστοποιητικών που χρησιμοποιούνται στα πλαίσια της προτεινόμενης λύσης, προκειμένου να επιτευχθούν οι σκοποί αυθεντικοποίησης και εξουσιοδότησης. Προς την αυτοματοποίηση των διαδικασιών λήψης απόφασης και για την κατάλληλη απόδοση των εννοιών και αναπαράσταση των συσχετίσεων που προκύπτουν από τη λειτουργία του συστήματος, επιλέχθηκε η αξιοποίηση ψηφιακών πιστοποιητικών δημοσίου κλειδιού (public key certificates) και ιδιοτήτων (attribute certificates) συμβατών με το διεθνές πρότυπο X.509 (International Telecommunication Union, 2008).

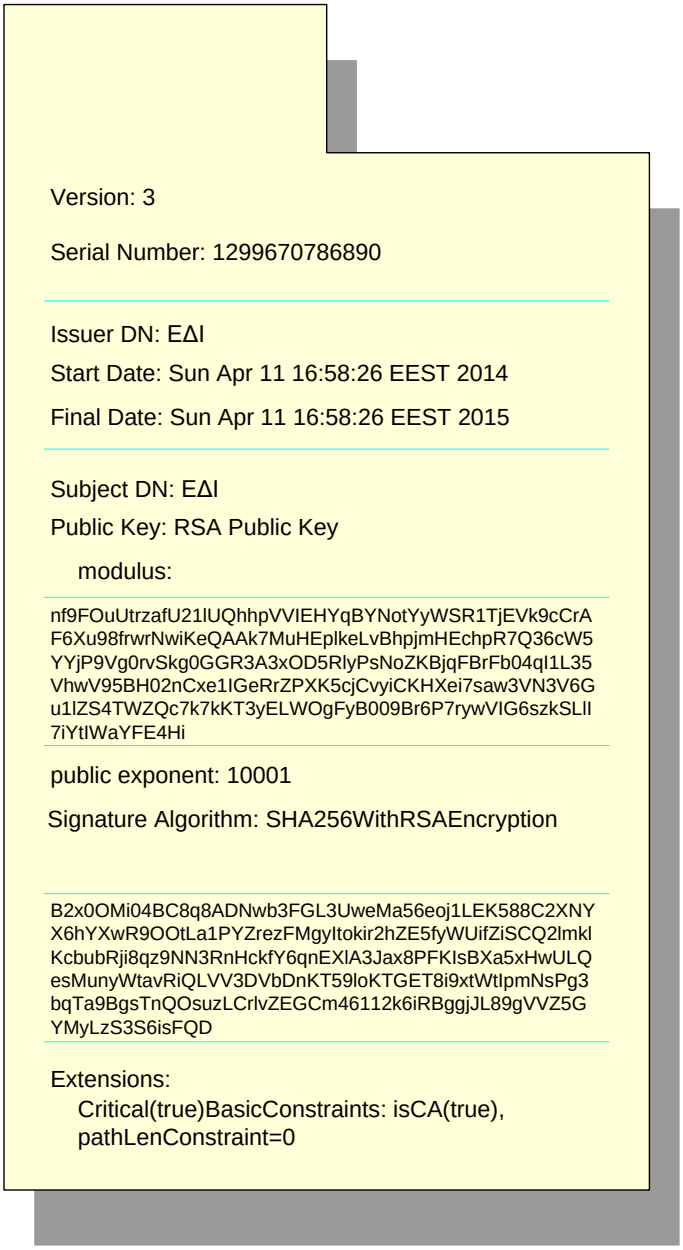
Για την κάλυψη των παραπάνω αξιοποιούνται τα ακόλουθα είδη πιστοποιητικών:

- Πιστοποιητικά δημοσίου κλειδιού X.509v3 ανταλλάσσονται μεταξύ των Οντοτήτων του συστήματος (Permanent Public Key Certificates – P-PKCs) (Εικόνα 32) που καταδεικνύουν την ύπαρξη αμοιβαίας εμπιστοσύνης μεταξύ τους.

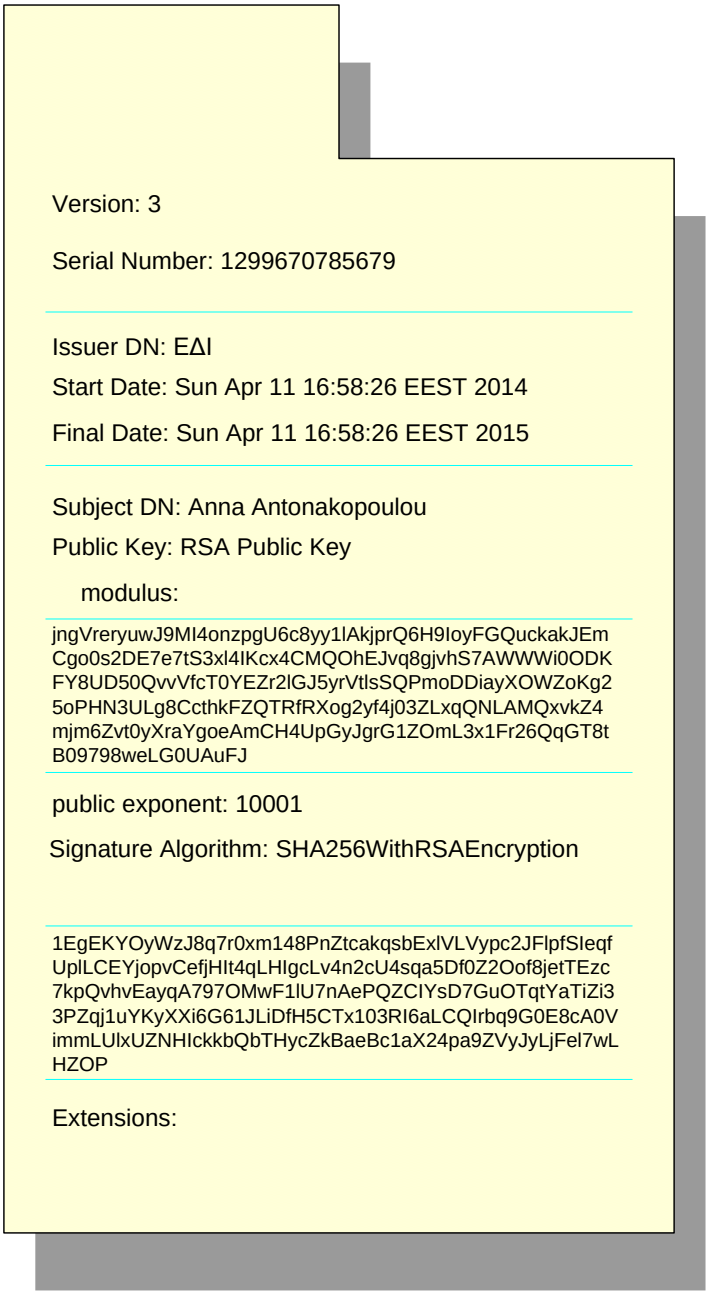
- Πιστοποιητικά δημοσίου κλειδιού X.509v3 που εκδίδονται από την Αρχή Πιστοποίησης προς του χρήστες του συστήματος (User Public Key Certificates – U-PKCs) (Εικόνα 33) και τα οποία καταγράφουν και επικυρώνουν το προσωπικό δημόσιο κλειδί.

- Πιστοποιητικά ιδιοτήτων X.509v2 που εκδίδονται από την Αρχή Πιστοποίησης προς του χρήστες του συστήματος και αποτελούν τα Πιστοποιητικά Ανάθεσης Ρόλου (Role Attribute Certificates – R-ACs) (Εικόνα 34) τα οποία πιστοποιούν ότι ο κάτοχός τους έχει τον αντίστοιχο/ους ρόλο/ους. Αυτό σημαίνει ότι τα πιστοποιητικά αυτά αποτελούν την υλοποίηση της σχέσης *RA*.

- Πιστοποιητικά ιδιοτήτων X.509v2 που εκδίδονται από την Αρχή Πιστοποίησης (Permitted Data Types Attribute Certificates – PDT-ACs) (Εικόνα 35) και καταγράφουν θετικές εξουσιοδοτήσεις χρηστών. Σε αντίθεση με τα παραπάνω πιστοποιητικά τα PDT-ACs ανήκουν στην Αρχή Πιστοποίησης που τα εκδίδει και εκδίδονται δυναμικά σε πραγματικό χρόνο κατά τη διάρκεια της λειτουργίας της πλατφόρμας, ενώ χαρακτηρίζονται από περιορισμένο χρόνο εγκυρότητας για την αποφυγή της επαναχρησιμοποίησής τους.



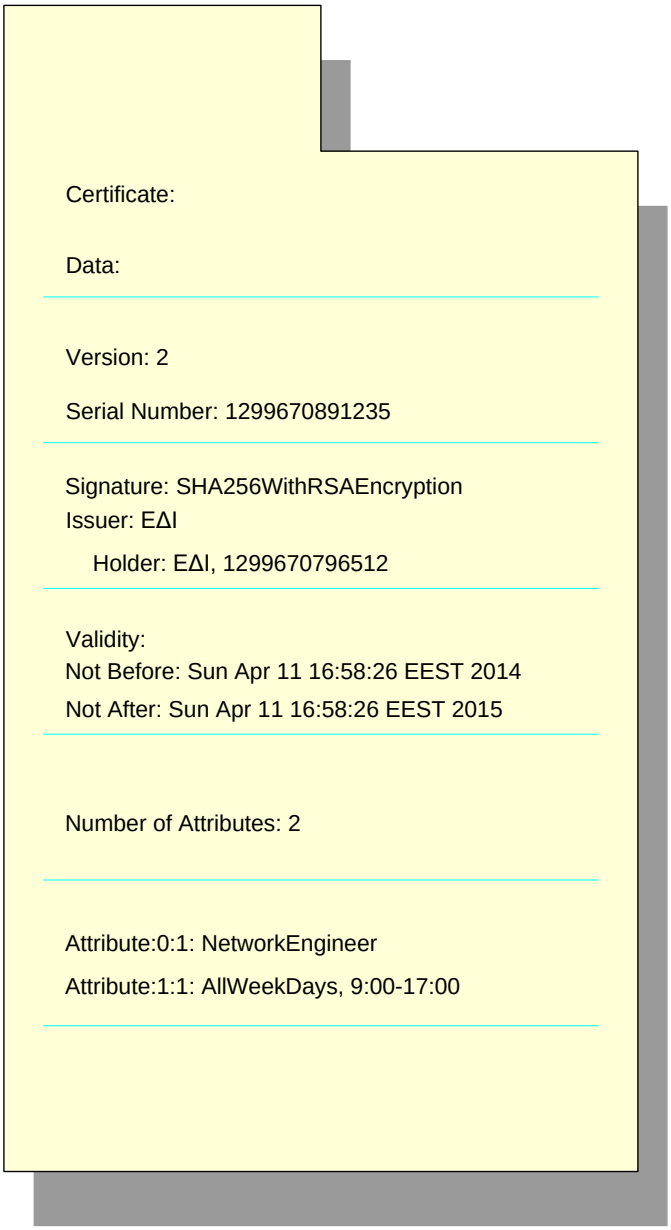
Εικόνα 32: Permanent Public Key Certificates – P-PKCs



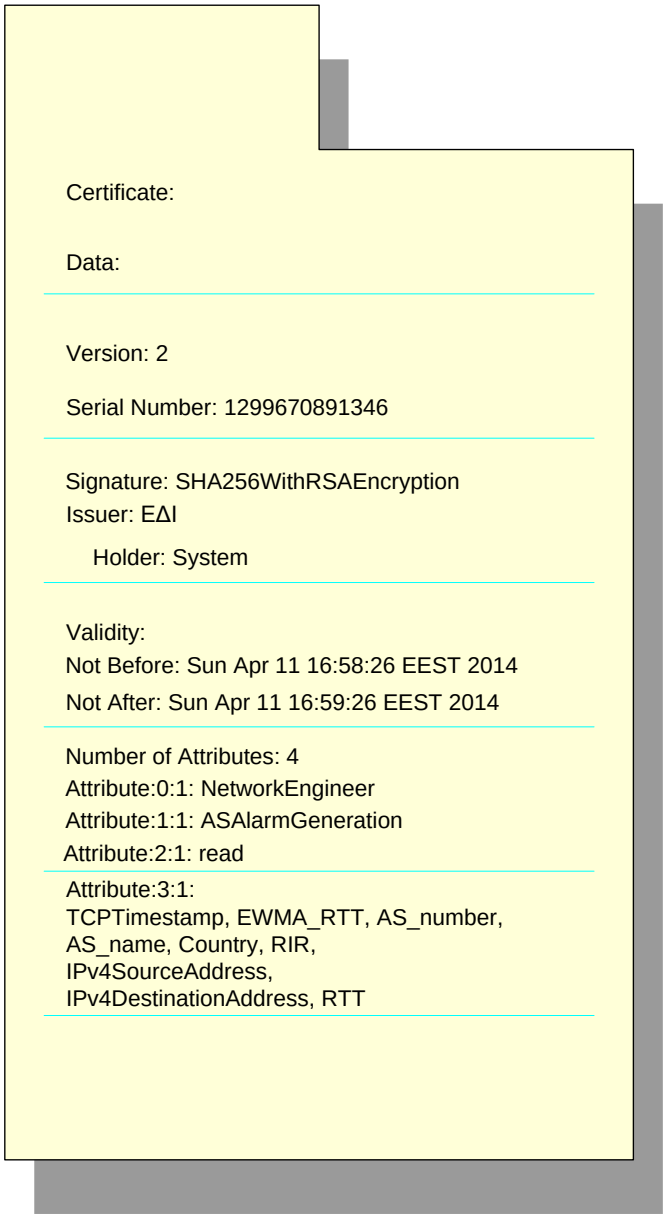
Εικόνα 33: User Public Key Certificates – U-PKCs

Ένα καινοτόμο χαρακτηριστικό του συστήματος είναι η αξιοποίηση των Πιστοποιητικών Δημόσιου Κλειδιού Μίας Χρήσης (Single Use Public Key Certificates – SU-PKCs). Ο όρος πιστοποιητικό μίας χρήσης αναφέρεται σε ένα τυπικό X.509 ψηφιακό πιστοποιητικό όπως το προαναφερθέν P-PKC, με την ξεχωριστή ανομοιότητα ότι έχει μια σχετικά μικρότερη περίοδος ισχύος. Στην πραγματικότητα, η περίοδος ισχύος τους είναι περίπου το διάστημα του χρόνου που απαιτείται για μία πλήρη διαδικασία χρήστη εφαρμογής → ελέγχου ταυτότητας / εξουσιοδότησης να ολοκληρωθεί. Τόσο η Πλατφόρμα

Διαχείρισης Εξουσιοδοτήσεων, καθώς και η Μονάδα Συλλογής Δεδομένων θα πρέπει να επικυρώσει και να επαληθεύσει ένα πιστοποιητικό μίας χρήσης, προκειμένου να καθορίσει αποτελεσματικά τα κατάλληλα ασφαλή κρυπτογραφημένα κανάλια επικοινωνίας.



Εικόνα 34: Role Attribute Certificates – R-ACs



Εικόνα 35: Permitted Data Types Attribute Certificates – PDT-ACs

Η εισαγωγή των SU-PKCs διευκολύνει τη λειτουργία του συστήματος με δύο τρόπους:

- Σε μια τυπική διαδικασία επικύρωσης των πιστοποιητικών, η οποία είναι υποχρεωτική για κάθε πλαίσιο ελέγχου ταυτότητας /εξουσιοδότησης, τα πιστοποιητικά που παραδίδονται αξιολογούνται στο πλαίσιο της κατάστασης ανάκλησης τους. Η ανάκληση των πιστοποιητικών αναφέρεται στη διαδικασία όπου η σχετική CA ή SoA των υποδομών PKI ή PMI αντίστοιχα, πρέπει να ακολουθήσει προκειμένου να ανακοινώσει ότι τα συγκεκριμένα πιστοποιητικά που εκδόθηκαν

έχουν ανακληθεί ή δεν ισχύουν πλέον, και ως εκ τούτου δεν θα πρέπει να χρησιμοποιηθούν. Ο μηχανισμός ανάκλησης πιστοποιητικών ενισχύει τη διαδικασία επικύρωσης του πιστοποιητικού, καθώς τα πιστοποιητικά μπορούν να ανακληθούν για πολλούς λόγους (π.χ. σε κίνδυνο του ιδιωτικού κλειδιού, παραβίαση των απαιτήσεων της πολιτικής CA). Ωστόσο, οι μέθοδοι ανάκλησης πιστοποιητικών που το πρότυπο X.509 ορίζει (ενημέρωση των Λιστών Ανάκλησης ή χρησιμοποιεί Online Certificate Status Protocol servers), δεν είναι κατάλληλοι για τη δυναμική φύση στην οποία ο μηχανισμός επικύρωσης του πιστοποιητικού γίνεται μέσα στο σύστημα (και ειδικά για την πραγματικού χρόνου λειτουργία της Μονάδας Συλλογής Δεδομένων). Με τη χρήση των SU-PKCs δεν χρειάζεται ρητός μηχανισμός κατάστασης ανάκλησης πιστοποιητικών, δεδομένου ότι η πραγματική CA αξιολογεί την εκάστοτε κατάσταση ανάκλησης και εκδίδει (ή όχι) μια δήλωση ότι τα πιστοποιητικά υπό αξιολόγηση δεν ανακαλούνται (SU-PKCs).

- Τα SU-PKCs χρησιμοποιούνται, λαμβάνοντας υπόψη ότι η Μονάδα Συλλογής Δεδομένων δεν πρέπει να εμπιστεύεται μια ενδεχομένως κακώς χρησιμοποιούμενη Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων ως ένα διακομιστή μεσολάβησης πιστοποιητικών. Ο λόγος που η Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων, δεν μπορεί να λειτουργήσει με ασφάλεια ως ένας διακομιστής μεσολάβησης πιστοποιητικών (προωθώντας στη Μονάδα Συλλογής Δεδομένων τα πιστοποιητικά του χρήστη της εφαρμογής) είναι ότι έχοντας τα πιστοποιητικά του χρήστη στην κατοχή της, μια κακώς χρησιμοποιούμενη Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων μπορεί στην πραγματικότητα να τα αποθηκεύσει και να προσπαθήσει να τα εκμεταλλευτεί ανά πάσα στιγμή προσωποποιώντας το χρήστη της εφαρμογής και να αιτηθεί στοιχεία που δεν δικαιούται να έχει. Η εκμετάλλευση των SU-PKCs εξαλείφει αυτή τη σημαντική απειλή για την ασφάλεια, ενώ μια ενδεχομένως κακώς χρησιμοποιούμενη Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων, δεν μπορεί να επωφεληθεί από ένα αποθηκευμένο SU-PKC κάποιου χρήστη της εφαρμογής διότι το πιστοποιητικό θα έχει λήξει από τη στιγμή που ο χρήστης της εφαρμογής έχει εξυπηρετηθεί.

Πιο συγκεκριμένα, τα P-PKCs που εκδίδονται αναφέρουν τους ιδιοκτήτες τους μαζί με τα δημόσια κλειδιά που δημιουργούνται. Αυτό το είδος των πιστοποιητικών κατέχει ένα

μοναδικό θετικό ακέραιο αριθμό ο οποίος έχει αποδοθεί από την Αρχή Πιστοποίησης αναφερόμενο ως πεδίο *SerialNumber* και ένα πεδίο το οποίο προσδιορίζει την Αρχή Πιστοποίησης, η οποία έχει υπογράψει και εκδώσει το πιστοποιητικό (πεδίο *IssuerField*). Τα δύο αυτά πεδία προσδιορίζουν ένα μοναδικό πιστοποιητικό.

Επιπλέον, το πεδίο *Validity* του πιστοποιητικού αντιπροσωπεύει το χρονικό διάστημα κατά το οποίο η Αρχή Πιστοποίησης θα διατηρήσει τις πληροφορίες για την κατάσταση του πιστοποιητικού. Το πεδίο παρουσιάζεται ως μια σειρά από δύο ημερομηνίες: την ημερομηνία κατά την οποία αρχίζει η περίοδος ισχύος του πιστοποιητικού και την ημερομηνία κατά την οποία λήγει η περίοδος ισχύος του πιστοποιητικού.

Το πεδίο *Subject* προσδιορίζει την οντότητα που σχετίζεται με το δημόσιο κλειδί που είναι αποθηκευμένο στο πεδίο *SubjectPublicKey*. Το πεδίο αυτό περιέχει ένα μοναδικό αποκλειστικό όνομα το οποίο προσδιορίζει την οντότητα που αποτελεί τον κάτοχο του πιστοποιητικού και η οποία συνδέεται με ένα δημόσιο κλειδί. Αυτό το δημόσιο κλειδί δηλώνεται μέσα στο πεδίο *SubjectPublicKeyInfo* του P-PKC. Επιπρόσθετα, το πεδίο *signatureAlgorithm* περιλαμβάνει ένα αναγνωριστικό του κρυπτογραφικού αλγορίθμου που αξιοποιήθηκε για την υπογραφή του πιστοποιητικού, ενώ το πεδίο *signatureValue* υποδεικνύει μια ψηφιακή υπογραφή υπολογισμένη στη βάση του χρησιμοποιούμενου ιδιωτικού κλειδιού και του πιστοποιητικού αυτού καθ' αυτού.

Τέλος, μέσω του πεδίου επέκτασης *AuthorityKeyIdentifier* η εκδότρια Αρχή δημοσιοποιεί το δημόσιο κλειδί της προς αξιοποίηση από τις οντότητες πιστοποίησης-επαλήθευσης με στόχο την επιβεβαίωση του γεγονότος της υπογραφής του πιστοποιητικού από την εκδότρια Αρχή.

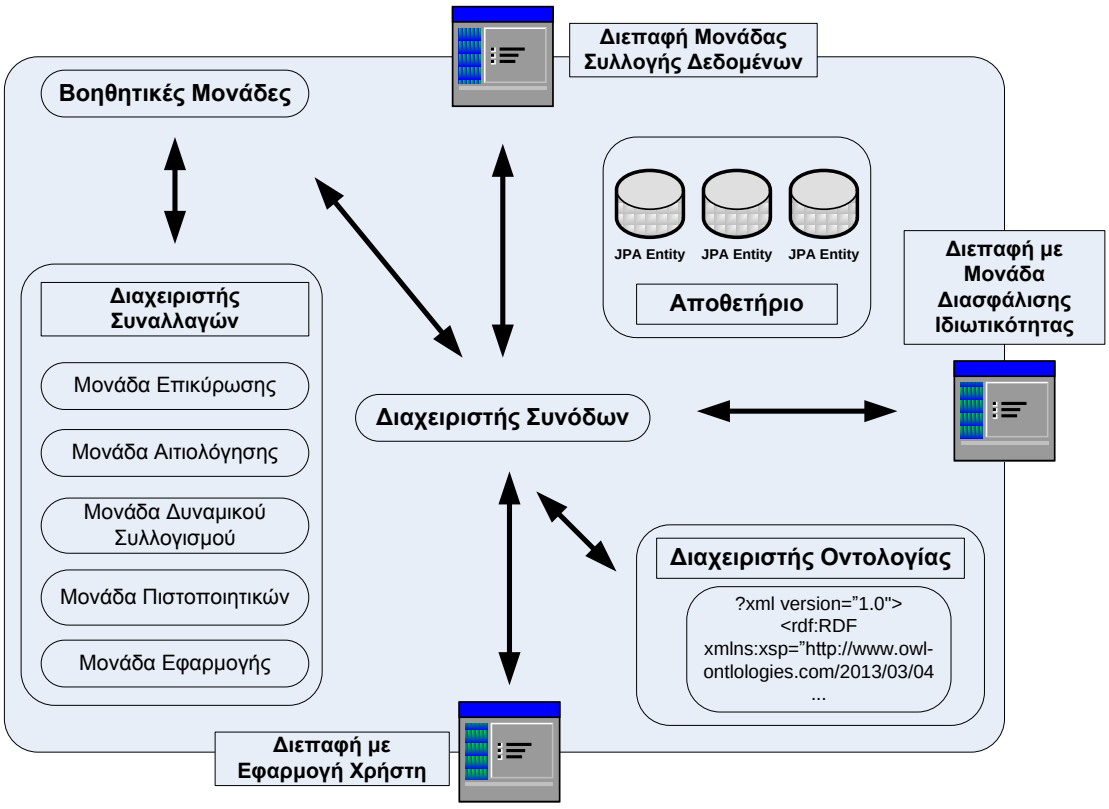
Τα Πιστοποιητικά Ανάθεσης Ιδιοτήτων Ρόλου των χρηστών (R-ACs) αποδίδουν συγκεκριμένες ιδιότητες στους χρήστες-κατόχους των αντίστοιχων P-PKCs όπως ρόλους ή πχ. ώρες ή μέρες εργασίας κτλ. Η σύνδεση των δύο πιστοποιητικών επιτυγχάνεται μέσω της επιλογής *baseCertificateId* του πεδίου *Holder* των R-ACs το οποίο επιλέγεται να αναπαριστά τον σειριακό αριθμό των αντίστοιχων P-PKCs. Επιπρόσθετα, κάθε ζευγάρι συνδεδεμένων P-PKCs – R-ACs διατηρεί κοινές τιμές στα πεδία *Issuer*. Ομοίως με τα πιστοποιητικά δημοσίου κλειδιού τα πιστοποιητικά ιδιοτήτων υπογράφονται από την εκδότρια Αρχή Πιστοποίησης, η οποία θέτει κατάλληλα τιμές στα πεδία *signatureAlgorithm, signatureValue* και *AuthorityKeyIdentifier*.

Τα πιστοποιητικά PDT-ACs ακολουθούν σε γενικές γραμμές τη δομή των R-ACs. Ειδικότερα, όμως τα πεδία που περικλείονται στα εν λόγω πιστοποιητικά αφορούν αποκλειστικά έννοιες που σημασιολογικά υποδεικνύουν θετικούς κανόνες πρόσβασης (τύπους δεδομένων, ρόλους, δράσεις και σκοπούς πρόσβασης). Η παραγωγή ενός πιστοποιητικού PDT-AC ισοδυναμεί με την προδιαγραφή ενός θετικού κανόνα πρόσβασης.

6.5 Δομή Πλατφόρμας Εξουσιοδοτήσεων

Στο υποκεφάλαιο αυτό παρουσιάζονται οι διακριτές μονάδες της πλατφόρμας για την κατάλληλη ενσωμάτωση των λειτουργιών που παρουσιάστηκαν παραπάνω σε μια ολοκληρωμένη πλατφόρμα διαχείρισης εξουσιοδοτήσεων.

Οι διακριτές μονάδες της Πλατφόρμας Διαχείρισης Εξουσιοδοτήσεων δρουν ως μεσολαβητές μεταξύ των πόρων υπό προστασία και των πιθανών καταναλωτών αυτών των πόρων. Σε αυτό το πλαίσιο και προς ικανοποίηση των λειτουργικών της καθηκόντων η πλατφόρμα χαρακτηρίζεται από μια εσωτερική δομή που συναπαρτίζεται από τις ακόλουθες λειτουργικές μονάδες όπως παρουσιάζεται και στην Εικόνα 36.



Εικόνα 36: Δομή Πλατφόρμας Διαχείρισης Εξουσιοδοτήσεων

Ο Διαχειριστής Συνόδων ενεργοποιείται για τη διαχείριση των διακριτών συνόδων (sessions), του συνόλου των ενεργοποιημένων Διαχειριστών Συναλλαγών και των αλληλεπιδράσεων της πλατφόρμας με τις υπόλοιπες οντότητες του συστήματος. Στη συνέχεια ο Διαχειριστής Συναλλαγών συνιστά τον πυρήνα της επιχειρησιακής λογικής της πλατφόρμας και ενσωματώνει τις κατάλληλες λειτουργίες για την εξυπηρέτηση των αιτήσεων εξουσιοδότησης.

Ο Διαχειριστής Οντολογίας επιτρέπει την αλληλεπίδραση των χρηστών της πλατφόρμας με την Οντολογία και το Αποθετήριο αναπαριστά την υποκείμενη υποδομή αποθήκευσης δεδομένων και πιστοποιητικών. Επίσης υπάρχουν και οι Διεπαφές Επικοινωνίας, προς τις λοιπές οντότητες της πλατφόρμας καθώς και οι Βοηθητικές Μονάδες (ΒΜ), που συνιστούν επιπρόσθετα εκτελεστικά εργαλεία εξειδικευμένων στόχων προς τη διεκπεραίωση αιτήσεων για εξουσιοδότηση.

Ειδικότερα, οι ΒΜ αξιοποιούνται για την τέλεση των απαιτούμενων ενεργειών που υποδεικνύουν οι συνθήκες εφαρμογής ενός κανόνα, και κυρίως αυτές της εφαρμογής τελεστών (greaterThan, atLeast, κ.ο.κ.) ή της ανωνυμοποίησης δεδομένων. Στη συνέχεια αναλύονται οι δύο βασικές λειτουργικές οντότητες του συστήματος, ο Διαχειριστής Συναλλαγών και ο Διαχειριστής Συνόδων.

6.5.1 Διαχειριστής Συναλλαγών

Ο Διαχειριστής Συναλλαγών συνιστά τη μονάδα εκείνη που συγκεντρώνει τις βασικές λειτουργίες για την εξυπηρέτηση των αιτήσεων για εξουσιοδότηση. Κάθε στιγμιότυπο του Διαχειριστή Συναλλαγών γίνεται αντιληπτό ως ο προσωπικός εκπρόσωπος των αιτούντων εντός της πλατφόρμας. Προς τούτο, καθ' όλη τη λειτουργία του συστήματος, κάθε στιγμιότυπο Διαχειριστή Συναλλαγών αντιστοιχίζεται αποκλειστικά στους διαφορετικούς χρήστες που αλληλεπιδρούν με την πλατφόρμα. Επομένως ο ίδιος χρήστης που αλληλεπιδρά μέσω μηνυμάτων για αίτηση πιστοποιητικών ιδιοτήτων ή δεδομένων (*requestACs* και *requestData* αντίστοιχα), αξιοποιεί το ίδιο αντικείμενο Διαχειριστή Συναλλαγών το οποίο εργάζεται ανεξάρτητα από τη λειτουργία των υπόλοιπων στιγμιότυπων. Με αυτόν τον τρόπο η πλατφόρμα έχει τη δυνατότητα να παρακολουθεί τα διαφορετικά στάδια επικοινωνίας της με τις διακριτές οντότητες αλληλεπίδρασης.

Για την εξυπηρέτηση των αιτήσεων για εξουσιοδότηση ενεργοποιούνται οι παρακάτω μονάδες:

- Μονάδα Επικύρωσης, αρμόδια για τη διεξαγωγή των κατάλληλων ενεργειών για την επικύρωση της ορθότητας και ισχύος των πιστοποιητικών που διαχειρίζεται το σύστημα στο πλαίσιο της εξυπηρέτησης συγκεκριμένων αιτήσεων.

- Μονάδα Αιτιολόγησης, η οποία επιστρέφει μια δυαδική απάντηση στο ερώτημα της καταλληλότητας και της επάρκειας των παρουσιασθέντων ψηφιακών πιστοποιητικών για την εξυπηρέτηση του κατατιθεμένου αιτήματος. Ουσιαστικά, τα πιστοποιητικά ελέγχονται για την εύρεση στιγμιότυπων *PDT* που εξουσιοδοτούν το υποκείμενο αίτημα.

- Μονάδα Δυναμικού Συλλογισμού, που επιφορτίζεται με τη διεκπεραίωση όλων των διαδικασιών που περιγράφηκαν στην ενότητα 6.3.2 και αφορούν την περαιτέρω επιβολή περιορισμών στις εξουσιοδοτήσεις που υποδεικνύονται από τη Μονάδα Αιτιολόγησης.

- Μονάδα Πιστοποιητικών, αρμόδια για τη διαχείριση των κατάλληλων πιστοποιητικών ταυτότητας και ιδιοτήτων που απαιτούνται τόσο για την αναγνώριση των χρηστών αλλά και την εξουσιοδότηση των αιτημάτων.

- Μονάδα Εφαρμογής, αποτελεί το Σημείο Εφαρμογής Πολιτικής, το οποίο είναι αρμόδιο τόσο για την υπόδειξη των απορρεόντων από την ισχύ των κανόνων εξουσιοδότησης υποχρεώσεων όσο και για την επιβολή της τελικής απόφασης εξουσιοδότησης.

6.5.2 Διαχειριστής Συνόδων

Ο Διαχειριστής Συνόδων αναπαριστά τη μονάδα εκείνη που ενορχηστρώνει τη λειτουργία των Διαχειριστών Συναλλαγών, ενώ ταυτόχρονα διαχειρίζεται την αλληλεπίδραση της πλατφόρμας με τις άλλες οντότητες του συστήματος. Ο Διαχειριστής Συνόδων υλοποιεί τις αντίστοιχες διεπαφές επικοινωνίας με τους χρήστες/εφαρμογές του συστήματος, τη Μονάδα Συλλογής Δεδομένων και τη Μονάδα Διασφάλισης Ιδιωτικότητας.

Βασικό τμήμα των αρμοδιοτήτων του Διαχειριστή Συνόδων αναφέρεται στην οργάνωση του κύκλου ζωής των Διαχειριστών Συναλλαγών της πλατφόρμας. Πιο

συγκεκριμένα, ο Διαχειριστής Συνόδων είναι υπεύθυνος για την ενεργοποίηση ενός νέου στιγμιότυπου Διαχειριστή Συναλλαγών για κάθε αίτημα από χρήστη για τον οποίο δεν έχουν κρατηθεί στοιχεία προηγούμενης σύνδεσής του με την πλατφόρμα. Επίσης, ευθύνεται για την ενεργοποίηση του μοναδικού στιγμιότυπου Διαχειριστή Συναλλαγών που αντιστοιχεί σε κάθε χρήστη για τον οποίο προκύπτουν στοιχεία προηγούμενης σύνδεσής του και τη μεταφορά των ληφθέντων ψηφιακών πιστοποιητικών και των αιτημάτων στο κατάλληλο στιγμιότυπο Διαχειριστή Συναλλαγών προς αποσαφήνιση των εξουσιοδοτήσεων.

Τέλος, για την εφαρμογή των αποφάσεων του κατάλληλου στιγμιότυπου Διαχειριστή Συναλλαγών και την απενεργοποίηση του μοναδικού στιγμιότυπου Διαχειριστή Συναλλαγών που αντιστοιχεί σε κάθε χρήστη ή και τη διαγραφή των σχετικών πληροφοριών ιστορικού κινήσεων κατά την αποσύνδεση τους από την πλατφόρμα.

6.6 Ελεγκτής Διασφάλισης Ιδιωτικότητας

Ο Ελεγκτής Διασφάλισης Ιδιωτικότητας αποτελεί πολύ σημαντική οντότητα του συστήματος η οποία έχει ποικιλία ευθυνών και είναι επιφορτισμένη με μια ποικιλία λειτουργιών. Κατά τη διάρκεια της λειτουργίας του συστήματος ο Ελεγκτής Διασφάλισης Ιδιωτικότητας ενεργεί ως σημείο εισόδου για τον ορισμό του σημασιολογικού μοντέλου και για τις προδιαγραφές του πλαισίου προστασίας της ιδιωτικότητας. Κατέχει το ρόλο της Αρχής Εξουσιοδότησης (SoA) και της Αρχής Πιστοποίησης (CA) των ενσωματωμένων PMI και PKI υποδομών αντίστοιχα. Επιπλέον, ενεργεί ως Αρχή Εγγραφής (AE) του συστήματος και αποτελεί το σημείο δημιουργίας και αξιολόγησης της εγκυρότητας των πιστοποιητικών.

Ο Ελεγκτής Διασφάλισης Ιδιωτικότητας αποτελείται από διάφορες διακριτές οντότητες καθεμία από τα οποίες είναι υπεύθυνη για την εκτέλεση ρητά οριζομένων των καθηκόντων. Σε αυτό το πλαίσιο, το Λογισμικό Προδιαγραφής Μοντέλου Ελέγχου Πρόσβασης, η Μονάδα Στατικής Συλλογιστικής και η Μονάδα Διαχείρισης Πιστοποιητικών αποτελούν τις τρεις βασικές οντότητες και είναι υπεύθυνες για τη δημιουργία της οντολογίας, την εκτέλεση της διαδικασίας στατικού συλλογισμού όπως περιγράφηκε στην ενότητα 6.3.1, καθώς και την παραγωγή πιστοποιητικών, αντίστοιχα. Οι λειτουργίες των οντοτήτων αυτών εκτελούνται από τις αντίστοιχες επιμέρους μονάδες για την οριοθέτηση και την εκπλήρωση των καθηκόντων τους.

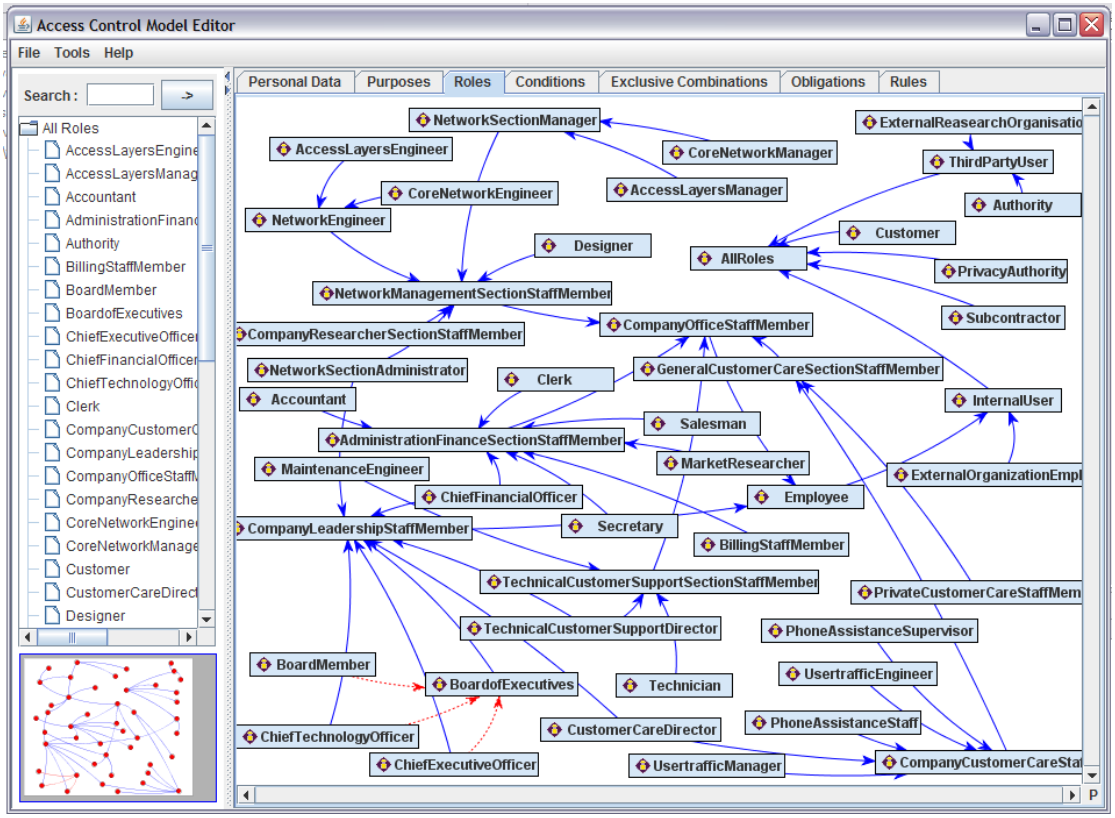
Η Μονάδα Διαχείρισης Πιστοποιητικών αποτελείται από διαφορετικές ενότητες που αφορούν διακριτές λειτουργίες, όπως η δημιουργία των πιστοποιητικών, η ανάκληση, η αποθήκευση και η παράδοσή τους. Τέλος, ο Ελεγκτής Διασφάλισης Ιδιωτικότητας έχει δύο διεπαφές: Τη γραφική διεπαφή χρήστη με το Λογισμικό Προδιαγραφής Μοντέλου Ελέγχου Πρόσβασης στην οποία έχει πρόσβαση ο διαχειριστής του συστήματος και τη διεπαφή με την εκάστοτε εφαρμογή που αντανακλά το σημείο πρόσβασής της με τον Ελεγκτή Πιστοποίησης Ιδιωτικότητας και της επιτρέπει, κατά τη διάρκεια της συνεργασίας της με το σύστημα, να αποκτήσει ορισμένα πιστοποιητικά για τους σκοπούς της πιστοποίησης και εξουσιοδότησης.

6.6.1 Λογισμικό Προδιαγραφής Μοντέλου Ελέγχου Πρόσβασης

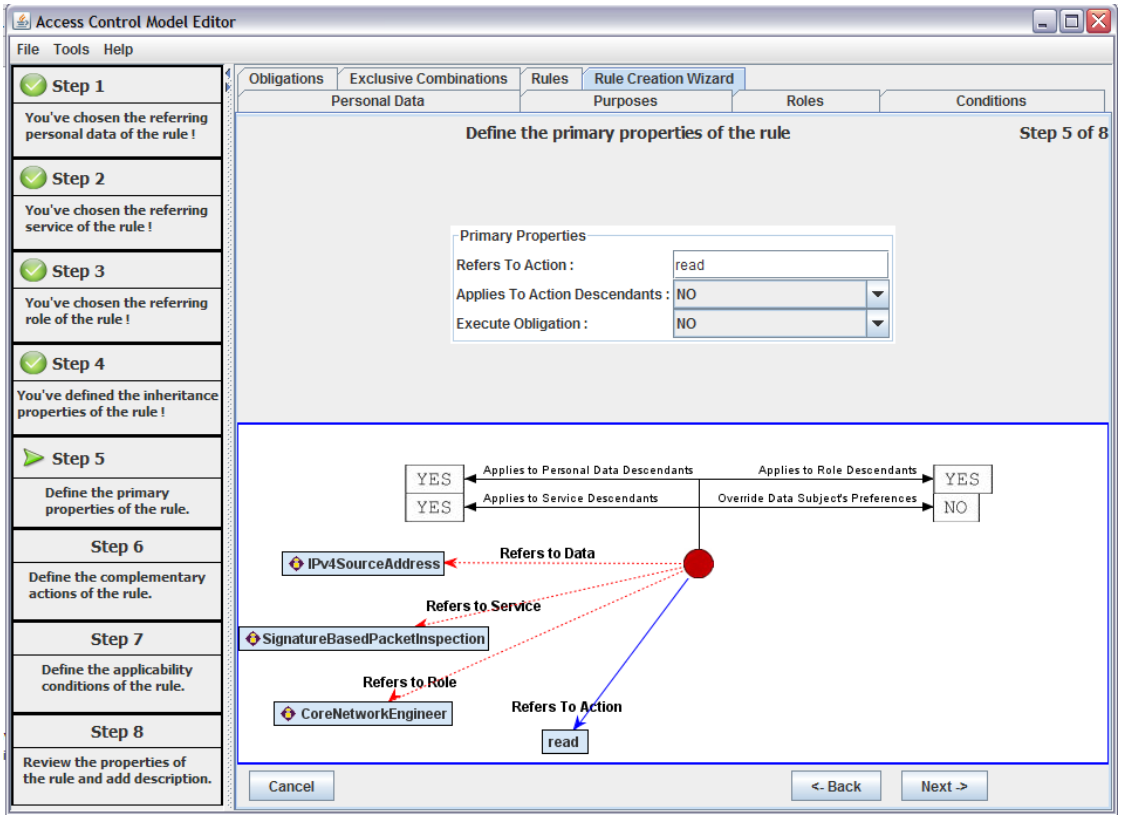
Η Οντολογία κατέχει κεντρικό ρόλο στις διαδικασίες και λειτουργίες που στοχεύουν στην παραγωγή σαφών αποφάσεων εξουσιοδότησης κι επομένως η διαχείρισή της αποκτά βαρύνουσα σημασία για την εύρυθμη λειτουργία του συστήματος. Για την προδιαγραφή του σχήματος της Οντολογίας, τον σχεδιασμό των επιθυμητών στιγμιότυπών της και την οργάνωση των μεταξύ τους συσχετίσεων αξιοποιήθηκε εξειδικευμένο λογισμικό προδιαγραφής οντολογιών, κατάλληλα προσαρμοσμένο στις ανάγκες της προτεινόμενης λύσης.

Το λογισμικό προδιαγραφής κανόνων ελέγχου πρόσβασης αποτελεί μια φιλική προς τον χρήστη εφαρμογή, που αναπτύχθηκε σε Java για την απόκρυψη των εμπλεκόμενων τεχνικών λεπτομερειών από τους χρήστες κατά τη διαχείριση OWL οντολογιών.

Η πλειοψηφία των υποστηριζόμενων λειτουργιών διαχείρισης οντολογιών και οπτικοποίησης των παραγόμενων ταξινομήσεων (Εικόνα 37) βασίζεται στις δυνατότητες των βιβλιοθηκών Jena (Jena, 2013) και JUNG (Java Universal Network/Graph Framework, 2013) αντίστοιχα, ενώ το λογισμικό περιλαμβάνει έναν αναλυτικό οδηγό προδιαγραφής κανόνων εξουσιοδότησης με ρυθμίσεις των απαραίτητων μεταβλητών βήμα-προς-βήμα (Εικόνα 38).

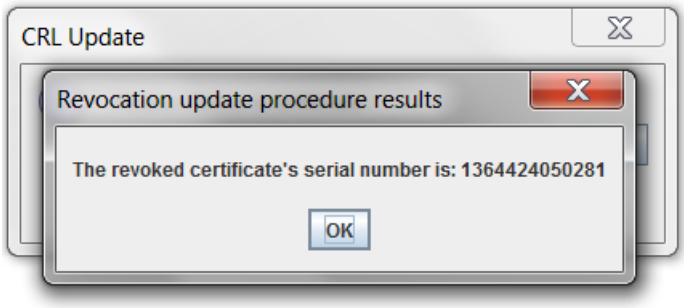


Εικόνα 37: Ο γράφος ρόλων



Εικόνα 38: Βήμα προς βήμα προδιαγραφή κανόνων εξουσιοδότησης

Βασικό τμήμα των λειτουργιών του λογισμικού αναφέρεται στη διαχείριση των χρηστών του συστήματος και ως επέκταση στη διαχείριση του κύκλου ζωής των εμπλεκόμενων πιστοποιητικών ταυτότητας και ιδιοτήτων. Προς τούτο, το λογισμικό παρέχει τη δυνατότητα καταγραφής των χρηστών και των ιδιοτήτων τους καθώς και δημιουργίας λιστών ανάκλησης πιστοποιητικών (Certificate Revocation Lists – CRLs) (Εικόνα 39), τις οποίες η Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων και ο Ελεγκτής Διασφάλισης Ιδιωτικότητας διατηρούν τοπικά και συμβουλεύονται κατά την επικύρωση των διαχειριζόμενων πιστοποιητικών από τις ενσωματωμένες Μονάδες Επικύρωσης.



Εικόνα 39: Οθόνη ενημέρωσης λίστας ανάκλησης πιστοποιητικών

6.7 Διαδικασία αυθεντικοποίησης και εξουσιοδότησης

Η διαδικασία που διενεργείται στο σύστημα σε σχέση με την επαλήθευση ταυτότητας και εξουσιοδότηση αποτελείται από τρία κύρια εννοιολογικά μέρη:

1. Χρήστης/Εφαρμογή – Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων αυθεντικοποίηση και εξουσιοδότηση.
2. Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων – Μονάδα Συλλογής Δεδομένων αυθεντικοποίηση.
3. Χρήστης/Εφαρμογή – Μονάδα Συλλογής Δεδομένων αυθεντικοποίηση και εξουσιοδότηση.

Κατά την έναρξη της διαδικασίας, ο χρήστης/εφαρμογή υποτίθεται ότι κατέχει ήδη ένα P-PKC, το οποίο αποτελεί τη θεμελιώδη ταυτότητά του και ένα πιστοποιητικό ρόλου R-AC που πιστοποιεί το λειτουργικό/επιχειρησιακό του ρόλο(ους). Συνοπτικά, η διαδικασία αποτελείται από τα ακόλουθα στάδια τα οποία παρουσιάζονται στην Εικόνα 40:

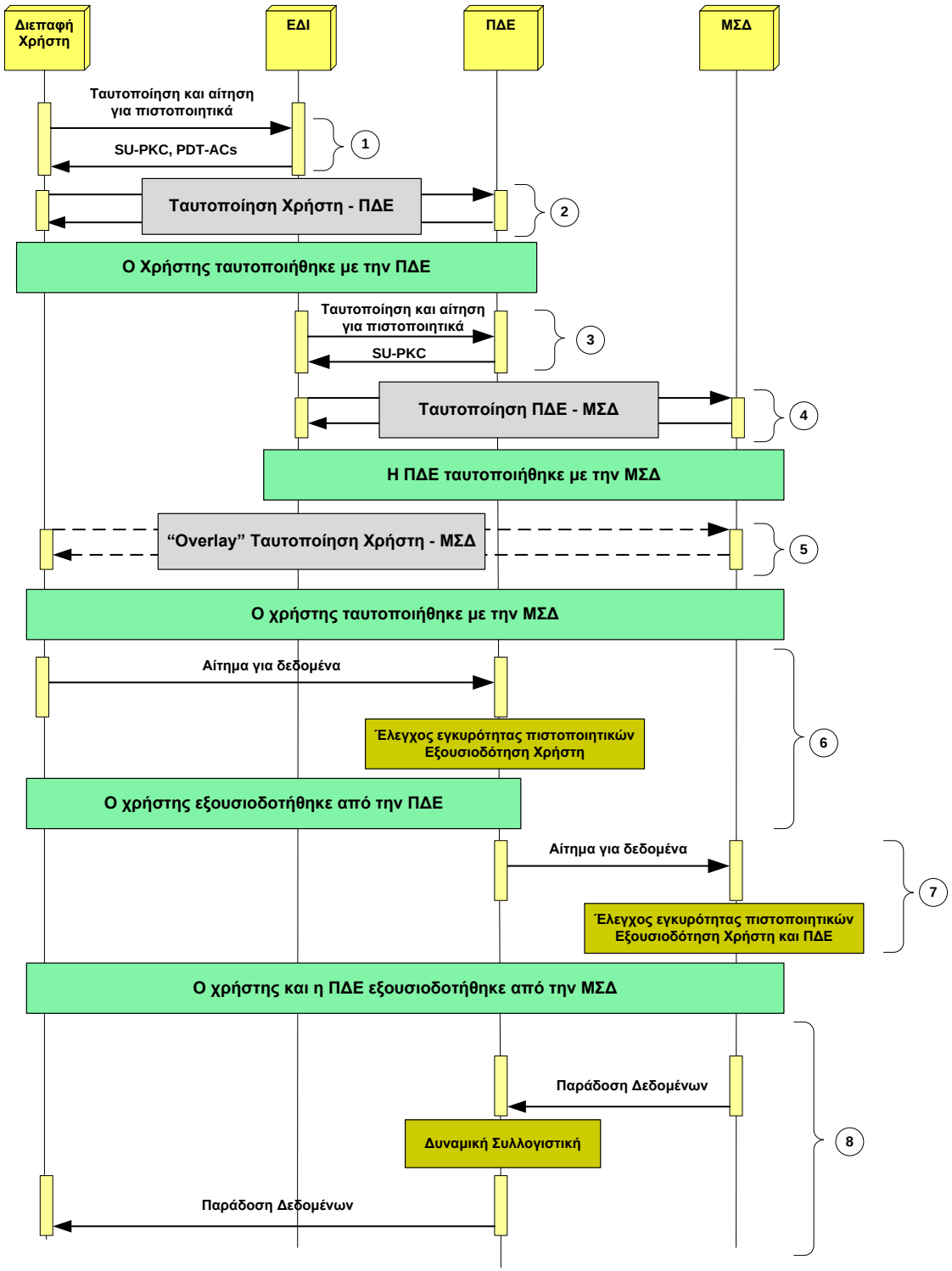
1. Ο χρήστης/εφαρμογή ταυτοποιεί τον εαυτό του στον ΕΔΙ με τη χρήση του P-PKC και αποκτά ένα SU-PKC το οποίο θα χρησιμοποιηθεί για το αίτημα για δεδομένα.

Επιπλέον, ο ίδιος αποκτά το πιστοποιητικό PDT-AC που αντιστοιχεί στα δεδομένα προσωπικού χαρακτήρα που αιτείται, καθώς και το ρόλο (ους) που θα ενεργοποιηθεί και το βασικό σκοπό (ους).

2. Ο χρήστης/εφαρμογή ταυτοποιείται με την Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων με χρήση του P-PKC. Στο πλαίσιο αυτό, ο χρήστης/εφαρμογή ξεκινά τη δημιουργία ενός ασφαλούς καναλιού με την Πλατφόρμα χρησιμοποιώντας το πρωτόκολλο χειραψίας TLS. Κατά τη διάρκεια αυτής της διαδικασίας, ο χρήστης/εφαρμογή επικοινωνεί το ζητούμενο P-PKC. Κατά την παραλαβή του, η Πλατφόρμα επαληθεύει ότι ο αυτός κατέχει το ιδιωτικό κλειδί που ταιριάζει με το δημόσιο κλειδί που περιλαμβάνεται στο μεταβιβασμένο P-PKC και αξιολογεί την εγκυρότητα του πιστοποιητικού.
3. Η Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων ταυτοποιεί τον εαυτό της στον ΕΔΙ χρησιμοποιώντας το δικό της P-PKC και λαμβάνει ένα SU-PKC.
4. Ομοίως με την αυθεντικοποίηση χρήστη/εφαρμογής-Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων, η Μονάδα Συλλογής Δεδομένων ταυτοποιεί την Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων σύμφωνα με το SU-PKC της.
5. Κατά τη διάρκεια του παραπάνω βήματος, η Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων έχει διαβιβάσει στη Μονάδα Συλλογής Δεδομένων, εκτός από τα δικά της διαπιστευτήρια, το P-PKC του χρήστη/εφαρμογής. Μια "overlay πρόκληση" λαμβάνει χώρα μεταξύ της Μονάδα Συλλογής Δεδομένων και χρήστη/εφαρμογής, στο πλαίσιο της οποίας η Μονάδα Συλλογής Δεδομένων δημιουργεί ένα μήνυμα κρυπτογραφημένο με το P-PKC δημόσιο κλειδί του χρήστη/εφαρμογής και ταυτοποιεί το χρήστη/εφαρμογή λαμβάνοντας, διάμεσο της Πλατφόρμας Διαχείρισης Εξουσιοδοτήσεων, την κατάλληλη απάντηση από τον χρήστη/εφαρμογή.
6. Ο χρήστης/εφαρμογή αιτείται τα δεδομένα, επικοινωνώντας στην Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων τα SU-PKC και R-AC μαζί με το σχετικό PDT-ACs πιστοποιητικά. Η Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων προχωρά με την επικύρωση των πιστοποιητικών και, κατόπιν επιτυχίας, εξουσιοδοτεί τον χρήστη/εφαρμογή σε σχέση με το αίτημά του.

7. Όλα τα πιστοποιητικά προωθούνται στη Μονάδα Συλλογής Δεδομένων, η οποία, εξουσιοδοτεί επίσης, τον χρήστη/εφαρμογή, καθώς και την Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων. Η εξουσιοδότηση της Πλατφόρμας Διαχείρισης Εξουσιοδοτήσεων αφορά την επικύρωση ότι, προκειμένου η Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων να παραδώσει στον χρήστη/εφαρμογή τα ζητούμενα δεδομένα, θα πρέπει η Μονάδα Συλλογής Δεδομένων να διαβιβάσει τα σχετικά ανεπεξέργαστα δεδομένα.

8. Σε αυτό το σημείο, η διαδικασία ελέγχου πιστοποίησης και εξουσιοδότησης έχει τελειώσει. Η Μονάδα Συλλογής Δεδομένων επικοινωνεί τα ανεπεξέργαστα δεδομένα στην Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων, η οποία, μετά από την κατάλληλη επεξεργασία (δηλαδή, η επίκληση των κατάλληλων ΒΜ για το μετασχηματισμό των δεδομένων), παραδίδει στον χρήστη/εφαρμογή τα ζητούμενα στοιχεία. Πριν από τη δημοσιοποίηση των στοιχείων στο χρήστη/εφαρμογή, η Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων εκτελεί τη διαδικασία που αναφέρεται ως "δυναμική συλλογιστική", για την αξιολόγηση και την εφαρμογή των προϋποθέσεων σε πραγματικό χρόνο και όποιων άλλων περιορισμών μπορεί να ισχύουν.



Εικόνα 40: Διαδικασία αυθεντικοποίησης και εξουσιοδότησης

.

Κεφάλαιο 7

Παράδειγμα Χρήσης και Αξιολόγηση

Η παρακολούθηση δικτύου αποτελεί μια σημαντική διαδικασία σχετικά με τη σταθερότητά του, δεδομένου ότι είναι χρήσιμη και σημαντική για σκοπούς όπως η λειτουργία του, η διαχείρισή του, ο σχεδιασμός και η συντήρησή του, η ασφάλεια του (π.χ., από την άποψη της ανίχνευσης και πρόληψης εισβολής), καθώς και για ζητήματα όπως η επιστημονική έρευνα η οποία βασίζεται σε πραγματικά ίχνη της κίνησης δικτύου, καθώς και η επιβολή του νόμου (π.χ. μέσω της διατήρησης των δεδομένων και νόμιμης παρακολούθησης).

Δεδομένου ότι η παρακολούθηση του δικτύου εξαρτάται από τη συλλογή και την επεξεργασία των πληροφοριών που σχετίζονται με την κίνηση δικτύου που μπορεί να περιέχει ένα σημαντικό ποσοστό προσωπικού περιεχομένου, εγείρει ζητήματα που σχετίζονται με την προστασία των προσωπικών δεδομένων. Στην πραγματικότητα, ο πυρήνας αναγνώρισης στον τομέα των επικοινωνιών είναι η διεύθυνση IP και, στο πλαίσιο αυτό, το άρθρο 29 του οργανισμού Προστασίας Δεδομένων – Data Protection Working Party (2007), καταλήγει στο συμπέρασμα ότι «*... εκτός εάν ο πάροχος είναι σε θέση να διακρίνει με απόλυτη βεβαιότητα ότι τα δεδομένα αντιστοιχούν σε χρήστες που δεν μπορεί να προσδιοριστούν, θα πρέπει να αντιμετωπίζει όλες τις πληροφορίες IP ως δεδομένα προσωπικού χαρακτήρα για να είναι στην ασφαλή πλευρά*», οι διευθύνσεις IP δεν αποτελούν "μόνο αριθμούς" (Lundevall - Unger and Tranvik, 2011) .

Συνεπώς, οι ανησυχίες για την προστασία της ιδιωτικότητας δεν περιορίζονται μόνο στο ωφέλιμο φορτίο των πακέτων δεδομένων αλλά και σε ευαίσθητες πληροφορίες οι οποίες μπορούν να εξαχθούν και να αναγεννηθούν από τις επικεφαλίδες πρωτόκολλου και οι οποίες αποκαλύπτουν ήδη πολλές πληροφορίες (π.χ. μια ιστοσελίδα που έχει επισκεφτεί κάποιος ή τους κόμβους μιας κλήσης VoIP), ακόμη και αν έχουν υποστεί ανωνυμία (Pang, Allman, Paxson and Lee, 2006) ή και από φαινομενικά "αθώα" πεδία της επικεφαλίδας (π.χ. Bellovin, 2002).

Στην πραγματικότητα, οι μηχανισμοί προστασίας της ιδιωτικότητας ευθυγραμμίζουν τις λειτουργίες τους για την πρόληψη και την καταγραφή περιστατικών παραβίασης της

ιδιωτικότητας στα διάφορα στρώματα της στοίβας δικτύου (Ruiz - Martinez, 2012). Η διαδικασία παρακολούθησης δικτύων σχετίζεται επίσης και με πολύ υψηλές ταχύτητες δεδομένων που υπερβαίνουν της τάξης των Gbps. Έτσι, οι μηχανισμοί που αναπτύσσονται για τη διατήρηση της ιδιωτικότητας πρέπει να είναι σε θέση να αντιμετωπίσουν τέτοιες αυστηρές απαιτήσεις. Επιπλέον, οι δραστηριότητες παρακολούθησης, καθώς και οι βασικές κατηγορίες των δεδομένων, έχουν αποτελέσει αντικείμενο ειδικών ρυθμίσεων, όπως (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2002) στην Ευρώπη. Παρά το γεγονός ότι κάποιες πληροφορίες παρέχονται στις ακόλουθες ενότητες, η λεπτομερής περιγραφή της νομοθεσίας είναι πέρα από το πεδίο εφαρμογής του παρούσας διατριβής έτσι ο αναγνώστης παραπέμπεται στα (Sicker, Ohm, and Grunwald, 2007) και (Lioudakis, Gaudino, Boschi, Bianchi, Kaklamani and Venieris, 2010).

Με σκοπό να εδραιωθεί η εμπιστοσύνη προς τους πελάτες τους, καθώς και να επιτευχθεί η συμμόρφωση με τη νομοθεσία προστασίας της ιδιωτικής ζωής, οι πάροχοι δικτύων θεσπίζουν πρακτικές διαχείρισης των δεδομένων υλοποιημένες από τις πολιτικές απορρήτου οι οποίες επιβάλλονται από τα συστήματα βασιζόμενα σε κανόνες.

7.1 Σχετικό Υπόβαθρο

Παρά το γεγονός ότι αρκετές λύσεις παρέχουν σημαντικά επιτεύγματα στους τομείς της ανωνυμοποίησης της κίνησης δικτύου, (Koukis, Antonatos, Antoniadis, Trimintzios and Markatos, 2006) και (Burkhart, Schatzmann, Trammell, Boschi and Plattner, 2010), αν και έχουν ως στόχο να είναι αρκετά γενικές, βασίζονται σε στατικές προδιαγραφές πολιτικών ανωνυμοποίησης. Επιπλέον, παρά το γεγονός ότι λειτουργούν καλά για εφαρμογές που χρησιμοποιούν δεδομένα κίνησης τα οποία έχουν συλλεχθεί στο παρελθόν, δεν ισχύουν για τους τομείς των εφαρμογών που απαιτούν δεδομένα σε πραγματικό χρόνο, όπως τα συστήματα ανίχνευσης εισβολής.

Από την άλλη πλευρά, πλαίσια ελέγχου πρόσβασης με επίγνωση ιδιωτικότητας στη βιβλιογραφία, π.χ. (Byun, Bertino and Li, 2005), (Ni, Trombetta, Bertino and Lobo , 2007) και (Bertino, Lobo, Brodie, Karat and Trombetta, 2010), καταφέρνουν να ενσωματώσουν την πλειοψηφία των χαρακτηριστικών προστασίας του πλαισίου ιδιωτικότητας που υπαγορεύεται από τις θεμελιώδεις αρχές προστασίας προσωπικών δεδομένων που περιγράφονται στο (OECD, 1980), αλλά κινούνται μακριά από την απλότητα του πνεύματος της διαχείρισης πολιτικών, όπως αυτά μελετήθηκαν στη βιβλιογραφία

(Antonakopoulou et al., 2012). Κατά συνέπεια, οι παραπάνω προσεγγίσεις σχετικά με τους τομείς της ανωνυμοποίησης κυκλοφορίας, προστασίας της ιδιωτικότητας και ελέγχου πρόσβασης με επίγνωση ιδιωτικότητας δεν πληρούν όλες τις απαιτήσεις για την παρακολούθηση δικτύων με επίγνωση ιδιωτικότητας.

Επιπρόσθετα, μερικές από τις τρέχουσες ερευνητικές προσεγγίσεις εκμεταλλεύονται την εκφραστική δύναμη της σημασιολογίας και των οντολογιών, για παράδειγμα, οι προσεγγίσεις (Kost and Freytag, 2012) και (Hecker, Dillon and Chang, 2008), προκειμένου οι πολιτικές απορρήτου τους να ενισχυθούν αποτελεσματικά, π.χ., με σημαντικά χαρακτηριστικά σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα, όπως η υπό όρους δημοσιοποίηση/επεξεργασία πληροφορίας, η εκπλήρωση των υποχρεώσεων ιδιωτικότητας και η ενσωμάτωση προτιμήσεων απορρήτου.

Στις παρακάτω προσεγγίσεις (Haidar, Cuppens-Boulahia, Cuppens and Debar, 2006), (Finin, Joshi, Kagal, Niu, Sandhu, Winsborough and Thuraisingham, 2008), (Ferrini and Bertino, 2009), (Ravari, Amini, Jalili and Jafarian, 2008) και (Ravari, Jafarian, Amini and Jalili, 2010), το υψηλό επίπεδο αφαιρετικότητας, σχετικά με τη σημασιολογική αναπαράσταση των οντοτήτων τους αποτελεί ένα σημαντικό πλεονέκτημα το οποίο οφείλεται στο γεγονός ότι, στο πλαίσιο αυτό, ένα μοντέλο μπορεί να εκφράσει άλλα μοντέλα ελέγχου πρόσβασης, ενώ η ενημέρωση και η διαχείριση των κανόνων πρόσβασης γίνονται πιο εύκολα.

Τέλος, αξίζει να αναφερθούν προσεγγίσεις στον τομέα χρήσης των οντολογιών όσον αφορά την ασφάλεια του δικτύου από τις οποίες το έργο μας εμπνεύστηκε και παρουσιάζονται στα παρακάτω: (Cuppens-Boulahia, Cuppens, Lopez De Vergara, Vazquez, Guerra and Debar, 2008), (Lopez De Vergara, Vazquez, Martin, Dubus and Lepareux, 2009) και (Chunlei, Qichang, Li, Hong, Zhongyang and Haibo, 2011). Αυτές οι λύσεις προτείνουν μια μεθοδολογία που βασίζεται σε οντολογίες, για τη συγκεκριμενοποίηση των πολιτικών ασφάλειας που παρεμποδίζουν τις επιθέσεις του δικτύου. Οι δύο πρώτες προσεγγίσεις βασίζονται στο μοντέλο που παρουσιάζεται στο (Cuppens and Cuppens-Boulahia 2008) και παρέχουν έναν τρόπο για να χαρτογραφήσουν τις ειδοποιήσεις/συναγερμούς σε πλαίσια επίθεσης, τα οποία στη συνέχεια χρησιμοποιούνται για να προσδιοριστούν οι πολιτικές που πρέπει να εφαρμοστούν στο δίκτυο για την επίλυση των αναδυόμενων απειλών.

7.2 Ζητήματα προστασίας της ιδιωτικότητας σε περιβάλλοντα παρακολούθησης δικτύων

Σε αυτή την ενότητα μελετάται το ζήτημα προστασίας της ιδιωτικότητας όσον αφορά σε περιβάλλοντα παρακολούθησης δικτύου από νομικής και τεχνικής πλευράς. Όπως έχει ήδη αναφερθεί, η διαδικασία παρακολούθησης δικτύου απαιτείται για την ομαλή λειτουργία και συντήρηση των δικτύων επικοινωνίας καθώς και για ζητήματα που αφορούν στην ανίχνευση απειλών και απατών. Συνήθως, ακατέργαστα ίχνη κίνησης σε επίπεδο πακέτου ανιχνεύονται χρησιμοποιώντας κατάλληλες συσκευές ανίχνευσης κίνησης και δίδονται στις εφαρμογές παρακολούθησης (IDS, κ.α) για ανάλυση, πάντα με πιθανό ρίσκο όσον αφορά τα νομικά δικαιώματα των πελατών για την προστασία της ιδιωτικότητας.

Με βάση τα παραπάνω, οι παραβάσεις οι οποίες σχετίζονταν με την παρακολούθηση δικτύου και την εποπτεία των επικοινωνιών άρχισαν να βγαίνουν σαν πρωτοσέλιδα και να τροφοδοτούν τις ανησυχίες των πολιτών. Σχετικά συμβάντα έχουν σημειωθεί αρκετά. Αξίζει να αναφερθούν για παράδειγμα οι υποκλοπές χωρίς ένταλμα του Εθνικού Γραφείου Ασφαλείας Ηνωμένων Πολιτειών οι οποίες εξουσιοδοτήθηκαν από την κυβέρνηση Bush (Risen and Lichtblau, 2005), ή και το σκάνδαλο με τις υποκλοπές που έλαβε χώρα πιο πρόσφατα στην Ελλάδα (Smith, 2006).

Κατά συνέπεια, ο σχεδιασμός ενός συστήματος παρακολούθησης δικτύου δε μπορεί να θεωρηθεί σαν μια στείρα τεχνικά διαδικασία, εφόσον είναι φανερή η επίδραση που έχει στην κοινωνία όσον αφορά τόσο τις επιπτώσεις στην ιδιωτικότητα όσο και τις συνέπειες στη δημόσια ασφάλεια. Οι δημόσιες πολιτικές και οι απαιτήσεις ιδιωτικότητας επηρεάζουν στην πραγματικότητα σε ένα μεγάλο εύρος τις τεχνικές απαιτήσεις ενός τέτοιου συστήματος.

Με βάση όλα τα παραπάνω, ο ρόλος της σημασιολογίας είναι καίριος. Καθώς η παρακολούθηση δικτύου δεν αποτελεί μία μεμονωμένη, καλά καθορισμένη διαδικασία, μία εργασία παρακολούθησης μπορεί να θεωρηθεί σαν ένα μέσο για να απαντηθεί ένα μοναδικό ερώτημα σε σχέση με την δραστηριότητα του δικτύου που βρίσκεται υπό παρακολούθηση Η λεπτομερής αποσαφήνιση στο ποια δεδομένα είναι «αυστηρώς απαραίτητα» για την εργασία παρακολούθησης εξαρτάται από το τι ζητήθηκε, κάτω υπό ποιες συνθήκες δικτύου και από ποιον, απαιτώντας μια εις βάθος διευκρίνιση των παρακάτω ζητημάτων:

- Ποιος είναι ο σκοπός της εργασίας παρακολούθησης (πχ. SLA, ανίχνευση εισβολής, εύρεση χαρακτηριστικών κίνησης, υπηρεσίες λογιστικής και τιμολόγησης, κ.α);
- Ποια συγκεκριμένη πληροφορία κίνησης απαιτείται για να εκπληρωθεί αυτός ο σκοπός;

Αυτή μπορεί να είναι είτε πληροφορία που βρίσκεται μέσα στα πακέτα δεδομένων (πχ. στα πεδία επικεφαλίδας ή σε τομείς φορτίου) ή απορρέει από μία ή περισσότερες λειτουργίες ανάλυσης οι οποίες εφαρμόζονται στα πακέτα (πχ. κατανομή μεγέθους ροής). Η πληροφορία που θεωρείται «αυστηρώς απαραίτητη» πρέπει να έχει το ελάχιστο πιθανό πληροφοριακό περιεχόμενο για αυτό το σκοπό. Για παράδειγμα, η ακατέργαστη πληροφορία της διεύθυνσης IP από την επικεφαλίδα του πακέτου δεν είναι απαραίτητη εάν ο αιτούμενος σκοπός μπορεί να χρησιμοποιήσει πληροφορία διεύθυνσης IP συναθροισμένης με το δίκτυο (όπως γίνεται συνήθως για σκοπούς διαχείρισης κίνησης) ή ανωνυμοποιημένη πληροφορία διεύθυνσης IP χωρίς βέβαια να χαθεί λειτουργικότητα.

- Ποια οντότητα (ο διαχειριστής συστήματος, ένα τμήμα στον οργανισμό παρόχου, η διεθνής ερευνητική κοινότητα, κτλ) εκτελεί την εργασία παρακολούθησης και έχει πρόσβαση σε δεδομένα εισόδου και αποτελέσματα;

  Προφανώς, οι παράγοντες αυτοί δεν είναι στατικοί σε γενικές γραμμές, αλλά μπορεί επίσης να εξαρτώνται από ενδιάμεσα αποτελέσματα της εφαρμογής παρακολούθησης και κατά συνέπεια να αλλάζουν δυναμικά με το χρόνο. Για παράδειγμα, ένα σύστημα ανίχνευσης εισβολής δικτύου το οποίο βρίσκεται περιμετρικά του δικτύου μπορεί να μη χρειάζεται απαραίτητα πρόσβαση στο επίπεδο IP έτσι ώστε να ανιχνεύσει εισβολή. Παρόλα αυτά μόλις η εισβολή ανιχνευτεί μπορεί να καταστεί απαραίτητο να αντιστοιχηθεί η επίθεση με ένα σύνολο διευθύνσεων πηγής και στόχου για να αντιμετωπίσουν την επίθεση. Η δυναμική φύση αυτής της αναγκαιότητας υπονοεί ότι υπάρχει κι άλλος ένας παράγοντας ο οποίος πρέπει να διευθετηθεί:
- Ποιο είναι το πλαίσιο κατά το οποίο η πληροφορία συλλέγεται και επεξεργάζεται και πως διαφοροποιήσεις σε αυτό επηρεάζουν τους προηγούμενους παράγοντες;

Με βάση όλα τα παραπάνω παρατηρούμε ότι τα απαιτούμενα για τον έλεγχο πρόσβασης με επίγνωση ιδιωτικότητας σε περιβάλλον παρακολούθησης δικτύου τα οποίο αποτελεί και την περίπτωση χρήσης στην παρούσα εργασία διέπονται από όλες εκείνες τις αρχές τις οποίες ακολουθήθηκαν για την περιγραφή της προτεινόμενης λύσης και οι οποίες περιγράφηκαν λεπτομερώς στα προηγούμενα κεφάλαια.

7.3 Βασικό Σενάριο Χρήσης

Για την καλύτερη κατανόηση όλων των παραπάνω εννοιών στη συγκεκριμένη ενότητα παρουσιάζεται ένα βασικό σενάριο ελέγχου πρόσβασης που αναφέρεται σε περιβάλλοντα παρακολούθησης δικτύων. Το σενάριο αυτό το οποίο έχει ως βάση έναν κανόνα πρόσβασης περιλαμβάνει όλες τις θεμελιώδεις έννοιες του προτεινόμενου μοντέλου καθώς και όλες εκείνες τις πληροφορίες πλαισίου που περιγράφηκαν στα προηγούμενα κεφάλαια. Το σενάριο χρήσης συνοψίζεται ως εξής: *Ένας χρήστης, ο οποίος κατέχει τη θέση του Μηχανικού Συστήματος Ασφαλείας (System Security Engineer) σε έναν οργανισμό, για να τελέσει την εργασία παρακολούθησης Ανίχνευση Εισβολής Δικτύου επιτρέπεται να έχει πρόσβαση με δικαιώματα ανάγνωσης στους παρακάτω συγκεκριμένους τύπους δεδομένων δικτύου των πακέτων: IPProtocolHeader, TCPDestinationPort, TCPSourcePort, UDPDestinationPort, UDPSourcePort, ICMPType και ICMPCode.*

Ο κανόνας εφαρμόζεται υπό την παρακάτω σύνθεση προϋποθέσεων και περιορισμών (***Condition #132 AND (Condition #36 OR Condition #367)) τηρώντας τις υποχρεώσεις Pre-Obligation #37 και Post-Obligation #56***:

- ***Condition #132:*** *Ο τύπος δεδομένου IPProtocolHeader επιτρέπεται να διατεθεί για ανάγνωση εάν υπάρχει μία IPAddress η οποία ανήκει στο υποδίκτυο του οργανισμού το οποίο περιέχει αυτό το στιγμιότυπο τύπου δεδομένου και για αυτή τη συγκεκριμένη IPAddress έχει ανιχνευθεί συναγερμός τύπου επίθεσης Ping of Death*
- ***Condition #367:*** *Εάν ο Μηχανικός Ασφαλείας Συστήματος (System Security Engineer) είναι συνδεδεμένος σε ένα τερματικό μέσα στο δίκτυο του οργανισμού.*
- ***Condition #36:*** *Εάν δεν έχει προηγηθεί προηγούμενη πρόσβαση στους παραπάνω τύπους δεδομένων με δικαιώματα ανάγνωσης για το ίδιο σκοπό και τον ίδιο ρόλο μεταξύ της χρονοθυρίδας 9πμ -5μμ.*
- ***Pre-Obligation #37:*** *Πριν την εφαρμογή του κανόνα θα πρέπει να δοθεί συναίνεση από τον Διαχειριστή Ασφαλείας του Συστήματος (Network Security Administrator)*
- ***Post-Obligation #56:*** *Μετά την εφαρμογή του κανόνα οι τύποι δεδομένων αυτοί θα διατηρηθούν για 30 λεπτά.*

Η οντολογική αναπαράσταση του παραπάνω κανόνα παρουσιάζεται στην Εικόνα 41. Ο κανόνας αυτός ενσωματώνει τα παρακάτω χαρακτηριστικά:

- Σύνθετες προϋποθέσεις

- Χρονικού τύπου πλαίσιο
- Χωρικού τύπου πλαίσιο
- Περιστασιακού τύπου πλαίσιο (Ιστορικό και Συναγερμού)
- Προ - Υποχρεώσεις
- Μετά – Υποχρεώσεις

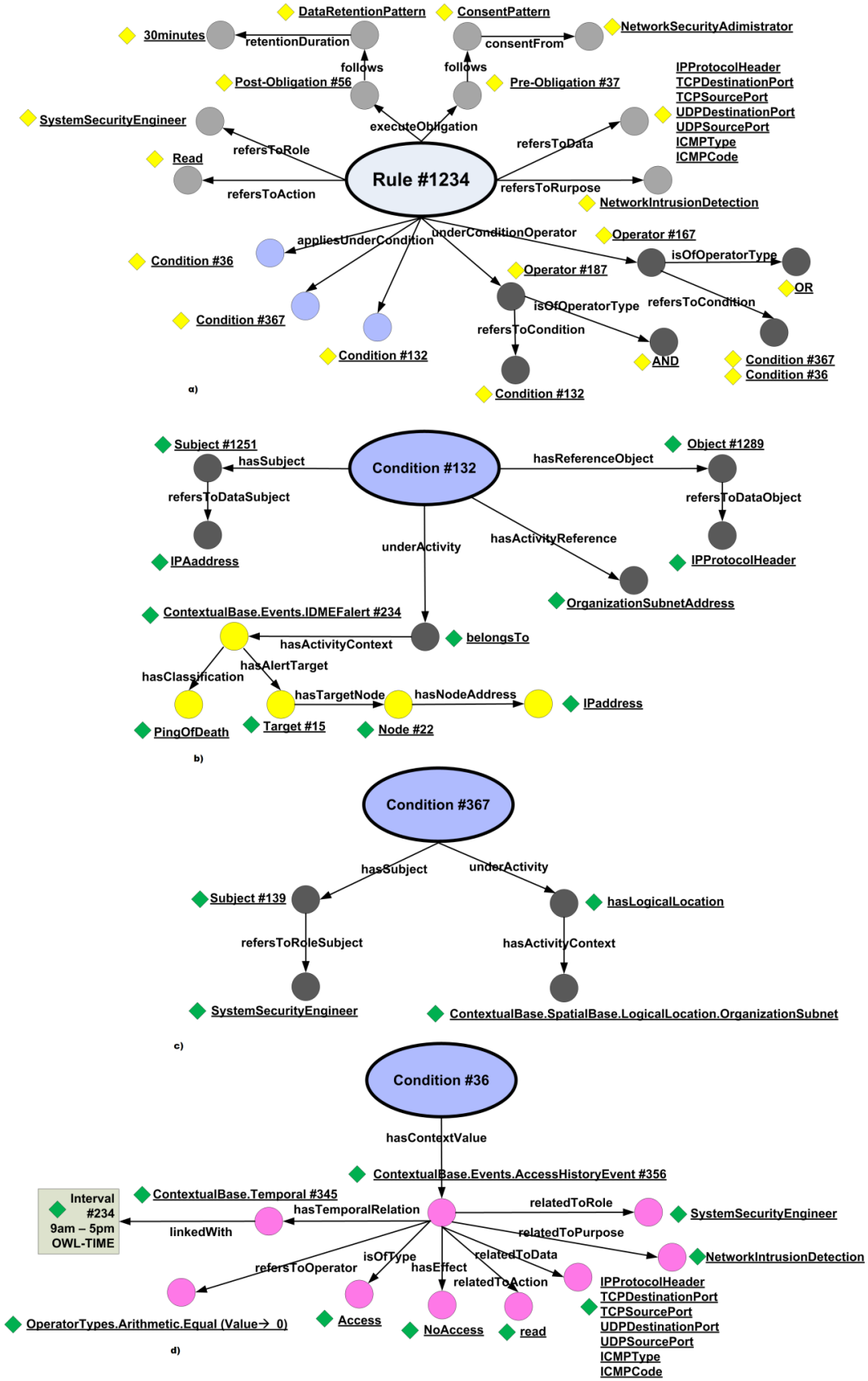
Πιο συγκεκριμένα, το πρώτο μέρος προϋποθέσεων του κανόνα (***Condition #132)*** είναι τύπου πλαισίου *Event.Alert*. Ο τύπος δεδομένου που επηρεάζεται από την προϋπόθεση είναι ο *IPProtocolHeader* το οποίο αναπαρίσταται σημασιολογικά από την κλάση *ReferenceObject*. Επιπλέον, η έννοια η οποία σχετίζεται με την προϋπόθεση και σημειώνεται ως *ConditionSubject*, είναι ο τύπος δεδομένου *IPAddress* υπό την δραστηριότητα (κλάση *Activity*) *belongsTo*. Η δραστηριότητα αυτή αναφέρεται στον τύπο δεδομένου *OrganizationSubnet*. Τέλος, το *Event.Alert* πλαίσιο δραστηριότητας προσδιορίζεται μέσα από τη χρήση των *Classification, Target, Node* και *Address IDMEFalert* κλάσεων.

Το δεύτερο μέρος προϋποθέσεων του κανόνα (***Condition #367)*** αφορά τύπο χωρικού πλαισίου και τα βασικά της προϋπόθεσης αποτελούν οι κλάσεις *ConditionSubject, Activity* και *ContextualBase*. Πιο λεπτομερώς, σαν υποκείμενο της προϋπόθεσης δηλώνεται ο ρόλος του Μηχανικού Ασφαλείας Συστήματος (*System Security Engineer*) και σαν δραστηριότητα η *hasLogicalLocation* η οποία ανήκει σε λογικού τύπου πλαίσιο και πιο συγκεκριμένα στο στιγμιότυπο *OrganizationSubnet*.

Το τρίτο μέρος προϋποθέσεων (***Condition #36)*** αφορά ιστορικό και χρονικό τύπο πλαισίου και αναπαρίσταται από την κλάση *Events.HistoryEvent*. Πιο συγκεκριμένα αναφέρεται στα στιγμιότυπα:

- *SystemSecurityEngineer*,
- *NetworkIntrusionDetection*,
- {*IPProtocolHeader, TCPDestinationPort, TCPSourcePort, UDPDestinationPort, UDPSourcePort, ICMPType* και *ICMPCode*},
- *Read* των κλάσεων *Roles, Purposes, PersonalData* και *Actions* αντιστοίχως.

Επίσης στα πλαίσια της προϋπόθεσης χρησιμοποιείται ο αριθμητικός τελεστής «*equal*» και το χρονικό πλαίσιο της προϋπόθεσης αναφέρεται σε στιγμιότυπο της κλάσης *Interval* της οντολογίας OWL-Time. Τέλος υπάρχει αναφορά στα στιγμιότυπα *NoAccess* και *Access* των κλάσεων *EventResult* και *EventTypes*.



Εικόνα 41: Οντολογική αναπαράσταση κανόνα σεναρίου χρήσης

7.4 Αξιολόγηση

Δεδομένου ότι οι δραστηριότητες που σχετίζονται με την παρακολούθηση δικτύου διαχειρίζονται μεγάλο όγκο προσωπικών αναγνωρίσιμων πληροφοριών (Personal Identifiable Information - PII), εγείρουν σοβαρές ανησυχίες για την προστασία της ιδιωτικότητας. Ως εκ τούτου, οι υποκείμενες τεχνολογίες πρέπει να υποβαθμίσουν κάθε αίσθημα δυσπιστίας που καλλιεργείται από μερική απώλεια του ελέγχου επί των ευαίσθητων πόρων.

Για το λόγο αυτό, ο ορισμός σύνθετων και αποτελεσματικών πολιτικών ασφαλείας που εξαρτώνται δυναμικά από πραγματικού χρόνου παραμέτρους απαιτείται. Προκειμένου να αντιμετωπιστούν αυτές οι απαιτήσεις, μελετήθηκαν οι υπάρχουσες λύσεις, περιγράφηκαν κάποια από τα μειονεκτήματά τους, και παρουσιάστηκε η προτεινόμενη λύση, η οποία αναγνωρίζει τη χρησιμότητα της σημασιολογίας και εκμεταλλεύεται την εκφραστική δύναμη των οντολογιών.

Η προτεινόμενη οντολογία έχει ως στόχο να αντιμετωπίσει τις ελλείψεις που αφορούν κυρίως την προστασία των προσωπικών δεδομένων όσον αφορά τον έλεγχο πρόσβασης, να αποτελέσει τη γνωσιακή βάση για τα συστήματα παρακολούθησης δικτύου αναπαριστώντας όλες τις σχετικές έννοιες και να παρέχει επαρκείς συσχετίσεις μεταξύ αυτών των πληροφοριακών στοιχείων, προκειμένου να καθοριστούν εκφραστικοί και κατά συνέπεια αποτελεσματικοί κανόνες ελέγχου πρόσβασης. Αυτό σημαίνει ότι, η οντολογική δομή ενσωματώνει σημαντικά χαρακτηριστικά που αφορούν την προστασία της ιδιωτικότητας και επίγνωσης πλαισίου που προέρχονται κυρίως από τη θεμελιώσεις αρχές της νομοθεσίας για την προστασία των προσωπικών δεδομένων.

Προφανώς, δεν εμπίπτουν όλες οι απαιτήσεις που απορρέουν από τη νομοθεσία στο πεδίο εφαρμογής της παρούσας έρευνας, όπως η προστασία των δικτύων ή των βάσεων δεδομένων ή η αλληλεπίδραση με μια Αρχή Προστασίας Προσωπικών Δεδομένων, καθώς και οι διατάξεις που σχετίζονται με την αλληλεπίδραση με το υποκείμενο των δεδομένων όπου συνήθως αντιμετωπίζονται με συμβατικές διατάξεις.

Από την άλλη πλευρά, μια πολύ βασική έννοια για την προστασία της ιδιωτικότητας που εμφανίζεται συχνά στις απαιτήσεις, αποτελώντας ένα θεμελιώδες στοιχείο νομιμότητας είναι ο σκοπός για τον οποίο υποβάλλονται σε επεξεργασία τα δεδομένα. Μέσω της οντολογίας, το προτεινόμενο σύστημα παρέχει τα μέσα για τον προσδιορισμό του σκοπού

του κάθε αιτήματος, προκειμένου να καταστεί δυνατή η συλλογή και η επεξεργασία των δεδομένων μόνο όταν οι εν λόγω δραστηριότητες διεξάγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς, προβλέπει μηχανισμούς για τον προσδιορισμό της συμβατότητας μεταξύ των σκοπών επεξεργασίας, ενώ παρέχει επίσης έλεγχο του κατά πόσον οι σκοποί επεξεργασίας συνάδουν με αυτούς για τους οποίους τα δεδομένα έχουν συλλεχθεί.

Οι αρχές της αναγκαιότητας, της επάρκειας και της αναλογικότητας είναι επίσης στενά συνδεδεμένες με το σκοπό . Στην πραγματικότητα , το σύστημα παρέχει τα μέσα για την προδιαγραφή της αναγκαιότητας, καθώς και να είναι σε θέση να εξετάσει κατά πόσον είναι αναγκαία η συλλογή ή η επεξεργασία των συγκεκριμένων δεδομένων για την παροχή της εν λόγω υπηρεσίας, δηλαδή, η εκπλήρωση του σκοπού. Αυτό υπονοεί η σχέση μεταξύ των δεδομένων, των δραστηριοτήτων επεξεργασίας, των ρόλων και των σκοπών που επιτρέπουν τον ορισμό της αναγκαιότητας και της αναλογικότητας των περιορισμών, καθώς και τον προσδιορισμό του τι αποτελεί ελάχιστη χρήση. Επιπλέον, η ανάγκη για ευελιξία και προσαρμοστικότητα του σχεδιασμού του συστήματος πηγάζει από την πολυπλοκότητα του νομικού περιβάλλοντος μέσα στο οποίο ένα σύστημα παρακολούθησης λειτουργεί, τις διαφορετικές νομικές απαιτήσεις μεταξύ διαφορετικών δικαιοδοσιών και τη φύση του νόμου η οποία αλλάζει από καιρό σε καιρό. Ως εκ τούτου, το σύστημα βασίζεται στις αρχές της αφαιρετικότητας και γενίκευσης, έτσι ώστε να είναι εύκολο να παραμετροποιηθεί, ενισχύοντας έτσι τη δυναμική προσαρμοστικότητα και τη διαλειτουργικότητα.

Επιπλέον, σε ορισμένες περιπτώσεις, η πρόσβαση στα δεδομένα περιλαμβάνει συμπληρωματικές δράσεις, μαζί με τα μέσα (π.χ. πολιτικές) για τον καθορισμό και την επιβολή της ενσωμάτωσή τους στα βήματα λειτουργίας της διαδικασίας παρακολούθησης, η οποία πρέπει να προηγείται ή να έπεται της πρόσβασης. Έτσι , η προτεινόμενη οντολογία επιβάλλει αυτό το είδος των δράσεων, που εκφράζονται ως προ-/μετά ενέργειες που πρέπει να πληρούνται. Αυτό αναφέρεται, για παράδειγμα, στην ανωνυμοποίηση των δεδομένων σε πραγματικό χρόνο για την προσαρμογή με την αρχή της αναλογικότητας. Επιπλέον, οι λειτουργίες καταγραφής είναι διαθέσιμες. Εκτός από το να αποτελούν μια συχνά απαιτούμενη συμπληρωματική δράση, η καταγραφή επιτρέπει την ιχνηλασιμότητα και, ως εκ τούτου, την εγκυρότητα των ενεργειών που εκτελούνται. Όσον αφορά την αποθήκευση δεδομένων, το σύστημα παρέχει τα μέσα για την αυτόματη ενημέρωση ή διαγραφή των δεδομένων, όταν αυτά είναι παρωχημένα ή ανακριβή. Η αυτόματη διαχείριση των βάσεων

δεδομένων έχει μεγάλη σημασία και στην περίπτωση της επιβολής των περιόδων διατήρησης των δεδομένων. Σε γενικές γραμμές , το σύστημα είναι σε θέση να ελέγχει, όπως υπαγορεύεται από τους κανονισμούς την αποθήκευση των δεδομένων για σκοπούς διατήρησης μέσω της χρήσης των πολιτικών που ορίζονται στην οντολογία για την εν λόγω υλοποίηση τέτοιου είδους ελέγχου. Επιπλέον, η υποχρέωση περιορισμού της πρόσβασης, σε συνδυασμό με όλα τα παραπάνω, τονίζει την ανάγκη για την επιβολή αποτελεσματικού ελέγχου πρόσβασης. Συνεπώς, ως ένα βήμα περαιτέρω στις υπάρχουσες λύσεις μέσω της προδιαγραφής οντολογίας και της συλλογιστικής το σύστημα επιτρέπει την εκτέλεση πολύπλοκων και δυναμικών διατάξεων ελέγχου πρόσβασης που απαιτούνται για μια ολοκληρωμένη λύση ελέγχου πρόσβασης.

Τέλος, προστιθέμενη αξία στην προτεινόμενη λύση αποτελεί η εφαρμογή λογισμικού επεξεργασίας οντολογίας η οποία απλοποιεί την εκπροσώπηση και τη διαχείριση όλων των σχετικών βασικών εννοιών, καθώς και την προδιαγραφή των πολιτικών.

Συμπεράσματα και μελλοντική εργασία

Η παρούσα πρόταση διατριβής έχει ως αντικείμενο την περιγραφή ενός συστήματος ελέγχου πρόσβασης πληροφοριακών συστημάτων το οποίο κάνει χρήση σημασιολογικών τεχνολογιών, έχει επίγνωση πλαισίου και θέτει ως βασικό στόχο την προστασία της ιδιωτικότητας. Με βάση αυτό προσδιορίστηκαν οι έννοιες της οντολογίας, της επίγνωσης πλαισίου καθώς και της ιδιωτικότητας και το πώς αυτή μπορεί να παραβιαστεί. Έγινε επισκόπηση των οδηγιών του σχετικού νομικού και κανονιστικού πλαισίου για την προστασία της ιδιωτικότητας του χρήστη έτσι ώστε το προτεινόμενο σύστημα να καλύπτει όλες τις πτυχές των οδηγιών αυτών.

Μελετήθηκε συγκριτικά η πλειοψηφία των μοντέλων ελέγχου πρόσβασης που παρουσιάζονται στη βιβλιογραφία τα οποία ενσωματώνουν τα σημαντικότερα χαρακτηριστικά ελέγχου πρόσβασης επίγνωσης πλαισίου και ιδιωτικότητας, βασίζονται σε ρόλους που έχουν ανατεθεί στους χρήστες και χρησιμοποιούν σημασιολογικές τεχνολογίες για την αναπαράσταση και την επεξεργασία των σχετικών πληροφοριών. Παρουσιάστηκαν τα πλεονεκτήματα και οι περιορισμοί των εν λόγω μοντέλων και χρησιμοποιήθηκαν ως βάση και πηγή γνώσης για την ανάπτυξη του προτεινόμενου μοντέλου ελέγχου πρόσβασης.

Είδαμε ακόμα τη σημασία που έχουν οι τεχνολογίες σημασιολογικού ιστού και πιο συγκεκριμένα οι οντολογίες, σαν εργαλείο αναπαράστασης και εξόρυξης γνώσης, όπου χρησιμοποιούνται για τον χαρακτηρισμό των βασικών εννοιών, την αντιμετώπιση της επίγνωσης του πλαισίου και ιδιωτικότητας καθώς και τη διαλειτουργικότητα μεταξύ των διαφορετικών οντοτήτων.

Σε αυτό το πλαίσιο αναπτύξαμε ένα γενικευμένο και αφαιρετικό σημασιολογικό μοντέλο ελέγχου πρόσβασης βασισμένο σε ρόλους μέσω μιας ενοποιημένης και ολοκληρωμένης οντολογίας με σκοπό τη μοντελοποίηση των πολιτικών ελέγχου πρόσβασης με επίγνωση ιδιωτικότητας και πλαισίου που μπορεί να πραγματοποιηθεί για κάθε σφαίρα δραστηριοτήτων σε οποιοδήποτε περιβάλλον πληροφοριακού συστήματος όπου αυτή υλοποιείται.

Τα πλεονεκτήματα τα οποία το προτεινόμενο σύστημα στοχεύει να προσφέρει αφορούν τη λειτουργικότητα του, δηλαδή την ευκολία χρήσης του από τον τελικό χρήστη, την αποδοτικότητά του όσον αφορά την αναπαράσταση και εξόρυξη γνώσης, την πλήρη μοντελοποίηση των βασικών κανόνων της ιδιωτικότητας και την ενσωμάτωση χαρακτηριστικών επίγνωσης πλαισίου όπως αυτά παρουσιάζονται στα σύγχρονα πληροφοριακά συστήματα. Οι κανόνες του χαρακτηρίζονται από υψηλό βαθμό εκφραστικότητας και, μέσω των καινοτόμων χαρακτηριστικών του, δύνανται να περιγράψουν περιορισμούς που τα υφιστάμενα μοντέλα αδυνατούν να ενσωματώσουν. Η ενσωμάτωση της έννοιας του «σκοπού» όπως αυτή περιγράφεται και χρησιμοποιείται αποτελεί τη βασική προϋπόθεση για την προστασία της ιδιωτικότητας σε ένα σύστημα ελέγχου πρόσβασης.

Η εξαγωγή γνώσης πραγματοποιείται σε δύο στάδια. Το πρώτο αφορά την εξαντλητική εξαγωγή γνώσης σε μη πραγματικό χρόνο και περιλαμβάνει την εξαγωγή επιτρεπτών τύπων δεδομένων από τους ρητά ορισμένους κανόνες στην Οντολογία παρέχοντας τη δυνατότητα για αποτίμηση μεμονωμένων ενεργειών πρόσβασης. Το δεύτερο στάδιο, εκμεταλλευόμενο τα αποτελέσματα του πρώτου, αφορά τη σε πραγματικό χρόνο λήψη αποφάσεων αναφορικά με την εξαγωγή περιορισμών και συμπληρωματικών ενεργειών που πρέπει να εκτελεστούν το οποίο δίνει τη δυνατότητα στο σύστημα να διατηρεί χαρακτηριστικά «αυτό-προσαρμοστικότητας» σε σχέση με δυναμικές μεταβολές παραμέτρων του περιβάλλοντος λειτουργίας. Με βάση την αξιολόγηση των σχετικών αλγόριθμων, οι πόροι που απαιτούνται σε όλα τα στάδια της διαδικασίας δεν κρίνονται υπερβολικοί, και υπερτερούν σε σχέση με υπάρχοντα εργαλεία ενώ η επιλογή της εκ των προτέρων εξαγωγής γνώσης οδήγησε ούτως ή άλλως σε σημαντική βελτίωση της επίδοσης του συστήματος.

Προς την αυτοματοποίηση των διαδικασιών λήψης απόφασης και για την κατάλληλη απόδοση των εννοιών και αναπαράσταση των συσχετίσεων που προκύπτουν από τη λειτουργία του συστήματος, επιλέχθηκε η αξιοποίηση ψηφιακών πιστοποιητικών δημοσίου κλειδιού (public key certificates) και ιδιοτήτων (attribute certificates) συμβατών με το διεθνές πρότυπο X.509.

Συνεπώς η μελλοντική ερευνητική εργασία αφορά βελτιώσεις και επεκτάσεις του συστήματος και κινείται στους παρακάτω άξονες:

Την ενσωμάτωση μηχανισμού διαχείρισης «Προτιμήσεων» και λειτουργική ένταξή του στην κλάση Rules. Την περεταίρω ανάλυση στην οντολογία της κλάσης Conditions. Τα μέλη της συγκεκριμένης κλάσης συνιστούν τις προϋποθέσεις κάτω από τις οποίες εφαρμόζεται ο έλεγχος πρόσβασης και αφορούν χρονικούς, χωρικούς, βασισμένους σε συμβάντα και άλλους περιορισμούς. Η πλήρης ανάλυση των στιγμιότυπων και των μεταξύ τους σχέσεων αυτής της κλάσης αποτελεί σημαντική μελλοντική εργασία της παρούσας διατριβής λόγω της πληθώρας και της ετερογένειας των περιορισμών αυτών. Η παρούσα διατριβή λοιπόν στοχεύει στην ακόμα πιο λεπτομερή αναπαράσταση όλων αυτών των προϋποθέσεων και πιο συγκεκριμένα των παρακάτω:

- Χωρικών περιορισμών που εκφράζουν λογικές αλλά και φυσικές τοποθεσίες με βάση τις δικτυακές διευθύνσεις και τις συντεταγμένες θέσης αντίστοιχα, καθώς και περιορισμών που αποτελούν σύνθεση χρονικών και χωρικών προϋποθέσεων.

- Άλλων περιορισμών οι οποίοι είναι συνήθεις σε μηχανισμούς ελέγχου πρόσβασης πληροφοριακών συστημάτων και αφορούν π.χ. στο διαχωρισμό καθηκόντων, σε καταστάσεις του συστήματος, κ.α.

Την ενσωμάτωση πλαισίου που σχετίζεται με «επιθέσεις» πληροφοριακών συστημάτων με στόχο την δημιουργία και εξαγωγή πολιτικών οι οποίες θα έχουν άμεση σχέση με το είδος κάθε απειλής.

Την εφαρμογή και αξιολόγηση του προτεινόμενου μοντέλου σε άλλες εφαρμογές σύγχρονων πληροφοριακών συστημάτων με αυξημένες απαιτήσεις ασφαλείας και προστασίας προσωπικών δεδομένων όπως π.χ. στην διαχείριση αποφάσεων σε συστήματα του τομέα υγείας. Με βάση αυτά, στοχεύουμε να ενσωματώσουμε τον πυρήνα του προτεινόμενου μοντέλου στην διαδικασία ελέγχου πρόσβασης των παραπάνω εφαρμογών δημιουργώντας τις κατάλληλες επεκτάσεις για την αντιμετώπιση των αντιστοίχων αναγκών. Στόχο αποτελεί η αξιολόγηση της γενικότητας, λειτουργικότητας, αποδοτικότητας και αφαιρετικότητας του προτεινόμενου μοντέλου στη χρήση του σε οποιαδήποτε εφαρμογή ελέγχου πρόσβασης.

Οι οντολογίες ως εννοιολογικές μορφοποιήσεις (conceptualizations) αποτελούν προϊόντα υποκειμενικής κρίσης, οπότε το ίδιο πεδίο ενδιαφέροντος είναι δυνατόν να περιγραφεί με διαφορετικούς τρόπους. Άρα οι οντολογίες που αναπτύσσονται αποτελούν ετερογενείς πηγές γνώσης. Το πρόβλημα που προκύπτει είναι αυτό της ετερογένειας (heterogeneity) και καλύπτεται από το συνδυασμό των οντολογιών που στοχεύει στη σημασιολογική διαλειτουργικότητα (semantic interoperability) των συστημάτων ή εφαρμογών οι οποίες χρησιμοποιούν τις "ετερογενείς" οντολογίες. Επομένως, μελλοντικό στόχο αποτελεί η ευθυγράμμιση της προτεινόμενης οντολογίας με υπάρχουσες οντολογίες οι οποίες περιγράφουν παρόμοιες έννοιες, με σκοπό την απάντηση περισσότερο σύνθετων ερωτημάτων.

Τέλος, για την ενίσχυση της διαλειτουργικότητας και ομοιογένειας μεταξύ των διαφόρων συστημάτων οι πολιτικές ελέγχου πρόσβασης που εξάγονται από την οντολογία στοχεύουμε να μετατραπούν σε XACML μορφή, που αποτελεί ευρέως διαδεδομένη γλώσσα αναπαράστασης πολιτικών ασφαλείας, ενσωματώνοντας όλα τα επιπρόσθετα χαρακτηριστικά επίγνωσης πλαισίου και ιδιωτικότητας.

Βιβλιογραφία

Acquisti, A. (2010). "*The Economics of Personal Data and the Economics of Privacy*". OECD Conference Centre. WPISP-WPIE Roundtable. Retrieved on January 31, 2012, from http://www.oecd.org/dataoecd/8/51/46968784.pdf.

Act of Congress, (1974). «Privacy Act», *United States Code*, Title 5, Paragraph 552a, 31 December 1974.

Agrawal, R., Kiernan, J., Srikant, R., & Xu, Y. (2002). "Hippocratic Databases". In *Proceedings of the 28th International Conference on Very Large Data Bases* (*VLDB '02*) (pp. 143-154). USA: VLDB Endowment.

Ajam, N., Cuppens, N., & Cuppens, F. (2010). "Privacy Administration in Distributed Service Infrastructure". In *Proceeding of the 6th International Conference on Security and Privacy in Communication Networks*. Publisher: Springer LNCS, Singapore, September 2010.

Bell David. E., & LaPadula, Leonard J. (1976). "*Secure computer system: Unified exposition and MULTICS interpretation*". Rapport technique.

Bertino, E., Catania, B., Damiani, M.L., & Perlasca, P. (2005). "GEO-RBAC: A spatially aware RBAC". In *Proceedings of the 11th ACM Symposium on Access Control Models and Technologies* (*SACMAT '06*) (pp. 29-37). New York: ACM.

Bhatti, R., Ghafoor, A., Bertino, E., & Joshi, J.B.D. (2005). "X-GTRBAC: an XML-based policy specification framework and architecture for enterprise-wide access control". *Journal of ACM Transactions of Information and System Security*, 8(2), 187-227. New York: ACM.

Biba, K. J. (1977). "*Integrity Considerations for Secure Computer Systems*". Rapport technique, MITRE Corp.

Birnhack, M. D. (2008). "The EU Data Protection Directive: An Engine of a Global Regime". *Computer Law and Security Report*, 24(6), 508-520.

Borst, W. N. (1997). "*Construction of Engineering Ontologies*" PhD Thesis, Center for telematica and information technology. University of Tweently, Enschede, NL, 1997.

Brewer, David F.C., & Nash, Micheal J. (1989). "The Chinese Wall Security Policy". *Security and Privacy*. IEEE Symposium on, vol. 0, page 206.

Butler W. Lampson. Protection. In *5th Princeton Symposium on Information Science and Systems*. Reprinted in ACM Operating Systems Review, vol. 8, no. 1, pages 18-24, 1974.

Byun, J., Bertino, E., & Li, N. (2005). "Purpose Based Access Control for Privacy Protection in Relational Database Systems". In *Proceedings of the 10th ACM symposium on Access control models and technologies*. New York: ACM.

Byun, J.-W., Bertino, E., & Li, N. (2005). "Purpose Based Access Control of Complex Data for Privacy Protection". In *Proceedings of the 10th ACM Symposium on Access Control Models and Technologies* (*SACMAT '05*) (pp. 102-110). New York: ACM.

Casassa Mont, M. (2004). "Dealing with Privacy Obligations: Important Aspects and Technical Approaches". In *Proceedings of the International Workshop on Trust and Privacy in Digital Business* (*TrustBus 2004*) (LNCS 3184, pp. 120-131). Berlin, Germany: Springer Berlin/Heidelberg.

Charalambides, M., Flegkas, P., Pavlou, G., Rubio-Loyola, J., Bandara, A.K., Lupu, E.C., Russo, A., Sloman, M., Dulay, N. (2006). "Dynamic Policy Analysis and Conflict Resolution for DiffServ Quality of Service Management". In *Proceedings of Network Operations and Management Symposium* (*NOMS 06*) (pp.294-304).

Computer Systems Lab Documentation. (2001). "*Access Control and AFS Groups*", http://www.cs.wisc.edu/csl/doc/.

Cuppens, F., & Cuppens-Boulahia, N. (2008). "Modeling contextual security policies". *Journal of ACM Transactions of Information and System Security*, 7(4), 285-305. Berlin, Germany: Springer-Verlag.

Cuppens, F., Cuppens-Boulahia, N., & Ghorbel, M.B. (2007). "High Level Conflict Management Strategies in Advanced Access Control Models". *Journal of Electronic Notes in Theoretical Computer Science*, 186, 3-26. Amsterdam: Elsevier Science Publishers B. V.

Dierks, T., & Rescorla, E. (2008). "RFC-5246: The Transport Layer Security (TLS) ProtocolVersion 1.2", Internet Engineering Task Force Request For Comments.

European Parliament and Council (1995). "Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data". *Official Journal of the European Communities*, L 281, 31-50.

European Parliament and Council (2002). "Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)". *Official Journal of the European Communities*, L 201, 37-47.

European Parliament and Council, (2006). "Directive 2006/24/EC of the European Parliament and Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and the amending Directive 2002/58/EC ', *Official Journal of the European Communities*, No. L. 105, pp. 54-63, April.

eXtensible Access Control Markup Language (XACML) (2005). *Version 2.0. s.l.: OASIS Standard*, 1 Feb 2005.

Fensel, D. (2001). "*Ontologies: Silver Bullet for Knowledge Management and Electronic Commerce*". Springer-Verlag, Berlin, 2001.

Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, R.D., & Chandramouli, R. (2001). "Proposed NIST Standard for Role-Based Access Control". *ACM Transactions on Information and System Security*, 4(3), 224-274.

Ferrini, R., & Bertino, E. (2009). "Supporting RBAC with XACML+OWL". In *Proceedings of the 14th ACM symposium on Access control models and technologies* (*SACMAT '09*) (pp. 145-154). New York: ACM.

Gallup Organization (2008). "Data protection in the European Union: Citizens' perceptions – Analytical Report (Flash Eurobarometer 225)", Retrieved November 29, 2010, http://ec.europa.eu /public_opinion/flash/fl_225_en.pdf.

Gruber, T. R. (1993). "*Towards principles for the Design of Ontologies used for knowledge sharing*". R. Poli, and N. Guarino editors, International Workshop on Formal Ontology, Padova, Italy.

Guarino, N. (1998). "Formal Ontology and Information Systems" In *Proceedings of the 1st International Conference on Formal Ontologies in Information Systems* (*FOIS' 98*), Trento, Italy, IOS Press, pp.3-15, 1998.

Haidar, D.A., Cuppens-Boulahia, N., Cuppens, F., & Debar, H. (2006). "An extended RBAC profile of XACML". In *Proceedings of the 3rd ACM workshop on Secure web services* (*SWS '06*) (pp. 13-22). New York: ACM.

Haseeb, H., Masood, A., Ahmed, M., & Ghafoor, A. (2009). "Integrating GSTRBAC spatial constraints in X-GTRBAC". In *Proceedings of the 6th International Conference on Frontiers of Information Technology* (*FIT '09*). New York: ACM.

Hilty, M., Basin, D.A., & Pretschner, A. (2005). "On Obligations". In *Proceedings of the 10th European Symposium on Research in Computer Security* (*ESORICS '05*). Berlin, Germany: Springer-Verlag.

International Telecommunication Union (2008). "*Information technology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks, ITU-T Recommendation X.509*". Retrieved January 31, 2012, from http://www.itu.int/rec/T-REC-X.509-200508-I.

Jasper, R., & Uschold, M. (1999). "A framework for understanding and classifying ontology applications" In *Proceedings of the Workshop on Ontologies and Problem- Solving Methods*, Stockholm, Sweden, 1999.

Java Community Process, (2007). «JSR 220: Enterprise JavaBeans™ 3.0», Java Specification Requests, 2007.

Java Secure Socket Extension. Retrieved April 2, 2014, from: docs.oracle.com/javase/7/docs/technotes/guides/security/jsse/JSSERefGuide.html

Java Universal Network/Graph Framework, Available: http://jung.sourceforge.net/

JavaBeans Open Source Software Application Server, (2009). Retrieved April 2, 2014, from: http://www.jboss.org/

Jena (2013). *The Jena Ontology API*, home page: http://jena.sourceforge.net/ontology/.

Joshi, J.B.D., Bertino, E., Latif, U., & Ghafoo, A. (2005). "A Generalized Temporal Role-Based Access Control Model". *Journal of IEEE Transactions on Knowledge and Data Engineering*, 15, 4-23. Los Alamitos, CA, USA: IEEE Computer Society.

Kagal, L., Berners-Lee, T., Connolly, D., & Weitzner, D. (2006). "*Promoting Interoperability between Heterogeneous Policy Domains*". Massachusetts Institute of Technology, Computer Science and Artificial Intelligence Lab. Cambridge, MA 02139.

Krishnamurthy, B., & Rexford, J. (2001) "*Web Protocols and Practice: HTTP/1.1" Networking Protocols, Caching, and Traffic Measurement* (Boston: Addison Wesley, 2001).

LeFevre, K., Agrawal, R., Ercegovac,V., Ramakrishnan, R., Xu, Y., & DeWitt, D.J. (2004). "Limiting Disclosure in Hippocratic Databases". In *Proceedings of the 30th International Conference on Very Large Databases* (*VLDB 2004*). Toronto, Canada.

Levy, Henry M. (1984). "*Capability-based computer systems*". *Butterworth-Heinemann*, Newton, MA, USA.

Lioudakis, G.V., Gaudino, F., Boschi, E., Bianchi, G., Kaklamani, D.I., & Venieris, I.S. (2010). "*Legislation-Aware Privacy Protection in Passive Network Monitoring*". In I. M. Portela, M. M. Cruz-Cunha (Ed.), Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues (ISBN: 978-161-5209-75-0). New York: IGI Global Pubs.

Masoumzadeh, A., & Joshi, J. (2008). "PuRBAC: Purpose-Aware Role-Based Access Control". In *Proceedings of the On the Move to Meaningful Internet Systems*: OTM 2008 (LNCS 5332). Berlin, Germany: Springer Berlin / Heidelberg.

Neches, R., Fikes, R. E., Finin, T. , Gruber, T. R. , Senator, T. , & Swartout, W. R. (1991). "*Enabling technology for knowledge sharing*". AI Magazine, Vol.12, No.3, pp.36-56.

Ni, Q., Bertino, E., Lobo, J., Brodie, C., Karat, C.M., Karat, J., & Trombetta, A. (2010). "Privacy-aware role-based access control". *Journal of ACM Transactions Information System Security*, 13(3), 1-31. New York: ACM.

Organization for Economic Co-operation and Development – OECD (1980). "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*". Retrieved April 7, 2014, from http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

Pfleeger C. P. (1997). "*Security In Computing* (Second Edition)". ISBN 0-13-337486-6. Prentice-Hall PTR.

Platform for Privacy Preferences (P3P) Project, *http://www.w3.org/P3P/*, The World Wide Web Consortium (W3C), 1994-2003.

Priebe, T., Fernandez, E. B., Mehlau, J. I., & Pernul, G. (2004). "A Pattern System For Access Control". In *in Research Directions in Data and Applications Security XVIII*, C. Farkas and P. Samarati (Eds.), Procs of the 18th. Annual IFIP WG 11.3 Working Conference on Data and Applications Security, pages 2528. Kluwer.

Ravari, A., Jafarian, J., Amini, M., & Jalili, R. (2010). "GTHBAC: A Generalized Temporal History Based Access Control Model". *Journal of Telecommunication Systems*, 45(2), 111-125. Netherlands: Springer.

Ravari, A.N., Amini, M., Jalili, R., & Jafarian, J.H. (2008). "A history based semantic aware access control model using logical time". In *Proceedings of the 11th International Conference on Computer and Information Technology* (*ICCIT 2008*) (pp. 43-50). Khulna, Bangladesh.

Rei Ontology Specifications, http://www.csee.umbc.edu/~lkagal1/rei/.

Samarati, P., 2001. "*Protecting respondents' identities in microdata release*". Trans. Knowledge Data Eng., 13: 1010-1027.

Samuel, A., Ghafoor, A., & Bertino, E. (2008). "*A Framework for Specification and Verification of Generalized Spatio-Temporal Role Based Access Control Model*". CERIAS Technical Report 2007-08. Purdue University.

Sandhu, R.S., Coyee, E.J., Ferinstein, H.L., & Youman, C.E. (1996). "Role-based access control model". *IEEE Computer*, 29(2), 38-47.

Sirin, E., Evren, Parsia, B., Grau, B.C., Kalyanpur, A., & Katz, Y. (2007). "Pellet: A practical owl-dl reasoned", in *Web Semantics: science, services and agents on the World Wide Web* Volume:5, pp. 51-53.

Solove, D. J. (2006). "*A Brief History of Information Privacy Law*". In C. Wolf (Ed), Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age (pp. 1-46). New York, NY, USA: Practising Law Institute.

TCSEC, (1985). Trusted Computer System Evaluation Criteria, December 1985.

Telecommunication Standardization Sector of International Telecommunication Union, (2008). «Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks», ITU-T Recommendation X.509, November.

The Legion of the Bouncy Castle, (2006). Retrieved April 2, 2014, from: http://www.bouncycastle.org/

United Nations (1948). "Universal Declaration of Human Rights", Retrieved January 31, 2012, from http://www.ohchr.org/EN/UDHR/Documents/60UDHR/bookleten.pdf.

United States Congress, (1996). «Health Insurance Portability and Accountability Act of 1996», *Public Law 104-191*, 21 August 1996.

Uschold, M., & Cruninger, M. (1996) "Ontologies: Principles, methods and applications". *Knowledge Engineering Review*, Vol. 11, No. 3, pp. 93-155, 1996.

Uszok, A., Bradshaw, J. M., & Jeffers, R. (2004). "*KAoS: A Policy and Domain Services Framework for Grid Computing and Semantic Web Services*". Institute for Human and Machine Cognition (IHMC) 40 S. Alcaniz, Pensacola, FL 32502.

Uszok, A., Bradshaw, J. M., Johnson, M., Jeffers, R., Tate, A., Dalton, J., & Aitken, S. (2004). "KAoS Policy Management for Semantic Web Services". *IEEE Intelligent Systems,* July 2004.

Warren, S. D., & Brandeis, L. D. (1890). "*The Right to Privacy*". Harvard Law Review, 4(5), 193-220.

WebDAV, (2000). "*WebDAV Access Control Protocol*". webdav.org, http://www.webdav.org/acl/.

Westerinen, A. et al., (2001). "Terminology for Policy-Based Management", *IETF RFC 3198*, November.

Westin, A. (1967). "*Privacy and Freedom*", New York: Atheneum, 487 pages.

World Wide Web Consortium (2006). "*Extensible Markup Language (XML) XML 1.1* (Second Edition)". Retrieved January 31, 2012, from http://www.w3.org/TR/2006/REC-xml11-20060816.

World Wide Web Consortium (W3C), (2004). "*RDF Vocabulary Description Language 1.0: RDF Schema*", W3C Recommendation, February 2004, home page: http://www.w3.org/TR/rdf-schema/.

Zope, (2003). "*Access Control in Zope*". Zope Book (zope.org). home page: http://zope.org/Documentation/Books/ZopeBook/2_6Edition/Security.stx.

Βουλή των Ελλήνων, (1997). «Νόμος 2472/1997: Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα», *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Τεύχος Πρώτο, Αρ. Φύλλου 50, 10 Απριλίου.

Βουλή των Ελλήνων, (2003). «Νόμος 3115/2003: Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών», *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Τεύχος Πρώτο, Αρ. Φύλλου 47, 27 Φεβρουαρίου 2003.

Βουλή των Ελλήνων, (2006). «Νόμος 3471/2006: Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Νόμου 2472/1997», *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Τεύχος Πρώτο, Αρ. Φύλλου 133, 28 Ιουνίου.

Βουλή των Ελλήνων, (2011). «Νόμος 3917/2011: Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό

υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις», *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Τεύχος Πρώτο, Αρ. Φύλλου 22, 21 Φεβρουαρίου.

Ζ' Αναθεωρητική Βουλή των Ελλήνων, (2001). «Το Σύνταγμα της Ελλάδας», Αθήνα, 6 Απριλίου.

Ηνωμένα Έθνη, (1996). «Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα», Απόφαση 2200 Α (XXI), 16 Δεκεμβρίου.

Ομοσπονδιακή Συνέλευση, (1787). «Σύνταγμα των Ηνωμένων Πολιτειών», 17 Σεπτεμβρίου.

Συμβούλιο της Ευρώπης, (1950). «Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου», 4 Νοεμβρίου.

Δημοσιεύσεις

Διεθνή επιστημονικά περιοδικά

F. I. Gogoulos, A. P. Antonakopoulou, G. V. Lioudakis, A. Mousas, D. I. Kaklamani and I. S. Venieris. "An Authorization Model for Cross-Enterprise Collaborations", Security and Communication Networks. 2014.

F. I. Gogoulos, A. P. Antonakopoulou, G. V. Lioudakis, A. Mousas, D. I. Kaklamani and I. S. Venieris. "On the design of a privacy aware authorization engine for collaborative environments", Electronic Markets. 2014.

A. P. Antonakopoulou, F. I. Gogoulos, G. V. Lioudakis, A. Mousas, D. I. Kaklamani and I. S. Venieris. "An Ontology for Privacy-aware Access Control in Network Monitoring Environments", Journal of Research and Practice in Information Technology. 2013.

Κεφάλαια σε βιβλία

F. I. Gogoulos, A. P. Antonakopoulou, G. V. Lioudakis, D. I. Kaklamani, I. S. Venieris, Trust In An Enterprise World: A Survey, in Handbook of Research on Enterprise 2.0, Maria Manuela, Cruz-Cunha Fernando, Moreira João Varajão (Ed.), 2012, IGI Global.

A. P. Antonakopoulou, G. V. Lioudakis, F. I. Gogoulos, D. I. Kaklamani, I. S. Venieris, Leveraging Access Control for Privacy Protection: A Survey,in Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards, G. Yee (Ed.), 2011, IGI Global.

Πρακτικά διεθνών επιστημονικών συνεδρίων

A. P. Antonakopoulou, F. I. Gogoulos, G. V. Lioudakis, A. S. Mousas, D. I. Kaklamani, I. S. Venieris, Semantic Information Model for Privacy-Aware Access Control,in Proceedings of the 14th Panhellenic Conference on Informatics (PCI 2010), Tripolis, Greece, September 10 - 12, 2010.

A. S. Mousas, A. P. Antonakopoulou, F. I. Gogoulos, G. V. Lioudakis, D. I. Kaklamani, I. S. Venieris, Visualising Access Control: The PRISM Approach,in Proceedings of the 14th Panhellenic Conference on Informatics (PCI 2010), Tripolis, Greece, September 10 - 12, 2010.

F. I. Gogoulos, A. P. Antonakopoulou, G. V. Lioudakis, A. S. Mousas, D. I. Kaklamani, I. S. Venieris, Privacy-Aware Access Control and Authorization in Passive Network Monitoring Infrastructures,in Proceedings of the 3rd IEEE International Symposium on Trust, Security and Privacy for Emerging Applications (IEEE TSP-2010), Bradford, UK, June 29 - July 1, 2010.

G. V. Lioudakis, F. I. Gogoulos, A. P. Antonakopoulou, A. S. Mousas, D. I. Kaklamani, I. S. Venieris, An Access Control Approach for Privacy-Preserving Passive Network Monitoring ,in Proceedings of the 4th International Conference for Internet Technology and Secured Transactions (ICITST-2009), London, UK, November 9-12, 2009

F. I. Gogoulos, A. P. Antonakopoulou, A. S. Mousas, G. V. Lioudakis, D. I. Kaklamani, I. S. Venieris, Privacy-Aware Passive Network Monitoring,in Proceedings of the 13th Panhellenic Conference on Informatics (PCI 2009), Corfu, Greece, September 10 - 12, 2009.

G. V. Lioudakis, F. I. Gogoulos, A. P. Antonakopoulou, D. I. Kaklamani, I. S. Venieris, Privacy Protection in Passive Network Monitoring: an Access Control Approach,IEEE 23rd International Conference on Advanced Information Networking and Applications (AINA-09), University of Bradford, Bradford, UK, May, 2009.

C. Papagianni, G. Karagiannis, N. D. Tselikas, E. Sfakianakis, I.P. Chochliouros, D. Kabilafkas, T. Cinkler, L. Westberg, P. Sjodin, M. Hidell, S. Heemstra de Groot, T. Kontos, C.Katsigiannis, C. Pappas, A. P. Antonakopoulou, I. S. Venieris, Supporting end-to-end resource virtualization for Web 2.0 applications using Service Oriented Architecture,2nd IEEE Workshop on Enabling the Future Service-Oriented Internet , New Orleans, LA, USA, November, 2008.

Συνοπτικό Βιογραφικό Σημείωμα

Η κ. Άννα Αντωνακοπούλου γεννήθηκε στην Αθήνα το 1983. Αποφοίτησε από το 2ο Γενικό Λύκειο Γλυφάδας το 2000 με βαθμό «Άριστα». Το ίδιο έτος εισήχθη στη Σχολή Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών του Πανεπιστημίου Πατρών απ'όπου και αποφοίτησε το 2006 με βαθμό «Λίαν Καλώς».

Το 2007 έγινε δεκτή ως υποψήφια Διδάκτορας του τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου και ερευνητικός συνεργάτης του ΕΜΠ και του Ερευνητικού Πανεπιστημιακού Ινστιτούτου Συστημάτων Επικοινωνιών και Υπολογιστών (ΕΠΙΣΕΥ). Κατά την ερευνητική της εργασία μελέτησε, σχεδίασε και ανέπτυξε πρωτότυπο σύστημα για τον έλεγχο πρόσβασης με επίγνωση ιδιωτικότητας και πλαισίου πληροφοριακών συστημάτων κάνοντας χρήση οντολογιών. Έχει συμμετάσχει σε ερευνητικά και αναπτυξιακά εθνικά και ευρωπαϊκά έργα.

Τα ερευνητικά της ενδιαφέρονται αφορούν κυρίως τις περιοχές της προστασίας προσωπικών δεδομένων, των τεχνολογιών λογισμικού, καθώς και τις εφαρμογές σημασιολογικών τεχνολογιών στις εν λόγω περιοχές. Έχει συγγράψει αρκετές επιστημονικές εργασίες σε διεθνή συνέδρια και επιστημονικά βιβλία.

Τέλος η κ. Αντωνακοπούλου έχει εργασθεί στον ιδιωτικό τομέα ως Μηχανικός Πληροφορικής, συμμετέχοντας σε πληθώρα αναπτυξιακών έργων, και είναι μέλος του Τεχνικού Επιμελητηρίου Ελλάδος (Τ.Ε.Ε.).