Ατομική Διπλωματική Εργασία

ΜΕΛΕΤΗ ΠΡΟΣΕΓΓΙΣΕΩΝ ΠΡΟΣΤΑΣΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΕ ΣΥΣΤΗΜΑΤΑ ΥΠΗΡΕΣΙΩΝ ΜΕ ΕΠΙΓΝΩΣΗ ΤΟΥ ΠΛΑΙΣΙΟΥ ΧΡΗΣΗΣ

Μαρία Αναστάση

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2012

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μελέτη προσεγγίσεων προστασίας της ιδιωτικότητας σε συστήματα με επίγνωση του πλαισίου χρήσης

Μαρία Αναστάση

Επιβλέπουσα Καθηγήτρια
Καπιτσάκη Γεωργία

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Μάιος 2012

Ευχαριστίες

Θα ήθελα να απευθύνω τις ευχαριστίες μου στην επιβλέπουσα καθηγήτρια της διπλωματικής μου εργασίας κα. Γεωργία Καπιτσάκη, για την καθοδήγηση της καθώς και για το βοηθητικό υλικό που μου παρέθεσε προς μελέτη. Ευχαριστώ επίσης την οικογένεια μου και τους κοντινούς μου ανθρώπους για την αμέριστη υποστήριξη και συμπαράσταση τους όλα αυτά τα χρόνια.

Περίληψη

Η χρήση του πλαισίου χρήσης είναι σημαντική για διαδραστικές εφαρμογές και ιδιαίτερα για εφαρμογές όπου το πλαίσιο του χρήστη μεταβάλλεται ραγδαία, όπως είναι το περιβάλλον του διάχυτου υπολογισμού. Η πληροφορία πλαισίου χρήσης αποτελεί σημαντική παράμετρο στην παροχή υπηρεσιών στην προσπάθεια προσφοράς υπηρεσιών που λαμβάνουν υπόψη στοιχεία που σχετίζονται με τα χαρακτηριστικά του περιβάλλοντος στο οποίο βρίσκεται ο χρήστης, όπως είναι η τοποθεσία, οι καιρικές συνθήκες, κτλ. Τα τελευταία χρόνια, το πρόβλημα της διαχείρισης του πλαισίου χρήσης, καθώς και η ανάπτυξη υπηρεσιών με επίγνωση του πλαισίου χρήσης, έχουν γίνει σημαντικές και ενδιαφέρουσες ερευνητικές περιοχές. Με την χρήση μικροσκοπικών αισθητήρων, φθηνών μικροεπεξεργαστών και ασύρματων επικοινωνιών, η τεχνολογία των υπολογιστών μπορεί να εισβάλλει στην καθημερινή μας ζωή με ένα απόλυτο διακριτικό τρόπο. Το βασικό μειονέκτημα των υπηρεσιών με επίγνωση του πλαισίου χρήσης (context-aware services) είναι η επίδραση τους στο δικαίωμα ιδιωτικότητας των χρηστών λόγω της χρήσης προσωπικών δεδομένων για την εκτέλεση τους και αυτό είναι και το θέμα που απασχολεί διάφορους ερευνητές τα τελευτέα χρόνια. Η εξασφάλιση τεχνικών μέσων που θα παρέχει πλήρη διασφάλιση της προστασίας της ιδιωτικότητας είναι κάτι αρκετά δύσκολο μέχρι τώρα, αλλά γίνονται ολοένα και περισσότερες προσπάθειες εύρεσης ενός καλού μηχανισμού προστασίας της ιδιωτικότητας (privacy), δηλαδή προστασίας των ευαίσθητων δεδομένων του χρήστη από την μη εξουσιοδοτημένη διάδοση και χρήση τους.

Κύριο μέλημα αυτής της διπλωματικής εργασίας ήταν η βιβλιογραφική μελέτη διαφόρων προσεγγίσεων που έχουν προταθεί για την προστασία της ιδιωτικότητας και την ενσωμάτωση διαδικασιών και αλγορίθμων διαφύλαξης της ιδιωτικότητας σε συστήματα υπηρεσιών με επίγνωση του πλαισίου χρήσης. Μέσα από αυτήν την βιβλιογραφική μελέτη προκύπτει μια συγκριτική μελέτη των προσεγγίσεων ούτως ώστε να εντοπιστούν πιθανές παραλείψεις και περιοχές βελτίωσης. Έπειτα, προτείνονται στοιχεία που θα ήταν χρήσιμο και ευνοικό να χαρακτηρίζουν μια αρχιτεκτονική που λαμβάνει υπόψη της και συνδυάζει στοιχεία από τις προσεγγίσεις που παρουσιάζονται.

Περιεχόμενα

Λίστα σχημάτων

Λίστα πινάκων

Κεφάλαιο 1

Εισαγωγή

1.1 Το Πρόβλημα

Η χρήση του πλαισίου χρήσης είναι σημαντική για διαδραστικές εφαρμογές και ιδιαίτερα για εφαρμογές όπου το πλαίσιο του χρήστη μεταβάλλεται ραγδαία, όπως είναι το περιβάλλον του διάχυτου υπολογισμού. Η πληροφορία πλαισίου χρήσης αποτελεί σημαντική παράμετρο στην παροχή υπηρεσιών στην προσπάθεια προσφοράς υπηρεσιών που λαμβάνουν υπόψη στοιχεία που σχετίζονται με τα χαρακτηριστικά του περιβάλλοντος στο οποίο βρίσκεται ο χρήστης, όπως είναι η τοποθεσία, οι καιρικές συνθήκες, κτλ. Τα τελευταία χρόνια, το πρόβλημα της διαχείρισης του πλαισίου χρήσης, καθώς και η ανάπτυξη υπηρεσιών με επίγνωση του πλαισίου χρήσης, έχουν γίνει σημαντικές και ενδιαφέρουσες ερευνητικές περιοχές. Με την χρήση μικροσκοπικών αισθητήρων, φθηνών μικροεπεξεργαστών και ασύρματων επικοινωνιών, η τεχνολογία των υπολογιστών μπορεί να εισβάλλει στην καθημερινή μας ζωή με ένα απόλυτο διακριτικό τρόπο. Η προστασία της ιδιωτικότητας (privacy) δηλαδή η προστασία της διάδοσης και χρήσης των ευαίσθητων δεδομένων του χρήστη, αποτελεί ένα σημαντικό ζήτημα για τις εφαρμογές με επίγνωση του πλαισίου χρήσης (context-aware services), οι οποίες σχετίζονται τόσο με προσωπικά στοιχεία του χρήστη όσο και με πληροφορίες για την τρέχουσα κατάσταση και τη δραστηριότητα του.

1.2 Σκοπός της Διπλωματικής

Σκοπός της διπλωματικής εργασίας ήταν η βιβλιογραφική μελέτη των διαφόρων προσεγγίσεων που έχουν προταθεί για την προστασία της ιδιωτικότητας και την

ενσωμάτωση διαδικασιών διαφύλαξης της ιδιωτικότητας σε συστήματα υπηρεσιών με επίγνωση του πλαισίου χρήσης. Το ζητούμενο ήταν να προκύψει μια συγκριτική μελέτη των προσεγγίσεων και να εντοπιστούν πιθανές παραλείψεις και περιοχές βελτίωσης. Για ευκολότερη σύγκριση των προσεγγίσεων, σχεδιάστηκαν πίνακες στους οποίους σημειώθηκε για κάθε διαφορετική προσέγγιση που μελετήθηκε, τα χαρακτηριστικά περιβάλλοντος κινητού υπολογισμού (mobile computing) με επίγνωση του πλαισίου χρήσης και της ιδιωτικότητας που κάλυπταν. Η συγκέντρωση των προτεινόμενων λύσεων και διαδικασιών διαφύλαξης της ιδιωτικότητας διευκολύνει το ξεκίνημα μίας νέας προσπάθειας επινόησης μηχανισμού προστασίας της ιδιωτικότητας με στόχο την κάλυψη των υφιστάμενων μηχανισμών όσο είναι δυνατό, καθώς και τον συνδυασμό των ισχυρών στοιχείων αυτών για ένα καλύτερο αποτέλεσμα.

Η δομή της εργασίας έχει ως ακολούθως. Στο κεφάλαιο 2 ορίζονται και περιγράφονται γενικές εισαγωγικές έννοιες για καλύτερη κατανόηση του θέματος, όπως είναι οι έννοιες του κινητού υπολογισμού, του διάχυτου υπολογισμού, του πλαισίου χρήσης καθώς και η έννοια των εφαρμογών με επίγνωση του πλαισίου χρήσης. Έπειτα στο κεφάλαιο 3 ορίζεται η έννοια της ιδιωτικότητας, η οποία αποτελεί την λέξη κλειδί σε ολόκληρο το κείμενο, περιγράφονται οι αρχές προστασίας της ιδιωτικότητας όπως αυτές πηγάζουν από τις Νομικές Αρχές και επίσης εξηγείται γιατί η ιδιωτικότητα είναι ένα φλέγον θέμα σε περιβάλλοντα διάχυτου υπολογισμού. Στο κεφάλαιο 4 περιγράφονται κάποιες υπάρχουσες γενικές τεχνολογίας διαχείρισης της ιδιωτικότητας όπως είναι η πλατφόρμα προτιμήσεων ιδιωτικότητας P3P για ιστοτόπους και οι γλώσσες σύνταξης επιχειρησιακών πολιτικών XACML και EPAL. Στο κεφάλαιο 5 ακολουθεί ανάλυση και περιγραφή των κυριοτέρων χαρακτηριστικών των προτεινόμενων προσεγγίσεων ανά κατηγορία. Βάσει των περιγραφών αυτών, δημιουργήθηκαν πίνακες στους οποίους φαίνεται συνοπτικά ποια χαρακτηριστικά πλαισίου χρήσης και ιδιωτικότητας καλύπτει κάθε προσέγγιση. Οι πίνακες αυτές φαίνονται στο κεφάλαιο 6. Στο κεφάλαιο 7 εξάγωνται κάποια συμπεράσματα σχετικά με στοιχεία που μπορούν να συνθέτουν μία αρχιτεκτονική προστασίας ιδιωτικότητας σε συστήματα με επίγνωση του πλαισίου χρήσης. Επίσης παρουσιάζονται επιθυμητά χαρακτηριστικά του μοντέλου πληροφορίας πλαισίου χρήσης και τέλος προτείνεται η χρήση οντολογίας για

αναπαράσταση της σημασιολογίας. Τέλος στο κεφάλαιο 8, διατυπώνονται διάφορα γενικά συμπεράσματα που προκύπτουν από τα προηγούμενα κεφάλαια.

Κεφάλαιο 2

Εισαγωγικές Έννοιες

2.1 Η έννοια του κινητού υπολογισμού (mobile computing)

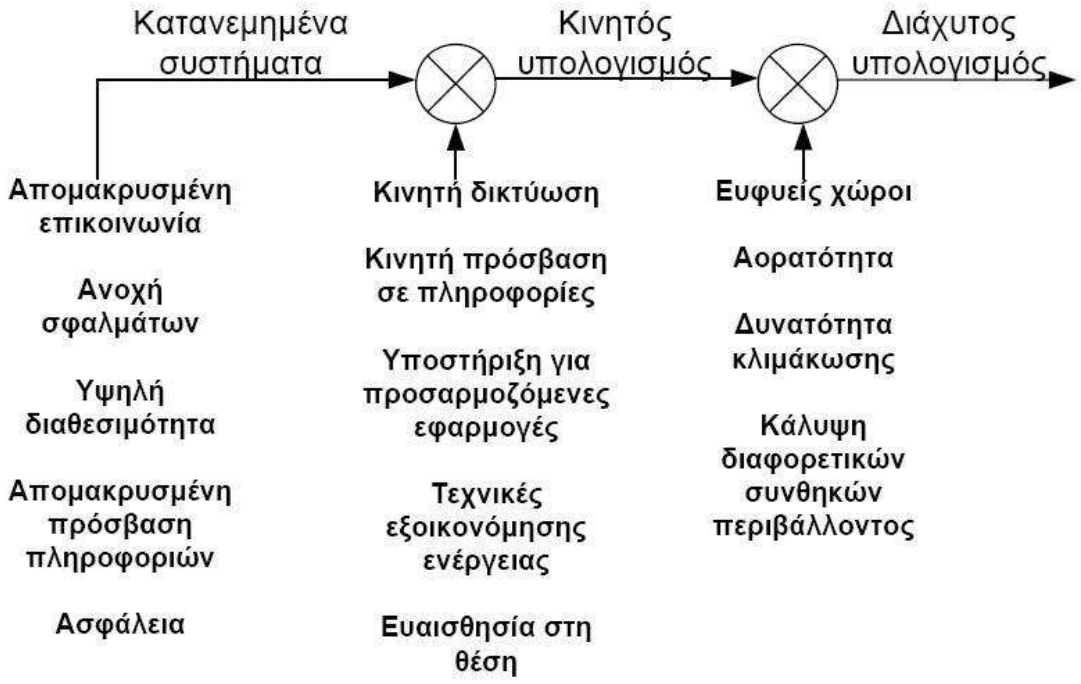
Ο κινητός υπολογισμός (mobile computing) [29] αποτελεί ένα κατανεμημένο σύστημα στο οποίο συμμετέχουν κόμβοι που κινούνται και επικοινωνούν μεταξύ τους ασύρματα. Οι τεχνολογικές εξελίξεις όσον αφορά την σμίκρυνση των συσκευών και την ασύρματη δικτύωση, έχουν οδηγήσει στην ολοκλήρωση μικρών και φορητών υπολογιστικών συσκευών σε κατανεμημένα συστήματα. Ο όρος κινητός υπολογισμός αποτελεί ένα γενικό όρο, που χρησιμοποιείται για να αναφερθούμε σε μία ποικιλία συσκευών που επιτρέπουν σε ένα χρήστη να έχει πρόσβαση σε δεδομένα και πληροφορίες οποιαδήποτε στιγμή και από όπου κι αν βρίσκεται. Περιλαμβάνει συνήθως τους υπολογιστές τσέπης, τους υπολογιστές παλάμης (palmtop) και τα κινητά τηλέφωνα τρίτης γενεάς ή έξυπνα τηλέφωνα (smartphones) που διαθέτουν λειτουργικό σύστημα.

Ο κινητός υπολογισμός είναι αυτό που δίνει ώθηση στην εξέλιξη του Διαδικτύου. Βασικό πλεονέκτημα των φορητών συσκευών είναι ακριβώς η φορητότητα τους και συνακόλουθα η απεξάρτηση τους από το χώρο και τα απαιτούμενα καλώδια για τη σύνδεση με το Διαδίκτυο. Το πλήθος και η ποικιλία φορητών τεχνολογιών που έχουν επικρατήσει στις μέρες μας, καθιστά την πρόσβαση στο Διαδίκτυο όχι μόνο δυνατή αλλά και αναπόσπαστο κομμάτι της καθημερινής ζωής των ατόμων. Η διείσδυση των τεχνολογιών αυτών στην καθημερινή ζωή των ατόμων, έχει αλλάξει κατά πολύ τον

τρόπο με τον οποίο επικοινωνούν, εργάζονται, αναζητούν πληροφορίες και οργανώνουν την ζωή τους.

2.2 Η έννοια του διάχυτου υπολογισμού (pervasive computing)

Ο διάχυτος υπολογισμός (pervasive computing), γνωστό και ως ubiquitous computing, αποτελεί την εξέλιξη του κινητού υπολογισμού (mobile computing). Οραματιστής του αναγνωρίζεται ευρέως ο Mark Weiser [34], ο οποίος πίστευε ότι στόχος του διάχυτου υπολογισμού είναι η εκτεταμένη χρήση πολλών υπολογιστών, οι οποίοι βρίσκονται κατανεμημένοι σε όλο το φυσικό περιβάλλον. Στη σημερινή εποχή πράγματι οι άνθρωποι περιβάλλονται από αντικείμενα και συσκευές που διαθέτουν ενσωματωμένη υπολογιστική ικανότητα, συνθέτοντας “περιρρέουσα νοημοσύνη” (ambient intelligence). Με την εφαρμογή της νέας αυτής γενιάς υπολογιστών, φαίνεται ότι επιβεβαιώνεται η γνωστή ρήση του Weiser: “Οι περισσότερες επιδραστικές τεχνολογίες είναι αυτές που δεν γίνονται αντιληπτές…”. [33]



Σχήμα 2.1 Η εξέλιξη των τεχνολογιών.

Οι διασυνδεδεμένοι υπολογιστικοί και δικτυακοί πόροι που είναι κατανεμημένοι στο φυσικό περιβάλλον, επιτρέπουν στους χρήστες μέσω φυσικών διεπαφών χρήσης, να έχουν πρόσβαση σε πληροφορίες και υπολογιστικούς πόρους από οπουδήποτε και

οποιαδήποτε χρονική στιγμή. Οι υπολογιστές αυτοί παρέχουν υπηρεσίες χωρίς ο χρήστης να γνωρίζει ή να αντιλαμβάνεται την ύπαρξη τους στο περιβάλλον. Οι παρεχόμενες υπηρεσίες χαρακτηρίζονται από την δυνατότητα πρόσβασης σε μεγάλο πλήθος δεδομένων και την ταχύτητα υλοποίησης και προσαρμογής τους στις απαιτήσεις, προτιμήσεις και ικανότητες του ανθρώπου και του περιβάλλοντος στο οποίο βρίσκεται κάθε φορά. Οι χρήστες επομένως δεν χρειάζεται να εκπαιδεύονται στη χρήση εξειδικευμένων συσκευών αφού η τεχνολογία ενσωματώνεται στο περιβάλλον του και λειτουργεί στο παρασκήνιο. Αντιθέτως, οι τεχνολογίες που περιβάλλουν τους χρήστες θα πρέπει να προσαρμόζονται στα χαρακτηριστικά τους και να τους υποστηρίζουν στο μέγιστο βαθμό, ώστε η αλληλεπίδραση με τα συστήματα να είναι φυσική, ευχάριστη και να μη γίνεται αντιληπτή από το χρήστη [34].

Οι δύο σημαντικές περιοχές στις οποίες βασίζεται ο διάχυτος υπολογισμός (pervasive computing) είναι τα κατανεμημένα συστήματα (distributed systems) και ο κινητός υπολογισμός. Στις αρχές της δεκαετίας του 1990, έκαναν την εμφάνιση τους οι φορητοί υπολογιστές (laptops) καθώς και τα ασύρματα δίκτυα (wireless LAN). Το γεγονός αυτό οδήγησε διάφορους ερευνητές στην ενασχόληση και αντιμετώπιση των προβλημάτων που προκύπτουν κατά τη δημιουργία ενός κατανεμημένου συστήματος με κινητούς χρήστες (κινητός υπολογισμός). Ένα σημαντικό στοιχείο για την επιτυχία τέτοιων συστημάτων που να χαρακτηρίζονται από διακριτική επικοινωνία είναι η ικανότητα τους να "αισθάνονται" ή να αντιλαμβάνονται το περιβάλλον και να αλλάζουν ή να προσαρμόζουν την συμπεριφορά τους ανάλογα με την εκάστοτε περιρρέουσα πληροφορία.

Οι εξελίξεις αυτές στις φορητές τεχνολογίες σε συνδυασμό με την αύξηση των αναγκών των χρηστών δημιούργησαν τις κατάλληλες προϋποθέσεις για την παροχή προηγμένων και πολύπλοκων υπηρεσιών, όπως είναι οι υπηρεσίες που βασίζονται στη θέση του χρήστη (Location-based Services) και οι υπηρεσίες με επίγνωση του πλαισίου χρήσης (Context-Aware Services). Τα συστήματα διάχυτου υπολογισμού καλούνται να διαχειριστούν την πληροφορία πλαισίου (context) που χαρακτηρίζει την περιρρέουσα κατάσταση διάφορων οντοτήτων όπως είναι για παράδειγμα το προφίλ της προσωπικότητας του χρήστη, τη θέση του χρήστη, τις συνθήκες του

περιβάλλοντός του κτλ. Εξαιτίας της ποικιλίας και της δυναμικής φύσης των εμπλεκόμενων συσκευών, τα περιβάλλοντα διάχυτου υπολογισμού εισάγουν νέες προκλήσεις στην ανάπτυξη εφαρμογών, όπως είναι η ανάπτυξη εφαρμογών ασφάλειας και ιδιωτικότητας.

2.3 Η έννοια του πλαισίου χρήσης (context)

Ως πλαίσιο χρήσης υπηρεσίας (context) [10] δύναται να οριστεί η οποιαδήποτε πληροφορία η οποία μπορεί να χρησιμοποιηθεί για να χαρακτηρίσει την κατάσταση μίας οντότητας. Ο όρος οντότητα μπορεί να αναφέρεται σε ένα άνθρωπο, μία τοποθεσία, μία συσκευή, μία εφαρμογή ή ένα αντικείμενο που σχετίζονται με την αλληλεπίδραση ανάμεσα στο χρήστη και την εφαρμογή, συμπεριλαμβανομένων του ίδιου του χρήστη και της εφαρμογής. Για παράδειγμα, η τοποθεσία του χρήστη είναι πληροφορία πλαισίου χρήσης επειδή μπορεί να χρησιμοποιηθεί για να χαρακτηρίσει την κατάσταση του χρήστη.

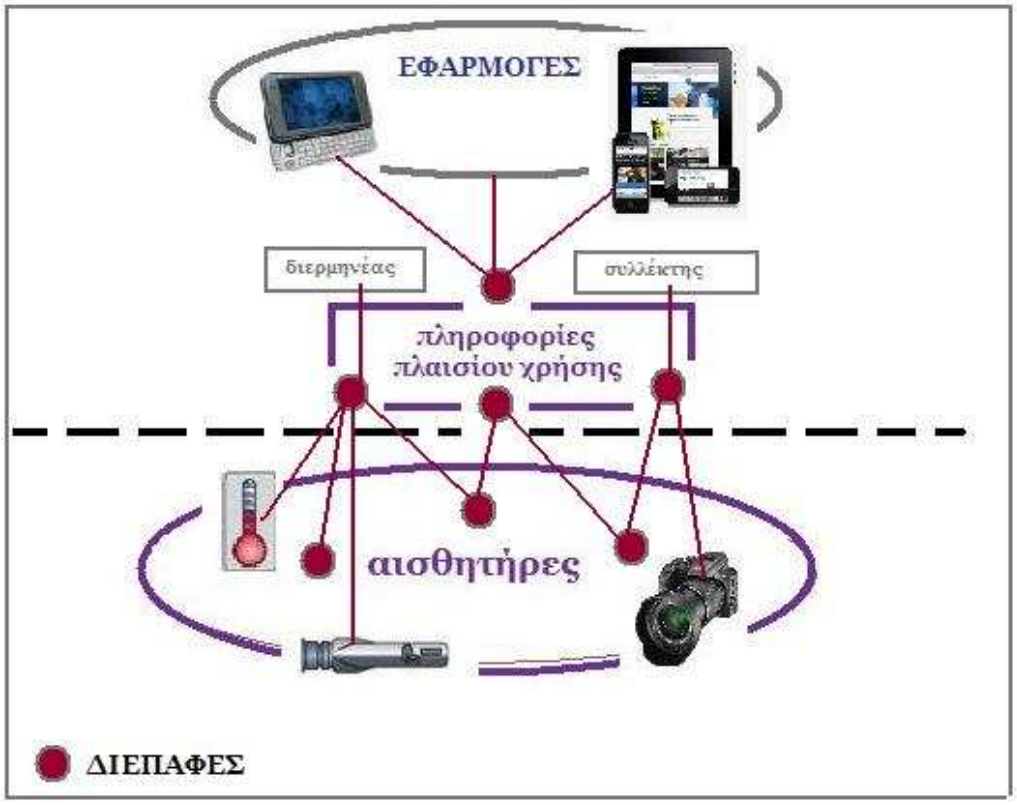
Οι πιο σημαντικές πληροφορίες πλαισίου χρήσης για να χαρακτηριστεί η κατάσταση μιας οντότητας, θεωρούνται από τους περισσότερους ερευνητές η ταυτότητα, η τοποθεσία, η δραστηριότητα (ενέργεια) του χρήστη και ο χρόνος. Από αυτά μπορούν να προκύψουν και άλλες πληροφορίες σχετικά με την οντότητα, το λεγόμενο δευτερεύων πλαίσιο χρήσης, όπως για παράδειγμα η διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη. Εξαιτίας της φορητότητας των υπολογιστών η πληροφορία πλαισίου χρήσης όπως είναι για παράδειγμα η τοποθεσία του χρήστη, τα αντικείμενα και οι άνθρωποι που περιβάλλουν τον χρήστη, μεταβάλλονται δυναμικά.

Η κατηγοριοποίηση του πλαισίου χρήσης κυρίως βοηθά τους σχεδιαστές εφαρμογών να ανακαλύψουν τα πιο πιθανά μέρη του πλαισίου χρήσης που θα είναι χρήσιμα στις δικές τους εφαρμογές. Το πλαίσιο χρήσης δύναται να κατηγοριοποιηθεί ως εξής: *πληροφορίες χρήστη (user context)*: θέση, ταυτότητα, προσωπικά δεδομένα, προτιμήσεις, ενδιαφέροντα, πρόσωπα στο τρέχον περιβάλλον, κοινωνική κατάσταση κλπ., *πληροφορίες υπολογιστικού περιβάλλοντος (computational context)*: διαθέσιμοι επεξεργαστές, τερματικές συσκευές προσβάσιμες από τον χρήστη και δυνατότητες τους, οθόνες, διαθέσιμα δίκτυα, δυνατότητες σύνδεσης στο δίκτυο κλπ., και *πληροφορίες φυσικών συνθηκών (physical context)*: φωτισμός, θερμοκρασία κλπ.

Η χρησιμότητα του πλαισίου είναι έκδηλη σε διάφορα επίπεδα επεξεργασίας και αξιοποίησης μέσα σε ένα σύστημα διάχυτου υπολογισμού. Σε μεγάλα κατανεμημένα συστήματα μπορεί να αξιοποιηθεί στην διαχείριση ενέργειας και πόρων. Σε μια κινητή εφαρμογή μπορεί να αξιοποιηθεί για προσαρμοστικότητα και αυτονομία αποφάσεων σε διάφορες καταστάσεις και απαιτήσεις του χρήστη.

2.4 Η έννοια των εφαρμογών με επίγνωση του πλαισίου χρήσης

Γενικότερα, εφαρμογές με επίγνωση του πλαισίου χρήσης [1,6] είναι εφαρμογές που αλλάζουν ή προσαρμόζουν δυναμικά την συμπεριφορά τους βάσει του πλαισίου χρήσης της εφαρμογής και του χρήστη. Η επίγνωση πληροφορίας πλαισίου δύναται να οριστεί ως «η ικανότητα ενός συστήματος να ανακαλύπτει, να συμπεραίνει, να αξιοποιεί και να συλλογίζεται βάσει της πληροφορίας που περιγράφει το πλαίσιο αυτό (περιρρέουσα πληροφορία) ώστε να παρέχει σχετικές πληροφορίες, να λαμβάνει αποφάσεις, να προβαίνει σε προκαθορισμένες ενέργειες και να προσαρμόζεται σε διάφορες καταστάσεις» [10].



Σχήμα 2.2 Συλλογή πληροφορίας πλαισίου χρήσης (context)

Οι κινητές συσκευές που έχουν ενσωματωμένες δυνατότητες επίγνωσης πλαισίου διαθέτουν πολλαπλούς αισθητήρες και αλγόριθμους για την όσο το δυνατόν πιο έξυπνη επεξεργασία των δεδομένων που συλλέγουν από το περιβάλλον με σκοπό την μετατροπή τους σε αξιοποιήσιμα δεδομένα για τις λειτουργίες τους και την παραγωγή συμπερασμάτων.

Οι σχεδιαστές εφαρμογών είναι σημαντικό να κατανοήσουν καλά την έννοια του πλαισίου χρήσης και το πώς αυτό μπορεί να χρησιμοποιηθεί, ώστε να είναι σε θέση να διακρίνουν ποια στοιχεία που αφορούν το πλαίσιο χρήσης είναι σχετικά με την εφαρμογή που θέλουν να αναπτύξουν, όπως επίσης και ποιες συμπεριφορές και γνωρίσματα με επίγνωση του πλαισίου θα υποστηρίζουν οι εφαρμογές τους. Οι συμπεριφορές που μπορούν να υποστηρίξουν οι εφαρμογές με επίγνωση του πλαισίου χρήσης μπορούν να κατηγοριοποιηθούν ως εξής σύμφωνα με τους Dey και Abowd στο [10]:

- παροχή πληροφοριών και υπηρεσιών στον χρήστη
- αυτόματη εκτέλεση μιας υπηρεσίας για τον χρήστη
- τοποθέτηση ετικετών (tagging) στην πληροφορία πλαισίου χρήσης, για μετέπειτα πιθανή ανάκτηση

Το βασικό μειονέκτημα των υπηρεσιών με επίγνωση του πλαισίου χρήσης τους είναι η επίδραση τους στο δικαίωμα ιδιωτικότητας των χρηστών λόγω της χρήσης προσωπικών δεδομένων για την εκτέλεση τους και αυτό είναι και το θέμα που απασχολεί διάφορους ερευνητές τα τελευτέα χρόνια. Η εξασφάλιση τεχνικών μέσων που θα παρέχει διασφάλιση της προστασίας της ιδιωτικότητας είναι κάτι αρκετά δύσκολο μέχρι τώρα, αλλά γίνονται ολοένα και περισσότερες προσπάθειες εύρεσης ενός σωστού μηχανισμού διαχείρισης της ιδιωτικότητας.

Κεφάλαιο 3

Ιδιωτικότητα και διάχυτα συστήματα

3.1 Η έννοια της ιδιωτικότητας

Για να δημιουργηθούν συστήματα με επίγνωση της ιδιωτικότητας, πρέπει αρχικά να οριστεί το νόημα της προστασίας της ιδιωτικότητας, πώς η ιδιωτικότητα κάποιου μπορεί να παραβιαστεί, οι κοινωνικές και νομικές αλήθειες της και τα τεχνικά εργαλεία που έχουμε στη διάθεσή μας. Η ασφάλεια (security) θεωρείται συχνά απαραίτητο συστατικό της προστασίας της ιδιωτικότητας, αφού διευκολύνει τον έλεγχο της ροής πληροφοριών. Εντούτοις, δεν μπορούμε να πούμε ότι συνεπάγει την προστασία της ιδιωτικότητας, διότι είναι πιθανό να υπάρχουν υψηλά επίπεδα ασφάλειας αλλά όχι προστασία της ιδιωτικότητας ή το αντίθετο.

Ένας από τους πιο ευρέως αποδεκτούς ορισμούς σχετικά με την ιδιωτικότητα των δεδομένων, έρχεται από τη δεκαετία του ’60, όταν η αυτοματοποιημένη επεξεργασία των δεδομένων πραγματοποιήθηκε για πρώτη φορά σε εθνική κλίμακα. Ο καθηγητής του πανεπιστημίου Columbia, μελετητής της πολιτικής Alan F. Westin ορίζει την ιδιωτικότητα ως εξής [35]:

“Ιδιωτικότητα είναι η αξίωση των ατόμων, των ομάδων ή των οργανισμών να καθορίσουν για τους εαυτούς τους πότε, πώς, και σε ποιο βαθμό οι πληροφορίες σχετικά με αυτούς κοινοποιούνται στους άλλους”

Η ιδιωτικότητα συνεπώς, αφορά την αυτονομία του ατόμου και την προστασία της ανεξαρτησίας του ατόμου να παίρνει κεντρικές αποφάσεις για το άτομο του. Ο Westin αυτό το περιγράφει ως εξής:

"Κάθε πρόσωπο γνωρίζει τη διαφορά ανάμεσα στο τι θέλει να είναι και αυτό που πραγματικά είναι , μεταξύ αυτού που ο υπόλοιπος κόσμος βλέπει σε αυτόν και αυτό που ξέρει ο ίδιος σαν την πιο πολύ σύνθετη πραγματικότητα του. Επιπλέον υπάρχουν κάποιες πτυχές του εαυτού του τις οποίες το άτομο δεν κατανοεί πλήρως, αλλά τις διαμορφώνει και διερευνά σιγά σιγά καθώς αναπτύσσεται" [35]

3.2 Ιδιωτικότητα και διάχυτος υπολογισμός

Η ανάπτυξη των τεχνολογιών του διάχυτου υπολογισμού (pervasive ή ubiquitous computing) δημιουργεί νέα δεδομένα και περαιτέρω απειλές για την ιδιωτική ζωή που οδηγούν σε νέες προκλήσεις για την προστασία της ιδιωτικότητας [2,16]. Καθώς ο χρήστης εξαρτάται όλο και πιο πολύ από ένα σύστημα διάχυτου υπολογισμού, το σύστημα γίνεται πιο πεπειραμένο σχετικά με τις μετακινήσεις του συγκεκριμένου χρήστη, τη συμπεριφορά του, την κατάσταση του και τις συνήθειες του, καθιστώντας έτσι σε πολύ μεγαλύτερο βαθμό δυνατή την παραβίαση της ιδιωτικής του ζωής. Για παράδειγμα οι μηχανισμοί εντοπισμού της θέσης του χρήστη είναι μηχανισμοί που παρακολουθούν τους χρήστες σε μόνιμη βάση και χρειάζονται ιδιαίτερη προσοχή.

Η ιδιωτικότητα είναι ένα σημαντικό ζήτημα σε συστήματα με επίγνωση του πλαισίου χρήσης διότι οι πληροφορίες ενός ατόμου που σχετίζονται με το πλαίσιο χρήσης περιέχουν μεγάλες ποσότητες προσωπικών πληροφοριών. Η περίπτωση απώλειας της ιδιωτικότητας μπορεί να αποτρέψει τους χρήστες από το να χρησιμοποιήσουν και να εμπλακούν σε ένα τέτοιο σύστημα. Ένα τέτοιο σύστημα πρέπει να βεβαιώνεται για την ταυτότητα του χρήστη πριν ανταποκριθεί στα αιτήματά του. Οι χρήστες εκτός από το να πληροφορούνται για την συλλογή και επεξεργασία των προσωπικών τους δεδομένων, πρέπει επίσης να ερωτούνται για την συγκατάθεση τους όσο αφορά την πρόσβαση των στοιχείων τους. Η πρόοδος των τεχνολογιών της πληροφορικής μπορεί ωστόσο να αξιοποιηθεί και να χρησιμοποιηθεί και για την προστασία της ιδιωτικής ζωής του ατόμου. Κάποιες πτυχές που θα μπορούσαν να ληφθούν υπόψη είναι να δίνεται η συγκατάθεση για τη συλλογή και την επεξεργασία των δεδομένων με

ευκολότερο και πιο προσιτό τρόπο, τα πληροφοριακά και επικοινωνιακά συστήματα να σχεδιάζονται έτσι ώστε να δίνεται στους χρήστες η δυνατότητα πρόσβασης στα προσωπικά τους δεδομένα, καθώς και ενημέρωση τους σχετικά με κάθε είδους χειρισμό τους όπως για παράδειγμα, ποιος τα συγκέντρωσε, τροποποίησε ή έλαβε γνώση. Επιπρόσθετα τεχνικές όπως η ανωνυμία μπορούν να υιοθετηθούν κατά τρόπο αποδεκτό από τον παροχέα των υπηρεσιών, ώστε να εξασφαλίζεται η πρόσβαση των χρηστών στις υπηρεσίες χωρίς να διακυβεύεται η ιδιωτικότητά τους.

Ακόμα κι αν ο χρήστης λειτουργεί κάτω από κάποιο ψευδώνυμο, εξαιτίας της σημασιολογίας κάποιων πληροφοριών που συλλέγονται, εύκολα μπορεί κάποιος να συμπεράνει πρόσθετες πληροφορίες πέραν αυτών που παρουσιάζονται. Η εξασφάλιση τεχνικών μέσων που θα παρέχουν πλήρη διασφάλιση της προστασίας της ιδιωτικότητας είναι κάτι αρκετά δύσκολο μέχρι τώρα. Οι μηχανισμοί ασφάλειας που εφαρμόζονται σήμερα, όπως μηχανισμοί κρυπτογραφίας (encryption) [22] ή μηχανισμοί ελέγχου πρόσβασης (access control), ναι μεν παρέχουν προστασία στα προσωπικά δεδομένα των χρηστών, αλλά δεν αποτρέπουν την μη εξουσιοδοτημένη περαιτέρω χρήση και εκμετάλλευσή τους. Έργο διάφορων ερευνητών καθώς και απαίτηση κάθε χρήστη τέτοιων υπηρεσιών είναι ένας μηχανισμός προστασίας της ιδιωτικότητας που να επιτρέπει στους χρήστες να προσδιορίζουν τις δικές τους πολιτικές για έλεγχο της ροής των δεδομένων, που πηγάζουν από αισθητήρες, δίνοντας βάση στις αλλαγές της πληροφορίας πλαισίου χρήσης των χρηστών. Είναι σημαντικό επίσης ένας τέτοιος μηχανισμός να μπορεί να χειρίζεται και πολιτικές ιδιωτικότητας που εξαρτώνται ή σχετίζονται με το πλαίσιο χρήσης (context-dependent). Επιπλέον, η πρόσβαση στα δεδομένα πρέπει να συνοδεύεται από ορισμένους κανόνες συμπεριφοράς του συστήματος ή της υπηρεσίας (complementary actions).

3.3 Αρχές προστασίας της ιδιωτικότητας

Οι αρχές αυτές χρησιμοποιούνται για να καθοδηγήσουν το σχεδιασμό, την ανάπτυξη και την υλοποίηση των πολιτικών ιδιωτικότητας και των ελέγχων διασφάλισης της ιδιωτικότητας. Οι βασικές αρχές όπως αυτές παρουσιάζονται στο [43] είναι:

- Αρχή της συγκατάθεσης και επιλογής

  Ένα άτομο πρέπει να είναι σε θέση να επιλέγει, ελεύθερα και με πλήρη γνώση, αν θα επιτρέψει ή όχι τη συλλογή, τη χρήση, τη μεταφορά, την αποθήκευση, την αρχειοθέτηση, ή τη διαγραφή προσωπικών πληροφοριών. Η συγκατάθεση μπορεί να επιτευχθεί σε μια βάση αποδοχής ή απόρριψης. Η έμμεση ή η ρητή συγκατάθεση λαμβάνεται από το άτομο πριν, κατά τη διάρκεια ή αμέσως μετά τη συλλογή των προσωπικών δεδομένων. Οι προτιμήσεις του ατόμου που εκφράζονται στη συγκατάθεσή του, επιβεβαιώνονται και υλοποιούνται.

- Αρχή του προσδιορισμού του σκοπού

  Ένας οργανισμός πρέπει να προσδιορίσει το σκοπό για τον οποίο συλλέγονται, χρησιμοποιούνται, μεταφέρονται, αποθηκεύονται ή διαγράφονται προσωπικά δεδομένα και να ανακοινώσει το σκοπό αυτό στο άτομο πριν ή κατά τη διάρκεια συλλογής των δεδομένων. Ο σκοπός αυτός πρέπει να είναι ξεκάθαρος, περιορισμένος και σχετικός με τις συνθήκες.

- Αρχή του περιορισμού της συλλογής

  Η συλλογή των προσωπικών δεδομένων πρέπει να είναι νόμιμη και να περιορίζεται σε εκείνο που είναι αναγκαίο για το συγκεκριμένο σκοπό.

- Αρχή του περιορισμού χρήσης, διατήρησης και αποκάλυψης

  Οι οργανισμοί χρησιμοποιώντας, διατηρώντας και γνωστοποιώντας προσωπικά δεδομένα χρειάζεται να περιορίσουν τη χρήση, διατήρηση και αποκάλυψη αυτών, στους σκοπούς μόνο για τους οποίους το άτομο έχει ενημερωθεί ή έχει εγκρίνει. Τα προσωπικά δεδομένα πρέπει να διατηρούνται μόνο όσο χρειάζεται για να εκπληρωθεί ο σκοπός που έχει δηλωθεί και στη συνέχεια να καταστραφούν με ασφάλεια ή να μετατραπούν σε ανώνυμα.

- Αρχή της ελαχιστοποίησης των δεδομένων

  Η ελαχιστοποίηση της συλλογής των δεδομένων σημαίνει την απαίτηση συλλογής με όσο το δυνατό λιγότερα δεδομένα. Ενώ, ο “περιορισμός της συλλογής” αναφέρεται σε περιορισμένα δεδομένα που συλλέγονται σε σχέση

με το συγκεκριμένο σκοπό, η "ελαχιστοποίηση των δεδομένων" αυστηρά ελαχιστοποιεί τη συλλογή των δεδομένων ανεξάρτητα από το σκοπό της. Επιπλέον δεδομένα μπορεί να ζητηθούν αν είναι ξεκάθαρο στο άτομο ότι αυτό είναι τελείως προαιρετικό και ότι το άτομο επωφελείται.

- Αρχή της ακρίβειας και ποιότητας
  Είναι αναγκαίο να διασφαλιστεί ότι τα επεξεργασμένα προσωπικά δεδομένα είναι ακριβή, ολοκληρωμένα, ενημερωμένα (όπου χρειάζεται) και επαρκή για τους σκοπούς χρήσης αυτών.

- Αρχή της προσβασιμότητας, της διαφάνειας και της ειδοποίησης
  Η προσβασιμότητα και η διαφάνεια είναι δύο έννοιες κλειδιά για την υπευθυνότητα. Οι ελεγκτές των προσωπικών δεδομένων πρέπει να παρέχουν ξεκάθαρες και εύκολα προσβάσιμες δηλώσεις ιδιωτικότητας σχετικά με τις πρακτικές τους, τις πολιτικές και τις διεργασίες σε σχέση με το χειρισμό των προσωπικών πληροφοριών.

- Αρχή της ατομικής συμμετοχής και πρόσβασης
  Τα άτομα των οποίων οι προσωπικές πληροφορίες συλλέγονται, χρησιμοποιούνται, μεταφέρονται, αποθηκεύονται, αρχειοθετούνται ή διαγράφονται, θα πρέπει να έχουν το δικαίωμα πρόσβασης και ελέγχου των προσωπικών τους δεδομένων, εφόσον καταστεί δυνατή η πιστοποίηση των ατόμων σε ένα κατάλληλο επίπεδο εμπιστοσύνης. Για παράδειγμα, η παροχή διεύθυνσης διαδικτύου (IP address) δεν είναι αρκετή καθώς αυτή μπορεί να είναι δυναμική. Στα πιστοποιημένα άτομα θα πρέπει να παρέχεται πρόσβαση στα προσωπικά τους δεδομένα και να ενημερώνονται για τη χρήση και γνωστοποίηση αυτών σε τρίτους.

- Αρχή της υπευθυνότητας
  Η συλλογή, χρήση, μεταφορά, αποθήκευση ή διαγραφή προσωπικών πληροφοριών συνεπάγεται την υποχρέωση της φροντίδας για την προστασία τους. Η ευθύνη για τις πολιτικές που σχετίζονται με την ιδιωτικότητα, τις διαδικασίες και τις πρακτικές πρέπει να τεκμηριώνεται και να γνωστοποιείται,

ανάλογα με την περίπτωση και να ανατίθεται σε ένα συγκεκριμένο πρόσωπο. Όταν μεταβιβάζονται προσωπικές πληροφορίες σε τρίτους, οι οργανισμοί πρέπει να επιδιώκουν προστασία της ιδιωτικότητας μέσω συμβατικών ή άλλων μέσων.

- Αρχή της ασφάλειας και της εμπιστευτικότητας

  Οι ελεγκτές των προσωπικών πληροφοριών, χρειάζεται να προστατεύσουν τα προσωπικά δεδομένα που κατέχουν με τους κατάλληλους ελέγχους ενάντια σε κινδύνους, όπως η απώλεια ή η μη πιστοποιημένη πρόσβαση σε προσωπικές πληροφορίες, η αθέμιτη καταστροφή, χρήση, τροποποίηση ή αποκάλυψη πληροφοριών. Τέτοιοι έλεγχοι χρειάζεται να βασίζονται τόσο σε κατάλληλα πρότυπα ασφάλειας όσο και σε τοπική νομοθεσία.

- Αρχή της συμμόρφωσης

  Οι οργανισμοί που συλλέγουν, χρησιμοποιούν, μεταφέρουν, αποθηκεύουν ή διαγράφουν προσωπικές πληροφορίες πρέπει να εφαρμόζουν τους κατάλληλους εσωτερικούς ελέγχους και ανεξάρτητους μηχανισμούς ελέγχου, με τρόπο που να διασφαλίζει τη συμφωνία στην τοπική νομοθεσία προστασίας δεδομένων και ιδιωτικότητας, αλλά και στην ασφάλειά τους.

Κεφάλαιο 4

Υπάρχουσες γενικές τεχνολογίες προστασίας προσωπικών δεδομένων

4.1 Τεχνολογίες για την διαχείριση της ιδιωτικότητας

Το κεφάλαιο αυτό παρουσιάζει συνοπτικά μερικές από τις πιο σημαντικές υφιστάμενες τεχνολογίες που έχουν εφαρμοστεί για την προστασία των προσωπικών δεδομένων. Οι τεχνολογίες για τη διαχείριση της ιδιωτικότητας αναφέρονται κυρίως σε μηχανισμούς για την αυτοματοποίηση της εφαρμογής πολιτικών ιδιωτικότητας και σε μηχανισμούς ελέγχου πρόσβασης. Οι μηχανισμοί για την αυτοματοποίηση της εφαρμογής πολιτικών ιδιωτικότητας αφορούν την κωδικοποίηση των πολιτικών ιδιωτικότητας σε κάποια γλώσσα που μπορεί να γίνει αντιληπτή από προγράμματα λογισμικού. Με αυτό τον τρόπο, ένας πράκτορας χρήστη μπορεί να αποφασίσει κατά πόσο η πολιτική ιδιωτικότητας βρίσκεται σε συμφωνία με τις αντίστοιχες προτιμήσεις και απαιτήσεις του χρήστη. Μια τεχνολογική λύση στο πρόβλημα της ιδιωτικότητας των χρηστών κυρίως στον ιστό αποτελεί η πλατφόρμα προτιμήσεων ιδιωτικότητας P3P. Άλλες σημαντικές προσεγγίσεις τεχνολογιών διαχείρισης ιδιωτικότητας είναι οι γλώσσες επιχειρησιακών πολιτικών ιδιωτικότητας που αντιστοιχούν την πολιτική σε κανόνες ελέγχου πρόσβασης και είναι ανεξάρτητες πλατφόρμας. Χαρακτηριστικά παραδείγματα είναι η EPAL (IBM) και η XACML (OASIS).

4.2 P3P/APPEL

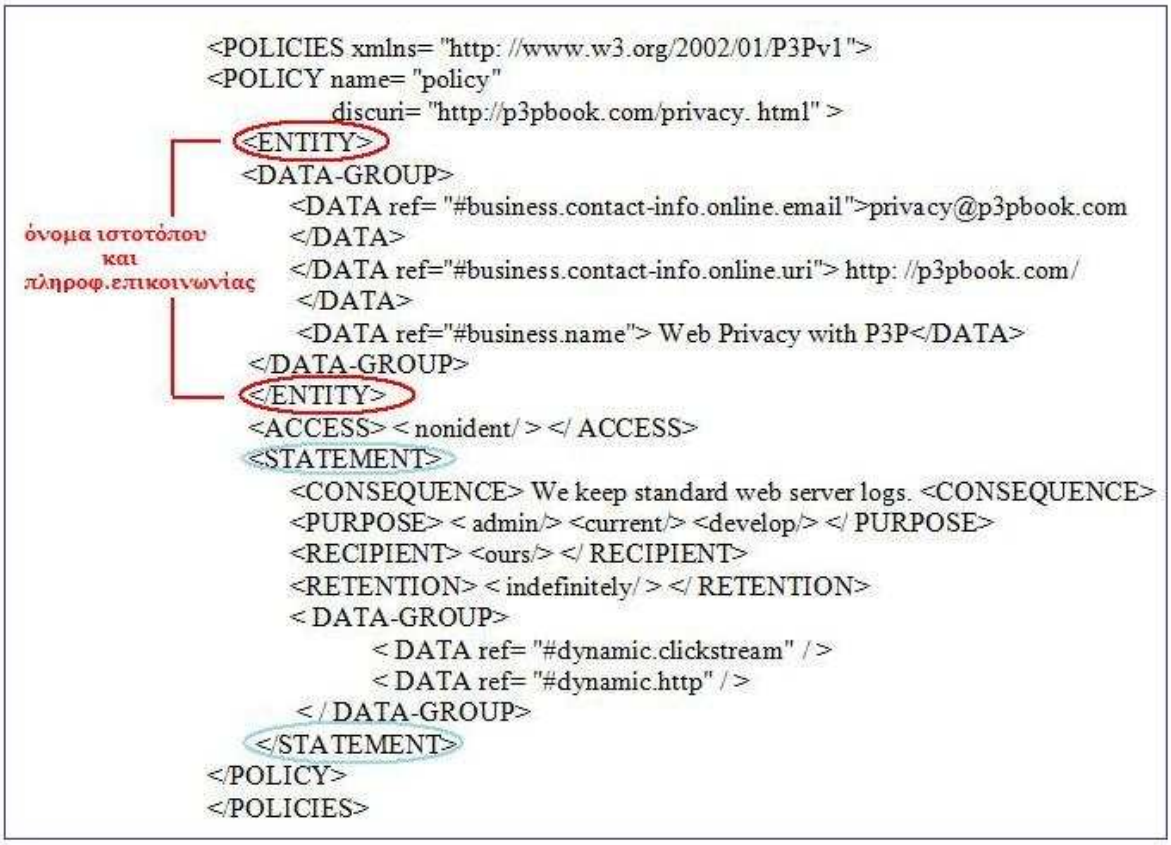
Το πρωτόκολλο Platform for Privacy Preferences (P3P) [41] είναι μια τεχνολογία για την προστασία του απορρήτου που αναπτύχθηκε από την κοινοπραξία World Wide Web Consortium (W3C) στις 16 Απριλίου το 2002. Το World Wide Web Consortium είναι ένας διεθνής οργανισμός που αναπτύσσει πρότυπα και προωθεί κοινά και διαλειτουργικά πρωτόκολλα. Σκοπός της τεχνολογίας P3P είναι να προστατεύσει τους χρήστες του διαδικτύου από τους κινδύνους παραβίασης της ιδιωτικότητας που κρύβεται στον ιστό (web). Η πλατφόρμα αυτή δίνει την δυνατότητα στις Διαδικτυακές ιστοσελίδες να εκφράσουν τις δικές τους πρακτικές ιδιωτικότητας αναφορικά με την συλλογή και επεξεργασία των προσωπικών δεδομένων σε μια συγκεκριμένη μορφή (format) έτσι ώστε να μπορούν να ανακτηθούν αυτόματα και να ερμηνευτούν εύκολα από τους πράκτορες των χρηστών (user agents). Γενικά, η P3P είναι συμπληρωματική σε κανονισμούς και αυτορυθμιζόμενα προγράμματα που παρέχουν μηχανισμούς επιβολής.

Μια πολιτική ιδιωτικότητας πλατφόρμας P3P, αποτελείται από μια ακολουθία XML στοιχείων τύπου STATEMENT. Τα υποστοιχεία που μπορούν να περιλαμβάνονται στην ακολουθία αυτή είναι τα ακόλουθα αναγνωριστικά: PURPOSE, RECIPIENT, RETENTION, DATA-GROUP, CONSEQUENCE. Το αναγνωριστικό PURPOSE προσδιορίζει τους σκοπούς για τους οποίους πραγματοποιείται η συλλογή της πληροφορίας. Μια πιθανή προκαθορισμένη τιμή που μπορεί να λάβει το στοιχείο PURPOSE είναι: < individual – analysis/ >. Η τιμή αυτή δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στον ιστότοπο (website), θα χρησιμοποιηθούν για την εξαγωγή συμπερασμάτων, σχετικά με τις συνήθειες ή ενδιαφέροντα του χρήστη, σε συνδιασμό με δεδομένα τα οποία φανερώνουν την ταυτότητα του χρήστη. Η ετικέτα RECIPIENT δηλώνει τους επιτρεπόμενους αποδέκτες της πληροφορίας η οποία συλλέγεται. Παρόμοια, μία πιθανή προκαθορισμένη τιμή που μπορεί να λάβει το στοιχείο RECIPIENT είναι: < ours/ >. Η τιμή αυτή δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στον ιστότοπο, θα χρησιμοποιηθούν μόνο από τον εν λόγω οργανισμό για την εκπλήρωση των δεδηλωμένων σκοπών. Μια πιθανή προκαθορισμένη τιμή που μπορεί να λάβει το στοιχείο RETENTION το οποίο δηλώνει την περίοδο διατήρησης των δεδομένων από τον συλλέκτη είναι: < stated-purpose/ >. Η τιμή αυτή δηλώνει ότι τα

δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στον ιστότοπο, δεν θα διατηρηθούν με κανένα τρόπο μετά την εκπλήρωση του σκοπού για τον οποίο παρέχονται. Η ετικέτα DATA-GROUP παρέχει τον κατάλογο των τύπων δεδομένων που συλλέγονται για τους δεδηλωμένους σκοπούς. Το στοιχείο DATA-GROUP περιέχει ένα ή περισσότερα υποστοιχεία DATA, τα οποία προσδιορίζουν τον κάθε τύπο δεδομένων. Κάθε στοιχείο DATA υποχρεωτικά περιλαμβάνει ένα XML γνώρισμα, το ref το οποίο δηλώνει το συγκεκριμένο τύπο δεδομένων που συλλέγεται και λαμβάνει ως τιμή ένα αναγνωριστικό τύπου μοναδικού αναγνωριστικού πόρου. Το πεδίο CONSEQUENCE προβάλλει κατανοητές εξηγήσεις στους χρήστες σε απλή γραφή αναφορικά με τις πρακτικές συλλογής και επεξεργασίας δεδομένων της ιστοσελίδας καθώς και τις επιπτώσεις τους.

Άλλα αναγνωριστικά που περιέχονται σε μία P3P πολιτική είναι το ENTITY, το οποίο καταγράφει πληροφορίες επικοινωνίας με την επιχείρηση, οργανισμό ή άτομο του οποίου ο ιστότοπος ανήκει. Η ετικέτα ACCESS δηλώνει αν τα άτομα μπορούν να ανακαλύψουν ποια προσωπικά δεδομένα τους κρατάει ένας ιστότοπος στις βάσεις δεδομένων του. Η ετικέτα DISPUTES περιγράφει τρόπους επίλυσης διενέξεων (disputes) με τον ιστοτόπο που σχετίζονται με την ιδιωτικότητα (για παράδειγμα σχετικούς νόμους και αρχές προστασίας της ιδιωτικότητας).

Ακολουθεί ένα μικρό παράδειγμα πολιτικής ιδιωτικότητας σε P3P, η οποία αποτελείται από μία δήλωση (statement) που περιέχει στοιχεία όπως ο σκοπός, τα δεδομένα, ο παραλήπτης και η περίοδος διατήρησης των δεδομένων.



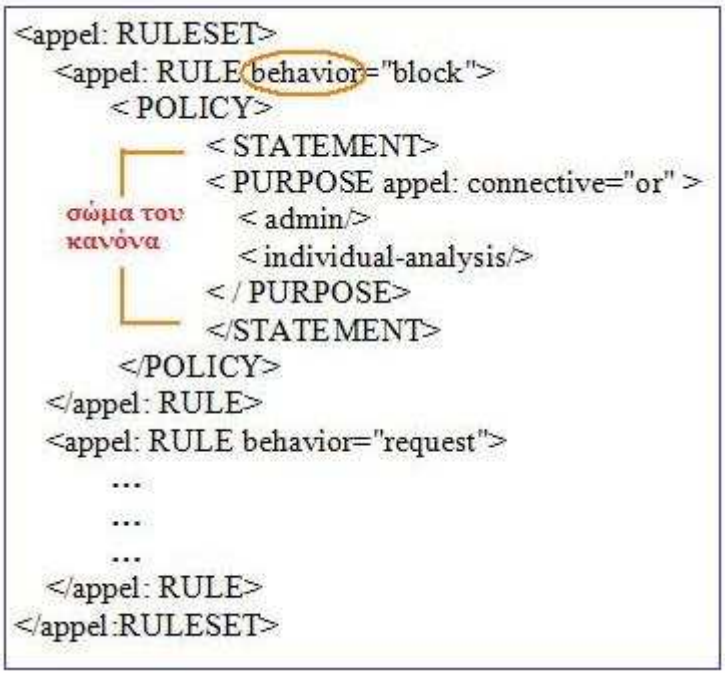

```
<POLICIES xmlns= "http: //www.w3.org/2002/01/P3Pv1">
<POLICY name= "policy"
        discuri= "http://p3pbook.com/privacy. html" >
  <ENTITY>
  <DATA-GROUP>
    <DATA ref= "#business.contact-info.online.email">privacy@p3pbook.com
    </DATA>
    </DATA ref="#business.contact-info.online.uri"> http: //p3pbook.com/
    </DATA>
    <DATA ref="#business.name"> Web Privacy with P3P</DATA>
  </DATA-GROUP>
  </ENTITY>
  <ACCESS> < nonident/ > </ ACCESS>
  <STATEMENT>
    <CONSEQUENCE> We keep standard web server logs. <CONSEQUENCE>
    <PURPOSE> < admin/> <current/> <develop/> </ PURPOSE>
    <RECIPIENT> <ours/> </ RECIPIENT>
    <RETENTION> < indefinitely/ > </ RETENTION>
    < DATA-GROUP>
        < DATA ref= "#dynamic.clickstream" / >
        < DATA ref= "#dynamic.http" / >
    < / DATA-GROUP>
  </STATEMENT>
</POLICY>
</POLICIES>
```

Σχήμα 4.1 Παράδειγμα πολιτικής ιδιωτικότητας πλατφόρμας P3P

Από την άλλη πλευρά, οι χρήστες καθορίζουν τις προτιμήσεις ιδιωτικότητας σε μορφή APPEL (P3P Preference Exchange Language) [42]. Η γλώσσα APPEL συμπληρώνει την πλατφόρμα P3P, είναι γλώσσα βασισμένη σε κανόνες που κωδικοποιείται επίσης σε XML. Οι ιστοσελίδες κοινοποιούν τις πρακτικές τους, δηλαδή την πολιτική ιδιωτικότητας τους, στους πράκτορες των χρηστών (user agents). Οι πράκτορες χρηστών με την σειρά τους μπορούν να ερμηνεύουν με αυτόματο τρόπο την πολιτική ιδιωτικότητας της ιστοσελίδας, να την συγκρίνουν με τους αντίστοιχους κανόνες APPEL που προκαθόρισε ο χρήστης και να αποφασίζουν κατά πόσο η πολιτική ιδιωτικότητας της ιστοσελίδας συμφωνεί με τα όσα είχε δηλώσει στις προτιμήσεις και απαιτήσεις του ο χρήστης. Οι χρήστες δεν χρειάζεται να διαβάζουν τις πολιτικές ιδιωτικότητας κάθε φορά που επισκέπτονται την σελίδα.

Ένας κανόνας που κωδικοποιείται σε γλώσσα προτιμήσεων APPEL αποτελείται από την συμπεριφορά του κανόνα (rule behavior) και το σώμα του κανόνα (rule body). Η συμπεριφορά ενός κανόνα καθορίζεται από την ενέργεια που θα πραγματοποιηθεί εφόσων οι υφιστάμενες συνθήκες ενεργοποιήσουν τον κανόνα. Η ενέργεια

εκφράζεται από το XML γνώρισμα behavior, του οποίου υποψήφιες τιμές είναι request όταν η πρακτική του κανόνα αποτελεί κάτι το αποδεκτό για το χρήστη, block όταν αντίστοιχα αποτελεί κάτι το μη αποδεκτό από τον χρήστη και limited όταν εκφράζει κάτι το αποδεκτό υπό κάποιους περιορισμούς. Το σώμα ενός κανόνα σε APPEL εκφράζει ένα υπόδειγμα πολιτικής ιδιωτικότητας, το οποίο συγκρίνεται με την πολιτική ιδιωτικότητας του ιστοτόπου για τις σχετικές αποφάσεις. Ακολουθεί ένα μικρό παράδειγμα προτιμήσεων ιδιωτικότητας χρήστη σε APPEL. Ο πρώτος APPEL κανόνας απαγορεύει όλους τους σκοπούς συλλογής δεδομένων πέραν από αυτόν της παροχής της υπηρεσίας όπως κάθε φορά ορίζεται.



Σχήμα 4.2 Παράδειγμα προτιμήσεων ιδιωτικότητας χρήστη σε APPEL

4.3 XACML και RBAC (Role Based Access Control)

Μία από τις πιο γνωστές γλώσσες για την υποστήριξη μοντέλων ελέγχου πρόσβασης είναι η γλώσσα eXtensible Access Control Markup Language (XACML) [45,46], η οποία ορίζει τη σύνταξη πολιτικών εξουσιοδότησης, αιτημάτων και αποκρίσεων του συστήματος ελέγχου πρόσβασης. Αποτελεί πρότυπο του οργανισμού Organization for the Advancement of Structured Information Standards (OASIS) από τον Φεβρουάριο του 2003. Οι πολιτικές που δημιουργούνται με την χρήση της XACML βασίζονται

στην XML. Η XACML επιτρέπει την χρήση αυθαίρετων χαρακτηριστικών στις πολιτικές, τον έλεγχο προσπέλασης βασισμένο σε ρόλους (role based access control), τις πολιτικές ευρετηρίου κλπ., χωρίς να απαιτούνται αλλαγές στις εφαρμογές οι οποίες χρησιμοποιούν XACML. Η γλώσσα XACML περιλαμβάνει τύπους δεδομένων, συναρτήσεις και συνδυαστική λογική τα οποία επιτρέπουν τον καθορισμό απλών και πολύπλοκων κανόνων. Η δομή της γλώσσας XACML, αποτελείται από κάποιες βασικές έννοιες. Μερικές απο αυτές είναι οι ακόλουθες: Πόρος (resource) όπως προσωπικά δεδομένα και υπηρεσίες, Ενέργεια (action), Υποκείμενο (subject), απόφαση εξουσιοδότησης (authorization decision), ιδιότητα (attribute), υποχρέωση (obligation) κτλ.

Η γλώσσα XACML περιλαμβάνει επίσης μια γλώσσα λήψης αποφάσεων πρόσβασης. Χρησιμοποιεί μηχανισμό ελέγχου πρόσβασης που βασίζεται σε έλεγχο πρόσβασης βάσει κανόνων (rule-based access control). Όταν δημιουργηθεί μια πολιτική που προστατεύει κάποιο πόρο και υπάρχει κάποια αίτηση για πρόσβαση σε αυτόν, τότε οι συναρτήσεις συγκρίνουν τα χαρακτηριστικά της αίτησης με τα χαρακτηριστικά που περιέχονται στους κανόνες της πολιτικής. Έτσι αν η αίτηση συμβαδίζει με τους κανόνες η αίτηση γίνεται αποδεχτή αλλιώς απορρίπτεται.

Η γλώσσα αυτή όπως προαναφέρθηκε χρησιμοποιείται για την εκτέλεση των πολιτικών ελέγχου πρόσβασης βάσει ρόλου (Role Based Access Control). Στο πρότυπο RBAC [13] οι άδειες πρόσβασης δίνονται σε σχέση με τον ρόλο που έχει ο χρήστης τις οποίες καθορίζει το κεντρικό σύστημα. Τα μοντέλα ελέγχου πρόσβασης των χρηστών βάσει ρόλων είναι τα πιο γνωστά μοντέλα εξουσιοδότησης. Χρησιμοποιούν ιεραρχίες ρόλων και πλήθος περιορισμών πρόσβασης και επομένως είναι δυνατόν μέσω των ρόλων να αποτυπωθεί μία πληθώρα πολιτικών ασφαλείας. Ο έλεγχος της πρόσβασης βάσει ρόλων προσφέρει αρκετά πλεονεκτήματα σε σχέση με τις κλασικές μεθόδους απόδοσης πρόσβασης στα πληροφοριακά συστήματα απευθείας στους χρήστες. Στα πλεονεκτήματα αυτά περιλαμβάνεται η απλοποίηση της διαχείρισης χρηστών και δικαιωμάτων πρόσβασης καθώς και η δυνατότητα αποτελεσματικού ελέγχου και απολογισμού των εξουσιοδοτήσεων των χρηστών. Εφαρμόζοντας ένα μοντέλο ελέγχου πρόσβασης βάσει ρόλων, τα δικαιώματα πρόσβασης ανατίθενται στους ρόλους και όχι στους χρήστες. Επομένως οποιαδήποτε τροποποίηση στα δικαιώματα πρόσβασης γίνεται στους ρόλους και αυτομάτως

τροποποιούνται τα δικαιώματα των χρηστών που τους έχουν λάβει, μειώνοντας το διαχειριστικό φόρτο. Για παράδειγμα, εάν ένας χρήστης μετακινηθεί από ένα Τμήμα κάποιου οργανισμού σε ένα άλλο, τότε απλά μπορούν να του ανατεθούν οι ρόλοι του νέου Τμήματος και της νέας θέσης εργασίας και να του αφαιρεθούν οι παλαιοί ρόλοι και ιδιότητες.

Η πιο ευρέως γνωστή προσέγγιση είναι το μοντέλο "NIST RBAC" [14] η οποία καθιερώθηκε ως πρότυπο το 2004 (ANSI INCITIS 359), προσδιορίζοντας τις αρχές και τους κανόνες για την υιοθέτηση ενός μοντέλου Ελέγχου της Πρόσβασης Βάσει Ρόλων.

4.4 EPAL

Η γλώσσα Enterprise Privacy Authorization Language (EPAL) [44] αποτελεί μία φορμαλιστική γλώσσα βασισμένη στην XML που χρησιμοποιείται σε οργανισμούς και επιχειρήσεις για τον προσδιορισμό και την εφαρμογή πολιτικών ιδιωτικότητας εντός του οργανισμού. Έχει αναπτυχθεί από την εταιρεία International Business Machines (IBM). Σε γενικές γραμμές χαρακτηρίζεται από αρκετά κοινά στοιχεία με τη γλώσσα XACML. Σε σχέση με την XACML, η γλώσσα EPAL παρουσιάζει το πλεονέκτημα της ιδέας του λεξιλογίου πολιτικής (policy vocabulary). Κάθε πολιτική EPAL περιλαμβάνει αναφορά σε αυτό το λεξιλόγιο, το οποίο ουσιαστικά αποτελεί μία αφηρημένη δομή όπου περιγράφονται τα χαρακτηριστικά, υποχρεώσεις και συνθήκες που χρησιμοποιεί ή είναι σε θέση να χρησιμοποιήσει η συγκεκριμένη πολιτική. Επίσης, η γλώσσα ορίζει ιεραρχικές κατηγορίες οντοτήτων οι οποίες μπορούν να είναι συσχετισμένες με διάφορες επιτρεπτές ή απαγορευμένες ενέργειες.
Μία EPAL πολιτική αποτελείται από ένα λεξιλόγιο και μία λίστα κανόνων ιδιωτικότητας. Ένα παράδειγμα EPAL πολιτικής είναι το ακόλουθο παράδειγμα που αναφέρεται σε πρόβλημα διαχείρισης βαθμολογιών.

```
<epal-vocabulary>
  <vocabulary-information id="GradeManagement">
  </vocabulary-information>

  <user-category id="employee"></user-category>
  <user-category id="secretary" parent="employee"></user-category>
        …
        …
  <data-category id="grades"></data-category>

  <purpose id="manage"></purpose>
  <purpose id="grading" parent="manage"></purpose>
        …
        …
  <action-id="change"></action>
        …
        …
</epal-vocabulary>

<epal-policy default-ruling="deny">
  <policy-information id= "n"></policy-information>

  <epal-vocabulary-ref id= "Grademanagement " />

  < rule id= "1" ruling = "deny">
        <user-category refid = "secretary"/>
        <data-category refid= "grades"/>
        < purpose refid= "grading"/>
        < action refid="change"/>
  </rule>
        …          άλλοι κανόνες
        …
</epal-policy>
```

Σχήμα 4.3 Παράδειγμα EPAL πολιτικής

Κεφάλαιο 5

Προτεινόμενοι Μηχανισμοί προστασίας ιδιωτικότητας

5.1 Σκοπός προτεινόμενων μηχανισμών

Σκοπός των προτεινόμενων μοντέλων και μηχανισμών είναι η παροχή λύσεων και βοήθειας προς τους μηχανικούς και αρχιτέκτονες λογισμικού και συστημάτων ώστε να διευθύνουν θέματα και ζητήματα που γενικά αφορούν την προστασία της ιδιωτικότητας των χρηστών που ενεπλέκονται σε ένα σύστημα με επίγνωση του πλαισίου χρήσης, καθώς και πώς η ιδιωτικότητα μπορεί να ελεγχθεί με συγκεκριμένο τρόπο.

Σε αυτό το κεφάλαιο, έχει γίνει μία κατηγοριοποίηση των προσεγγίσεων που μελετήθηκαν, με βάση το κύριο συστατικό τους στην προσπάθεια διασφάλισης ιδιωτικότητας των χρηστών. Οι κατηγορίες που διακρίθηκαν είναι: προσεγγίσεις βασισμένες στην χρήση μοντέλου ελέγχου πρόσβασης RBAC, προσεγγίσεις βασισμένες στην χρήση συσκότισης (obfuscation) της πληροφορίας, προσεγγίσεις βασισμένες στην χρήση μηχανισμού εκτίμησης εμπιστοσύνης (trust-based), προσεγγίσεις βασισμένες στην χρήση πολιτικών ιδιωτικότητας (policy-based) και τέλος προσεγγίσεις που βασίζονται στην χρήση οντολογιών. Μεταξύ αυτών, διακρίνουμε επίσης και υβριδικές προσεγγίσεις που συνδυάζουν μηχανισμούς από τις

παραπάνω κατηγορίες. Οι κατηγορίες φαίνονται στον παρακάτω πίνακα αντίστοιχα με τις σχετικές αναφορές σε άρθρα που περιγράφουν τους προτεινόμενους μηχανισμούς.

Κατηγορία προσεγγίσεων	**Σχετικές αναφορές**
Βασισμένες στην χρήση μοντέλου RBAC	[9, 25, 26, 27]
Βασισμένες στην χρήση μηχανισμού συσκότισης πληροφορίας	[18, 21, 30, 31, 32, 36, 37]
Βασισμένες στην χρήση μηχανισμού εκτίμησης της εμπιστοσύνης	[21, 32]
Βασισμένες στην χρήση πολιτικών	[5, 17, 18,]
Βασισμένες στην χρήση οντολογιών	[8, 18, 36, 37, 38]
Υβριδικές προσεγγίσεις	[18, 21, 32, 36, 37]
Διαφορετικές προσεγγίσεις	[12,23]

Πίνακας 5.1 Κατηγορίες προσεγγίσεων διαφύλαξης της ιδιωτικότητας

5.2 Προσεγγίσεις βασισμένες στην χρήση μοντέλου RBAC

5.2.1 Το μοντέλο RBAC

Μία κατηγορία προσεγγίσεων για διαφύλαξη της προστασίας της ιδιωτικότητας είναι αυτές που βασίζονται στη χρήση μοντέλων ελέγχου πρόσβασης ή "access control". Ο έλεγχος πρόσβασης σε ένα σύστημα αποτελεί θεμελιώδη πτυχή για την προστασία της ιδιωτικότητας. Τα μοντέλα ελέγχου της πρόσβασης των χρηστών βάσει ρόλων (Role Based Access Control – RBAC) είναι τα πιο γνωστά μοντέλα εξουσιοδότησης. Χρησιμοποιούν ιεραρχίες ρόλων και πλήθος περιορισμών της πρόσβασης και επομένως είναι δυνατόν μέσω των ρόλων να αποτυπωθεί μία πληθώρα πολιτικών ασφαλείας. Επιπλέον, η χρήση ρόλων για την οργάνωση των δικαιωμάτων πρόσβασης απλοποιεί τον τρόπο διαχείρισης της ασφάλειας στην πρόσβαση σε λειτουργίες και δεδομένα. Ο διαχωρισμός των καθηκόντων αποτελεί ένα σημαντικό ζήτημα το οποίο είναι απολύτως σχετικό με τη υιοθέτηση των ρόλων για τον έλεγχο της πρόσβασης των χρηστών. Η σημασία του διαχωρισμού των καθηκόντων έγκειται

στη μείωση του κινδύνου απάτης, μη επιτρέποντας στον οποιονδήποτε να έχει επαρκή πρόσβαση μέσα στο σύστημα για να διαπράξει την απάτη. Τέτοιοι περιορισμοί πρόσβασης μπορούν εύκολα να εκφραστούν χρησιμοποιώντας τη λογική του διαχωρισμού των καθηκόντων στο μοντέλο των ρόλων, στις αναθέσεις ρόλων σε χρήστες και στις αναθέσεις των δικαιωμάτων πρόσβασης στους ρόλους.

Ο έλεγχος της πρόσβασης βάσει ρόλων προσφέρει αρκετά πλεονεκτήματα σε σχέση με τις κλασικές μεθόδους απόδοσης πρόσβασης στα πληροφοριακά συστήματα απευθείας στους χρήστες. Στα πλεονεκτήματα αυτά περιλαμβάνεται η απλοποίηση της διαχείρισης χρηστών και δικαιωμάτων πρόσβασης καθώς και η δυνατότητα αποτελεσματικού ελέγχου και απολογισμού των εξουσιοδοτήσεων των χρηστών. Εφαρμόζοντας ένα μοντέλο ελέγχου της πρόσβασης βάσει ρόλων, τα δικαιώματα πρόσβασης ανατίθενται στους ρόλους και όχι στους χρήστες. Επομένως οποιαδήποτε τροποποίηση στα δικαιώματα πρόσβασης γίνεται στους ρόλους και αυτομάτως τροποποιούνται τα δικαιώματα των χρηστών που τους έχουν λάβει, μειώνοντας το διαχειριστικό φόρτο. Για παράδειγμα, εάν ένας χρήστης μετακινηθεί από ένα Τμήμα του οργανισμού σε ένα άλλο, τότε απλά μπορούν να του ανατεθούν οι ρόλοι του νέου Τμήματος και της νέας θέσης εργασίας και να του αφαιρεθούν οι παλαιοί ρόλοι.

Επιπλέον, η ανάθεση ρόλων στους χρήστες και η αφαίρεση ρόλων από αυτούς μπορεί να γίνεται αυτόματα χρησιμοποιώντας ειδικά συστήματα ροής εργασίας, τα οποία διευκολύνουν αρκετά τη σχετική διαδικασία. Η παροχή πληροφορίας στους χρήστες περιορίζεται σε αυτήν που προβλέπουν οι ρόλοι που ανατίθενται σε αυτούς, ενώ είναι ευκολότερη η επιβολή της όποιας πολιτικής ασφάλειας των πληροφοριών.

5.2.2 Επέκταση μοντέλου NIST RBAC

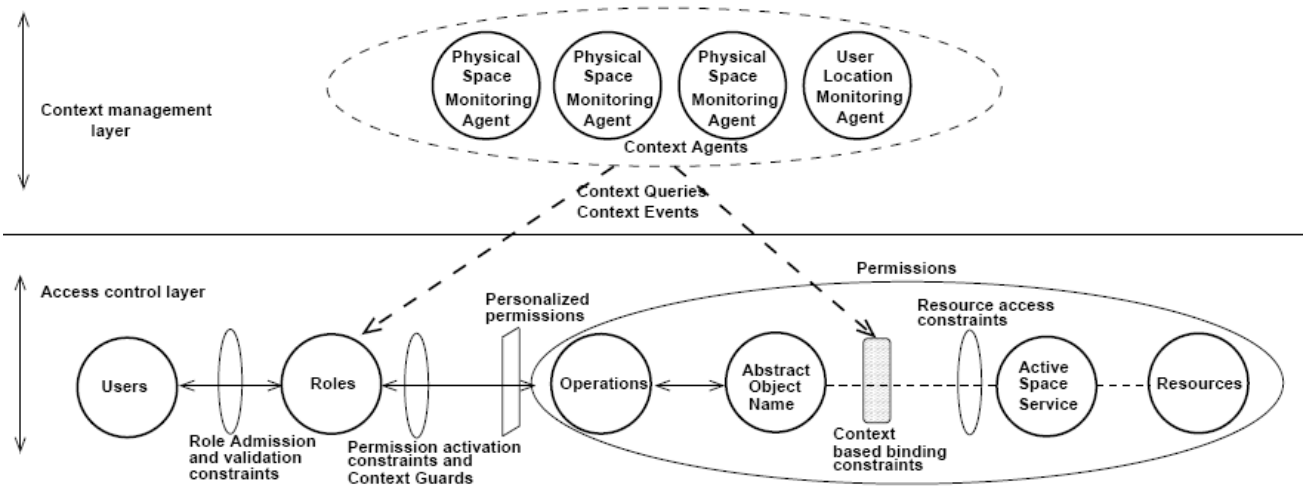
Κομμάτι του σχεδιασμού αυτού του μοντέλου [9] είναι και ο ορισμός των ρόλων. Οι χρήστες προστίθενται σε ρόλους όταν η εφαρμογή έχει αναπτυχθεί ή οι χρήστες μπορούν να επιβάλουν αίτημα ένταξης σε κάποιο ρόλο καθώς η εφαρμογή εκτελείται. Οι ρόλοι σε μία εφαρμογή θα διαρκούν όσο και η διάρκεια της λειτουργίας της εφαρμογής. Ο ορισμός ρόλου σε ένα χρήστη μπορεί να εξαρτάται από διάφορα είδη πληροφοριών όπως πιθανό κάποιοι προσωρινοί περιορισμοί του συστήματος, βασικές ιδιότητες μέλους σε άλλους ρόλους, η τοποθεσία του χρήστη κτλ. Η πρόσβαση σε

κάποιο πόρο τους συστήματος επίσης μπορεί να προυποθέτει συγκεκριμένη πληροφορία πλαισίου χρήσης, όπως η ταυτότητα και η τοποθεσία του μέλους ενός ρόλου. Αυτές οι προκλήσεις είναι κάτι που προσπαθεί να διαχειριστεί η προτεινόμενη προσέγγιση.

Στο NIST RBAC μοντέλο [14], το σύνολο των αντικειμένων για τα οποία χρειάζεται επιβολή ελέγχου πρόσβασης είναι γνωστά εκ των προτέρων. Το σύνολο των προσβάσιμων αντικειμένων που επιτρέπει μία άδεια είναι επίσης πάντοτε το ίδιο για όλα τα μέλη ενός ρόλου. Στο NIST μοντέλο δεν υπάρχει σαφής ορισμός της ανάκλησης μελών από κάποιο ρόλο.

Στο επεκτεινόμενο NIST μοντέλο ελέγχου πρόσβασης προτείνονται οι πιο κάτω μηχανισμοί. Κάθε φορά που ένας χρήστης, μέλος ενός ρόλου, επιχειρήσει να εκτελέσει μια λειτουργία του ρόλου, γίνεται αξιολόγηση των περιορισμών επικύρωσης της άδειας (validation constraints). Σε περίπτωση που οι προυποθέσεις και οι περιορισμοί όσον αφορά την κατάσταση των πληροφοριών πλαισίου χρήσης που ενεμπλέκονται αποτύχουν να διατηρηθούν, γίνεται ανάκληση της ιδιότητας του χρήστη αυτού από τον ρόλο που τον χαρακτήριζε.

Το μοντέλο υποστηρίζει επίσης εξατομικευμένες άδειες σε μέλη ενός ρόλου, οι οποίες εκτελούνται σε διαφορετικά αντικείμενα από διαφορετικό μέλος του ρόλου. Τα αντικείμενα που είναι προσβάσιμα από όλα τα μέλη ενός ρόλου δηλώνονται ως διαμοιραζόμενα (shared) και private, αυτά που για κάθε διαφορετικό μέλος ενός ρόλου είναι ιδιωτικά. Για παράδειγμα σε ένα ιατρικό σύστημα, η κάθε νοσοκόμα έχει πρόσβαση στον εκτυπωτή που βρίσκεται στο δωμάτιο που βρίσκεται η κάθε μία. Κάθε διαδραστικό ενεργό session (σύνοδος) προυποθέτει την ύπαρξη κάποιων συνθηκών αναφορικά με την πληροφορία πλαισίου χρήσης που χρησιμοποιεί. Όταν αυτές οι συνθήκες σταματήσουν να ισχύουν, τότε ο υπεύθυνος μηχανισμός, εδώ αναφερόμενος ως context guard mechanism, θα ανακαλέσει την εκτέλεση αυτού του session. Για παράδειγμα σε ένα ιατρικό σύστημα πάλι, μία ενεργή σύνοδος πρέπει να τερματίζεται όταν η νοσοκόμα φύγει από τον θάλαμο όπου ήταν υπεύθυνη.



Σχήμα 5.1 Context-aware RBAC μοντέλο

Οι Devdatta και Tripathi αναφέρουν επίσης πως μία εφαρμογή είναι σημαντικό να εμπιστεύεται τους πράκτορες (agents) πλαισίου χρήσης από τους οποίους αποκτά τις απαιτούμενες πληροφορίες πλαισίου χρήσης, επειδή οι πληροφορίες αυτές αποτελούν τον περιορισμό και την απάντηση για την απόφαση ελέγχου πρόσβασης.

5.2.3 Context- RBAC (βάσει ρόλου της πληροφορίας)

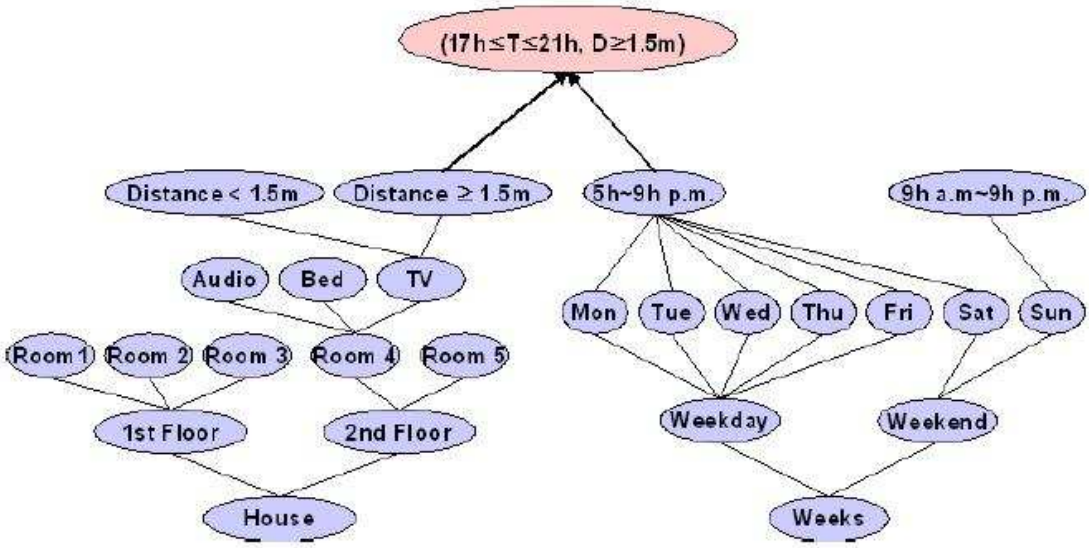
Η προσέγγιση αυτή [27] αποτελεί επέκταση του κλασικού προτύπου RBAC [13]. Οι Park, Han et al., αναφέρουν ότι το μειονέκτημα του κλασικού μοντέλου RBAC είναι ότι οι ρόλοι που ανατίθενται επικεντρώνονται αποκλειστικά στο υποκείμενο, δηλαδή το χρήστη. Το νέο γνώρισμα που προστίθεται είναι η έννοια του ρόλου της πληροφορίας πλαισίου χρήσης (context-role). Ο ρόλος αυτός αναπαριστά την κατάσταση του περιβάλλοντος, το τρέχον πλαίσιο χρήσης. Υποστηρίζουν ότι είναι σημαντικό για μία απόφαση ελέγχου πρόσβασης να μη συμμερίζεται μόνο ο ρόλος του χρήστη αλλά και οι πληροφορίες πλαισίου χρήσης που μπορεί να έχουν κάποια επιρροή στην απόφαση.

Ο φορμαλισμός που χρησιμοποιείται είναι βασισμένος σε αυτόν του κλασικού RBAC. Οι οντότητες που αποτελούν το μοντέλο είναι οι χρήστες, οι πληροφορίες πλαισίου χρήσης, οι ρόλοι, οι άδειες και τα sessions(οι συνόδοι). Ένας ρόλος έχει άλλους δύο ρόλους, τον ρόλο χρήστη και τον ρόλο της πληροφορίας. Οι αντιστοιχίσεις μεταξύ οντοτήτων που μπορούν να υπάρξουν είναι ανάμεσα σε ένα

χρήστη και κάποιο ρόλο, ανάμεσα σε μία πληροφορία και κάποιο ρόλο και ανάμεσα ενός ρόλου και κάποιες άδειες. Μία συγκεκριμένη ενέργεια προς εκτέλεση από το σύστημα διατυπώνεται υπό μορφή της πλειάδας < user_role, context_role, permission >. Μία βάση που διατηρεί τις πολιτικές (policy database) περιέχει μία λίστα με τους κανόνες πολιτικών. Οι κανόνες πολιτικών είναι πολιτικές που συνοδεύονται από μία ένδειξη άδειας (permission_bit), το οποίο υποδεικνύει εάν η αναφερόμενη ενέργεια επιτρέπεται ή απορρίπτεται από το σύστημα. Ένα παράδειγμα ενός τέτοιου κανόνα είναι:

< < παιδί, (19h < T < 1h, D> 2m) , TV_ON > , ALLOW >

Το παιδί δηλώνει το ρόλο του χρήστη, το (19h < T < 1h , D> 2m) δηλώνει το ρόλο της πληροφορίας πλαισίου, τις επιτρεπτές τιμές δηλαδή των πληροφοριών, το **TV_ON** αποτελεί την άδεια και το **ALLOW** υποδεικνύει ότι η πιο πάνω ενέργεια επιτρέπεται. Τέτοιοι κανόνες πολιτικών (policy rules) πρέπει να φυλάγονται σε μία βάση πολιτικών ασφαλείας και να ελέγχονται κάθε φορά που παρουσιάζεται αίτημα ελέγχου πρόσβασης.



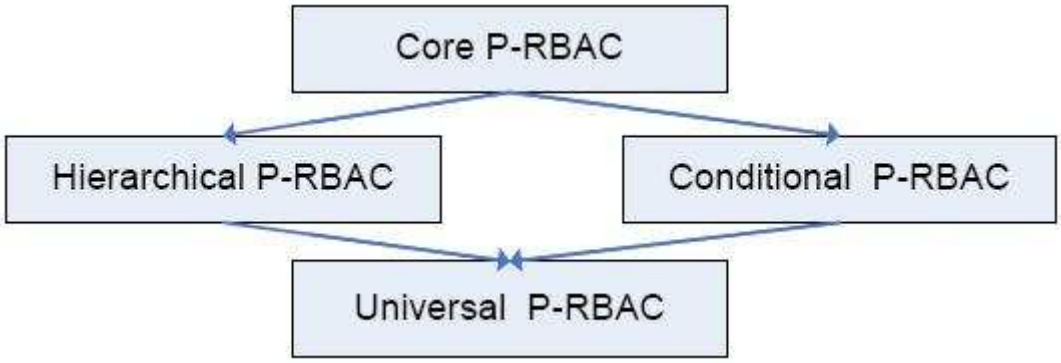
Σχήμα 5.2 Context-RBAC

5.2.4 Οικογένεια εννοιολογικών RBAC μοντέλων

Η προσέγγιση αυτή [24, 25] αποτελεί μία οικογένεια, μία ομαδοποίηση RBAC μοντέλων, επεκτάσεις του κλασικού προτύπου RBAC. Στόχοι της δουλειάς αυτής

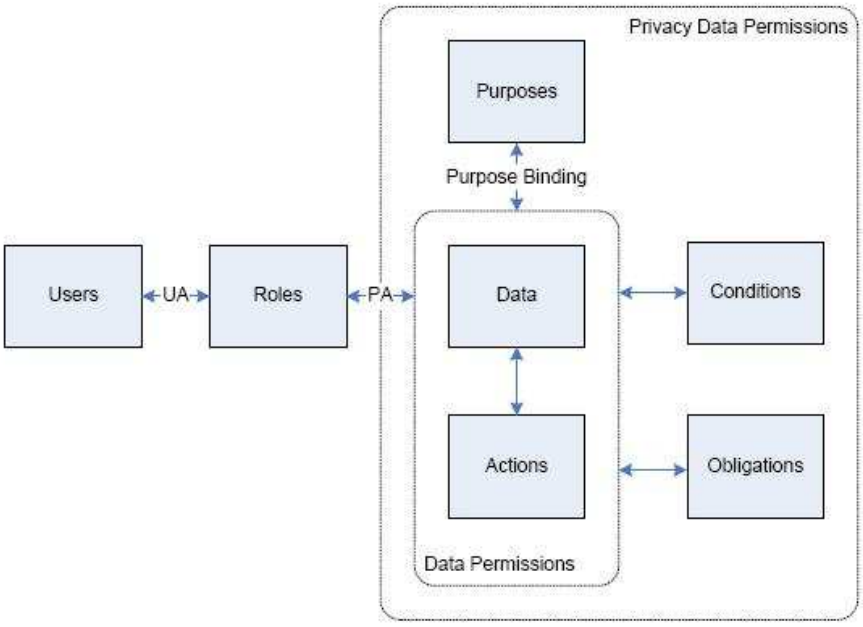
είναι η υποστήριξη ελέγχου πρόσβασης που να έχει επίγνωση την ιδιωτικότητα, η υποστήριξη πολιτικών ιδιωτικότητας λαμβάνοντας συνάμα υπόψη χαρακτηριστικά όπως είναι ο σκοπός πρόσβασης, οι προυποθέσεις και οι υποχρεώσεις. Η σημαντικότητα των χαρακτηριστικών αυτών πηγάζει από τις OECD Guidelines[49] για την προστασία της ιδιωτικότητας των προσωπικών δεδομένων, από τους σύγχρονους νόμους ιδιωτικότητας στην Αμερική και δημόσιες πολιτικές ιδιωτικότητας γνωστών οργανισμών. Τα δεδομένα που συλλέγηκαν για κάποιο σκοπό δεν πρέπει να χρησιμοποιούνται για κάποιο άλλο σκοπό χωρίς την συγκατάθεση του χρήστη. Υποχρεώσεις (obligations) είναι ενέργειες που πρέπει να ακολουθήσουν την εκτέλεση κάποιας άλλης ενέργειας πάνω σε δεδομένα. Προυποθέσεις είναι καταστάσεις που πρέπει να ικανοποιηθούν πριν την εκτέλεση κάποιας ενέργειας, για παράδειγμα συγκατάθεση γονέα για οτιδήποτε αφορά το παιδί.

Το γενικό μοντέλο αποτελείται από τα ακόλουθα μοντέλα ελέγχου πρόσβασης βάσει ρόλων: Core P-RBAC model , Hierarchical P-RBAC model, Conditional P-RBAC model, Universal P-RBAC model. Το κάθε μοντέλο έχει τις δικές του δυνατότητες.



Σχήμα 5.3 Ιεραρχία εννοιολογικών μοντέλων RBAC

Βασικό μοντέλο είναι το Core P-RBAC. Συμπεριλαμβάνει διάφορα σύνολα οντοτήτων όπως οι χρήστες, οι ρόλοι, τα δεδομένα (οποιαδήποτε σχετική πληροφορία αναγνωρίσιμου χρήστη), οι ενέργειες, οι σκοποί (purposes), οι υποχρεώσεις (obligations) και οι προυποθέσεις (conditions). Οι προυποθέσεις εκφράζονται μέσω μίας απλής γλώσσας (LC_0**)** με την βοήθεια μεταβλητών πληροφορίας πλαισίου χρήσης (context variables), για παράδειγμα μεταβλητές όπως OwnerConsent, OwnerAge, CurrentTime. Οι μεταβλητές αυτές είναι πληροφορίες που χρειάζονται να ληφθούν υπόψη πριν την επιβολή των αδειών ιδιωτικότητας.



Σχήμα 5.4 Core P-RBAC

Σύνθετα περιβάλλοντα όπως μεγάλες επιχειρήσεις που συνήθως πρέπει να ακολουθούν πολύπλοκες πολιτικές ασφαλείας και ιδιωτικότητας είναι πιθανό να συναντήσουν ασυνέπεια και συγκρούσεις (conflicts) ανάμεσα στις πολιτικές αυτές. Οι αναθέσεις αδειών είναι πολύ πιθανό να έρθουν σε σύγκρουση μεταξύ τους εξαιτίας νέων απαιτήσεων, νέων κανόνων ή ακόμα εξαιτίας ανθρώπινου λάθους. Η προσέγγιση αυτή αναφέρεται σε αλγόριθμους ανίχνευσης τέτοιων συγκρούσεων έτσι ώστε να υπάρχει εγγύηση συνέπειας ανάμεσα στο σύνολο των αναθέσεων αδειών πρόσβασης. Οι αλγόριθμοι PA-Conflict-Detection (permission assignment 1, permission assignment 2) και PAL-Conflict-Detection (list of permission assignments) ανιχνεύουν συγκρούσεις ανάμεσα σε δύο αναθέσεις αδειών και ανάμεσα σε ένα σύνολο αναθέσεων αδειών αντίστοιχα.

Η λειτουργία του βασικού αυτού μοντέλου επεκτείνεται σε δύο άλλα μοντέλα , το Hierarchical P-RBAC και το Conditional P-RBAC. Το Hierarchical P-RBAC ενισχύει την αποδοτικότητα και την εκφραστικότητα του βασικού μοντέλου με ιεραρχικές οργανώσεις – συσχετίσεις για τρεις σημαντικές του οντότητες : Ιεραρχία Ρόλων (Role Hierarchy), Ιεραρχία Δεδομένων (Data Hierarchy) και Ιεραρχία σκοπών (Purpose Hierarchy). Οι ιεραρχίες ρόλων αναπαριστούν μία σημαντική έννοια στο πρότυπο RBAC, η οποία ορίζεται βάση των αρχών και της ευθύνης του οργανισμού.

Η ιεραρχία σκοπών αναπαριστάται ως ένα δέντρο, όπου ένας κόμβος-γονέας αναπαριστά ένα πιο γενικό σκοπό σε σχέση με τους κόμβους-παιδιά του. Πρόσβαση σε κάποιο σκοπό-γονέα επιτρέπεται μόνο όταν επιτρέπεται η πρόσβαση σε όλους τους σκοπούς-παιδιά του. Η ιεραρχία δεδομένων επίσης αναπαριστάται ως ένα δέντρο και ισχύει ο ίδιος κανόνας πρόσβασης. Η ιδέα αυτή της ιεραρχίας συμπυκνώνει τις αναθέσεις αδειών και περιπλέκει τον έλεγχο συνέπειας.

Το Conditional P-RBAC μοντέλο υποστηρίζει πιο εκφραστικές γλώσσες διατύπωσης των προυποθέσεων (conditions) από ότι η απλή γλώσσα προυποθέσεων του Core P-RBAC και πιο ευέλικτες συσχετίσεις ανάμεσα στις αναθέσεις αδειών. Με την εισαγωγή μιας νέας ανάθεσης άδειας απαιτείται έλεγχος για πλεονασμό, έλεγχος σύγκρουσης με υπάρχουσα άδεια και έλεγχος για ιντετερμινισμού. Ως μοντέλο που δεν λειτουργεί με ιεραρχίες, οι πιο πάνω ελέγχοι διενεργούνται μόνο σε άδειες με τον ίδιο ρόλο (δεδομένα, ενέργεια, σκοπός), αφού κάθε ρόλος είναι ανεξάρτητος. Τέλος το Universal P-RBAC συνδυάζει τις λειτουργικότητες των προηγούμενων άλλων δύο μοντέλων και κληρονομεί τα χαρακτηριστικά τους.

5.3 Προσεγγίσεις με μηχανισμό συσκότισης πληροφορίας

5.3.1 Τι είναι η συσκότιση πληροφορίας

Η τεχνική συσκότισης (obfuscation), ή αλλιώς γενίκευσης (generalization) οδηγεί στην μεγιστοποίηση της χρησιμότητας των δεδομένων και παράλληλα ελαχιστοποιεί την αποκάλυψη ευαίσθητων προσωπικών δεδομένων των χρηστών. Με πιο απλά λόγια η πραγματική τιμή μιας πληροφορίας αντικαταστάται με μία πιο γενική τιμή λιγότερης ακρίβειας. Οι πληροφορίες πλαισίου χρήσης μπορούν να οργανωθούν μέσω ιεραρχιών που θα επιτρέπουν την αποκάλυψη τους σε διαφορετικά επίπεδα διακριτότητας (granularity). Οι κατόχοι δεδομένων μπορούν να προσδιορίζουν τις δικές τους απαιτήσεις και προτιμήσεις ιδιωτικότητας συνοδεύοντας τις με το επιθυμητό επίπεδο γενίκευσης. Στα πιο ευαίσθητα προσωπικά δεδομένα όπου επιβάλλεται υψηλότερο επίπεδο προστασίας, απαιτείται υψηλότερο επίπεδο γενίκευσης, δηλαδή χαμηλό βαθμό λεπτομέρειας της αποκάλυψης. Το μέγιστο όριο διακριτότητας (generalization boundary) χρειάζεται να προσδιοριστεί από την αρχή,

ούτως ώστε το αποτέλεσμα που παρουσιάζεται να παραμένει μία χρήσιμη πληροφορία.

5.3.2 Μηχανισμός συσκότισης μέσω οντολογικών περιγραφών

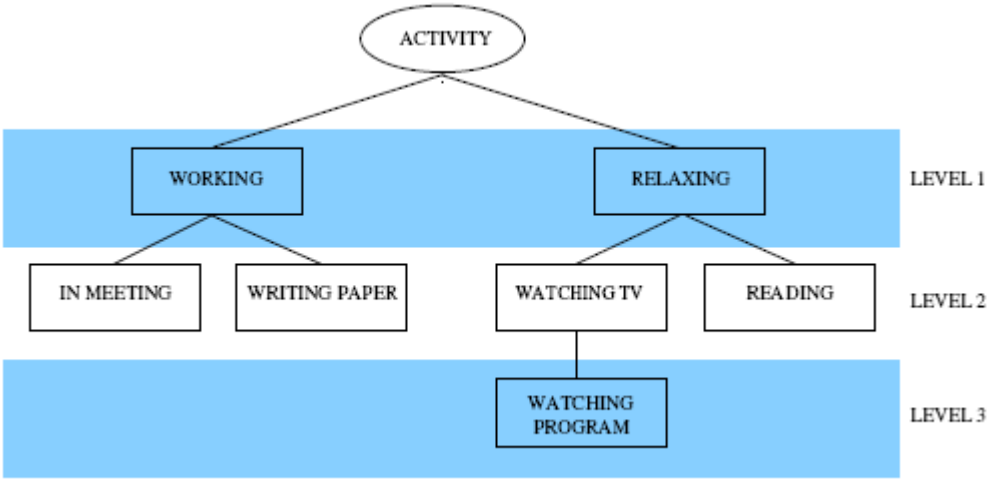
Η προσέγγιση αυτή μπορεί να ενταχθεί επίσης στην κατηγορία προσεγγίσεων που κάνουν χρήση οντολογιών, αφού όπως περιγράφεται πιο κάτω ο μηχανισμός συσκότισης που προτείνουν υποστηρίζεται από οντολογίες.

Οι Wishart, Henricksen et al., στο άρθρο τους [36] υποστηρίζουν ότι ένας μηχανισμός προστασίας ιδιωτικότητας είναι περισσότερο αποτελεσματικός και λειτουργικός όταν πέραν της υποστήριξης κανόνων και πολιτικών που ορίζουν οι χρήστες όσον αφορά την επιθυμία τους να αποκαλυφθούν ή όχι τα δεδομένα τους, προσφέρει την δυνατότητα προσδιορισμού του επιπέδου διακριτότητας (granularity) της επιτρεπτής αποκάλυψης της πληροφορίας πλαισίου χρήσης.

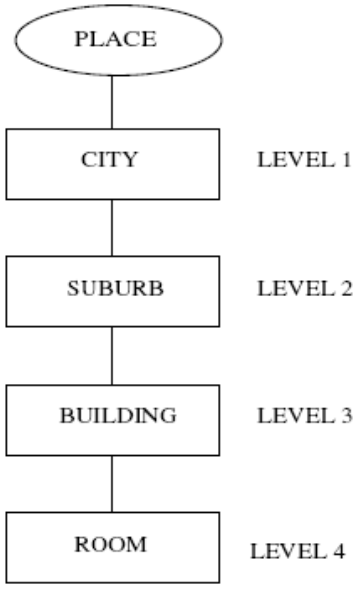
Ο μηχανισμός που προτείνεται ρυθμίζει το βαθμό αποκάλυψης μιας πληροφορίας ανάλογα με τις προτιμήσεις που προσδιορίζει ο κάτοχος της συγκεκριμένης πληροφορίας μέσω κάποιου μοντέλου προτιμήσεων. Η διαδικασία αυτή της συσκότισης (obfuscation) υποστηρίζεται μέσω λεπτομερών οντολογικών περιγραφών (ιεραρχίες) οι οποίες εκφράζουν τον βαθμό διακριτότητας για κάθε ειδική περίπτωση κάποιου τύπου αντικειμένου. Μία γενική επιλογή προτίμησης γενίκευσης πληροφορίας δεν συνδέεται με συγκεκριμένη προτίμηση ιδιωτικότητας αλλά αναφέρεται σε τύπους αντικειμένων του μοντέλου πληροφορίας πλαισίου χρήσης όπως για παράδειγμα για την ενέργεια, την τοποθεσία ή για το άτομο. Μπορεί να χρησιμοποιηθεί για πέραν από μία προτίμηση ιδιωτικότητας.

Για την υποστήριξη της συσκότισης των δεδομένων, η προσέγγιση αυτή προτείνει χρήση οντολογιών. Κάθε τύπος αντικειμένου, για παράδειγμα το άτομο, η τοποθεσία, που υπάρχει στο μοντέλο πλαισίου χρήσης περιγράφεται βάσει μιας οντολογίας. Διαφορετικά στιγμιότυπα μιας οντολογίας παρουσιάζουν και διαφορετικό επίπεδο λεπτομέρειας της αποκάλυψης. Αντικείμενα που αντιστοιχούν με τα παιδιά μιας πληροφορίας που αναπαριστά η οντολογία θεωρούνται πληροφορίες υψηλότερου βαθμού διακριτότητας αποκάλυψης της πληροφορίας. Αντίστοιχα, αντικείμενα που

αντιστοιχούν με τους προγόνους θεωρούνται πληροφορίες χαμηλότερου βαθμού διακριτότητας, παρουσιάζουν δηλαδή κάτι πιο γενικό και αόριστο.



Σχήμα 5.5 Οντολογία δραστηριότητας



Σχήμα 5.6 Οντολογία τοποθεσίας

Ο χρήστης έχει την δυνατότητα να προσδιορίσει δύο είδη προτιμήσεων όσον αφορά τους κανόνες απόκρυψης και αποκάλυψης των προσωπικών του πληροφοριών που θέλει να θέσει. Πρώτα είναι οι προτιμήσεις ιδιωτικότητας (privacy preferences) στις οποίες δηλώνει ποιές πληροφορίες και σε ποιους επιτρέπει να διαδοθούν και κατά δεύτερον είναι οι προτιμήσεις διακριτότητας (granularity preferences) στις οποίες ρυθμίζει το επίπεδο συσκότισης, αλλιώς το επίπεδο λεπτομέρειας που θα χαρακτηρίζει την αποκάλυψη μιας πληροφορίας (granularity/ blurring level).

5.3.3 Μηχανισμός που προσαρμόζει δυναμικά το επίπεδο συσκότισης

Η προσέγγιση αυτή μπορεί να ενταχθεί επίσης στην κατηγορία προσεγγίσεων που κάνουν χρήση οντολογιών, αφού όπως περιγράφεται πιο κάτω ο μηχανισμός συσκότισης που προτείνουν υποστηρίζεται από οντολογίες.

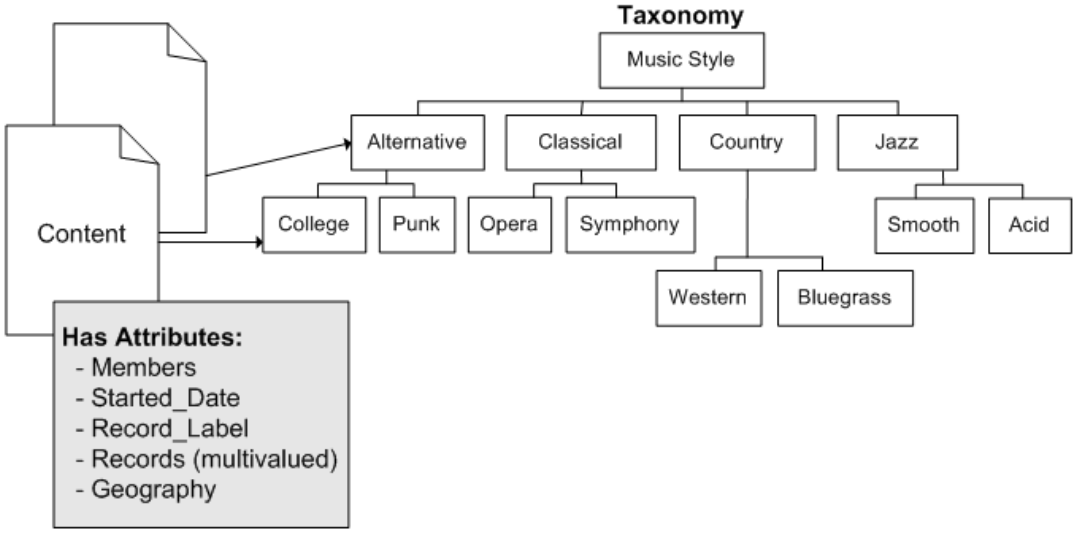
Οι Wishart, Henricksen et al., σε νεότερο τους άρθρο [37], έχοντας υπόψη τα χαρακτηριστικά ενός περιβάλλοντος διάχυτου υπολογισμού, παρουσιάζουν ένα μηχανισμό ιδιωτικότητας που υποστηρίζει: 1) σχέσεις ιδιοκτησίας πληροφοριών πλαισίου χρήσης που εξαρτώνται από το πλαίσιο χρήσης, σχέσεις κοινής ιδιοκτησίας μιας πληροφορίας (multi-party), 2) δίνει τη δυνατότητα στους κατόχους δεδομένων να προσδιορίσουν τις δικές τους προτιμήσεις ιδιωτικότητας, στις οποίες δηλώνουν στοιχεία όπως σε ποιον επιτρέπουν την αποκάλυψη των πληροφοριών πλαισίου χρήσης που τους χαρακτηρίζουν, κάτω από ποιες συνθήκες επιτρέπεται η αποκάλυψη αυτή, καθώς και το επίπεδο λεπτομέρειας αποκάλυψης της πληροφορίας αφού σε ορισμένες περιπτώσεις ο χρήστης δεν επιθυμεί αποκάλυψη της ακριβής τιμής μιας προσωπικής του πληροφορίας, αλλά μέρος αυτής.

Σε υφιστάμενα συστήματα οι μηχανισμοί συσκότισης που χρησιμοποιούν περιορίζονται σε συσκότιση συγκεκριμένων τύπων πληροφοριών πλαισίου χρήσης, όπως για παράδειγμα η τοποθεσία. Επίσης, οι τιμές που επιστρέφονται ως αποτέλεσμα της συσκότισης είναι προκαθορισμένες ή υποστηρίζουν ένα καθορισμένο αριθμό επιπέδων λεπτομέρειας για όλους τους τύπους δεδομένων. Για την επίτευξη της συσκότισης των δεδομένων στην προσέγγιση αυτή, εισάγεται ένας νέος μηχανισμός συσκότισης που βασίζεται στην "δυναμική εξεύρεση και επεξεργασία των πληροφοριών πλαισίου χρήσης". Ο μηχανισμός αυτός προσαρμόζει και χειρίζεται δυναμικά το επίπεδο λεπτομέρειας αποκάλυψης της πληροφορίας, σύμφωνα με τις απαιτήσεις του κατόχου της πληροφορίας.

Για την μοντελοποίηση της πληροφορίας πλαισίου χρήσης χρησιμοποιείται η γλώσσα Context Modeling Language (CML). Οι κύριες οντότητες σε ένα περιβάλλον, όπως για παράδειγμα η τοποθεσία, η ενέργεια, αναπαριστώνται ως τύποι αντικειμένων στο μοντέλο πληροφορίας. Αντικείμενα είναι τα στιγμιότυπα των τύπων αντικειμένων,

λόγω χάρην μια συγκεκριμένη τοποθεσία. Οι σχέσεις ανάμεσα σε τύπους αντικειμένων μοντελοποιούνται ως τύποι γεγονότων, καθώς οι σχέσεις ανάμεσα σε αντικείμενα αναπαριστώνται ως γεγονότα (context facts). Κάθε τύπος πληροφορίας (fact type) μπορεί να έχει τους δικούς του κανόνες για ανάθεση ιδιοκτησίας. Οι κανόνες αυτοί συνδέουν κάθε πληροφορία πλαισίου χρήσης με μηδέν, ένα ή πολλαπλούς ιδιοκτήτες. Αν η ζητούμενη πληροφορία σε ένα αίτημα, είναι πληροφορία που δεν ανήκει σε κάποιον τότε η πρόσβαση σε αυτή επιτρέπεται αφού αποτελεί κοινή πληροφορία που μπορεί ελεύθερα να αποκαλυφθεί. Αν ο αιτητής πρόσβασης σε πληροφορία είναι ένας από τους κάτοχους της συγκεκριμένης πληροφορίας τότε και πάλι η αίτηση επιτρέπεται. Στην περίπτωση που ο αιτητής δεν ανήκει στους ιδιοκτήτες της πληροφορίας, η απόφαση επέρχεται βάσει των προτιμήσεων και απαιτήσεων των κατόχων της.

Για την υποστήριξη της διαδικασίας συσκότισης, βασίζονται σε προκαθορισμένες οντολογίες για κάθε τύπο αντικειμένων. Οι οντολογίες αυτές αποτελούνται από τιμές που διατάσσονται σε μία ιεραρχία ανάλογα με το επίπεδο λεπτομέρειας, οι κόμβοι-πατέρας μιας ιεραρχίας αποτελούν πιο γενικές τιμές από ότι τα παιδιά σε μία ιεραρχική δομή. Η εύρεση συσχετίσεων ανάμεσα σε συγκεκριμένα στιγμιότυπα αντικειμένων που αναπαριστώνται μέσω οντολογίας, μπορεί να επιτευχθεί μέσω λεπτομερών ταξινομιών (taxonomies) δηλαδή ονομασία, περιγραφή και ιεράρχηση εννοιών.



Σχήμα 5.7 Απλό παράδειγμα ταξινομίας

Η χρήση ταξινομιών όμως δεν είναι πάντα η καλύτερη λύση, κυρίως για ένα περιβάλλον διάχυτου υπολογισμού που μεταβάλλεται δυναμικά και οι ταξινομίες θα έπρεπε να προσδιορίζονται εκ νέου. Στο άρθρο αυτό περιγράφεται μία διαφορετική προσέγγιση στην οποία οι κανόνες επεξεργασίας των δεδομένων που χρησιμοποιούνται για την συσκότιση των πληροφοριών που βασίζεται σε κανόνες και δεν απαιτεί χρήση μεγάλων και λεπτομερών ταξινομιών. Το σύστημα δυναμικά ανακαλύπτει κανόνες που αφορούν την συσκότιση των δεδομένων, οι οποίοι μπορούν να υλοποιηθούν ως δυναμικά ανιχνεύσιμα προγράμματα επεξεργασίας δεδομένων.

Για σκοπούς επίδειξης του μηχανισμού συσκότισης χρησιμοποιείται ένα σύστημα διαχείρισης πληροφοριών πλαισίου χρήσης (CMS). Το σύστημα αυτό είναι ικανό να ανακαλύψει νέες πηγές πληροφοριών, να επεξεργαστεί δεδομένα που έχουν ήδη εξαχθεί μέσω αισθητήρων με την βοήθεια των SensorML περιγραφών και παρατηρήσεων των αισθητήρων.

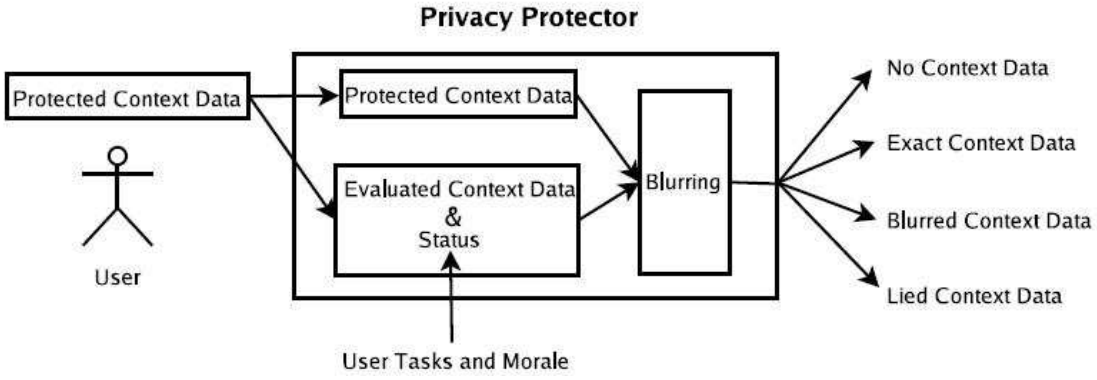
5.3.4 Μοντέλο πλαισίου χρήσης με επίγνωση ιδιωτικότητας

Το προτεινόμενο μοντέλο του E.I.Tatli στο άρθρο[30] αποτελεί επέκταση του μοντέλου πληροφορίας πλαισίου χρήσης που προτάθηκε από τους Schmid et al. [39]. Σύμφωνα με το μοντέλο τους, η πληροφορία πλαισίου χρήσης μπορεί να πηγάζει από ανθρώπινους παράγοντες ή από το φυσικό περιβάλλον. Στο σχετικό κείμενο τους "There is more to Context than Location" τονίζουν επίσης ότι παρόλο που η τοποθεσία αποτελεί μια πληροφορία που χρησιμοποιείται περισσότερο από κάθε άλλη πληροφορία ως πλαίσιο χρήσης, υπάρχουν πολλές άλλες σημαντικές πληροφορίες πλαισίου χρήσης που μπορεί να αυξήσουν την λειτουργικότητα μιας εφαρμογής. Ένα μοντέλο όμως που δεν λάμβανε υπόψη την ιδιωτικότητα των δεδομένων πλαισίου χρήσης και τις αλληλεπιδράσεις ανάμεσα σε δεδομένα. Έχοντας υπόψη το μείον αυτό, ο Tatli στο άρθρο αυτό θίγει κάποια θέματα ιδιωτικότητας που μπορούν να ληφθούν υπόψη και να οδηγήσουν στην κατασκευή ενός μοντέλου που θα μπορούσε να ευκολύνει την διαχείριση της ιδιωτικότητας σε εφαρμογές με επίγνωση του πλαισίου χρήσης.

Συγκεγκριμένα αναφέρει τις παρακάτω πτυχές που μπορούν να συμβάλουν σε θέματα προστασίας της ιδιωτικότητας. Το πρώτο έχει να κάνει με την κατηγοριοποίηση των

πληροφοριών πλαισίου χρήσης σε protected και not protected. Δεδομένα που πιθανό να αποκαλυφούν σε τρίτα άτομα εντός των εφαρμογών πρέπει ρητά να ανήκουν στην ομάδα protected. Τα υπόλοιπα δεδομένα ανήκουν στην κατηγορία evaluated context, τα οποία μπορεί να μην στέλνονται σε άλλους αλλά ωστόσο επηρεάζουν το επίπεδο ιδιωτικότητας των δεδομένων του χρήστη που θα διαδοθούν σε άλλους (protected). Ένα παράδειγμα τέτοιας εξάρτησης ανάμεσα σε δεδομένα πλαισίου χρήσης των διαφορετικών κατηγοριών θα μπορούσε να είναι: Ο χρήστης Α δεν επιθυμεί αποκάλυψη της τοποθεσίας του σε συγκεκριμένες ημερομηνίες. Η ανάγκη αυτή προέρχεται από το γεγονός ότι η κατάσταση των δεδομένων που αποτελούν το πλαίσιο χρήσης μπορεί να αλλάζει συχνά και αυτό μπορεί να επηρεάσει τις προτιμήσεις ιδιωτικότητας του χρήστη όσον αφορά μια άλλη πληροφορία πλαισίου χρήσης. Επομένως για να προστατευτούν τα ευαίσθητα δεδομένα που αποτελούν την κατηγορία protected context, επιβάλλονται πολιτικές ιδιωτικότητας που βασίζονται τόσο στην πρώτη κατηγορία δεδομένων όσο και στην δεύτερη. Αυτό είναι που ονομάζεται «context privacy dependence».

Μία άλλη μέθοδος που προτείνεται ως κίνητρο για αύξηση της προστασίας της ιδιωτικότητας είναι η μέθοδος «context blurring». Η λειτουργία αυτή δίνει την δυνατότητα στον χρήστη να φανερώσει κάποιο μέρος μιας πληροφορίας έναντι της ακριβής τιμής της. Οι πολιτικές αυτές μπορούν επίσης να ορισθούν βάσει και των δύο κατηγοριών πληροφοριών του πλαισίου χρήσης. Για παράδειγμα ο χρήστης μπορεί να «θολώσει» την πληροφορία τοποθεσίας του (protected context) αν η κατάσταση (evaluated context) του σημειώνεται ως «away».



Σχήμα 5.7 Αλληλεπίδραση πληροφοριών πλαισίου χρήσης

Σε άρθρο που ακολούθησε, ο Tatli [31] περιγράφει τα σχέδια του για επέκταση της πλατφόρμας P3P έτσι ώστε να είναι σε θέση να υποστηρίξει εφαρμογές με επίγνωση του πλαισίου χρήσης. Το προτεινόμενο μοντέλο πληροφορίας πλαισίου χρήσης που είχε προτείνει [30] αναφέρει πως χρειάζεται επίσημο ορισμό έτσι ώστε τα δεδομένα να μπορούν να ενσωματωθούν στην επεκτεινόμενη πλατφόρμα P3P. Βάσει αυτής της επέκτασης, θα σχεδιαστεί αρχιτεκτονική ιδιωτικότητας που θα έχει επίκεντρο τον χρήστη. Για την επιβολή των πολιτικών ιδιωτικότητας θα υλοποιηθούν κατάλληλες κρυπτογραφικές μεθόδοι και πρωτόκολλα ασφαλείας. Τέλος αναφέρει ότι οι επεκτεινόμενες P3P πολιτικές θα ενσωματωθούν στις εφαρμογές και θα χρησιμοποιηθούν για τον προσδιορισμό πολιτικών ιδιωτικότητας.

5.4 Προσεγγίσεις με μηχανισμό εκτίμησης εμπιστοσύνης

5.4.1 Εμπιστοσύνη και αξιοπιστία χρήστη

Εμπιστοσύνη σημαίνει ευθύνη, σημαίνει αξιοπιστία μιας συμπεριφοράς ενός έμπιστου χρήστη. Είναι σημαντικό τα δεδομένα των χρηστών να είναι προσβάσιμα από έμπιστα άτομα, γιατί αυτό συνεπάγει μικρότερη πιθανότητα απειλής της ιδιωτικότητας του ατόμου.

5.4.2 Μηχανισμός ελέγχου πρόσβασης με διαχείριση εμπιστοσύνης

Η προσέγγιση αυτή [21] προτείνει μία πολιτική αποφάσεων βασισμένη στην εκτίμηση της εμπιστοσύνης του αιτούντα για διαχειρισμό της ασφάλειας πρόσβασης. Το προτεινόμενο μοντέλο ελέγχου προσβάσεων λειτουργεί ως εξής: πριν την πρόσβαση κάποιου αιτούντα, εκτιμάται η εμπιστοσύνη του βάσει παρατηρήσεων ενεργειών του στο παρελθόν, μέσα από την βάση ιστορικού (history) που διατηρεί το σύστημα. Η τελική εκτίμηση γίνεται συνδυάζοντας το ιστορικό αυτό με συστάσεις άλλων χρηστών που έχουν παραθέσει στην βάση συστάσεων του συστήματος. Όταν ο βαθμός εμπιστοσύνης αυτού που θέλει να χρησιμοποιήσει τα δεδομένα είναι λιγότερος από το κατώφλι εμπιστοσύνης που έχει ορίσει ο ιδιοκτήτης δεδομένων στις απαιτήσεις του όσον αφορά άδειες πρόσβασης, τότε η εκτέλεση της ζητούμενης ενέργειας απαγορεύεται.

Οι χρήστες μπορούν να προσδιορίσουν τις δικές τους απαιτήσεις διαφύλαξης ιδιωτικότητας ορίζοντας το επίπεδο γενίκευσης που επιθυμούν σε ευαίσθητα τους δεδομένα. Δεδομένα στα οποία επιβάλλεται υψηλότερο επίπεδο προστασίας όπως είναι για παράδειγμα η ταυτότητα ενός χρήστη ή η τοποθεσία του, απαιτείται υψηλότερο επίπεδο γενίκευσης. Το ανώτατο επιτρεπτό επίπεδο γενίκευσης μιας πληροφορίας μπορεί να διαφέρει ανάλογα με τον σκοπό πρόσβασης σε αυτήν. Χρειάζεται επίσης προσδιορισμός ορίου γενίκευσης (generalization boundary) για κάθε δεδομένο, ούτως ώστε ο χρήστης να δηλώσει μέχρι ποιο βαθμό πιστεύει ότι θα μπορούσε να γενικευτεί και το αποτέλεσμα να παραμένει μια χρήσιμη πληροφορία. Η γενίκευση (generalization) των δεδομένων βοηθά στην μεγιστοποίηση της χρηστικότητας των δεδομένων και ελαχιστοποιεί την αποκάλυψη ευαίσθητων ιδιωτικών δεδομένων μέσω των διάφορων επιπέδων γενίκευσης που προσφέρει, αφού η πραγματική τιμή αντικαταστάται με μία λιγότερο συγκεκριμένη.

Ενώ λοιπόν αρχικά επιβεβαιώνεται ότι ο χρήστης που παραθέτει κάποιο αίτημα είναι αυτός που ισχυρίζεται ότι είναι μέσω της πιστοποίησης του (authentication), στη συνέχεια το μοντέλο ελέγχου πρόσβασης είναι σε θέση να καθορίσει τα δικαιώματα αυτού του χρήστη, δηλαδή τις ενέργειες που μπορεί να εκτελεί (εξουσιοδότηση). Κατά την διάρκεια της πρόσβασης εφαρμόζονται πολιτικές ελέγχου πρόσβασης όπου η απόφαση βασίζεται τώρα στην ερώτηση "πόση πληροφορία μπορεί να επιτραπεί για τον συγκεκριμένο χρήστη", με άλλα λόγια το επίπεδο γενίκευσης των δεδομένων όπως αυτά ορίζονται από τον κάτοχο τους, καθώς και πόση να είναι η περίοδος διατήρησης τους. Η περίοδος διατήρησης συνήθως ορίζεται όσο ο χρόνος που χρειάζεται για την εκπλήρωση του στόχου, για τον οποίο συλλέχθηκε η συγκεγκριμένη πληροφορία.

Μία γενικευμένη άδεια εξουσιοδότησης δηλώνει ότι ένας χρήστης U έχει εξουσιοδοτηθεί για χρήση της πληροφορίας D, με βαθμό διακριτότητας της αποκάλυψης GL, για τον σκοπό P, εντός των χρονικών περιθωρίων [t1, t2]. Για παράδειγμα η πιο κάτω άδεια εξουσιοδότησης ([10/05/2011, 10/06/2011], Maria, income, read, admin, M) θα σήμαινε ότι "Ο χρήστης Μαρία εξουσιοδοτήθηκε το προνόμιο διαβάσματος του εισοδήματος του χρήστη σε μεσαίου (M) βαθμού διακριτότητας αποκάλυψης για σκοπούς διαχειριστή".

5.4.3 Μοντέλο βασισμένο στην εκτίμηση εμπιστοσύνης

Το "Trust-based" μοντέλο που προτείνεται βασίζεται στην ενσωματωμένη εμπιστοσύνη και κίνδυνο (risk) [32]. Στο παρόν άθρο, ο ορισμός που δίνεται για το πλαίσιο χρήσης περιορίζεται στην πληροφορία τοποθεσίας. Το μήνυμα που θέλουν να περάσουν οι Wagealla et al., είναι ότι η εκτίμηση της εμπιστοσύνης μπορεί να συμβάλει στην προστασία ιδιωτικότητας του χρήστη. Τα συμπεράσματα που ανάγονται για την αξιοπιστία των παραληπτών των πληροφοριών, αυτών δηλαδή που ζητούν να χρησιμοποιήσουν πληροφορίες, βοηθούν στην απόφαση της ποσότητας πληροφορίων που μπορούν να αποκαλυφθούν σε αυτούς. Ο γενικός ορισμός ενός έμπιστου χρήστη είναι ο χρήστης που τείνει να συμπεριφέρεται με ένα θετικό τρόπο.

Οι χρήστες είναι πρόθυμοι να επιτρέψουν την αποκάλυψη της πληροφορίας τοποθεσίας του, μόνο εάν αυτή η αποκάλυψη επιφέρει κάποιο όφελος. Όφελος μπορεί να προκύψει συνεπώς αν η πληροφορία αποκαλυφθεί σε αξιόπιστους μόνο χρήστες. Για εξαξωγή τέτοιων συμπερασμάτων χρειάζεται η ενσωμάτωση της ρητής έννοιας του κινδύνου. Η εμπιστοσύνη συνδέεται εγγενώς με τον κίνδυνο. Η ανάλυση και εκτίμηση του κινδύνου μιας εμπλεκόμενης κατάστασης μπορεί να εκτιμηθεί αφού γίνει αναγνώριση πιθανών αποτελεσμάτων της. Ο κάτοχος των δεδομένων εκτιμά τα πιθανά κόστη (costs) και ωφέλη (benefits) για κάθε αποτέλεσμα μιας αποκάλυψης πληροφοριών του που έχει αναγνωριστεί. Ο κυριότερος κίνδυνος που μπορεί να προκύψει είναι η διάδοση της πληροφορίας σε τρίτους χωρίς την περαιτέρω συγκατάθεση του κατόχου της πληροφορίας. Στο κείμενο γίνεται αναφορά σε ένα "cost-probability density function", το οποίο κατοπτρίζει τις πιθανότητες διάφορων κόστων. Με λίγα λόγια, υποδεικνύει το προφίλ και την συμπεριφορά που αναμένεται από συγκεκριμένους χρήστες, πώς ο χρήστης για παράδειγμα πιθανό να εκμεταλλευτεί την φανερωθείς πληροφορία. Η όλη διαδικασία του κινδύνου βασίζεται στην θεωρία των πιθανοτήτων, δεν υπάρχει βεβαιότητα και σιγουριά για τα αποτελέσματα μιας ενέργειας.

Η πρόσβαση σε πληροφορία πλαισίου χρήσης ρυθμίζεται ανάλογα με τους κανόνες πολιτικών προστασίας ιδιωτικότητας που δηλώνουν οι κάτοχοι των πληροφοριών (information owner), την οποία εκφράζουν αναλογιζόμενοι τον βαθμό αξιοπιστίας

των αιτούντων και το μέγιστο κόστος κινδύνου που μπορούν να δεχθούν. Ο βαθμός εμπιστοσύνης των χρηστών που ζητούν μια πληροφορία καθορίζει το ποσό της πληροφορίας που μπορεί να αποκαλυφθεί και η ανάλυση του κινδύνου μας επιτρέπει να εκτιμήσουμε το αναμενόμενο όφελος ή τίμημα από αυτή την αποκάλυψη. Οι αποφάσεις ελέγχου πρόσβασης δύναται να είναι θετικές, αρνητικές ή να ζητούν περαιτέρω λεπτομέρειες για το συγκεκριμένο αίτημα, όπως για παράδειγμα τον σκοπό πρόσβασης στα δεδομένα.

Στο προτεινόμενο μοντέλο η εμπιστοσύνη αναπαριστάται με τον ακόλουθο τρόπο. Ορίζεται ένα εύρος τιμών (trust values), μία κλίμακα ανάλογα με το βαθμό αξιοπιστίας των χρηστών, όπου για παράδειγμα σε ένα άγνωστο χρήστη προς το σύστημα θα σημειωνόταν η χαμηλότερη τιμή της κλίμακας και σε γνωστούς έμπιστους χρήστες το υψηλότερο. Η ανάλυση του κινδύνου όπως προαναφέρθηκε συνεπάγει μια αβεβαιότητα. Για την αναπαράσταση εμπιστοσύνης ενσωματώνεται ρητά και η έννοια της αβεβαιότητας. Ο τρόπος με τον οποίο χειρίζονται την έννοια της αβεβαιότητας είναι προσδιορίζοντας ένα διάστημα για το διατεταγμένο εύρος τιμών εμπιστοσύνης, εντός του οποίου η τιμή εμπιστοσύνης να θεωρείται έγκυρη και ακριβής.

Για εξωμάλυνση της αβεβαιότητας, προτείνεται η χρήση εμπειρικών (experiential) μηχανισμών μάθησης από παρατηρήσεις ενεργειών στο παρελθόν (past experiences), οι οποίοι οδηγούν σε καλύτερες αποφάσεις για τις μελλοντικές αλληλεπιδράσεις συγκεκριμένων χρηστών με πληροφορία πλαισίου χρήσης.

Το μοντέλο που περιγράφεται τέθηκε σε εφαρμογή σε χώρο ενός πανεπιστημίου το οποίο διαθέτει εξυπηρετητή πληροφορίας πλαισίου χρήσης (context information server). Ο εξυπηρετητής αυτός ανιχνεύει την τοποθεσία των χρηστών και παρέχει πληροφορίες σχετικά με αυτή όταν ζητηθεί.

5.5 Προσεγγίσεις ελέγχου πρόσβασης βάσει πολιτικών

5.5.1 Μηχανισμός ελέγχου πρόσβασης στην πληροφορία τοποθεσίας του χρήστη βάσει ευέλικτων πολιτικών

Οι Hengartner και Steenkiste στο άρθρο τους [17] τονίζουν ότι η τοποθεσία ενός χρήστη αποτελεί ευαίσθητη πληροφορία που αποκαλύπτοντας την σε άλλες οντότητες, θα μπορούσε να δημιουργήσει κινδύνους παραβίασης της ιδιωτικότητας. Ένα σύστημα που επιστρέφει πληροφορία σχετικά με την τοποθεσία ενός χρήστη πρέπει να χειριστεί τον έλεγχο πρόσβασης με ένα κατανεμημένο τρόπο, έχοντας υπόψη τις διάφορες πηγές, συσκευές και την αλληλεπίδραση μεταξύ αιτημάτων που πιθανό να αναφέρονται στην ίδια πληροφορία. Στο άρθο αυτό αρχικά παρουσιάζονται κάποια ζητήματα που πιθανό να προκύψουν προσδιορίζοντας πολιτικές για την τοποθεσία (location policies).

Οι πολιτικές τοποθεσίες δημιουργούνται ούτως ώστε να παρεμποδιστεί η φανέρωση της τοποθεσίας ενός χρήστη σε μη εξουσιοδοτημένες οντότητες. Αίτημα πρόσβασης σε πληροφορίες από κάποιο χρήστη ή υπηρεσία σε σύστημα εντοπισμού τοποθεσίας, μπορεί να αναφέρεται είτε για την τοποθεσία ενός χρήστη είτε για τα άτομα που βρίσκονται σε μια συγκεκριμένη τοποθεσία, όπως για παράδειγμα σε ένα δωμάτιο ενός κτιρίου. Άδεια πρόσβασης σε πληροφορία που αφορά ένα άτομο ή άτομα που βρίσκονται σε κάποιο χώρο παραχωρείται μόνο εάν επιτρέπεται από την πολιτική του ατόμου και του δωματίου, αντίστοιχα.

Οι πολιτικές χρηστών (user policies) και δωματίων (room policies) πρέπει να ορίζονται έτσι ώστε η ροή των δεδομένων να περιορίζεται όσο είναι δυνατόν. Η εισαγωγή της ιδιότητας της διακριτότητας (granularity) μπορεί να συμβάλλει στον περιορισμό αυτό. Για παράδειγμα μια πολιτική ενός χρήστη προσδιορίζει ότι για την τοποθεσία του θα αποκαλυπτεί το κτίριο, έναντι του πραγματικού δωματίου στο οποίο βρίσκεται. Μια πολιτική ενός δωματίου θα μπορούσε να ήταν ότι θα φανερωθεί ο αριθμός των ατόμων που βρίσκονται εντός του δωματίου και όχι οι ταυτότητες των ατόμων. Επιπρόσθετα, οι δύο ειδών πολιτικές μπορούν να ελέγχουν τα αιτήματα πρόσβασης που αναφέρονται σε συγκεκριμένες τοποθεσίες και χρήστες, που έχουν ορίσει σε κάποιες λίστες, και να απαντούν μόνο σε αυτά. Δεν διαχειρίζονται αιτήματα

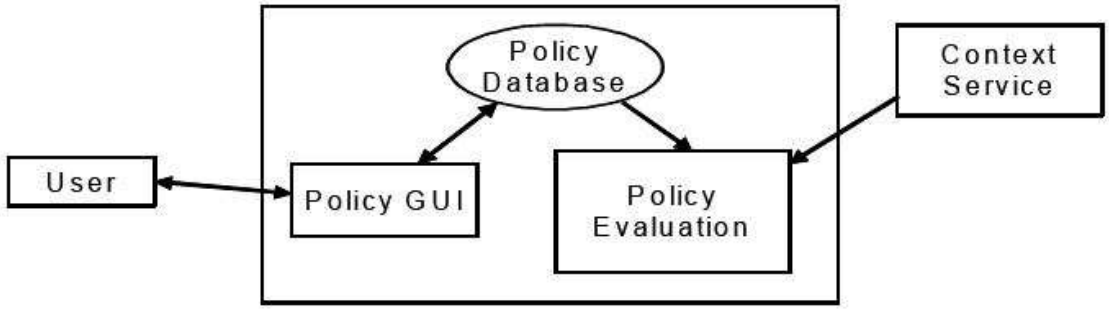
σχετικά με άγνωστη προς το σύστημα τοποθεσία ή άγνωστους προς το σύστημα χρήστες.

Σε ένα πολύπλοκο σύστημα εντοπισμού τοποθεσίας, πιθανή είναι η εμφάνιση συγκρούσεων (conflicts) ανάμεσα σε πολιτικές χρηστών και πολιτικές δωματίων. Για παράδειγμα μια τέτοια σύγκρουση θα μπορούσε να ήταν: ο χρήστης Α δεν επιτρέπει στον χρήστη Β να μάθει για την τοποθεσία του, αλλά ο χρήστης Γ επιτρέπει στον χρήστη Β να μάθει για τα άτομα που βρίσκονται στο γραφείο του. Αν ο χρήστης Α βρίσκεται στο γραφείο του χρήστη Γ, τότε ο χρήστης Β θα έπρεπε ή όχι να μάθει για αυτό; Είναι θέμα και τακτική συστήματος το πως θα αποφασίσει να χειριστεί το ζήτημα αυτό, για παράδειγμα μία πολιτική του συστήματος θα μπορούσε να ήταν ότι για κάθε αίτημα να αναζητά τα δύο είδη πολιτικών που έρχονται σε σύγκρουση, χρήστη και δωματίου, και να επιστρέφει οτιδήποτε μόνο εάν είναι αποδεκτό και από τις 2 πολιτικές.

Ένα σύστημα ανίχνευσης τοποθεσίας μπορεί να αποτελείται από πολλές υπηρεσίες. Το σύστημα θα πρέπει να διαβεβαιώνεται ότι πληροφορίες σχετικά με τοποθεσία των χρηστών δίνονται μόνο σε αξιόπιστες υπηρεσίες που υλοποιούν ελέγχους διαχείρισης πρόσβασης με επίγνωση της ιδιωτικότητας. Στο άρθρο περιγράφεται επίδειξη πρακτικότητας του μηχανισμού, μίας υλοποίησης που βασίζεται σε ψηφιακά πιστοποιητικά (digital certificates).

5.5.2 Μηχανή Ιδιωτικότητας (Context Privacy Engine)

Ο μηχανισμός (middleware component) που προτείνεται στο [5], αναφερόμενος ως "Context Privacy Engine" (CPE), αποτελεί μία μηχανή ιδιωτικότητας που ρυθμίζει και ελέγχει την πρόσβαση σε πληροφορία πλαισίου που χαρακτηρίζουν ένα άτομο. Η CPE δεν επιβάλλει κατευθείαν προστασία της ιδιωτικότητας αλλά χρησιμοποιείται από μία υπηρεσία πλαισίου χρήσης για να συμβάλλει στην ελεγχόμενη αποκάλυψη ευαίσθητων πληροφοριών. Μία σημαντική πτυχή του σχεδιασμού της μηχανής ήταν η ανάγκη εμφάνισης και διαχείρισης πολιτικών που εξαρτώνται από την πληροφορία πλαισίου χρήσης (context-dependent privacy policies). Το μοντέλο πολιτικών αυτό κληρονομεί κλασικούς μηχανισμούς ελέγχου πρόσβασης (ACL mechanisms) με ελεγχόμενη χρήση των δεδομένων.



Σχήμα 5.8 Συστατικά αρχιτεκτονικής της CPE

Η μηχανή προστασίας ιδιωτικότητας πληροφοριών πλασίου χρήσης δέχεται αιτήματα της μορφής: < αιτητής, υποκείμενο, εφαρμογή, πληροφορία >, με άλλα λόγια το ζητούμενο είναι αν η εφαρμογή Ε που εκτελείται από το χρήστη Χ μπορεί να αποκτήσει πρόσβαση στην πληροφορία Π που χαρακτηρίζει κάποιο υποκείμενο και κάνοντας έλεγχο στο σύνολο των υπάρχουσων πολιτικών για να αποφασίσει αν το αίτημα πρόσβασης θα πρέπει να γίνει αποδεκτό ή να απορριφθεί.

5.5.3 Υποδομή βασισμένη σε πολιτικές για περιορισμό ροής δεδομένων

Στο [18] περιγράφεται μία υποδομή που βασίζεται σε πολιτικές (policy-based), για τον έλεγχο της ροής δεδομένων εντός μίας εφαρμογής με επίγνωση του πλαισίου χρήσης. Η προσέγγιση αυτή μπορεί να ενταχθεί επίσης στην κατηγορία προσεγγίσεων που κάνουν χρήση οντολογιών. Επιτρέπει στους χρήστες να προσδιορίσουν τις δικές τους προτιμήσεις ιδιωτικότητας, οι οποίες λαμβάνουν υπόψη στατικές και δυναμικές πληροφορίες του χρήστη, μαζί και κανόνες γενίκευσης που ρυθμίζουν την ακρίβεια του αποτελέσματος. Δύο σημαντικοί πόροι που τονίζεται ότι πρέπει να προστατεύονται είναι η τοποθεσία και η ενέργεια του χρήστη. Η προτεινόμενη υποδομή αποτελεί θεμέλιο που μπορεί να επεκταθεί και να ενσωματωθεί σε υφιστάμενα κοινωνικά δίκτυα συμπεριλαμβανομένων κινητών κοινωνικών δικτύων βάσει τοποθεσίας.

Η οντολογία πλαισίου χρήσης (context ontology) της προτεινόμενης υποδομής είναι μία OWL (Web Ontology Language) [47] οντολογία που αναπαριστά γνώση για την τοποθεσία του χρήστη και αυτά που τον περιβάλλουν, για την παρουσία άλλων

ατόμων και συσκευών και για τις δραστηριότητες που ασχολούνται. Κίνητρο της ανάπτυξης της οντολογίας είναι η αναπαράσταση των δυναμικών πτυχών μίας κινητής εφαρμογής με επίγνωση του πλαισίου χρήσης. Η οντολογία υποστηρίζει γενίκευση πληροφοριών πλαισίου χρήσης, δημιουργώντας ιεραρχικά μοντέλα για διαφορετικά στιγμιότυπα μίας πληροφορίας, όπως για παράδειγμα η τοποθεσία και η δραστηριότητα. Επιτρέπει στους χρήστες να διαδόσουν πληροφορίες τους σε διαφορετικά επίπεδα ακρίβειας για διαφορετικούς τύπους δεδομένων.

Ο χρήστης μπορεί να δημιουργήσει το δικό του προφίλ, βάζοντας μέσα πληροφορίες όπως το όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου, χόμπυ και ενδιαφέροντα, όπως επίσης μπορεί να διαχειριστεί διαφορετικές ομάδες με τα άτομα που συσχετίζεται. Πέραν από τις στατικές πληροφορίες που χαρακτηρίζουν ένα χρήστη, το σύστημα έχει επίγνωση των δυναμικών πληροφοριών του πλαισίου χρήσης του χρήστη, όπως η τρέχουσα τοποθεσία ή δραστηριότητα του, τα οποία μπορούν να συλλεχθούν από διάφορους αισθητήρες (sensors) που εξοπλίζουν μία κινητή εφαρμογή (κινητό τηλέφωνο).

Ο χρήστης μπορεί να προσδιορίσει τις προτιμήσεις ιδιωτικότητας, οι οποίες είναι κανόνες ελέγχου πρόσβασης που περιγράφουν πώς ο χρήστης επιθυμεί να μοιραστεί τις πληροφορίες του, δηλαδή με ποιον και κάτω από ποιες συνθήκες και προυποθέσεις. Μπορεί επίσης να προσδιορίσει πολιτικές ιδιωτικότητας για να προστατεύσει τα δεδομένα που ανιχνεύονται από αισθητήρες. Όλες οι πολιτικές ιδιωτικότητας δημιουργούνται και αποθηκεύονται σε μορφή κανόνων N3[50] τόσο στην πλευρά του διακομιστή (server) όσο και του χρήστη, και ανακτώνται όταν ο μηχανισμός συμπερασμού το απαιτεί.

Ο μηχανισμός συμπερασμού (reasoning engine) είναι υπεύθυνος για τον χειρισμό αιτημάτων, την διαδικασία συμπερασμού δηλαδή την εξαγωγή νέας γνώσης από υπάρχουσα γνώση και κανόνες και την εξαγωγή αποφάσεων ελέγχου πρόσβασης βάσει των πολιτικών του χρήστη, χρησιμοποιώντας Jena Semantic Web εργαλεία λογισμικού [48].

5.6 Προσεγγίσεις που χρησιμοποιούν οντολογίες

5.6.1 Η έννοια των οντολογιών

Σημαντικό ρόλο στην προσπάθεια αυτή της προστασίας της ιδιωτικότητας κατέχει και η σημασιολογική μοντελοποίηση των πολιτικών ιδιωτικότητας. Η σημασιολογία της ίδιας της υπηρεσίας, η υποκείμενη συλλογή και οι σκοποί επεξεργασίας, όπως και οι εμπλεκόμενες οντότητες είναι όλα εξίσου σημαντικά. Η μοντελοποίηση αυτή είναι εφικτή με την βοήθεια οντολογιών, οι οποίες μπορούν να συλλάβουν την σημασιολογική έννοια του πλαισίου χρήσης. Για τους ανθρώπους καθιστούν ικανή την καλύτερη πρόσβαση στην πληροφορία και στοχεύουν στην κοινή κατανόηση . Για τους υπολογιστές διευκολύνουν την κατανόηση της πληροφορίας και την πιο εκτεταμένη επεξεργασία.

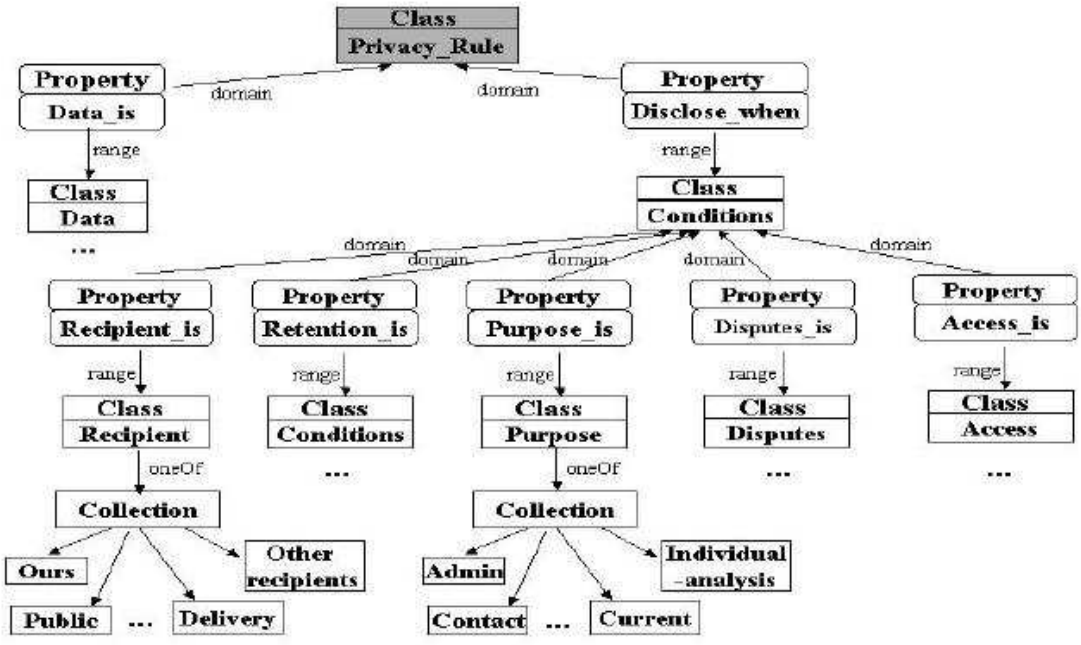
Οι οντολογίες εξαιτίας του φορμαλισμού τους, διευκολύνουν το διαμοιρασμό και την επαναχρησιμοποίηση της γνώσης για να επιτρέψουν την επικοινωνία μεταξύ ετερογενών συστημάτων και κατανεμημένων εφαρμογών. Η οντολογία ουσιαστικά αποτελεί το φορμαλιστικό ορισμό των κανόνων πρόσβασης και εκτέλεσης ενεργειών, όπως επίσης το φορμαλιστικό προσδιορισμό των απαιτήσεων, προτιμήσεων των χρηστών όσον αφορά την διαφύλαξη της ιδιωτικότητας. Η γνώση στις οντολογίες τυποποιείται χρησιμοποιώντας 5 κατηγορίες συστατικών: κλάσεις, σχέσεις, συναρτήσεις, αξιώματα και στιγμιότυπα.

Τα μοντέλα αναπαράστασης γνώσης που βασίζονται σε οντολογίες:

- Αποτελούν τις πιο πρόσφατες προσπάθειες μοντελοποίησης του πλαισίου χρήσης
- Στο πεδίο των πληροφοριών πλαισίου χρήσης, αποτελούν ένα πολύ υποσχόμενο εργαλείο για την αναπαράσταση πληροφοριών που περιγράφουν και χρησιμοποιούνται στην καθημερινή ζωή, με τη μορφή δομών δεδομένων.
- Επιτρέπουν τον ορισμό εννοιών, υπο-εννοιών και συσχετισμών, οι οποίοι αποτελούν κοινά αποδεκτή ονοματολογία από τις εμπλεκόμενες οντότητες, διευκολύνοντας έτσι την από κοινού χρήση και επαναχρησιμοποίηση της πληροφορίας πλαισίου χρήσης.
- Επιτρέπουν την εξαγωγή συμπερασμάτων (inference).

5.6.2 Οντολογία Ιδιωτικότητας

Το κείμενο στο [38] παρουσιάζει και προτείνει την ανάπτυξη μίας οντολογίας ιδιωτικότητας για την μοντελοποίηση δυναμικών προτιμήσεων ιδιωτικότητας και κανόνων σε περιβάλλοντα υπολογισμού με επίγνωση του πλαισίου χρήσης. Η οντολογία ιδιωτικότητας για να εκφράσει λεξιλόγιο και κανόνες σχετικά με την διαφύλαξη της ιδιωτικότητας, αναπτύχθηκε βασισμένη στην ορολογία και τις πολιτικές που προσδιορίστηκαν στην πλατφόρμα P3P [41]. Οι κλάσεις και οι ιδιότητες που δημιουργήθηκαν ήταν ανάλογες με αυτές που χειρίζεται η πλατφόρμα P3P. Οι προτιμήσεις ιδιωτικότητας που ορίζουν οι χρήστες αναπαριστώνται στην κλάση Privacy_Rule. Η κλάση Privacy_Rule έχει δύο ιδιότητες: Data_is και Disclose when. Κάθε κανόνας ιδιωτικότητας εκφράζεται με δύο στοιχεία: την κλάση Δεδομένων (Data Class) και την κλάση Συνθηκών (Condition class), η οποία περιέχει όλες τις συνθήκες κάτω από τις οποίες ένας χρήστης είναι πρόθυμος να αποκαλύψει τα δεδομένα. Σύμφωνα με τις προδιαγραφές της P3P, οι συνθήκες μπορούν να αποτελούνται από ιδιότητες όπως τους παραλήπτες, των σκοπών συλλογής δεδομένων, χρόνος διατήρησης δεδομένων από τους παραλήπτες κτλ.



Σχήμα 5.9 Προσδιορισμός κανόνα ιδιωτικότητας μέσω οντολογίας

Εκμεταλλευόμενοι τις δυνατότητες των οντολογιών να συμπεραίνουν βάσει λογικής, η προσέγγιση αυτή έχει σκοπό την διευκόλυνση αυτοματοποιημένων διαδικασιών για τον έλεγχο προστασίας ιδιωτικότητας. Μία τέτοια οντολογία θα μπορούσε να ενσωματωθεί και να χρησιμοποιηθεί από μηχανισμούς ιδιωτικότητας που βασίζονται σε κανόνες (rule-based).

5.6.3 Οντολογία πολιτικών SOUPA (CoBra)

Στο άρθρο αυτό[8] οι H.Chen et al., περιγράφουν τον σχεδιασμό μιας υποδομής προστασίας ιδιωτικότητας που εκμεταλλεύεται τις δυνατότητες που προσφέρει η οντολογία πολιτικών SOUPA (Standard Ontology for Ubiquitous and Pervasive Applications). Η υλοποίηση της υποδομής και του σχετικού αλγορίθμου συμπερασμού πολιτικών πραγματοποιείται μέσα στην αρχιτεκτονική Context Broker architecture (CoBra). Η CoBra [40] είναι μια broker-centric agent αρχιτεκτονική που υποστηρίζει διάχυτα συστήματα με επίγνωση του πλαισίου χρήσης. Η αρχιτεκτονική CoBra χρησιμοποιεί την Web Ontology Language (OWL) [47] για να ορίσει οντολογίες που υποστηρίζουν διαμοιρασμό δεδομένων, συγχώνευση δεδομένων και διαδικασίες συμπερασμού πληροφοριών πλαισίου χρήσης.

Η οντολογία πολιτικών που περιγράφεται στο κείμενο είναι μέρος της οντολογίας SOUPA. Οι πολιτικές ορίζονται χρησιμοποιώντας την οντολογία πολιτικών SOUPA. Για να υπολογιστούν οι άδειες που επιτρέπονται από μια πολιτική ενός χρήστη, ο broker πλαισίου του συστήματος υλοποιείται με τη βοήθεια ενός αλγορίθμου συμπερασμού πολιτικών. Αυτός ο αλγόριθμος εκμεταλλεύεται τα αξιώματα και κατασκευάσματα (class constructs) της γλώσσας OWL-DL για να αποφασίσει αν μια ενέργεια πρόσβασης σε προσωπικά δεδομένα κάποιου χρήστη είναι επιτρεπτή ή όχι. Η OWL-DL είναι το πιο χρήσιμο και διαδεδομένο είδος της γλώσσας περιγραφής οντολογιών OWL. Το είδος αυτό, όπως υποδηλώνει και το όνομά του, έχει την εκφραστικότητα που παρέχεται από τις τυπικές Περιγραφικές Λογικές (Description Logics). Η OWL-DL υποστηρίζει πλήρη συμπερασμό που περιλαμβάνει έλεγχο ικανοποίησης (satisfiability check), έλεγχο συνέπειας (consistency check) και ταξινόμηση (classification). Τα παραπάνω είδη συμπερασμού ελέγχουν αν μια έννοια μπορεί να έχει στιγμιότυπα, αν παραβαίνει τα αξιώματα και τους περιορισμούς του μοντέλου και ανακαλύπτουν υπονοούμενες σχέσεις ιεραρχίας.

Σε ένα περιβάλλον διάχυτου υπολογισμού οι πολιτικές ορίζονται από τους χρήστες για να επιτρέψουν ή να απαγορεύσουν σε άλλες οντότητες να εκτελέσουν διάφορες ενέργειες. Μια ενέργεια αποτελείται από ιδιότητες όπως για παράδειγμα ποιος είναι ο actor χρήστης και ποιος ο παραλήπτης. Ο αλγόριθμος για λογικό συμπερασμό των πολιτικών με την οντολογία SOUPA περιγράφει μια διαδικασία που μπορεί να υλοποιηθεί από μια κεντρική αρχή (authority), με σκοπό να δώσει απαντήσεις σε αιτήματα για τα δικαιώματα εκτέλεσης μιας ενέργειας. Ο αλγόριθμος παίρνει ως είσοδο μια βάση δεδομένων που περιέχει γνώση για τον χρήστη, μια description logic inference μηχανή που υποστηρίζει την OWL-DL διαδικασία συμπερασμού και την ενέργεια που προτίθεται να εκτελέσει. Επιστρέφει μια τιμή που αναπαριστά την υπολογισμένη άδεια εκτέλεσης μιας ενέργειας, που είναι είτε FORBID είτε PERMIT.

5.7 Υβριδικές-Διαφορετικές Προσεγγίσεις

5.7.1 Υποδομή βασισμένη σε RBAC και P3P

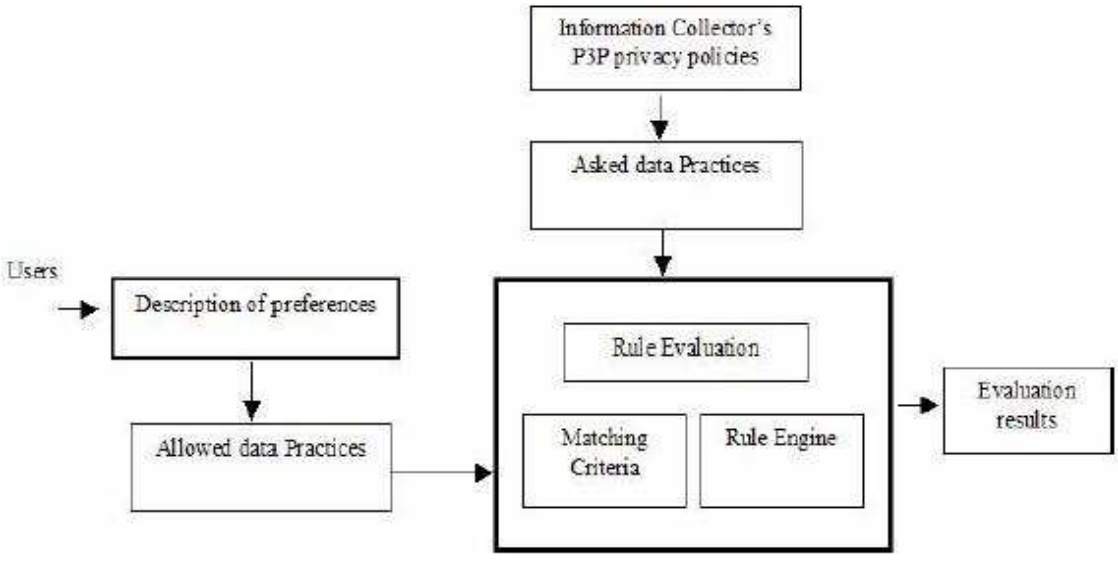
Οι P.Osbakk και N.Ryan προτείνουν την δική τους αρχιτεκτονική [26] η οποία βασίζεται στο γνωστό κλασικό μοντέλο ελέγχου πρόσβασης βάσει ρόλων RBAC αλλά και στις πολιτικές της πλατφόρμας P3P [41]. Τονίζουν ότι ένας καλός μηχανισμός προστασίας ιδιωτικότητας πρέπει να είναι σε θέση να διαχειριστεί τόσο γνωστούς, όσο και άγνωστους παράγοντες μέχρι εκείνη την στιγμή (context consumer ή context producer). Η υποδομή της αρχιτεκτονικής που προτείνεται έχει ως εξής. Κάθε οντότητα συνδέεται με τουλάχιστον ένα διαχειριστή (context manager), ο οποίος είναι υπεύθυνος για την αποθήκευση, την επεξεργασία και την προστασία των πληροφοριών πλαισίου χρήσης που χαρακτηρίζουν την οντότητα αφού όλες οι πληροφορίες ρέουν μεταξύ των διάφορων διαχειριστών πλαισίου χρήσης. Ο κάθε διαχειριστής (context manager) είναι υπεύθυνος για την αξιολόγηση ενός αιτήματος ώστε να αποφευχθούν μη εξουσιοδοτημένες ενέργειες. Το πρώτο στάδιο της αξιολόγησης αυτής αποτελεί η πιστοποίηση του ατόμου μέσω κάποιου συνδυασμού ονόματος και κωδικού για ήδη γνωστούς χρήστες είτε μέσω κάποιου μηχανισμού δημοσίου κλειδιού (public key mechanism). Η εξουσιοδότηση ενός πιστοποιημένου χρήστη επιτυγχάνεται μέσω ενός μηχανισμού ελέγχου πρόσβασης, που συνδυάζει το μοντέλο RBAC για μείωση του διαχειριστικού φόρτου και τις πολιτικές της πλατφόρμας P3P. Ο μηχανισμός αυτός αποτελεί τον πυρήνα του κάθε διαχειριστή

(CM). Το μοντέλο ελέγχου πρόσβασης βάσει ρόλων που χρησιμοποείται για να διαχειριστεί τους γνωστούς χρήστες προς το σύστημα, διαφέρει από το παραδοσιακό μοντέλο στο ότι εδώ οι ρόλοι ενεργοποιούνται αυτόματα έτσι ώστε να δίνεται στον χρήστη η καλύτερη δυνατή πρόσβαση σε οποιοδήποτε session. Οι άδειες που περιέχονται στους ρόλους είναι λίστες ελέγχων πρόσβασης που συνδέονται με πληροφορίες πλαισίου χρήσης.

Για να επιτραπεί η πρόσβαση σε άγνωστους χρήστες, μπορούν να χρησιμοποιηθούν πολιτικές P3P. Μία πολιτική P3P αποτελεί μία σύμβαση που αναφέρει πώς οι πληροφορίες μπορούν να χρησιμοποιηθούν. Μία πολιτική P3P που συνοδεύει ένα αίτημα, αξιολογείται και συγκρίνεται με το σύνολο κανόνων που έχουν οριστεί από την οντότητα. Ένα σύνολο κανόνων αντικατοπτρίζει τις απαιτήσεις και προυποθέσεις εκτέλεσης μιας ενέργειας και μπορεί να συνδεθεί με οποιοδήποτε αριθμό ρόλων στο RBAC μοντέλο. Κάθε σύνολο κανόνων που ταιριάζει με μία πολιτική, προσθέτει προσωρινά τους ρόλους που σχετίζονται με αυτό σε αυτούς που έχουν ήδη ανατεθεί στον πράκτορα αιτητή.

5.7.2 Αρχιτεκτονική Προτιμήσεων Ιδιωτικότητας

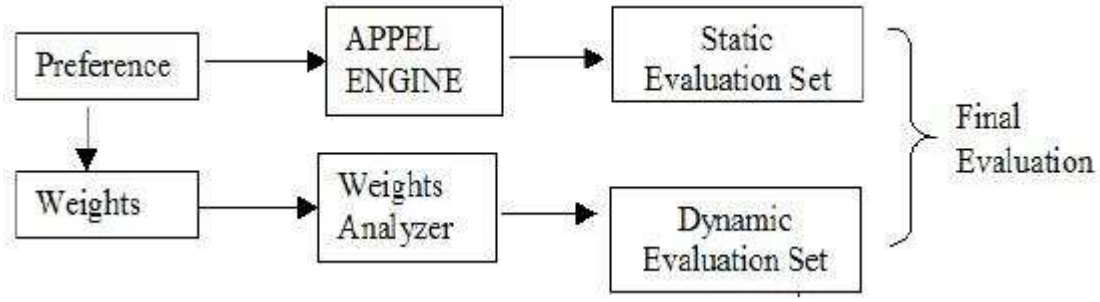
Η αρχιτεκτονική αυτή [12] για την περιγραφή προτιμήσεων ιδιωτικότητας του χρήστη βασίστηκε στην λειτουργία comp_pref που προτάθηκε στην αρχιτεκτονική [11], η οποία υποστηρίζει τους χρήστες να αποφασίζουν με την συγκατάθεση τους.



Σχήμα 5.10 Αρχιτεκτονική comp_pref

Η αρχιτεκτονική αυτή λαμβάνει υπόψη την δυναμική αλλαγή των πληροφοριών σε ένα περιβάλλον με επίγνωση του πλαισίου χρήσης και την λήψη αποφάσεων μέσω συγκατάθεσης του χρήστη για τον σχεδιασμό των προτιμήσεων ιδιωτικότητας και κανόνων ελέγχου πρόσβασης. Χρησιμοποιεί ένα μηχανισμό στάθμισης (weighting mechanism) για τον υπολογισμό μιας τιμής που υποδεικνύει τον βαθμό απειλής της ιδιωτικότητας. Η τιμή απειλής της ιδιωτικότητας προκύπτει από το "ζύγισμα" όλων των βαρών των δεδομένων που συνθέτουν ένα αίτημα, για παράδειγμα πληροφορίες όπως ο σκοπός, ο παραλήπτης. Για την εύρεση των βαρών είναι υπεύθυνος ο αναλυτής βαρών (weights analyzer), ο οποίος θα αναζητήσει τον συνδυασμό αυτό στην πολιτική ιδιωτικότητας του παροχέα υπηρεσιών.

Μία πρακτική δεδομένων (data practice), δηλαδή μία προτίμηση χρήστη αποτελείται από ένα συνδυασμό παραλήπτη, σκοπού πρόσβασης, περιόδου διατήρησης των δεδομένων και μίας τιμής (βαθμός απειλής ιδιωτικότητας). Υπάρχουν δύο τύποι πρακτικών δεδομένων, asked, τα οποία προέρχονται από τις P3P πολιτικές ιδιωτικότητας των συλλεκτών πληροφοριών και allowed, τα οποία προέρχονται από τις προτιμήσεις ιδιωτικότητας των χρηστών που λαμβάνονται μέσω φορμών. Οι προτιμήσεις των χρηστών προσδιορίζονται με την βοήθεια κανόνων της γλώσσας APPEL[42]. Η μηχανή κανόνων (rule engine) συγκρίνει και αξιολογεί και τα δύο είδη πρακτικών.



Σχήμα 5.11 Αξιολόγηση προτιμήσεων-Μηχανή κανόνων

Για σκοπούς προσομοίωσης της δυναμικής αυτής πλατφόρμας πολιτικών ιδιωτικότητας, αναπτύχθηκε ένα εργαλείο προσομοίωσης χρησιμοποιώντας περιβάλλον visualbasic.net, στο οποίο φαίνεται πώς οι δυναμικές προτιμήσεις μπορούν να περιγραφούν και να εκτιμηθούν.

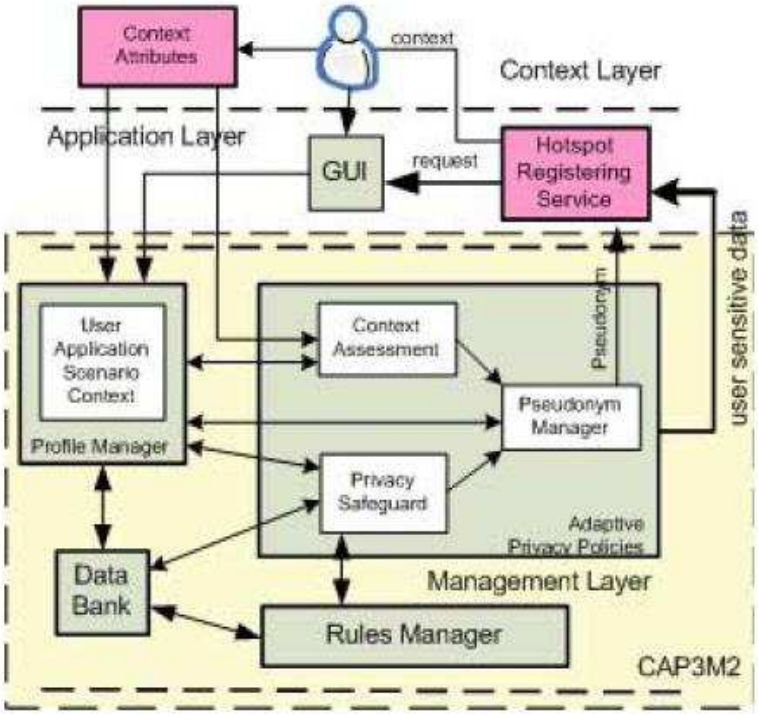
5.7.3 Διαχείριση προφίλ χρήστη για προστασία ιδιωτικότητας

Το προτεινόμενο μοντέλο[23] προστασίας ιδιωτικότητας σε σύστημα με επίγνωση του πλαισίου χρήσης αποτελείται από ένα διαχειριστή των διάφορων προφίλ (Profile manager), ο οποίος διατηρεί περιγραφές του προφίλ χρήστη (προτιμήσεις, χαρακτηριστικά, ρόλοι, προτιμήσεις ιδιωτικότητας), της πληροφορίας πλαισίου χρήσης, του σεναρίου και της υπηρεσίας και μία οντότητα διαφύλαξης της ιδιωτικότητας (Privacy Safeguard).

Κάθε χρήστης μπορεί να διατηρεί περισσότερα από ένα προφίλ, για κάθε διαφορετικό ρόλο του, για παράδειγμα εργαζόμενος, γονέας, ασθενής κτλ. Σε κάθε προφίλ, ο χρήστης ορίζει τις προτιμήσεις του όσον αφορά την αποκάλυψη προσωπικών πληροφοριών, οι οποίες συνθέτουν τις πολιτικές πρόσβασης στα δεδομένα. Ο χρήστης αναθέτει "privacy flags" (PF) στις ευαίσθητες πληροφορίες του, οι οποίες ενδείξεις ιδιωτικότητας αυτές φανερώνουν το πώς ο χρήστης θέλει να χειριστούν ή να αποκαλυφθούν από τον μηχανισμό προστασίας ιδιωτικότητας του συστήματος. Οι πιθανές ενδείξεις (PF) είναι: A= "always give", C= "check with the profile manager", R= "ask the user", N= "never give".

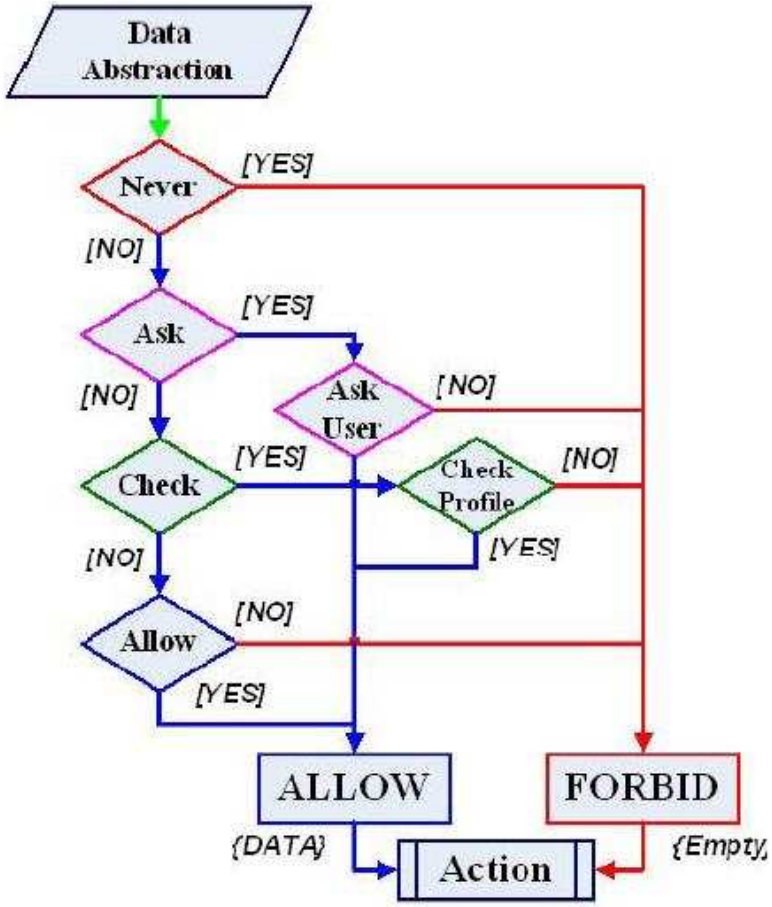
Ο χρήστης έχει επίσης την δυνατότητα να αναθέσει "privacy flags" για σκοπούς αφαιρετικότητας των δεδομένων, δηλώνοντας το επιθυμητό πρότυπο. Ο χρήστης μπορεί επίσης να ορίσει δικό του ψευδώνυμο, μπορεί να αλλάξει και να ανανεώσει όλες τις πληροφορίες που βρίσκονται στα προφίλ του καθώς και να δημιουργήσει νέους ρόλους.

Ο διαχειριστής κανόνων (Rule Manager) επεξεργάζεται τους κανόνες για φιλτράρισμα των ευαίσθητων δεδομένων του χρήστη και είναι υπεύθυνος για τις αποφάσεις πρόσβασης που βασίζονται στην αξιολόγηση πληροφοριών όπως ο ρόλος αιτητή, η τοποθεσία αιτητή, ο ρόλος και η τοποθεσία του κατόχου των ζητούμενων και το τρέχον σενάριο.



Σχήμα 5.12 Συστατικά προτεινόμενου μοντέλου

Ο αλγόριθμος Privacy Safeguard παίρνει ως είσοδο τις πληροφορίες πλαισίου χρήσης και τις ενδείξεις ιδιωτικότητας (privacy flags) του χρήστη για το επίπεδο διακριτότητας της αποκάλυψης και αποφασίζει πως θα προστατευτεί η ιδιωτικότητα του χρήστη. Πριν επιτραπεί οποιαδήποτε φανέρωση ευαίσθητων δεδομένων, ακολουθούνται κάποιοι κανόνες για φιλτράρισμα τους.



Σχήμα 5.13 Διάγραμμα καταστάσεων αλγόριθμου privacy safeguard

Κεφάλαιο 6

Συγκριτική μελέτη προσεγγίσεων

Στο κεφάλαιο αυτό, έχοντας υπόψη τις περιγραφές των προτεινόμενων λύσεων, μπορούμε να παρατηρήσουμε ποια χαρακτηριστικά περιβάλλοντος κινητού υπολογισμού τηρούν έχοντας επίγνωση το πλαίσιο χρήσης και υπόψη την ιδιωτικότητα. Οι παρατηρήσεις φαίνονται συνοπτικά και στους πίνακες που ακολουθούν στην υποενότητα 6.2 (Πίνακας 6.1 και Πίνακας 6.2).

6.1 Ανάλυση του πίνακα σύγκρισης

Στο άρθρο αυτό [9], πλαίσιο χρήσης ενός ατόμου ορίζεται η τοποθεσία του, οι συσκευές που είναι γύρω του και χρησιμοποιά, το δίκτυο στο οποίο είναι συνδεδεμένες οι συσκευές όπως και διάφορες ενέργειες του χρήστη. Η προσέγγιση που αποτελεί την επέκταση του RBAC μοντέλου "NIST" [14] πληρεί τα ακόλουθα χαρακτηριστικά. Ο σκοπός χρήσης δεδομένων προσδιορίζεται βάσει του ρόλου του χρήστη και γίνεται πιο εξειδικευμένος ανάλογα για ποιο αντικείμενο δεδομένων αναφέρεται. Τα δεδομένα κατακρατούνται όσο διαρκεί η εξουσιοδοτημένη ενέργεια πρόσβασης σε αυτά. Οι περιορισμοί και προσδιορισμοί αδειών πρόσβασης στους χρήστες δύναται να είναι εξατομικευμένοι και όχι βάση ρόλων. Κάθε διαφορετικό αντικείμενο με δεδομένα μπορεί να διαθέτει τον δικό του περιορισμό πρόσβασης που να περιορίζει τους χρήστες και τις ενέργειες που είναι επιτρεπτές. Για την μοντελοποίηση πληροφορίας χρησιμοποιείται η ορολογία του κλασικού προτύπου μοντέλου ελέγχου πρόσβασης RBAC. Για τον προσδιορισμό πολιτικών ιδιωτικότητας χρησιμοποιείται η γλώσσα XML. Ο προτεινόμενος μηχανισμός έχει δοκιμαστεί σε

ιατρικό σύστημα, όπου ρόλοι και άδειες προσβάσεων δίνονται σε νοσοκόμες και ιατρούς.

Το προτεινόμενο RBAC Μοντέλο βάσει ρόλου πληροφορίας πλαισίου χρήσης [27], όπως και σε κάθε μοντέλο ελέγχου πρόσβασης βάσει ρόλων, τα δικαιώματα πρόσβασης ανατίθενται στους ρόλους και όχι στους χρήστες. Στο μοντέλο αυτό, εκτός από τους ρόλους των χρηστών, λαμβάνονται υπόψη και οι ρόλοι των πληροφοριών για να αποφασιστούν τα δικαιώματα πρόσβασης. Για την μοντελοποίηση πληροφορίας χρησιμοποιείται η ορολογία και ο φορμαλισμός του κλασικού προτύπου μοντέλου ελέγχου πρόσβασης RBAC. Συγκεκριμένα αν η τιμή της μεταβλητής PermissionBit ισούται με "ALLOW", τότε το αίτημα πρόσβασης γίνεται αποδεκτό. Το μοντέλο τέθηκε σε εφαρμογή για αξιολόγηση σε ένα έξυπνο (smart) σπίτι εξοπλισμένο με διάφορους δικτυωμένους αισθητήρες και actuator devices, όπως για παράδειγμα κάμερες, μικρόφωνα κτλ. Ως πλαίσιο χρήσης ορίζουν την οποιαδήποτε πληροφορία που μπορεί να χρησιμοποιηθεί για να χαρακτηρίσει μία οντότητα (άτομα, τοποθεσίες, αντικείμενα).

Στη προσέγγιση με την προτεινόμενη ιεραρχία RBAC μοντέλων [24,25] απαιτείται η συγκατάθεση του κατόχου δεδομένων των οποίων ζητείται πρόσβαση σε αυτά, όπως και προσδιορισμός σκοπού χρήσης δεδομένων. Έπειτα, ο χρήστης θα ενημερωθεί για τον σκοπό αυτό και τα δεδομένα που θα δοθούν για κάποιο σκοπό διατηρούνται στο προσκήνιο όσο και ο χρόνος εκτέλεσης της συγκεκριμένης ενέργειας. Λαμβάνονται υπόψη ενέργειες όπως είναι οι υποχρεώσεις (obligations), δηλαδή ενέργειες που πρέπει να ακολουθήσουν την εκτέλεση κάποιας άλλης ενέργειας πάνω στα δεδομένα.
Οι προσδιορισμοί προσβάσεων των χρηστών σε πληροφορίες γίνονται βάσει ρόλων, που έχουν οριστεί εξ αρχής από το σύστημα. Κάθε χρήστης ανήκει σε μία κατηγορία ρόλου, η οποία κατηγορία χαρακτηρίζεται από τις δικές της άδειες και εξουσιοδοτήσεις πρόσβασης και σε ποια δεδομένα. Προτείνεται επίσης ένας μηχανισμός ανίχνευσης πιθανών συγκρούσεων μεταξύ διαφορετικών αδειών πρόσβασης, ο οποίος για να πραγματοποιήσει τον έλεγχο αυτό, κάνει χρήση δύο αλγορίθμων: PA-Conflict-Detection και PAL-Conflict-Detection. Για την σημασιολογική αναπαράσταση της πληροφορίας πλαισίου χρήσης χρησιμοποιείται μία απλή γλώσσα συνθηκών (condition) που χειρίζεται μεταβλητές που αναπαριστούν τις πληροφορίες πλαισίου χρήσης. Η λύση που προτείνεται στο άρθρο αυτό

υλοποιήθηκε μερικώς για το OCR project "Privacy and security policy management" της IBM.

Κύριο χαρακτηριστικό της προσέγγισης [36] είναι η συσκότιση πληροφορίας πλαισίου χρήσης μέσω οντολογικών περιγραφών. Η συγκατάθεση του χρήστη λαμβάνεται υπόψη εφόσων οποιαδήποτε ενέργεια αφορά δεδομένα του κρίνεται επιτρεπτή ή όχι, σύμφωνα με τις δικές του προτιμήσεις ιδιωτικότητας. Ο χρήστης προσδιορίζει τις προτιμήσεις ιδιωτικότητας και τις προτιμήσεις διακριτότητας αποκάλυψης πληροφορίας (granularity preferences). Μία επιλογή προτίμησης βαθμού διακριτότητας της αποκάλυψης μπορεί να είναι γενική και κοινή για διάφορες προτιμήσεις ιδιωτικότητας που έχει εκφράσει. Οι τεχνικές συσκότισης, αλλιώς ανακρίβειας της πληροφορίας, επιτυγχάνονται μέσω οντολογικών περιγραφών που εκφράζουν το επίπεδο λεπτομέρειας της αποκάλυψης. Μπορεί να εφαρμοστεί σε όλους τους τύπους αντικειμένων του μοντέλου πλαισίου χρήσης. Οι χρήστες, οι οποίοι κατέχουν δικαιώματα ιδιοκτησίας στα δικά τους δεδομένα, προσδιορίζουν περιορισμούς και προτιμήσεις σε αυτά όσον αφορά το βαθμό διακριτότητας της αποκάλυψης τους. Έχοντας υπόψη τους περιορισμούς και τις προτιμήσεις ιδιωτικότητας που όρισαν οι κάτοχοι των δεδομένων, προσδιορίζονται οι άδειες πρόσβασης και ο βαθμός αποκάλυψης της ζητούμενης πληροφορίας. Για την μοντελοποίηση της πληροφορίας χρησιμοποιείται η γλώσσα CML (context modeling language), υπάρχουν οντολογίες για τους διάφορους τύπους αντικειμένων του μοντέλου πλαισίου χρήσης όπου φαίνεται η ιδιοκτησία της πληροφορίας.

Η προσέγγιση αυτή [37] αποτελεί επέκταση του προηγούμενου μηχανισμού [36], υποστηρίζεται από την δυναμική εξεύρεση και επεξεργασία πηγών πλαισίου χρήσης. Κύριο συστατικό της ένας μηχανισμός συσκότισης που προσαρμόζει δυναμικά το επίπεδο λεπτομέρειας της αποκάλυψης πληροφοριών σε σχέση με τις απαιτήσεις του χρήστη. Ο μηχανισμός υποστηρίζεται από οντολογίες συσκότισης οι οποίες μπορούν να υπάρχουν για κάθε τύπο δεδομένων. Ο αριθμός των επιπέδων λεπτομέρειας αποκάλυψης δεν είναι στατικός. Μπορεί να χειρίζεται πολιτικές ιδιωτικότητας που εξαρτώνται ή σχετίζονται με το πλαίσιο χρήσης (context-dependent), καθώς και να υποστηρίζει multi-party ιδιοκτησία (μία πληροφορία να χαρακτηρίζει περισσότερους από ένα χρήστη). Ομοίως με την προηγούμενη λύση, για την μοντελοποίηση της πληροφορίας χρησιμοποιείται η γλώσσα CML (context modeling language). Έχει

υλοποιηθεί σε πολυεπίπεδο σύστημα διαχείρισης πλαισίου χρήσης (CMS) το οποίο ανακαλύπτει δυναμικά νέα πληροφορία πλαισίου χρήσης (Sensor Layer, SensorML, Interface Layers, Context Manager Layer).

Στο προτεινόμενο μοντέλο [30], που αποτελεί επέκταση του μοντέλου πληροφορίας πλαισίου χρήσης των Schmidt et al, για επίγνωση της ιδιωτικότητας, η συγκατάθεση του κατόχου δεδομένων λαμβάνεται υπόψη. Εφαρμόζονται τεχνικές συσκότισης, ανακρίβειας δηλαδή της πληροφορίας στα δεδομένα που ανήκουν στην κατηγορία "protected context". Λαμβάνονται επίσης τυχόν εξαρτήσεις ιδιωτικότητας μιας πληροφορίας πλαισίου χρήσης με κάποια άλλη, είτε αυτή ανήκει στο protected group είτε στο evaluated group. Άδειες πρόσβασης δίνονται ανάλογα με τις πολιτικές ιδιωτικότητας που έχει καθορίσει ο χρήστης πάνω στα δεδομένα που ανήκουν στην ομάδα πληροφοριών πλαισίου χρήσης που χρειάζονται προστασία. Η αναπαράσταση της πληροφορίας γίνεται αντίστοιχα με αυτή του μοντέλου πληροφορίας των Schmidt et al. Ως πλαίσιο χρήσης ορίζεται η οποιαδήποτε πληροφορία που χαρακτηρίζει την κατάσταση μιας οντότητας.

Η προτεινόμενη αρχιτεκτονική που αποτελεί επέκταση των πολιτικών της πλατφόρμας P3P [31] διαχειρίζεται context_to_context συσχετίσεις. Έχει προταθεί για κινητές εφαρμογές επιχειρήσεων με επίγνωση του πλαισίου χρήσης. Η αναπαράσταση της πληροφορίας βασίζεται στην αντίστοιχη του μοντέλου πληροφορίας των Schmidt et al.[14]. Οι πληροφορίες πλαισίου χρήσης χωρίζονται σε δύο κατηγορίες, protected και evaluated context. Δεν θεωρούν μόνο την τοποθεσία του χρήστη ως πληροφορία πλαισίου χρήσης.

Ο έλεγχος πρόσβασης με επίγνωση της ιδιωτικότητας στο [21] γίνεται μέσω της βοήθειας ενός μηχανισμού διαχείρισης εμπιστοσύνης. Ο κάτοχος δεδομένων καθορίζει τον επιτρεπόμενο σκοπό χρήσης, την χρονική περίοδο διατήρησης και το επίπεδο γενίκευσης των προσωπικών δεδομένων του που πιθανό να διαδοθούν. Ο προσδιορισμός σκοπού χρήσης δεδομένων ζητείται και εδώ. Λόγω της ύπαρξης τεχνικών γενίκευσης (generalization) δεδομένων, ο χρήστης έχει την δυνατότητα να επιλέξει πληροφορίες του που θεωρεί περισσότερο ευαίσθητες και δεν επιθυμεί την αποκάλυψη της ακριβής τους τιμής και να προσδιορίσει τον βαθμό γενίκευσης τους όταν αυτά θα αποκαλυφθούν σε τρίτους. Ο προσδιορισμός αδειών πρόσβασης

επιτυγχάνεται μέσω του μηχανισμού απόφασης βάσει της εκτίμησης της εμπιστοσύνης του αιτούντα (trust-based decision mechanism) και κατά την διάρκεια επεξεργασίας των δεδομένων οποιοδήποτε περαιτέρω αίτημα πρόσβασης ελέγχεται από ένα αλλο μηχανισμό πρόσβασης (ongoing access control mechanism). Η εκτίμηση εμπιστοσύνης του αιτούντα προκύπτει μέσα από συνδυασμό των συστάσεων άλλων χρηστών (βάση δεδομένων συστάσεων) και του ιστορικού του χρήστη αυτού όπως έχει καταγραφεί στην βάση του συστήματος. Ο μηχανισμός αυτός δοκιμάστηκε για ένα σύνολο δεδομένων της πραγματικής ζωής (CENSUS). Η προσέγγιση αυτή αναφέρεται για εφαρμογή της σε υπηρεσίες δικτύου (web services).

Το μοντέλο ελέγχου πρόσβασης που περιγράφεται στο [32] διαχειρίζεται ένα μηχανισμό που επίσης βασίζεται στην εκτίμηση εμπιστοσύνης του αιτούντα. Η συγκατάθεση κατόχου δεδομένων απαιτείται για οποιαδήποτε πρόσβαση σε δικά του δεδομένα. Χρησιμοποιούνται τεχνικές συσκότισης πληροφορίας, δηλαδή παρουσίαση ενός μέρου της πληροφορίας και όχι η ακριβή της τιμή. Ο προσδιορισμός άδειας πρόσβασης κάποιου χρήστη εξαρτάται από ένα μηχανισμό εύρεσης κινδύνου (risk) και βαθμού εμπιστοσύνης (trust) του χρήστη. Η εκτίμηση εμπιστοσύνης του αιτούντα προσδιορίζεται βάση ενός μηχανισμού που παρατηρεί το ιστορικό (history) του χρήστη (experiential learning mechanism). Η ανάλυση αυτή του κινδύνου και της εμπιστοσύνης αφού γίνουν γνωστά στον κάτοχο δεδομένων, αυτός με την σειρά του δηλώνει την δική του πολιτική διαχείρισης ιδιωτικότητας και δικαιώματα πρόσβασης που βάσει αυτών θα γίνει δεχτό ή όχι ένα αίτημα. Στο άρθρο αυτό αναφέρεται μόνο η τοποθεσία χρήστη ως πληροφορία πλαισίου χρήσης, γι’ αυτό και οι πιο πάνω μηχανισμοί τέθηκαν σε εφαρμογή για αξιολόγηση τους, σε ένα σύστημα ανίχνευσης τοποθεσίας χρήστη εντός ενός κτιρίου πανεπιστημίου.

Το άρθρο [17] ασχολείται ειδικότερα με την τοποθεσία του χρήστη και αναφέρεται σε προστασία πρόσβασης στην πληροφορία τοποθεσίας του χρήστη. Η συγκατάθεση του χρήστη υπολογίζεται εφόσων του δίνεται ευκαιρία να δηλώσει τις δικές του πολιτικές διαφύλαξης της τοποθεσίας. Δυνατότητα συσκότισης για την πληροφορία τοποθεσίας του χρήστη. Ο χρήστης δηλώνει πολιτικές διαφύλαξης της τοποθεσίας του (location policies), καθορίζωντας έτσι και τον χρόνο διατήρησης της πληροφορίας τοποθεσίας του. Προτείνει μηχανισμό ανίχνευσης συγκρούσεων μεταξύ πολιτικών του χρήστη και πολιτικών του δωματίου σε κάποιο κτίριο. Πραγματοποιήθηκε πειραματική

υλοποίηση του μηχανισμού που βασίζεται σε ψηφιακά πιστοποιητικά (digital certificates).

Στο [5] προτείνεται μια μηχανή "Context Privacy Engine". Ο χρήστης προσδιορίζει πολιτικές που εξαρτώνται ή σχετίζονται με το πλαίσιο χρήσης (context-dependent). Μία πολιτική υψηλότερου επιπέδου μπορεί να επικαλύψει όλες τις πολιτικές μικρότερου επιπέδου. Για τον προσδιορισμό προσβάσεων και περιορισμών στους χρήστες είναι υπεύθυνος ένας αλγόριθμος εκτίμησης και ελέγχου του συνόλου των πολιτικών που έχουν δηλωθεί (Policy Evaluation Algorithm). Υπάρχει μηχανισμός ανίχνευσης συγκρούσεων μεταξύ πολιτικών ο οποίος ελέγχει το επίπεδο της πολιτικής, επιλέγει την υψηλότερη στην ιεραρχία, αλλιώς το αίτημα απορρίπτεται. Για την αναπαράσταση των πολιτικών ιδιωτικότητας χρησιμοποιείται η γλώσσα XML. Η μηχανή αυτή (Context Privacy Engine) έχει αναπτυχθεί ως εφαρμογή βασισμένη σε Java, για σκοπούς αξιολόγησης.

Η Υποδομή βασισμένη σε πολιτικές [18] εφαρμόζει τεχνικές συσκότισης, ανακρίβειας πληροφορίας σε δύο σημαντικές πληροφορίες πλαισίου χρήσης, όπως είναι η τοποθεσία και η δραστηριότητα. Για τον προσδιορισμό αδειών προσβάσεων, χρησιμοποιείται ένα μοντέλο συμπερασμού, το Privacy_Control_Module, το οποίο αποτελείται από οντολογίες και μία μηχανή διαδικασίας συμπερασμού που διευκολύνουν την εξαγωγή συμπερασμάτων και αποφάσεων. Τα δεδομένα που μπορούν να σταλούν στον εξυπηρετητή (server) είναι μόνο αυτά που επιτρέπει ο χρήστης. Για την μοντελοποίηση πληροφορίας χρησιμοποιείται μία OWL (Ontology Web Language) οντολογία, λόγω της ανάγκης επεξεργασίας της πληροφορίας και όχι απλά παρουσίαση της. Επιπλέον γίνεται συνδυασμός της γλώσσας OWL-DL με κανόνες Jena για τις πολιτικές (N3 μορφή). Η υποδομή αυτή δοκιμάστηκε σε συσκευές χρήστη όπως iPhones, καθώς και σε Android phones (client devices). Υπάρχει δυνατότητα υλοποίησης και ενσωμάτωσης της υποδομής σε υφιστάμενα κοινωνικά δίκτυα.

Στο [38] περιγράφεται μία οντολογία ιδιωτικότητας. Ο κάτοχος δεδομένων καθορίζει κάτω από ποιους σκοπούς μπορούν να συλλεγούν και να χρησιμοποιηθούν τα δεδομένα, καθώς και τον χρόνο διατήρησης τους (ορίζεται στην κλάση Condition). Για την μοντελοποίηση πληροφορίας χρησιμοποιείται οντολογία η οποία είναι

βασισμένη στην ορολογία και πολιτικές της πλατφόρμας P3P. Εξαιτίας του φορμαλισμού και των δυνατοτήτων μιας οντολογίας, η εξαγωγή λογικών συμπερασμάτων όσον αφορά την συσχέτιση των πληροφοριών διευκολύνεται. Υπεύθυνη για τον προσδιορισμό και περιορισμό αδειών πρόσβασης είναι η κλάση Privacy_Rule_Class. Η οντολογία αυτή μπορεί να ενσωματωθεί σε μελλοντικούς μηχανισμούς ιδιωτικότητας βάσει κανόνων. Μερικά παραδείγματα πληροφορίας πλαισίου χρήσης που παρουσιάζονται στο άρθρο αυτό είναι η τοποθεσία του χρήστη, η ενέργεια του χρήστη, τα γύρω άτομα και συσκευές, η ώρα κτλ.

Το [8] αναφέρεται στην χρήση και εκμετάλλευση των δυνατοτήτων της οντολογίας πολιτικών SOUPA. Η οντολογία SOUPA επιτρέπει στους χρήστες να ορίζουν τους δικούς τους κανόνες πολιτικών ιδιωτικότητας. Για τις αποφάσεις των αιτημάτων πρόσβασης χρησιμοποιείται ένας αλγόριθμος συμπερασμού πολιτικών (policy reasoning algorithm) που λαμβάνει υπόψη του τις πολιτικές όπως ορίστηκαν από τον χρήστη. Η μοντελοποίηση των πολιτικών επιτυγχάνεται μέσω οντολογίας πολιτικών σε OWL (Ontology Web Language). Η οντολογία που προτείνεται έχει υλοποιηθεί στην αρχιτεκτονική CoBrA (Context Broker Architecture). Πρωτότυπο του CoBrA έχει δοκιμαστεί σε σύστημα έξυπνου δωματίου συνεδριών (smart meeting room). Ως πλαίσιο χρήσης στο παρόν άρθρο ορίζεται ως οι πληροφορίες που σχετίζονται με μία οντότητα, όπου η πληροφορία μπορεί να είναι η ίδια η οντότητα (άτομα, τοποθεσίες, πράγματα).

Η προτεινόμενη προσέγγιση στο [26] προτείνει υποδομή ελέγχου πρόσβασης που συνδυάζει μοντέλο ελέγχου πρόσβασης βάσει ρόλων (RBAC) και πολιτικές της πλατφόρμας P3P για τον έλεγχο πρόσβασης. Τα δικαιώματα περιέχονται στους ρόλους και όχι στους χρήστες. Οι P3P πολιτικές συγκρίνονται με τις προτιμήσεις της οντότητας, δηλαδή του χρήστη. Για την διαχείριση της πληροφορίας πλαισίου χρήσης υπάρχουν πολλοί και συγχρονισμένοι διαχειριστές πλαισίου χρήσης (Context Managers), ένας για κάθε διαφορετική οντότητα του συστήματος.

Η αρχιτεκτονική προτιμήσεων ιδιωτικότητας στο [12] στηρίζεται στην λειτουργία αρχιτεκτονικής comp_pref [11]. Η συγκατάθεση κατόχου δεδομένων απαιτείται ρητά αφού ο χρήστης έχει την δυνατότητα να προσδιορίσει τις δικές του προτιμήσεις ιδιωτικότητας. Διαφορετική ένδειξη απειλής της ιδιωτικότητας εκτιμάται ανάλογα με

τι είδους δεδομένα συνδυάζεται συγκεκριμένος σκοπός χρήσης σε αίτημα πρόσβασης ενός χρήστη. Ο κάτοχος δεδομένων μπορεί να καθορίσει τον χρόνο διατήρησης των δεδομένων που συνήθως είναι μόνο όσο χρειάζεται για να εκπληρωθεί ο δεδηλωμένος σκοπός. Ο μηχανισμός εκτίμησης της απειλής ιδιωτικότητας είναι αυτός που περιορίζει, καθορίζει τις αποφάσεις άδειας πρόσβασης (weighting mechanism indicating privacy threat). Για τον προσδιορισμό πολιτικών ιδιωτικότητας οι χρήστες χρησιμοποιούν κανόνες APPEL (P3P Preference Exchange Language). Για αξιολόγηση της προσέγγισης αναπτύσσεται ένα εργαλείο προσομοίωσης, το οποίο καθορίζει πως οι προτιμήσεις που αλλάζουν δυναμικά μπορούν να περιγραφούν και να εκτιμηθούν από τους ίδιους τους χρήστες.

Η προσέγγιση του [23] αναφέρεται σε ένα διαχειριστή προφίλ (Profile Manager) που διατηρεί προφίλ για χρήστες, για πληροφορίες πλαισίου χρήσης και για τα σενάρια. Η συγκατάθεση του χρήστη απαιτείται όταν μία πολιτική ιδιωτικότητας αποτελείται από το αναγνωριστικό "ask the user" (privacy flags). Προτείνεται χρήση τεχνικών συσκότισης πάνω σε ευαίσθητα δεδομένα του χρήστη, έτσι ώστε να γίνεται απόκρυψη της ακριβής πληροφορίας που πιθανό να δημιουργούσε προβλήματα παραβίασης της ιδιωτικότητας. Οι αποφάσεις για τις άδειες πρόσβασης προκύπτουν βάσει του αλγόριθμου "Privacy Safeguard Algorithm". Για την αναπαράσταση της πληροφορίας χρησιμοποιούνται περιγραφές προφίλ για χρήστες, για πληροφορίες πλαισίου χρήσης και για σενάρια, τα οποία δημιουργούνται με γλώσσα XML. Ο χρήστης δηλώνει στο δικό του προφίλ "privacy flags" πάνω σε δεδομένα καθώς και προτιμήσεις βαθμού λεπτομέρειας τυχόν αποκάλυψης τους (data abstraction). Ο χρήστης έχει την δυνατότητα αλλαγής και ενημέρωσης του προφίλ του, δυνατότητα κατοχής ψευδωνύμου, όπως και δυνατότητα κατοχής νέου προφίλ για κάθε διαφορετικό του ρόλο. Δοκιμάστηκε σε ένα ιατρικό σενάριο που αποτελείται από ασθενείς και ιατρούς.

6.2 Πίνακες σύγκρισης

Ακολουθούν οι πίνακες στους οποίους φαίνονται οι παρακάτω συμβολισμοί:

✔ - υποστηρίζεται από την συγκεγκριμένη προσέγγιση
Δ.Α – δεν αναφέρεται στην αναφερόμενη πηγή

ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΛΥΣΕΙΣ- ΜΗΧΑΝΙΣΜΟΙ										
		CA- RBAC (NIST extension) [9]	**Context-RBAC [27]**	**PA-RBAC model [24,25]**	**Context Obfuscation-ontological descriptions [36]**	**Context Obfuscation supported by Dynamic Con. Source Disc. and Proc.[37]**	**PA-Context Data Model (based Schmidt. et al) [30]**	**User-centric privacy architecture (based on P3P) [31]**	**PA-Access Control with Trust management [21]**	**Trust-based model for privacy control [32]**
Privacy Features	Συγκατάθεση κατόχου δεδομένων (αν απαιτείται)			✔	✔	✔	✔	✔	✔	✔
	Προσδιορισμός σκοπού χρήσης δεδ./ Ενημέρωση χρήστη	Βάση ρόλων κ. εξειδ. για ποιο αντικειμενο	✔	✔					✔	
	Συσκότιση/ανακρίβεια πληροφορίας (και σε ποια δεδομένα)				✔ Μέσω οντολογικών περιγραφών: όσο μεγαλύτ. το επίπεδο (ρίζα=επιπ.1)τόσο υψηλότερο granularity Για όλους τους τύπους αντικειμ.(π.χ τοποθεσία, δραστηριότητα)	✔ Μηχανισμός που προσαρμόζει δυναμικά το επ.λεπτομ. ανάλογα με τις απαιτ.του χρήστη -οντολογίες (για όλους τους τύπους αντικ., μη στατικό αριθμό επ.λεπτομ.)	✔ σε δεδομένα που ανήκουν στο «protected context group»	✔ σε δεδομένα που ανήκουν στο «protected context group»	✔ ο χρήστης ορίζει το επίπεδο γενίκευσης στα δεδομένα που επιθυμεί -προσδιορ. Ορίου γενίκευσης (generalization boundary)	✔
	Συμπληρωματικές ενέργειες			✔ -υποχρεώσεις (obligations)		συσχετίσεις context-dependent & multi-party ownership	✔ privacy dependence of context data	✔ (context-to-context συσχετίσεις) privacy dependence of context data		

		CA- RBAC (NIST extension) [9]	**Context-RBAC [27]**	**PA-RBAC model [24,25]**	**Context Obfuscation-ontological descriptions [36]**	**Context Obfuscation supported by Dynamic Con. Source Disc. and Proc.[37]**	**PA-Context Data Model (based Schmidt.) [30]**	**User-centric privacy architecture (based on P3P) [31]**	**PA-Access Control with Trust management [21]**	**Trust-based model for privacy control [32]**
	Χρόνος διατήρησης δεδ. (Όσο χρειάζεται; / (Πώς και ποιος τον καθορίζει;)	✔		✔					✔ ο κάτοχος δεδ. το καθορίζει	
	Προσδιορισμός προσβάσεων/ περιορισμών για τον χρήστη	✔ Βάση ρόλων (personalized permissions, permissions on objects : private, shared)	Βάση user role + context role (=κατάσταση πληρ.πλαισίου) - iff *PermissionBit* of policy rule =ALLOW	✔ Βάση ιεραρχιών ρόλων, δεδομένων και σκοπών (αν πρόσβαση σε όλα child-nodes, τότε και στο parent-node)	-granularity constraints (οι κάτοχοι δεδ. ορίζουν) -ownership δικαιώματα για την πληροφορία	-granularity constraints (οι κάτοχοι δεδ. ορίζουν) -ownership δικαιώματα για την πληροφορία(συγκατάθεση όλων των κατόχων της)	Ανάλογα με privacy policies πάνω στα protected δεδ.	Ανάλογα με privacy policies των protected δεδ.	✔ trust-based decision Mechanism + ongoing (κατά την διάρκεια πρόσβασης) access control mechanism για καθορισμό δικαιωμάτων	✔ Μετά από εύρεση κινδύνου + εμπιστοσύνης αιτούντα βάση εκτιμήσεων κατόχου (θεωρία πιθανοτήτων) +access rights μόνο σε αξιόπιστους χρήστες
	Ανίχν.συγκρούσεων μεταξύ αδειών (μηχαν.)			✔ *χρήση σχετικών αλγορίθμων:* -PA-Conflict-Detection (pa1, pa2) -PAL-Conflict-Detection(list of permission assignments)						

		CA- RBAC (NIST extension) [9]	Context-RBAC [27]	PA-RBAC model [24,25]	Context Obfuscation-ontological descriptions [36]	Context Obfuscation supported by Dynamic Con. Source Disc. and Proc.[37]	PA-Context Data Model (based Schmidt.) [30]	User-centric privacy architecture (based on P3P) [31]	PA-Access Control with Trust management [21]	Trust-based model for privacy control [32]
	Εκτίμηση εμπιστοσύνης αιτούντα (με ποιο μηχανισμό)								✔ Βάση συστάσεων άλλων χρηστών και βάση ιστορικού ιδίου του χρήστη	✔ Βάση ιστορικού χρήστη (experiential learning mechanism)
	Μοντελοποίηση πληροφορίας /πολιτικών ιδιωτικότητας	- Ορολογία κλασικού προτύπου RBAC -XML	Based on formalization of traditional RBAC	*Για τις προυποθέσεις:* simple condition language (LC_0) & context variables	-CML (context modeling language) -Οντολογία για κάθε τύπο αντικειμένου [κρατείται + ownership of context information]	CML (context modeling language) + χρήση οντολογιών	Βασ. στο μοντέλο πλαισίου των Schmidt et al. (+διαχωρισμός σε protected& evaluated context)	-Βασισμένο στο μοντέλο πλαισίου χρήσης των Schmidt et al.	Δ.Α	Δ.Α.
	Συμμετοχή κατόχου δεδομένων/ Δυνατότητα χρήστη να καθορίζει τι δεδομένα βλέπει μια εφαρμογή και ποια όχι				✔ Ο χρήστης καθορίζει Privacy + granularity preferences - Μία γενική επιλογή gpi επαναχρησ.σε πολλές pp	Ο χρήστης καθορίζει context-dependent privacy + granularity preferences			Ο κάτοχος δεδ. καθορίζει το σκοπό, την περίοδο χρήσης και το επίπεδο γενίκευσης που επιτρέπεται σε συγκεκρ. χρήστες	✔ Μετά από ανάλυση risk & trust, ο χρήστης δηλώνει τη δική του πολιτική διαχείρισης ιδιωτικότητας

		CA- RBAC (NIST extension) [9]	Context-RBAC [27]	PA-RBAC model [24,25]	Context Obfuscation-ontological descriptions [36]	Context Obfuscation supported by Dynamic Con. Source Disc. and Proc.[37]	PA-Context Data Model (based Schmidt.) [30]	User-centric privacy architecture (based on P3P) [31]	PA-Access Control with Trust management [21]	Trust-based model for privacy control [32]
	Σύστημα στο οποίο δοκιμάστηκε / προτάθηκε	Ιατρικό σύστημα (ρόλοι και άδειες προσβάσεων σε νοσοκόμες και ιατρούς)	Έξυπνο σπίτι εξοπλισμένο με διάφορους networked sensors και actuator devices (camera etc.)	Μερικώς στο OCR project: "Privacy and security policy management" (IBM)	Δ.Α.	υλοποίηση σε layered CMS (δυναμ. ανακαλύπτει νέο context) - -Sensor Layer -SensorML Interface layers -Context Manag. Layer	Δ.Α.	-προορίζεται για Context-aware mobile business applications	δοκιμάστηκε σε real-life σύνολο δεδομένων CENSUS	Ανίχνευση τοποθεσίας χρήστη εντός πανεπιστημίου
	Πώς ορίζεται η έννοια context	Context του ατόμου ορίζεται η τοποθεσία του, οι συσκευές που χρησ., δίκτυο στο οποίο είναι συνδεδ., ενέργειες του χρήστη	Πληροφορία που να μπορεί να χαρακτηρίσει μια οντότητα (άτομα, τόποι, πράγματα)	Δ.Α.	Δ.Α	Δ.Α	Θεωρείται οποιαδήποτε πληροφορία που χαρακτηρίζει την κατάσταση μιας οντότητας	Θεωρείται οτιδήποτε μπορεί να χαρακτηρίσει την κατάστ. μιας οντότητ. και όχι μόνο η πληροφ. τοποθεσίας	**Η λύση αυτή αναφέρεται ειδικότερα για web services.	Στο paper αυτό αναφέρεται μόνο η τοποθεσία για πληροφορία πλαισίου χρήσης

Πίνακας 6.1 Πίνακας ανάλυσης προσεγγίσεων βάσει των χαρακτηριστικών επίγνωσης πλαισίου χρήσης και ιδιωτικότητας(1)

	Protecting access to people location information [17]	**Privacy Engine for C-Aware Enterprise App.Services [5]**	**Policy-based framework [18]**	**Privacy Ontology [38]**	**SOUPA ontology for privacy protection (in CoBrA) [8]**	**RBAC + P3P Infrastructure [26]**	**Pr.Preferences Architecture (βάση λειτ. Comp_pref) [12]**	**C-A Privacy Prot. with profile management [23]**
Συγκατάθεση κατόχου δεδομένων (αν απαιτείται)	✔	✔	✔	✔	✔		✔	✔ (ask the user-privacy flags)
Προσδιορισμός σκοπού χρήσης δεδ./ Ενημέρωση χρήστη				ο κάτοχος δεδ. καθορίζει κάτω από ποιους σκοπούς μπορούν να συλλεγούν τα δεδ.			✔ διαφορ. ένδειξη απειλής ιδιωτ. ανάλογα με τι δεδ.συνδιάζεται ο σκοπός	
Συσκότιση/ανακρίβεια πληροφορίας (και σε ποια δεδομένα)	User policy: στην πληροφορία τοποθεσίας Room policy: αριθμός ατόμων έναντι ταυτοτήτων		✔ Π.χ τοποθεσία και δραστηριότητα (ιεραρχίες λεπτομέρειας)					✔ στα ευαίσθητα δεδομένα του χρήστη
Συμπληρωματικές ενέργειες		*μία πολιτική υψηλοτερου επιτ. μπορεί να επικαλύψει όλες τις μικρότερου επιπέδου		✔ logic-based inference & reasoning (δυνατ. οντολογίας)	logic-based inference & reasoning (δυνατ. οντολογίας)			
Χρόνος διατήρησης δεδ. (πώς και ποιος τον καθορίζει)	✔ ο χρήστης στις location policies του			✔ καθορ. από τον κάτοχο δεδ. (condition class)			✔ καθορίζεται από τον κάτοχο δεδ.	

	Protecting access to people location information [17]	**Privacy Engine for C-Aware Enterprise App.Services [5]**	**Policy-based framework [18]**	**Privacy Ontology [38]**	**SOUPA ontology for privacy protection (in CoBrA) [8]**	**RBAC + P3P Infrastructure [26]**	**Pr.Preferences Architecture (βάση λειτ. Comp_pref) [12]**	**C-A Privacy Prot. with profile management [23]**
Προσδιορισμός προσβάσεων/ περιορισμών για τον χρήστη	Περιορισμοί πρόσβασης ανάλογα με τις πολιτικές του χρήστη και τις πολιτικές του δωματίου	-ACL traditional mechanisms -Βάση αποτελ.. Policy evaluation algorithm (έλεγχος συνόλου πολιτικών)	✔ Privacy_control: ontologies & reasoning engine (OWL-DL& Jena Rules)	Οι χρήστες ορίζουν προτ.ιδιωτικ. (κλάση Privacy_rule) : -Data Class & Condition Class	Άδεια FORBID/PERMIT βάσει *«Policy reasoning algorithm»* (γνώση για χρήστη & OWL-DL inference engine & ενέργεια)	✔ τα δικαιώματα περιέχονται στους ρόλους - σύγκριση P3P πολιτικών με προτιμ. της οντοτητας	✔ Weighting mechanism indicating privacy threat	Rule Manager: Βάσει απόφασης του *Privacy Safeguard Algorithm* (πληροφορίες πλαισίου χρήσης + granularity προτιμήσεις χρήστη)
Ανίχνευση συγκρούσεων μεταξύ αδειών (μηχανισμοί)	✔ συγκρούσεις ανάμεσα σε user & room policies	(μεταξύ πολιτικών) -έλεγχος policy level -επέλεξε την υψηλότερη στην ιεραρχία -αλλιώς απόρριψη αιτήματος						
	Protecting access to people location information [17]	Privacy Engine for C-Aware Enterprise App.Services [5]	Policy-based framework [18]	Privacy Ontology [38]	SOUPA ontology for privacy protection (in CoBrA) [8]	RBAC + P3P Infrastructure [26]	Pr.Preferences Architecture (βάση λειτ. Comp_pref) [12]	C-A Privacy Prot. with profile management [23]
Μοντελοποίηση πληροφορίας /πολιτικών ιδιωτικότητας		XML-text / (Περιγραφή 'Privacy policy model')	-OWL context ontology & OWL-Description Logics -policy rules: N3 format	Οντολογία βασισμένη στην ορολογία + πολιτικές της P3P (dyn. Pr. Pref. + rules)	OWL Policy Ontology (part of SOUPA)	(πολλοί και συγχρονισμένοι Context Managers, τουλάχιστον ένας για κάθε οντότητα)	- APPEL rules	profile descriptions: XML (user, context, scenarios profiles etc.)

	Protecting access to people location information [17]	Privacy Engine for C-Aware Enterprise App.Services [5]	Policy-based framework [18]	Privacy Ontology [38]	SOUPA ontology for privacy protection (in CoBrA) [8]	RBAC + P3P Infrastructure [26]	Pr.Preferences Architecture (βάση λειτ. Comp_pref) [12]	C-A Privacy Prot. with profile management [23]
Συμμετοχή κατόχου δεδομένων/ Δυνατότητα χρήστη να καθορίζει τι δεδομένα βλέπει μια εφαρμογή και ποια όχι	✔Ο χρήστης καθορίζει τις δικές του «User policies»	✔Ο χρήστης καθορίζει context-dependent privacy policies	✔ο χρήστης δηλώνει προτιμήσεις ιδιωτ. & κανόνες γενίκευσης δεδ. -Μόνο δεδ. που επιτρέπει ο χρήστης μπορούν να σταλούν στον server	✔user privacy policies (σε ποια δεδομένα και υπό ποιες συνθήκες)	Με την βοήθεια της SOUPA , οι χρήστες μπορούν να ορίζουν τους δικούς τους κανόνες ιδιωτ.			✔ο χρήστης αναθέτει privacy Flags στο profile του (π.χ 'always give', 'never give') στα δεδ. -επιλογές αφαιρετικότητας δεδομένων -δυνατ.αλλαγής και ενημερ. του profile του - δυνατ. κατοχής ψευδωνύμου -νέο προφίλ για διαφορ.ρόλο
Σύστημα στο οποίο δοκιμάστηκε / προτάθηκε	υλοποίηση που βασίζεται σε digital certificates	Context Privacy Engine ως Java-based εφαρμογή	-δοκιμάστηκε σε iPhones, Android ph. (client devices) -δυνατ. ενσωμάτωσης σε υπάρχουσα κοινωνικά δίκτυα	**η οντολογία αυτή μπορεί να χρησιμ. σε μελλ.. Rule-based privacy mechanisms	-υλοποίηση στην αρχιτεκτονική CoBrA - CoBrA prototype in smart meeting room system	Δ.Α	Simulation tool: πώς οι δυναμικές προτιμήσεις μπορούν να περιγραφ. και να εκτιμηθούν από τους ίδιους τους χρήστες	ιατρικό σενάριο (ασθενείς και ιατροί)
Πώς ορίζεται η έννοια context	το άρθρο ασχολείται ειδικότερα για την πληροφ. τοποθεσίας του χρήστη	Δ.Α	Δ.Α.	Πληροφ. όπως τοποθεσία και ενέργεια χρήστη,γύρω άτομα και συσκευές, ώρα κ.τ.λ	Δ.Α	Πληροφ.σχετικά με μία οντότητα (η ίδια οντότητα, άτομα, τόποι, πράγματα)	Δ.Α.	Δ.Α

Πίνακας 6.2 Πίνακας ανάλυσης προσεγγίσεων βάσει των χαρακτηριστικών επίγνωσης πλαισίου χρήσης και ιδιωτικότητας(2)

Κεφάλαιο 7

Προτεινόμενα Χαρακτηριστικά Αρχιτεκτονικής

7.1 Περιγραφή συστατικών αρχιτεκτονικής προστασίας ιδιωτικότητας

Μία καλή αρχιτεκτονική με επίκεντρο τον χρήστη πρέπει να δίνει την δυνατότητα στους χρήστες να καθορίζουν οι ίδιοι τις δικές τους προτιμήσεις ιδιωτικότητας και διακριτότητας αποκάλυψης των πληροφοριών, κανόνες πρόσβασης δηλαδή που περιγράφουν πώς ο χρήστης επιθυμεί την διάδοση προσωπικών του δεδομένων, σε ποιους το επιτρέπει, κάτω από ποιες συνθήκες και σε ποιο επίπεδο λεπτομέρειας οι προσωπικές τους πληροφορίες μπορούν να φανερωθούν. Η εφαρμογή μηχανισμού προστασίας ιδιωτικότητας του πράκτορα χρήστη είναι υπεύθυνη για την επιβολή πολιτικών ιδιωτικότητας προκειμένου να ελεγχθεί αν ένα αίτημα κρίνεται αποδεκτό ή όχι. Ένα αίτημα γίνεται αποδεκτό από το σύστημα μόνο αν τα στοιχεία του αιτήματος συμφωνούν με τους περιορισμούς που καθόρισε ο κάτοχος του πόρου που ζητείται, καθώς επίσης αν συμμορφώνεται με τους κανόνες και αρχές της ιδιωτικότητας. Η μηχανή συμπερασμού θα δέχεται αιτήματα, θα εκτελεί την διαδικασία συμπερασμού βάσει των προτιμήσεων ιδιωτικότητας που όρισαν οι χρήστες και θα είναι υπεύθυνη για την εξαγωγή λογικών συμπερασμάτων και αποφάσεων. για εξαγωγή αποφάσεων πρόσβασης. Η μηχανή αυτή πρέπει να είναι σε θέση να συμπεράνει επιπρόσθετη γνώση με την βοήθεια των οντολογιών και των κανόνων πρόσβασης.

Βοηθητική είναι η ύπαρξη ενός συνόλου οντολογιών για την περιγραφή πολιτικών και αιτημάτων πρόσβασης, ύπαρξη βάσης δεδομένων χρήστη όπου προσωπικά στοιχεία φυλάγονται, καθώς και βάση προτιμήσεων ιδιωτικότητας χρηστών. Οι χρήστες καλό θα

είναι να μπορούν να δημιουργούν το δικό τους προφίλ στο οποίο θα παρουσιάζουν προσωπικά στοιχεία όπως όνομα, ενδιαφέροντα κλπ.

Η διαδικασία συσκότισης είναι αναγκαία και επιθυμητή για την ενθάρρυνση της αναταλλαγής πληροφοριών σε διαφορετικούς χρήστες μειώνοντας τον ενδεχόμενο κίνδυνο παραβίασης ιδιωτικότητας των κατόχων των δεδομένων. Ένα αίτημα αφού γίνει αποδεκτό, ο μηχανισμός συσκότισης πρέπει να είναι σε θέση να προσαρμόσει δυναμικά το επίπεδο λεπτομέρειας της πληροφορίας που θα φανερωθεί, σύμφωνα με τις επιλογές που δήλωσε ο κάτοχος της πληροφορίας αυτής στην περίπτωση αποκάλυψης της. Η διαδικασία αυτή της συσκότισης που ολοκληρώνει την απόφαση για κάποιο αίτημα μπορεί να υποστηριχτεί μέσω οντολογικών περιγραφών που αναπαριστούν τα διάφορα επίπεδα λεπτομέρειας της αποκάλυψης.

7.2 Επιθυμητά χαρακτηριστικά μοντέλου πληροφορίας πλαισίου χρήσης

Ένα μοντέλο πληροφορίας πλαισίου χρήσης για να είναι αποτελεσματικό και λειτουργικό πρέπει να χαρακτηρίζεται από κάποια επιθυμητά χαρακτηριστικά όπως είναι τα ακόλουθα. Ένα μοντέλο πληροφορίας πλαισίου χρήσης πρέπει κυρίως να χαρακτηρίζεται από δομή. Η δομημένη και ομοιόμορφη αναπαράσταση της πληροφορίας δίνει την δυνατότητα οργάνωσης, ελέγχου, ερμηνείας και επεξεργασίας των πληροφοριών με πιο αποτελεσματικό τρόπο. Άλλα επιθυμητά χαρακτηριστικά που πρέπει να χαρακτηρίζουν ένα τέτοιο μοντέλο είναι η ανταλλαξιμότητα (interchangeability) και μεταφερσιμότητα, η δυνατότητα σειριοποιημένης αναπαράστασης του πλαισίου χρήσης επιτρέπει την μεταφορά και ανταλλαγή του εντός ενός συστήματος. Η δυνατότητα σύνθεσης, αποσύνθεσης και επανασύνθεσης της πληροφορίας πλαισίου χρήσης επιτρέπει την διαχείριση, αποθήκευση και εκμετάλλευση του σε κατανεμημένα περιβάλλοντα. Επίσης, η επεκτασιμότητα αποτελεί απαραίτητο χαρακτηριστικό προκειμένου το σύστημα να είναι ευέλικτο και επεκτάσιμο όσον αφορά τον εμπλουτισμό των πληροφοριών που αναπαριστά. Τέλος, η χρήση προτύπων για την ανάπτυξη ενός μοντέλου πλαισίου χρήσης διευκολύνει την υιοθέτηση του από περισσότερα εμπλεκόμενα μέρη στην αλυσίδα παροχής υπηρεσιών με επίγνωση του πλαισίου χρήσης τους.

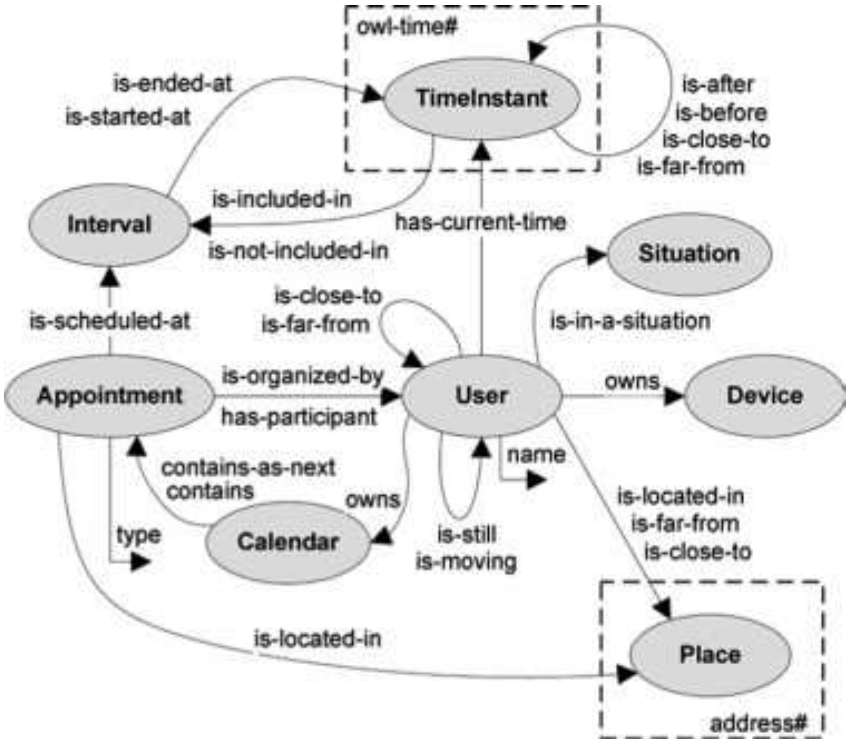
7.3 Αναπαράσταση της Σημασιολογίας με οντολογία

Με τον όρο σημασιολογία (semantics) εννοούμε όλη τη μετα-πληροφορία (metadata) που σχετίζεται με ένα αντικείμενο ή μια έννοια, η οποία μας βοηθά να κατανοήσουμε τόσο τα χαρακτηριστικά τους όσο και άλλα στοιχεία όπως οι περιορισμοί (constraints) τους, ο σκοπός τους, οι σχέσεις τους με άλλα αντικείμενα και έννοιες κλπ. Η αναπαράσταση της σημασιολογίας έχει μεγάλη σημασία κατά την ανάπτυξη συστημάτων ή εφαρμογών καθώς μας δίνει τη δυνατότητα να κατανοήσουμε καλύτερα τις εμπλεκόμενες έννοιες, να τις λάβουμε πιο ενεργά υπόψη κατά την εκτέλεση των διάφορων διαδικασιών και να εξάγουμε χρήσιμα συμπεράσματα για αυτές.

Ως βάση της λειτουργίας του συστήματος προτείνεται ο σχεδιασμός μίας οντολογίας για την αναπαράσταση της γνώσης που σχετίζεται με ένα σύστημα με επίγνωση του πλαισίου χρήσης. Το σημασιολογικό αυτό πλαίσιο μοντελοποιεί τις θεμελιώδεις, βασικές αρχές και κανόνες αναφορικά με την προστασία των προσωπικών δεδομένων, όπως αυτές πηγάζουν την Νομοθεσία. Είναι σημαντικό επίσης ο χρήστης να μπορεί να καθορίζει ο ίδιος τις δικές του πολιτικές ιδιωτικότητας ανάλογα με τις προτιμήσεις του. Με άλλα λόγια, να μπορεί να καθορίζει ποιος θα έχει πρόσβαση στα προσωπικά του δεδομένα, αλλά και ποια από αυτά θα κοινοποιούνται και σε ποια τρίτα άτομα. Η οντολογία αποτελεί τον φορμαλιστικό ορισμό των σχετικών κανόνων πρόσβασης και εκτέλεσης συμπληρωματικών ενεργειών οι οποίες πρέπει να γίνουν στο πλαίσιο, καθώς και τον φορμαλιστικό προσδιορισμό των απαιτήσεων και προτιμήσεων των χρηστών αναφορικά με την ιδιωτικότητα. Η οντολογία αποτελεί το σημασιολογικό μοντέλο, την γνωσιακή βάση για την εξαγωγή λογικών συμπερασμάτων σχετικά με την συλλογή, την επεξεργασία, και περαιτέρω μετάδοση των προσωπικών δεδομένων.

Τεχνικά μία οντολογία αποτελεί μία ιεραρχία εννοιών (κλάσεων). Η γνώση στις οντολογίες τυποποιείται χρησιμοποιώντας τις κατηγορίες στοιχείων: γνωρίσματα/ιδιότητες των εννοιών (attributes), διάφοροι περιορισμοί (restrictions) ιδιοτήτων για παράδειγμα στην τιμή ή πληθικότητα, αξιώματα (axioms), ρόλοι ή συσχετίσεις (roles) και στιγμιότυπα κλάσεων.

Τα μοντέλα που βασίζονται σε οντολογίες φαίνεται ότι υπερτερούν σε σχέση με άλλες σημαντικές υφιστάμενες προσεγγίσεις μοντελοποίησης της πληροφορίας. Μία σχετική έρευνα είναι αυτή των Strang και Popien [28]. Η έρευνα παρουσιάζει την καταλληλότητα των μοντέλων αξιολογώντας τα βάση κάποιων απαιτήσεων που πρέπει να χαρακτηρίζουν ένα μοντέλο πλαισίου χρήσης, όπως για παράδειγμα η κατανεμημένη σύνθεση, ο πλούτος και η ποιότητα της πληροφορίας, τα οποία στοιχεία θεωρεούνται ευνοικά και σημαντικά σε ένα περιβάλλον διάχυτου υπολογισμού. Η σύγκριση των μοντέλων βασισμένων σε οντολογίες γίνεται μεταξύ μοντέλων όπως μοντέλα κλειδιού-τιμής (key-value), μοντέλα markup scheme, γραφικά μοντέλα (όπως UML διαγράμματα) κτλ.



Σχήμα 7.1 Παράδειγμα οντολογίας πλαισίου χρήσης

Κεφάλαιο 8

Συμπεράσματα 75

Η εξέλιξη των φορητών συσκευών και εφαρμογών χαρακτηρίζεται εντυπωσιακή στην σημερινή εποχή. Οι εξελιγμένες αυτές συσκευές είναι σήμερα διάχυτες και πλέον αποτελούν αναπόσπαστο κομμάτι της καθημερινής ζωής πολλών ατόμων. Η εμφάνιση τους σήμανε νέες υπηρεσίες και νέους τρόπους υποστήριξης ανθρώπινων εργασιών. Ωστόσο, αυτές οι ταχέως εμφανιζόμενες και εξελισσόμενες τεχνολογίες επέτρεψαν στις συσκευές αυτές να εξοπλισθούν με αισθητήρες και υλικό το οποίο επιτρέπει τη συλλογή πληροφοριών από το περιβάλλον καθώς και προσωπικά στοιχεία, με αποτέλεσμα να προκληθούν νέα ερευνητικά προβλήματα όσον αφορά την προστασία της ιδιωτικότητας των ατόμων. Οι αρχιτεκτονικές που ενθαρύνουν την επίγνωση πλαισίου χρήσης (context-awareness) θα πρέπει να επανεξεταστούν ώστε να ενσωματώσουν στο σχεδιασμό τους την διαφύλαξη της ιδιωτικότητας και οι νομικές αρχές περί προστασίας των προσωπικών δεδομένων να αποτελούν αναπόσπαστο κομμάτι των υπηρεσιών τους.

Μία σημαντική παράμετρος στην προσπάθεια προστασίας της ιδιωτικότητας αποτελεί το γεγονός ότι στον κόσμο των φορητών υπολογιστών το περιβάλλον και το πλαίσιο επίγνωσης αλλάζουν δυναμικά με γρήγορο ρυθμό. Η συνεχής αλλαγή του περιβάλλοντος στο οποίο γίνεται η χρήση και του πλαισίου επίγνωσης της χρήσης πρέπει να λαμβάνεται σοβαρά υπόψη από τις τεχνολογίες προστασίας της ιδιωτικότητας. Οι προτιμήσεις και απαιτήσεις ιδιωτικότητας ενός χρήστη δύναται να αλλάξουν εξαρτώμενες από την τρέχουσα κατάσταση πληροφοριών πλαισίου χρήσης και αυτό κάνει τα πράγματα πιο περίπλοκα. Το κύριο χαρακτηριστικό ενός μοντέλου ελέγχου πρόσβασης πρέπει να είναι η ικανότητα του να πάρει αποφάσεις πρόσβασης βάσει της πληροφορίας πλαισίου χρήσης.

Από την στιγμή που μία πληροφορία διατεθεί σε κάποιον πάροχο υπηρεσίας, δεν υπάρχει κάποιο τεχνικό μέσο που να μπορεί να διασφαλίσει ότι η περαιτέρω

επεξεργασία και χρήση της θα είναι σύντομη και θεμιτή. Οι χρήστες δεν διαθέτουν καμία εγγύηση αναφορικά με την εφαρμογή ή μη της πολιτικής ιδιωτικότητας που μπορεί να δηλώνει ο πάροχος υπηρεσίας. Για τον λόγο αυτό σε μία αρχιτεκτονική συστήματος με επίγνωση του πλαισίου χρήσης, όπου ρέουν ασταμάτητα προσωπικά δεδομένα των χρηστών, επιβάλλεται η χρήση μηχανισμών προστασίας απορρήτου που θα ελέγχουν και θα διευθύνουν την θεμιτή πρόσβαση σε πόρους του συστήματος.

Δύο βασικά βήματα που προδιαθέτουν την προσπάθεια διαφύλαξης της ιδιωτικότητας των χρηστών που εμπλέκονται σε ένα σύστημα είναι η πιστοποίηση (authentication) του αιτούντα κάποιου πόρου του συστήματος και έπειτα η εξουσιοδότηση (authorization) του ατόμου αυτού. Ο όρος πιστοποίηση δηλώνει ότι πρέπει ένα σύστημα να είναι σε θέση να διασφαλίσει τους νόμιμους χρήστες και ότι κάποιος τρίτος δεν θα μπορεί να οικοιοποιηθεί την ταυτότητα ενός μόνιμου χρήστη. Η διαδικασία εξουσιοδότησης είναι κάτι που έπεται της διαδικασίας πιστοποίησης. Ενώ λοιπόν αρχικά επιβεβαιώνεται ότι ο πελάτης κάποιας υπηρεσίας είναι αυτός που ισχυρίζεται ότι είναι, στη συνέχεια το σύστημα θα πρέπει να είναι σε θέση να καθορίσει τα δικαιώματα (rights) αυτού του χρήστη, δηλαδή τις ενέργειες που μπορεί να εκτελέσει.

Η χρήση ψευδωνύμων και η πιθανότητα του να είσαι ανώνυμος είναι κλασικοί μηχανισμοί προστασίας της ιδιωτικότητας που χρειάζονται περαιτέρω διερεύνηση για να διαπιστωθεί αν μπορούν τελικά να βελτιώσουν την προστασία της ιδιωτικότητας σε διάχυτα περιβάλλοντα. Η χρήση ρόλων για τους χρήστες μιας εφαρμογής, μειώνει κατά πολύ το διαχειριστικό φόρτο, αφού οι άδειες ανατίθενται σε ρόλους και όχι σε χρήστες. Ένας χρήστης πολύ πιο συχνά μπορεί να αλλάξει ρόλο από ότι τα δικαιώματα και ιδιότητες ενός συγκεκριμένου ρόλου. Ωστόσο, η χρήση ενός μοντέλου ελέγχου πρόσβασης βάσει ρόλων είναι περισσότερο ευνοικό και βοηθητικό σε συστήματα όπου οι ρόλοι είναι εκ των προτέρων γνωστοί, όπως για παράδειγμα σε μία ιατρική κλινική όπου οι βασικοί υποψήφιοι ρόλοι είναι αυτοί του ιατρού, της νοσοκόμας και του ασθενή.

Η τεχνική συσκότισης (obfuscation) πληροφορίας, ή αλλιώς γενίκευσης (generalization) είναι τεχνική που οδηγεί στην μεγιστοποίηση της χρησιμότητας των δεδομένων και παράλληλα ελαχιστοποιεί την αποκάλυψη ευαίσθητων προσωπικών

δεδομένων των χρηστών. Η δυνατότητα ενός χρήστη να αποκρύψει την πραγματική τιμή μιας πληροφορίας αντικαταστώντας την με μία πιο γενική τιμή λιγότερης ακρίβειας είναι πολύ ευνοική. Τα μοντέλα ελέγχου πρόσβασης (access control models) μπορούν επαρκώς να υποστηρίξουν τον προσδιορισμό και επιβολή πολιτικών προστασίας της ιδιωτικότητας. Ένα λειτουργικό στοιχείο ενός τέτοιου μοντέλου είναι η απόφαση πρόσβασης να μην είναι απλά θετική ή αρνητική όπως σε ένα κλασικό μοντέλο ελέγχου πρόσβασης (access control), αλλά να βασίζεται στην ερώτηση "πόση πληροφορία επιτρέπεται για τον συγκεγκριμένο χρήστη" έναντι του "αν η πληροφορία επιτρέπεται ή όχι". Είναι εδώ που εμφανίζεται ο μηχανισμός συσκότισης της πληροφορίας που λειτουργεί βάσει των επιλογών και απαιτήσεων του κατόχου δεδομένων αντίστοιχα για τα δεδομένα που συνθέτουν το αίτημα πρόσβασης.

Ένα άλλο ζήτημα που συχνά τα συστήματα κανόνων είναι πιθανό να αντιμετωπίζουν είναι οι συγκρούσεις μεταξύ κανόνων, δηλαδή τι γίνεται όταν διαφορετικοί κανόνες μπορούν να εφαρμοστούν ταυτόχρονα και κυρίως όταν αυτοί οδηγούν σε συγκρουόμενα αποτελέσματα. Το πρόβλημα αυτό όπως είδαμε φαίνεται να απασχόλησε κάποιες από τις προσεγγίσεις διαφύλαξης της ιδιωτικότητας. Η επίλυση τέτοιων συγκρούσεων εξαρτάται σε μεγάλο βαθμό από την επικάλυψη της σημασιολογίας των κανόνων. Μία προσέγγιση εξωμάλυνσης του προβλήματος θα μπορούσε να ήταν η κατηγοριοποίηση των κανόνων έτσι ώστε μέσω αυτής να αντανακλάται εν μέρει η διαφορετική τους σημασιολογία και η εφαρμογή τους σε διαφορετικές φάσεις της ροής του συστήματος.

Ένα μεγάλο επίσης ερευνητικό θέμα σήμερα είναι οι προκλήσεις που αντιμετωπίζονται στην αναπαράσταση της πληροφορίας πλαισίου χρήσης. Οι οντολογίες είναι κοινά αποδεκτό ότι αποτελούν ένα από τα καλύτερα και ισχυρότερα μέσα αναπαράστασης γνώσης. Στα περιβάλλοντα διάχυτου υπολογισμού οι οντολογίες χρησιμοποιούνται για να χαρακτηρίσουν τις κύριες έννοιες ενός τέτοιου περιβάλλοντος, να αντιμετωπίσουν ζητήματα που αφορούν την επίγνωση του πλαισίου, την ανακάλυψη υπηρεσιών και την διαλειτουργικότητα μεταξύ διαφορετικών οντοτήτων. Μία καλώς ορισμένη δηλωτική σημασιολογία μέσω οντολογιών παρέχει μέσα σε έξυπνους πράκτορες χρηστών (user agents) για την εξαγωγή λογικών συμπερασμάτων αναφορικά με την πληροφορία πλαισίου (contextual information). Η οντολογία αποτελεί επίσης τον φορμαλιστικό

ορισμό των κανόνων πρόσβασης και απαιτήσεων των χρηστών. Επιβάλλεται η ανάγκη να μοντελοποιηθεί ένα περιβάλλον διάχυτου υπολογισμού με τέτοιο τρόπο ώστε να υπάρξει σημασιολογική ομοιογένεια μεταξύ των πόρων, που θα διευκολύνει αυτοματοποιημένες διαδικασίες και επιβολή μηχανισμών για έλεγχο προστασίας της ιδιωτικότητας τόσο των χρηστών όσο και των υπόλοιπων πόρων του συστήματος.

Βιβλιογραφία

[1] Abowd, G.D., Dey, A.K., Orr, R., Brotherton, J. (1997). "Context-Awareness in Wearable and Ubiquitous Computing", 1st International Symposium on Wearable Computers, pp.179-180.

[2] M.Ackerman, T.Darrell, D.J.Weitzner. (2001). "Privacy in Context", *Human-Computer Interaction*, Vol.16, pp.167-176.

[3] C.Anagnostopoulos, A.Tsounis, S.Hadjiefthymiades. (2006). "Context Awareness in Mobile Computing Environments", Wireless Personal Communications, vol.42, pp.445-464.

[4] S.Bessler, J.Zeiss. (2006). "Semantic Modelling of policies for context-aware services", World Wireless Research Forum (WWRF), 17.Meeting, Heidelberg.

[5] M.Blount, J.Davis, M.Ebling, et al. (2008). "Privacy Engine for Context- aware enterprise application services", IBM T J Watson Research Center and Ling Fling, Inc.

[6] P.J.Brown, J.D.Bovey, X.Chen. (1997). "Context-Aware Applications: From the Laboratory to the Marketplace", IEEE Personal Communications, Vol.4(5), pp. 58-64.

[7] J.Camenisch, E.V.Herreweghen. (2002). "Design and implementation of Idemix Anonymous Credential System", IBM Zurich Research Laboratory.

[8] H.Chen, T.Finin and A.Joshi. (2004). "A pervasive computing ontology for user privacy protection in the context broker architecture", Department of Computer Science & Electrical Engineering, University of Maryland, Baltimore County.

[9] K.Devdatta and T.Anand. (2008). "Context-aware Role-based access control in pervasive computing system", In Proceedings of the 13th ACM Symposium on Access Control models and technologies, New York.

[10] A.K.Dey, G.D.Abowd. (2000). "Towards a better understanding of Context and Context-Awareness", In HUC '99: Proceedings of the 1st International Conference of Human Factors in Computing Systems.

[11] A.A.Eldin, and R.Wagenaar. (2004). "Towards a users driven privacy control", In the IEEE conference on Systems, Man, and Cybernetics.

[12] A.A.Eldin, R.Wagenaar. (2006). "A Privacy Preferences Architecture for Context aware applications", In proceedings of the IEEE International Conference on Computer Systems and Applications, pp.110-113.

[13] D.F.Ferraiolo and D.R.Kuhn. (1992). Role-Based Access Controls, 15th National Computer Security Conference, Baltimore, pp.554-563.

[14] D.F.Ferraiolo, R.Sandhu, S.Gavrila, et al. (2001). "Proposed NIST Standard for Role-Based Access Control", ACM Transactions on Information and System Security, Vol.4, No. 3.

[15] F.Fransen, E.Olk, S.Lachmund, L.Bussard. (2006). "An Infrastructure for Gaining Trust in Context Information", In proceedings of the Workshop on The Value of Security through Collaboration at IEEE SECURECOMM conference, Baltimore, MD, USA.

[16] T.Heiber, P.J.Marron. (2005). "Exploring the relationship between context and privacy", In proceedings of the Workshop on Security and Privacy in Pervasive Computing.

[17] U.Hengartner and P.Steenkiste. (2003). "Protecting access to people location information", In proceedings of the 1st International Conference of Security in Pervasive Computing, pp.25-38

[18] P.Jagtap, A.Joshi, T.Finin, L.Zavala. (2011). "Preserving Privacy in Context-aware systems", In proceedings of the 5th IEEE International Conference on Semantic Computing.

[19] M.Langheinrich, "Privacy in Ubiquitous Computing", in *Ubiquitous Computing*, J.Krumm, Ed.: Chapman&Hall / CRC Press, 2009, Chapter 3.

[20] M.Langheinrich, "Privacy Invasions in Ubiquitous Computing", In proceedings of the Workshop on Socially-Informed Design of Privacy-Enhancing Solutions (Ubicomp 2002).

[21] M.Li, X.Sun, H.Wang, Y.Zhang, Ji Zhang. (2011). "Privacy-aware access control with trust management in web service", World Wide Web, Vol.14 (4), pp.407-430.

[22] A.Lysyanskayal, et al. (1999) Pseudonym Systems. In the sixth Annual Workshop on selected areas in Cryptography: Springer-Verlag LNCS.

[23] A.Mitseva, M.Imine, N.R.Prasad. (2006). "Context-Aware Privacy Protection with Profile Management", WMASH '06 Proceedings of the 4th International Workshop on Wireless mobile applications and services on WLAN hotspots, pp.53-62.

[24] Q.Ni, E.Bertino, A.Trombetta, J.Lobo. (2007). "Privacy-aware Role Based Access Control", In proceedings of the 12th ACM Symposium on Access Control models and technologies, ACM Press, France.

[25] Q.Ni, D.Lin, E.Bertino, J.Lobo. (2007). "Conditional Privacy-Aware Role Based Access Control", In proceedings of the 12th European Symposium on Research in Computer Security, Vol.4734, pp.72-89, Germany.

[26] P.Osbakk and N.Ryan. (2003). "A privacy enhancing infrastructure for context-awareness", The Kent UbiComp Group, University of Kent.

[27] S.H.Park, Y.J.Han, and T.M.Chung. (2006). "Context-Role Based Access Control for Context-Aware Application", In High Performance Computing and Communications, LNCS, vol.4208, pp.572-580.

[28] T. Strang and C. Linhoff- Popien. (2004). "A context modeling survey", Proceedings of UbiComp: 1st International Workshop on Advanced Context Modeling, Reasoning and Management.

[29] A.Talukder and R.Yavagal. (2005). Mobile Computing, McGraw-Hill, pp.7-10.

[30] E.I.Tatli. (2006). "Context Data Model for Privacy", PRIME Standardization Workshop, IBM Zurich Research Center.

[31] E.I.Tatli. (2006). "Privacy in context-aware mobile business applications", PRIME Standardization Workshop, IBM Zurich Research Center.

[32] W.Wagealla, S.Terzis, C.English. (2003). "Trust-based model for privacy control in context-aware systems", In 2nd Workshop on Security in Ubiquitous Computing at the 5th Annual Conference on Ubiquitous Computing (UbiComp2003), Washington, USA.

[33] M.Weiser, J.S.Brown. (1995). *Designing Calm Technology*. Xerox PARC.

[34] M.Weiser. (1991). The computer for the 21st century. *Scientific American*, pp.66- 75.

[35] A.Westin. (1967). "Privacy and Freedom", Atheneum, New York.

[36] R.Wishart, K.Henricksen and J.Indulska. (2005). "Context obfuscation for privacy via ontological descriptions", In Proceedings of the 1st International Workshop on Location and Context-Awareness, Germany, pp.276-288.

[37] R.Wishart, K.Henricksen and J.Indulska. (2007). "Context Privacy and Obfuscation supported by dynamic context source discovery and processing in a context management system", In Proceedings of the 4th International Conference on Ubiquitous Intelligence and Computing, Hong Kong.

[38] N.Zhang, C.Todd. (2009). "Developing a privacy ontology for privacy control in context-aware systems", Department of Electronic & Electrical Engineering, University College London.

[39] A.Schmidt, M.Beigl et al. (1999). "There is more to context than location", Computers and Graphics, 23(6), pp. 893-901.

[40] H.Chen, T.Finin and A.Joshi. (2004). "An ontology for context-aware pervasive computing environments", Special Issue on Ontologies for Distributed Systems, Knowledge Engineering Review, 18(3), pp. 197-207.

[41] The World Wide Web Consortium (W3C), The Platfrom for Privacy Preferences (P3P) Project, online: http://www.w3c.org/P3P.

[42] A P3P Preference Exchange Language (APPEL), http://www.w3.org/TR/P3P-preferences , World Wide Web Consortium (W3C).

[43] "The ISO 29100 Privacy Principles", pp.12-15, 2008.

[44] The enterprise privacy authorization language (epal 1.1). IBM Zurich Research Laboratory, Switzerland, http://www.zurich.ibm.com/security/enterprise-privacy/epal/Specification.

[45] OASIS, "eXtensible Access Control Markup Language (XACML) Version 2.0", February 2005, http://docs.oasis-open.org/xacml/2.0/.

[46] OASIS, "eXtensible Access Control Markup Language (XACML) Version 1.0", February 2003, http://www.oasis-open.org/committes/xacml/repository/.

[47] OWL, http://www.w3.org/TR/owl-features/.

[48] Jena, http://jena.sourceforge.net/inference/.

[49] OECD Guidelines, http://oecdprivacy.org/.

[50] Notation 3 Logic (N3), http://www.w3.org/DesignIssues/Notation3.html.