Ατομική Διπλωματική Εργασία

ΑΝΑΛΥΣΗ ΓΛΩΣΣΩΝ ΠΟΛΙΤΙΚΩΝ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Αλέξια Ιωακείμ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2014

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΝΑΛΥΣΗ ΓΛΩΣΣΩΝ ΠΟΛΙΤΙΚΩΝ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Αλέξια Ιωακείμ

Επιβλέπουσα Καθηγήτρια
Άννα Φιλίππου

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

Μάιος 2014

Ευχαριστίες

Η παρούσα διπλωματική εργασία σηματοδοτεί το τέλος του κύκλου της πανεπιστημιακής μου ζωής στο Πανεπιστήμιο Κύπρου ως προπτυχιακή φοιτήτρια. Στο σημείο αυτό αισθάνομαι έντονα την ανάγκη να εκφράσω τις θερμές μου ευχαριστίες στα άτομα που συνέβαλαν στο να ολοκληρώσω αυτό το σημαντικό κεφάλαιο της ζωής μου.

Πρώτα απ' όλα, θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτριά μου Κ. Άννα Φιλίππου, για τη συνεργασία που είχαμε, που μου εμπιστεύτηκε την παρούσα διπλωματική και που με στήριζε και με βοηθούσε όποτε τη χρειαζόμουν.

Επίσης, θεωρώ πως οφείλω και είναι υποχρέωσή μου να ευχαριστήσω όλους εκείνους που στάθηκαν δίπλα μου αυτά τα τέσσερα χρόνια, μου έμαθαν να ξεπερνώ τις δυσκολίες και να μην τα παρατώ εύκολα. Ευχαριστώ πολύ τους φίλους μου για την κατανόησή τους και την ηθική υποστήριξη που μου παρείχαν, ιδιαίτερα κατά τη διάρκεια των τελευταίων μηνών της προσπάθειάς μου. Πάνω απ' όλα όμως, θα ήθελα να εκφράσω την ευγνωμοσύνη μου στην οικογένειά μου. Θέλω να ευχαριστήσω θερμά τους γονείς μου, καθώς και τον αδερφό μου, για την ολόψυχη αγάπη και στήριξη που μου παρείχαν όλο αυτό το διάστημα, χωρίς την οποία τίποτα δε θα κατάφερνα.

Σε αυτούς που με τη συνεχή συμπαράστασή τους, τη θετική τους σκέψη και την πίστη τους σε εμένα, συνέβαλαν στην εκπλήρωση των στόχων μου, αφιερώνεται η εργασία αυτή. Χρωστάω σε όλους ένα μεγάλο ευχαριστώ.

Ευχαριστώ,
Αλέξια Ιωακείμ

Περίληψη

Ένα αδιαμφισβήτητο γεγονός που παρατηρείται στις μέρες μας είναι βεβαίως, η ραγδαία ανάπτυξη της τεχνολογίας. Σίγουρα η ανάπτυξη αυτή, παίζει σημαντικό ρόλο στην ζωή του σύγχρονου ανθρώπου και έχει σίγουρα καταφέρει σημαντικά επιτεύγματα στον κόσμο γενικά και την εξέλιξη του πολιτισμού. Όμως, με την ραγδαία αυτή εξέλιξη της τεχνολογίας και του διαδικτύου γενικότερα, βγαίνουν στην επιφάνεια πολλά θέματα που σχετίζονται με την προστασία των προσωπικών δεδομένων των χρηστών και γενικά με την ικανότητα διασφάλισης της ιδιωτικότητας τους.

Ένα από τα σημαντικότερα θέματα που πρέπει να αφορά τον καθένα μας σήμερα, είναι ο τρόπος με τον οποίο μπορούμε να διαφυλάξουμε τις προσωπικές μας πληροφορίες. Γενικά, παρατηρείται ότι αρκετός κόσμος φοβάται και σκέφτεται πριν δώσει πληροφορίες ή δεδομένα σε ένα ιστότοπο γιατί πιστεύει πως θα γίνει καταπάτηση των προσωπικών του δεδομένων και πληροφοριών. Έτσι λοιπόν, είναι πολύ σημαντική η ικανότητα ύπαρξης ελέγχου της ιδιωτικότητας και του σωστού χειρισμού των δεδομένων που συλλέγονται.

Στην παρούσα διπλωματική εργασία, μελετούμε την έννοια της ιδιωτικότητας και των παραβιάσεων που μπορούν να προκύψουν. Συγκεκριμένα ασχολούμαστε με την μελέτη των γλωσσών πολιτικών ιδιωτικότητας και το πώς απαιτήσεις και περιορισμοί που αφορούν την ιδιωτικότητα μπορούν να διατυπωθούν, να αναπτυχθούν και να εφαρμοστούν, με σκοπό να διασφαλίζεται η προστασία των δεδομένων και να αποτρέπονται όσο περισσότερες παραβιάσεις γίνεται.

Στόχος της διπλωματικής εργασίας, είναι η μελέτη κάποιων γλωσσών πολιτικών ιδιωτικότητας και των χαρακτηριστικών τους, έτσι ώστε να αξιολογηθούν η κάθε μια ξεχωριστά για το τι μπορεί να κάνει, αλλά και να γίνει σύγκριση της μιας με την άλλη. Ακολούθως, γίνεται και μια ανασκόπηση της πολιτικής που χρησιμοποιείται στις υπηρεσίες κοινωνικής δικτύωσης, Facebook και Twitter και γίνεται μια αναφορά στο πώς οι γλώσσες που μελετήθηκαν σχετίζονται με τις πολιτικές αυτές.

Περιεχόμενα

ΚΑΤΑΛΟΓΟΣ ΜΕ ΣΧΗΜΑΤΑ

ΚΑΤΑΛΟΓΟΣ ΜΕ ΠΙΝΑΚΕΣ

Κεφάλαιο 1

Εισαγωγή

1.1 Κίνητρα

Είναι πλέον γεγονός πως με την περιδιάβασή μας στο διαδίκτυο, πολλές φορές μας ζητείται να δώσουμε προσωπικές μας πληροφορίες για την διεκπεραίωση διαφόρων ενεργειών. Οι πληροφορίες αυτές, μαζεύονται σταδιακά και σιγά σιγά μπορούν να συνδυαστούν και να προκύψει η εικόνα μας. Έτσι, προκύπτουν σοβαρά θέματα όπως η προστασία των προσωπικών μας δεδομένων, ο χειρισμός των πληροφοριών που συλλέγονται, η ηθική και ορθή επικοινωνία μέσω της τεχνολογίας και το γεγονός πως με την περιδιάβασή μας στο διαδίκτυο, πιθανόν να αφήσουμε ίχνη.

Στέλνοντας ηλεκτρονικά μηνύματα, θέλοντάς το ή μη, σίγουρα παρέχουμε πληροφορίες στο άτομο με το οποίο επικοινωνούμε. Όμως, αν δεν είμαστε προσεκτικοί, πολύ πιθανόν οι πληροφορίες μας να διαρρεύσουν και να τις παραλάβει οποιοσδήποτε βρίσκεται στην διαδρομή του μηνύματος που στέλνουμε προς τον παραλήπτη.

Επίσης, κοινωνικά δίκτυα όπως το Facebook και το Twitter, μας παρέχουν την δυνατότητα αποστολής φωτογραφιών, δημοσίευσης προσωπικών καταστάσεων και την ανταλλαγή απόψεων και προσωπικών πληροφοριών. Οι χρήστες συνηθίζουν να δημοσιεύουν τις σκέψεις τους, το τι κάνουν και πολλές φορές μπορεί οι πληροφορίες που δίνουν να παραληφθούν από κακόβουλους χρήστες.

Ακόμη, πολλές ιστοσελίδες που επισκεπτόμαστε, κρατούν δεδομένα για την επίσκεψή μας στον υπολογιστή, για να τα χρησιμοποιήσουν στο μέλλον. Τα δεδομένα αυτά είναι γνωστά ως "Cookies" και είναι μικρά κομμάτια από πληροφορίες όπως το όνομα χρήστη, προτιμήσεις που μπορεί να δηλώνει και λοιπά. Πολλές εταιρείες που είναι νόμιμες, κρατάνε τα Cookies για να τα χρησιμοποιήσουν και να κάνουν προσφορές σε χρήστες που τους επισκέπτονται ξανά. Υπάρχουν όμως και οι παράνομες εταιρείες, που κρατούν τα Cookies για να τα χρησιμοποιούν έτσι ώστε να παίρνουν πληροφορίες για τους χρήστες και να τις πουλούν σε εταιρείες που σκοπός τους είναι το εμπόριο και θέλουν να ξέρουν τι αρέσει στους χρήστες για να είναι πιο αποτελεσματικές.

Η διαφύλαξη των προσωπικών όσο και των επαγγελματικών πληροφοριών είναι απαραίτητη ειδικά σήμερα που η τεχνολογία αναπτύσσεται συνεχώς. Κανείς δεν μπορεί να αμφισβητήσει ότι η ραγδαία ανάπτυξη της τεχνολογίας και κυρίως του διαδικτύου, φέρνει στην επιφάνεια πολλά θέματα σχετικά με την προστασία των προσωπικών δεδομένων των χρηστών και το δικαίωμα προστασίας της ιδιωτικότητας τους.

Με την αύξηση της χρήσης του διαδικτύου και την αύξηση της απευθείας σύνδεσης μέσω του διαδικτύου (online) με μια επιχείρηση, οι καταναλωτές αναμένουν υψηλά επίπεδα προστασίας της ιδιωτικής τους ζωής. Συχνά παρατηρούνται καταγγελίες πολιτών ενάντια σε ιστοσελίδες κοινωνικής δικτύωσης και άλλων οργανισμών στο διαδίκτυο, που αφορούν τη συγκέντρωση και χρήση προσωπικών πληροφοριών για εμπορικούς σκοπούς. Όπως ανέφερα και προηγουμένως, πολλές εταιρείες αποθηκεύουν τις δράσεις των χρηστών με σκοπό να τους προωθούν κατάλληλες διαφημίσεις. Με τον τρόπο αυτό οι εταιρείες επωφελούνται, αλλά οι χρήστες δυσαρεστούνται γιατί αντιλαμβάνονται πως με το να λαμβάνουν διαφημίσεις σχετικά με τις προτιμήσεις και τα ενδιαφέροντα τους, σημαίνει πως οι πληροφορίες που έδωσαν μέχρι τώρα στην εταιρεία είναι αποθηκευμένες και τις χρησιμοποιούν εν αγνοία τους.

Οι καταναλωτές αναφέρουν συχνά την έλλειψη εμπιστοσύνης ως ένα από τους λόγους για τους οποίους δεν κάνουν αγορές από το διαδίκτυο. Από την πλευρά του οργανισμού, η ανάγκη για την προστασία της ιδιωτικής ζωής των καταναλωτών και η συμμόρφωση με τη νομοθεσία προστασίας της ιδιωτικής ζωής, είναι μια αυξανόμενη ανησυχία. Εάν οι οργανισμοί δεν ακολουθούν αποτελεσματικές πρακτικές προστασίας

προσωπικών δεδομένων, οι καταναλωτές μπορούν να φύγουν από αυτούς και επίσης, προβλήματα με τον νόμο μπορεί να προκύψουν.

Έτσι, η επισημοποίηση των υποσχέσεων ενός οργανισμού σχετικά με τις πρακτικές προστασίας της ιδιωτικής ζωής είναι μια σημαντική πτυχή για τη διαχείριση των σχέσεων με τους πελάτες. Οργανισμοί εκφράζουν εσωτερικές πρακτικές προστασίας της ιδιωτικής ζωής ως δηλώσεις στις πολιτικές προστασίας της ιδιωτικής ζωής και οι καταναλωτές είναι σε θέση να αναλύουν τη δεδηλωμένη δέσμευση του οργανισμού για την προστασία της ιδιωτικής τους ζωής μέσα από αυτές τις πολιτικές προστασίας.

Έχοντας υπόψη όλα αυτά που απασχολούν τους χρήστες και τους οργανισμούς, σε αυτήν την διπλωματική εργασία, θα επικεντρωθούμε στην μελέτη των γλωσσών πολιτικών ιδιωτικότητας που προσφέρονται και στο τι κάνει και πώς λειτουργεί η κάθε μια με σκοπό την προστασία της ιδιωτικότητας. Θα μας απασχολήσει επίσης και η μελέτη παραβιάσεων ιδιωτικότητας και πώς μπορούμε να τις ελέγχουμε μέσω πολιτικών.

1.2 Σκοπός

Στην παρούσα διπλωματική εργασία μελετούμε την έννοια της ιδιωτικότητας και των παραβιάσεων που μπορούν να προκύψουν. Συγκεκριμένα ασχολούμαστε με την μελέτη των γλωσσών πολιτικών ιδιωτικότητας και το πώς απαιτήσεις και περιορισμοί που αφορούν την ιδιωτικότητα μπορούν να διατυπωθούν, να αναπτυχθούν και να εφαρμοστούν, με σκοπό να διασφαλίζεται η προστασία των δεδομένων και να αποτρέπονται όσο περισσότερες παραβιάσεις γίνεται.

Στόχος της διπλωματικής εργασίας, είναι η μελέτη κάποιων γλωσσών πολιτικών ιδιωτικότητας και των χαρακτηριστικών που έχει η κάθε μια, για να δούμε πώς ακριβώς διαχειρίζονται τις παραβιάσεις ιδιωτικότητας που υπάρχουν, αλλά και γενικά πώς χειρίζονται την ιδιωτικότητα. Συγκεκριμένα θα ασχοληθούμε με τις πολιτικές P3P, EPAL και XACML, θα τις αξιολογήσουμε και θα τις συγκρίνουμε. Σκοπός μας είναι να δούμε τι προσφέρει η κάθε μια, πώς λειτουργεί και μέσα από τις συγκρίσεις να βγάλουμε κάποια συμπεράσματα για το ποιες δυνατότητες και περιορισμούς έχει η

κάθε γλώσσα, όσον αφορά την προστασία της ιδιωτικότητας και τον έλεγχο προσβασιμότητας.

1.3 Δομή Εργασίας

Η παρούσα πτυχιακή εργασία αποτελείται από 5 κεφάλαια. Στο Κεφάλαιο 2, γίνεται αναφορά στην έννοια της ιδιωτικότητας, όπου μελετούνται οι παραβιάσεις ιδιωτικότητας που υπάρχουν με βάση την ταξινόμηση της ιδιωτικότητας από τον Daniel J.Solove. Στο Κεφάλαιο 3, γίνεται αναφορά στις γλώσσες πολιτικών Ιδιωτικότητας P3P, EPAL και XACML. Στο Κεφάλαιο 4, γίνεται η αξιολόγηση της κάθε πολιτικής και οι συγκρίσεις ανά μεταξύ τους. Γίνεται και μια μελέτη που αφορά τις πολιτικές ιδιωτικότητας των κοινωνικών δικτύων Facebook και Twitter, για να δούμε αν και πώς οι γλώσσες που μελετήσαμε μπορούν να συσχετιστούν με τις πολιτικές αυτές και κατά πόσον συνεισφέρουν στην βελτίωση τους. Τέλος στο Κεφάλαιο 5, υπάρχουν τα συμπεράσματα που προκύπτουν από την αξιολόγηση και σύγκριση των γλωσσών, καθώς και η μελλοντική εργασία που μπορεί να γίνει.

Κεφάλαιο 2

Ιδιωτικότητα και παραβιάσεις Ιδιωτικότητας

2.1 Εισαγωγή στην Ιδιωτικότητα

Η χρήση του διαδικτύου είναι συναρπαστική. Όλο και περισσότερος κόσμος καθημερινά εξοικειώνεται με τη χρήση του και ενθουσιάζεται με τα πόσα πολλά πράγματα του προσφέρονται τόσο απλά στο διαδίκτυο. Μέσω των δυνατοτήτων που μας παρέχει, ανοίγεται ένας ολόκληρος κόσμος νέων εμπειριών σε χώρες, γλώσσες, πολιτισμούς και πληροφορίες. Παρατηρείται, πως η δραστηριοποίησή μας στο διαδίκτυο έχει πολλά κοινά με τη ζωή μας στο φυσικό κόσμο. Επακόλουθο της εξέλιξης και της μεγάλης χρήσης του διαδικτύου, είναι να προκύπτουν σοβαρά θέματα όπως η προστασία των προσωπικών μας δεδομένων, ο χειρισμός των πληροφοριών που συλλέγονται, η ηθική και ορθή επικοινωνία μέσω της τεχνολογίας και το γεγονός πως με την περιδιάβασή μας στο διαδίκτυο, πιθανόν να αφήσουμε ίχνη.

Ουσιαστικά, ιδιωτικότητα σημαίνει ατομικότητα. Ο κάθε χρήστης του διαδικτύου πρέπει να έχει την δυνατότητα να έχει μια συγκεκριμένη προσωπικότητα που να είναι σεβαστή και να προστατεύει το σύνολο της διαδικτυακής του παρουσίας από τυχόν παραβιάσεις της ιδιωτικής του ζωής. Πρέπει να μπορεί να τον προστατεύει από

κακόβουλες ενέργειες και να απαγορεύεται η οποιαδήποτε δευτερεύουσα χρήση των πληροφοριών που αναπόφευκτα παράγονται κατά την περιδιάβασή του στο διαδίκτυο.

Η ιδιωτικότητα για πολύ καιρό ήταν ένα από τα μεγαλύτερα ζητήματα που απασχολούσαν κοινωνικούς επιστήμονες, δικηγόρους και φιλοσόφους. Με την άφιξη των υπολογιστών στην ζωή μας και την αύξηση των δραστηριοτήτων και ικανοτήτων στα σύγχρονα πληροφοριακά συστήματα και δίκτυα επικοινωνίας, εγείρονται σημαντικά θέματα ιδιωτικότητας. Η προσωπική ιδιωτικότητα, στην σύγχρονη εποχή που ζούμε, κινδυνεύει όλο και περισσότερο, ειδικότερα τώρα που οδεύουμε σε μια παγκόσμια κοινωνία πληροφοριών.

Η ιδιωτικότητα για να κατανοηθεί και να οριστεί πρέπει να λάβεις υπόψη σου την κοινωνία και τους εξωτερικούς παράγοντες γενικότερα. Τα όρια της ιδιωτικότητας ορίζονται από τα πιστεύω και τις αντιλήψεις της εποχής και τα ήθη μιας κοινωνίας, παράγοντες που αλλάζουν συνεχώς. Μια κοινωνία είναι γεμάτη από συγκρούσεις και τριβές. Με την προστασία της ιδιωτικότητας επικρατεί μια ανακούφιση από όλα αυτά. Πολλές φορές όμως, δεν σημαίνει ότι όταν μια πράξη είναι επιβλαβής ή προβληματική, αυτόματα πρέπει να υπάρξει νομική παρέμβαση για να την σταματήσουν. Μπορεί ο νόμος να μην μπορεί να επέμβει ή μπορεί τα συμφέρονται να είναι αντίθετα. Υπάρχουν σίγουρα στιγμές που οι ανθρώποι πρέπει να λογοδοτήσουν για τις ιδιωτικές τους δραστηριότητες.

Η ιδιωτικότητα και κατ' επέκταση η προστασία προσωπικών δεδομένων είναι ένα σημαντικό δικαίωμα, διότι είναι προϋπόθεση για άλλα δικαιώματα, όπως η ελευθερία και η προσωπική αυτονομία. Συνεπώς, υπάρχει μια σχέση μεταξύ της προστασίας της ιδιωτικής ζωής, της ελευθερίας και της ανθρώπινης αξιοπρέπειας. Σεβασμός της ιδιωτικής ζωής ενός ατόμου είναι να αναγνωριστεί το δικαίωμα ενός τέτοιου ατόμου στην ελευθερία και να αναγνωριστεί ότι το άτομο αυτό είναι αυτόνομο ανθρώπινο ον. Η υποχρέωση για σεβασμό της ιδιωτικής ζωής ενός ατόμου είναι καθήκον για όλους μας. Η ιδιωτικότητα διατυπώνεται ως δικαίωμα, συχνά συνδεδεμένο με το δικαίωμα της προσωπικότητας.

Η λέξη ιδιωτικότητα προέρχεται από την λατινική λέξη "privatus" και ερμηνεύεται ως την απομόνωση από τους άλλους ή τον περιορισμό κατά την εκτέλεση μιας εργασίας. Γενικά, η έννοια της ιδιωτικότητας χωρίζεται σε τρεις μορφές: Την Εδαφική Ιδιωτικότητα, που αφορά την προστασία της στενής φυσικής περιοχής που περιβάλλει ένα πρόσωπο, δηλαδή οικιακά και άλλα περιβάλλοντα όπως ο εργασιακός ή ο δημόσιος χώρος, την Ιδιωτικότητα του Ατόμου, που αφορά την προστασία ενός προσώπου από την αδικαιολόγητη παρέμβαση, όπως ο σωματικός έλεγχος, η δοκιμή φαρμάκων ή οι πληροφορίες που παραβιάζουν την ηθική αίσθηση του ατόμου και την Πληροφοριακή Ιδιωτικότητα, που αφορά τον έλεγχο του αν και πώς τα προσωπικά στοιχεία μπορούν να συγκεντρωθούν, να αποθηκευτούν, να υποστούν επεξεργασία ή να διαδοθούν επιλεκτικά.

Αρχικά δόθηκε το 1980 μια διατύπωση από δύο έγκριτους νομικούς, τους Samuel Warren και Louis Brandeis, που αναφέρουν ότι το πιο σημαντικό δικαίωμα είναι η διασφάλιση της ασφάλειας του ατόμου, αλλά και το πώς αυτή πρέπει να διασφαλιστεί. Έκαναν το άρθρο "The Right to Privacy" [24] και χρησιμοποίησαν την φράση "the right to be left alone" (το δικαίωμα να μείνεις μόνος), για να περιγράψουν το δικαίωμα στην ιδιωτικότητα του ατόμου. Το 1960 έχουμε τον νομικό William Prosser, που έκανε το σύγγραμμα "Privacy" [30] όπου παρουσιάζει ένα σύνολο από νομοθετικούς κανόνες για διασφάλιση της ιδιωτικότητας του ατόμου και νομικά. Το 1967 έχουμε τον Alan Westin, που έγραψε το βιβλίο "Privacy and Freedom" [2], στο οποίο ενισχύει την ανάγκη για θεσμοθέτηση και ενδυνάμωση του ορισμού της ιδιωτικότητας. Στον ορισμό που μας δίνει ο Westin για την ιδιωτικότητα αναφέρει ότι η ιδιωτικότητα καταπατείται μέσω διάφορων μορφών παρακολούθησης που αρχικά καταγράφονται προσωπικές πληροφορίες και στη συνέχεια δημοσιεύονται χωρίς τη συγκατάθεση του ατόμου. Ακόμη αναφέρει ότι ο κάθε άνθρωπος έχει την ανάγκη για ιδιωτική ζωή και αναφέρεται σε διάφορες μεθόδους που χρησιμοποιούν τα άτομα για να αποτρέψουν την παραβίαση της ιδιωτικής τους ζωής. Η πιο πρόσφατη συμβολή για τον τομέα αυτό γίνεται το 2006 από τον Daniel Solove, ο οποίος παρουσιάζει μια ταξινόμηση [5] για την καλύτερη κατανόηση των δυνατών παραβιάσεων στην ιδιωτικότητα, εμπλουτίζοντας το νομικό πλαίσιο στα πλαίσια της τεχνολογικής ανάπτυξης.

2.2 Η ταξινόμηση της ιδιωτικότητας από τον Daniel J.Solove

Ο Daniel J.Solove μέσα από την ταξινόμηση που δίνει ταξινομεί τις δυνατές παραβιάσεις που υπάρχουν. Η ταξινόμηση της ιδιωτικότητας όπως προτάθηκε από τον Solove [5], αποτελείται από 4 βασικές ομάδες : την συλλογή της πληροφορίας, την επεξεργασία της πληροφορίας, την μεταβίβαση της πληροφορίας και την εισβολή της πληροφορίας.

2.2.1 Η συλλογή της πληροφορίας

Η πρώτη ομάδα είναι η συλλογή πληροφοριών που μπορεί να προκαλέσει αρκετά προβλήματα έστω και αν αυτές οι πληροφορίες δεν αποκαλυφθούν σε άλλα άτομα. Έστω και αν τα δεδομένα δεν αποκαλυφθούν σε τρίτα πρόσωπα, η ίδια η διαδικασία και μόνο μπορεί να προκαλέσει επώδυνες καταστάσεις.

Η συλλογή πληροφοριών μπορεί να γίνει είτε με παρακολούθηση όπου είναι μια συνεχής επιτήρηση του ατόμου, είτε με ανάκριση όπου γίνονται διάφορες ερωτήσεις στο άτομο για να ανακτηθούν οι πληροφορίες.

Η παρακολούθηση (surveillance), είναι η επιτήρηση που προϋποθέτει παρατήρηση, ακρόαση και καταγραφή των κινήσεων ενός ατόμου. Πολλές φορές έχουμε ακούσει ή δει κάτι που οι άλλοι ίσως να μην θέλουν αλλά δεν το θεωρήσαμε ως πρόβλημα. Όταν όμως η παρακολούθηση γίνεται με συγκεκριμένο τρόπο και συνέχεια, έχουμε προβληματικές συνέπειες. Δημιουργούνται στον άνθρωπο συναισθήματα άγχους και δυσφορίας. Κάνουν το άτομο να νιώθει άβολα αλλά και να αλλάζει την συμπεριφορά του.

Η ανάκριση (interrogation), αποτελείται από διάφορες μορφές εξέτασης, έρευνας πληροφοριών. Πιέζουν τα άτομα να αποκαλύψουν πληροφορίες. Η ανάκριση κάνει τους ανθρώπους να ανησυχούν για το πώς θα απαντήσουν για να εξηγήσουν ή για το πώς η άρνησή τους να απαντήσουν θα φανεί στους άλλους. Επίσης με την ανάκριση μπορούμε να καταλήξουμε και στην παραμόρφωση πληροφοριών. Ο ανακριτής μπορεί

με τον τρόπο του να πάρει τη συζήτηση εκεί που θέλει για να δημιουργήσει τις εντυπώσεις και τα συμπεράσματα που θέλει.

2.2.2 Η επεξεργασία της Πληροφορίας

Η δεύτερη ομάδα είναι η επεξεργασία της πληροφορίας όπου οι πληροφορίες που πάρθηκαν από την πρώτη ομάδα αποθηκεύονται, επεξεργάζονται και χρησιμοποιούνται. Μορφές επεξεργασίας πληροφορίας είναι η συσχέτιση, η ταύτιση, η μη επαρκής παροχή ασφάλειας, η δευτερογενής χρήση και ο αποκλεισμός.

Η συσχέτιση (aggregation) περιλαμβάνει τον συσχετισμό διάφορων δεδομένων που αφορούν ένα άτομο. Είναι η συγκέντρωση πληροφοριών για ένα άτομο. Αυτό κάνει και η Amazon για παράδειγμα. Συλλέγει δεδομένα και πληροφορίες από τις αγορές που έκανε κάποιο άτομο και βρίσκει τα βιβλία που μπορεί να τον ενδιαφέρουν και τα προτείνει. Όμως για τα άτομα η συσχέτιση των πληροφοριών δεν είναι καλή. Μπορεί με την συσχέτιση να προκύψουν στοιχεία για τα άτομα που δεν ήταν γνωστά. Οι άνθρωποι δίνουν σε διάφορους τόπους λίγα από τα στοιχεία τους και πιστεύουν πως έτσι προστατεύονται, όταν όμως αυτά τα στοιχεία συγχωνευτούν από κοινού, τότε προκύπτουν πολλές περισσότερες πληροφορίες για τη ζωή του ατόμου, χωρίς να το γνωρίζει. Όπως και η επιτήρηση η συσχέτιση είναι ένας τρόπος συλλογής στοιχείων, όμως το κάνει αυτό με το να συνδυάζει διάχυτα κομμάτια πληροφοριών παρά να συλλέγει νέα.

Η ταύτιση (identification), συνδέει πληροφορίες σε συγκεκριμένα άτομα. Η ταύτιση καθιστά τις πληροφορίες ποιο διαθέσιμες και μπορεί να αλλάξει τον τρόπο με τον οποίο ένα άτομο αντιμετωπίζεται. Η ταύτιση μπορεί να εμποδίσει την ικανότητα του ατόμου να είναι ανώνυμος, να ψηφίσει, να μιλήσει ελεύθερα.

Η μη επαρκής παροχή ασφάλειας (Insecurity), αναφέρεται στην αφελή προστασία αποθηκευμένων δεδομένων από την πιθανότητα απώλειας πληροφοριών. Κάνει τις πληροφορίες διαθέσιμες σε αυτούς που δεν έχουν δικαίωμα πρόσβασης και συχνά οδηγεί σε στρέβλωση των δεδομένων αν τα δεδομένα εισαχθούν λάθος.

Η δευτερογενής χρήση (Secondary use), είναι μια μορφή όπου στοιχεία που έχουν συλλεχθεί για ένα σκοπό στο τέλος χρησιμοποιούνται για κάποιο άλλο σκοπό χωρίς τη συγκατάθεση του εμπλεκόμενου ατόμου. Τα άτομα δίνουν πληροφορίες μόνο για κάποιο συγκεκριμένο σκοπό. Το να χρησιμοποιούν τα δεδομένα αυτά για άλλους σκοπούς χωρίς τα άτομα να το γνωρίζουν, κάνει τα άτομα να μην θέλουν να δίνουν πληροφορίες. Οι δυνατότητες για δευτερεύουσα χρήση δημιουργούν φόβο και αβεβαιότητα για το πώς οι πληροφορίες ενός ατόμου θα πρέπει να χρησιμοποιηθούν στο μέλλον, δημιουργώντας ένα αίσθημα αδυναμίας.

Ο αποκλεισμός (exclusion), αφορά την περίπτωση όπου το άτομο για το οποίο πήραμε τις πληροφορίες δεν έχει ιδέα και δεν ξέρει ότι οι άλλοι χειρίζονται τις πληροφορίες του για κάποιο σκοπό. Το πρόβλημα του αποκλεισμού δημιουργείται όταν στους χρήστες δεν παρέχεται η δυνατότητα πρόσβασης, διόρθωσης και ελέγχου των προσωπικών τους δεδομένων. Ο αποκλεισμός όμως των χρηστών προκαλεί προβλήματα, τα οποία σχετίζονται μια τα αισθήματα ανασφάλειας που προκαλούνται από τα συχνά ανεπαρκή επίπεδα ασφάλειας των δεδομένων. Το άτομο αισθάνεται ότι δεν ενημερώνεται για την χρήση των δεδομένων του και θεωρεί ότι είναι εντελώς ανίκανο να κάνει κάτι ώστε να την επηρεάσει.

2.2.3 Η μεταβίβαση της Πληροφορίας

Η τρίτη ομάδα είναι η μεταβίβαση της πληροφορίας, όπου αφορά το πώς οι πληροφορίες που συλλέχθηκαν και επεξεργάστηκαν, τώρα παρέχονται στις διάφορες οντότητες. Μορφές μεταβίβασης της πληροφορίας είναι η παραβίαση απορρήτου, η παράθεση, η έκθεση, η αυξημένη προσβασιμότητα, ο εκβιασμός, η οικειοποίηση και η αλλοίωση.

Η παραβίαση απορρήτου (breach of confidentiality), σπάζει την υπόσχεση να κρατήσει μυστικές κάποιες πληροφορίες για ένα άτομο. Παραβιάζει την εμπιστοσύνη σε μια συγκεκριμένη σχέση. Είναι η αναίρεση μιας υπόσχεσης που έχει δοθεί για την διατήρηση των προσωπικών πληροφοριών ενός ατόμου εμπιστευτικά.

Η παράθεση (disclosure), περιλαμβάνει την αποκάλυψη πληροφοριών σχετικά με κάποιο πρόσωπο που η αποκάλυψη αυτή επηρεάζει τον τρόπο με τον οποίο οι άλλοι συμπεριφέρονται σε αυτό. Αποκαλύπτονται αληθοφανείς πληροφορίες με επιπτώσεις στον τρόπο που αντιμετωπίζεται το άτομο.

Η έκθεση (exposure), είναι η αποκάλυψη προσωπικών πληροφοριών ενός ατόμου με σκοπό να εκτεθεί αρνητικά και να μειωθεί η δημόσια εικόνα του. Οι άνθρωποι με την έκθεση μπορούν να βιώσουν μια σοβαρή και μερικές φορές εξουθενωτική ταπείνωση και απώλεια της αυτοεκτίμησης.

Η αυξημένη προσβασιμότητα (increased accessibility), ενισχύει την δυνατότητα πρόσβασης σε αυστηρώς προσωπικά δεδομένα. Δημιουργεί προβλήματα, όπως η αυξημένη πιθανότητα αποκάλυψης. Οι πληροφορίες μπορούν εύκολα να αξιοποιηθούν για σκοπούς άλλους από εκείνους για τους οποίους προορίζονταν.

Ο εκβιασμός (blackmail), γίνεται σε άτομα για να αποκαλύπτουν προσωπικές τους πληροφορίες. Περιλαμβάνει τον εξαναγκασμό ενός ατόμου, απειλώντας να εκθέσει προσωπικά μυστικά του, αν δεν προσχωρήσει στις απαιτήσεις του εκβιαστή, που συχνά περιλαμβάνουν την καταβολή δωροδοκίας. Με τη μέθοδο του εκβιασμού δέχονται απειλητικά μηνύματα για διάδοση αυστηρών προσωπικών πληροφοριών.

Η οικειοποίηση (Appropriation), είναι η χρήση της ταυτότητας ενός ατόμου με σκοπό να χρησιμοποιήσει τους στόχους και τα συμφέροντα άλλων. Επηρεάζει αρνητικά τον άνθρωπο και τον κάνει να μην μπορεί να παρουσιάσει τον εαυτό του όπως πραγματικά θέλει.

Η αλλοίωση (Distortion), αναφέρεται στην διαστρέβλωση της αλήθειας και την παροχή παραπλανητικών στοιχείων για κάποιο άτομο.

2.2.4 Η εισβολή της Πληροφορίας

Η τέταρτη και τελευταία ομάδα είναι η εισβολή της πληροφορίας όπου αναφέρεται στη παραβίαση των προσωπικών πληροφοριών ενός ατόμου.

Γίνεται καταπάτηση (intrusion), έτσι ώστε με κάποιες πράξεις να διαταραχθεί η απομόνωση και η ηρεμία του ατόμου. Γίνεται επίσης παρεμβολή λήψεως αποφάσεων (decisional interference), έτσι ώστε οι κυβερνήσεις να εμποδίζουν τα άτομα να πάρουν αποφάσεις για προσωπικά θέματα.

2.3 Διασφάλιση ιδιωτικότητας

Η ιδιωτικότητα ενός ατόμου για να διασφαλιστεί προϋποθέτει κάποιες ενέργειες από το ίδιο το άτομο αλλά και τους παράγοντες που αλληλεπιδρούν μαζί του. Η ιδιωτικότητα που αφορά τον πραγματικό κόσμο μπορεί να διασφαλιστεί από ενέργειες των ατόμων όπως για παράδειγμα να προσέχουν που φυλάνε τα πράγματα τους, τι μεταφέρουν μαζί τους, και λοιπά.

Η ιδιωτικότητα που προκύπτει για τα άτομα που εκθέτονται στο διαδίκτυο μπορεί να διασφαλιστεί μέσω διαφόρων ενεργειών που οι ίδιοι οι χρήστες μπορούν να κάνουν αλλά και μέσω μεθόδων που οι οργανισμοί και οι ιστοσελίδες πρέπει να έχουν. Ένας χρήστης στο διαδίκτυο πρέπει να βεβαιώνεται ότι ξέρει ποιος είναι ο παραλήπτης των πληροφοριών που δίνει. Επίσης, καλό είναι να γίνεται κρυπτογράφηση των δεδομένων ενός χρήστη. Με τη χρήση λογισμικού κρυπτογράφησης, γίνεται κρυπτογράφηση των πληροφοριών που στέλνονται μέσω του διαδικτύου. Ένα εικονίδιο "κλειδαριάς" στη γραμμή κατάστασης του προγράμματος περιήγησης στο διαδίκτυο σημαίνει ότι οι πληροφορίες του χρήστη θα είναι ασφαλής όταν μεταδίδονται. Οι ψηφιακές υπογραφές, αλλά και τεχνολογίες ασφαλείας όπως συστήματα ανίχνευσης εισβολής καθώς και φίλτρα spam είναι πολύ βοηθητικές για την διασφάλιση ιδιωτικότητας.

Ακόμη, μαθηματικές μέθοδοι που προτάθηκαν για διάφορες μορφές ιδιωτικότητας είναι πολύ χρήσιμες για την καθοδήγηση και ανάπτυξη τεχνολογιών προστασίας της ιδιωτικής ζωής για διευκόλυνση εντοπισμού παραβιάσεων. Οι χρήστες επίσης, καλό θα ήταν να κρατούν τους κωδικούς πρόσβασης τους μυστικούς και να βάζουν όσο πιο περίπλοκους κωδικούς μπορούν. Πολλά συστήματα ιστοσελίδων όταν βλέπουν πως ο κωδικός που δίνει ο χρήστης είναι απλός και εύκολος του λένε να δίνει πιο μεγάλο και περίπλοκο (που να περιλαμβάνει για παράδειγμα και αριθμούς και γράμματα).

Όμως, η κυριότερη μέθοδος που προτάθηκε για τη διασφάλιση της ιδιωτικότητας είναι η ύπαρξη πολιτικών ιδιωτικότητας σε μια ιστοσελίδα ή ένα οργανισμό. Για την προστασία της ιδιωτικής ζωής, οι οργανισμοί θα πρέπει να έχουν πολιτικές ιδιωτικότητας που αντιμετωπίζουν απαιτήσεις προστασίας της ιδιωτικής ζωής και θέτουν ελέγχους για την ασφάλεια των δεδομένων. Για την έκφραση των πολιτικών αυτών αναπτύχθηκαν γλώσσες και τεχνολογίες τις οποίες θα δούμε στη συνέχεια.

Κεφάλαιο 3

Γλώσσες Πολιτικών Ιδιωτικότητας

3.1 Έλεγχος πρόσβασης

Ο έλεγχος πρόσβασης είναι μια βασική έννοια για την προστασία των πληροφοριών από κακόβουλη κοινοποίηση, τροποποίηση και χρήση. Είναι ένα σύνολο από τις τεχνικές και τις διαδικασίες σύμφωνα με τις οποίες μια πρόσβαση επιτρέπεται ή απαγορεύεται. Τα συστήματα ελέγχου πρόσβασης, συμβατικά, δεν ασχολούνται με το για ποιους είναι οι πληροφορίες. Το δικαίωμα για γράψιμο ή διάβασμα μπορεί να επιτρέπεται ή να απορρίπτεται, αλλά η απόφαση δεν βασίζεται στο ποιος περιγράφεται από τις πληροφορίες στο αρχείο. Σε γενικές γραμμές, οι πολιτικές ελέγχου πρόσβασης εισάγουν ένα σύστημα που αποφασίζει εάν μια συγκεκριμένη δράση επιτρέπεται, εξάγοντας μια σχέση μεταξύ των θεμάτων, των αντικειμένων και των δράσεων.

Υπάρχουν πολλές κατηγορίες Ελέγχων Πρόσβασης, αλλά εμάς θα μας απασχολήσει ο έλεγχος πρόσβασης βάσει ρόλων (RBAC) [4]. Για τις πολιτικές που ανήκουν στην

κατηγορία αυτή, οι χρήστες αποκτούν πρόσβαση σε ένα σύστημα, ανάλογα από τις υποχρεώσεις και τις δραστηριότητες που τους έχουν αναθέσει στο σύστημα αυτό. Οι πολιτικές αυτές δηλαδή βασίζονται σε ρόλους, οι οποίοι μπορεί να είναι ένα σύνολο ενεργειών που μια ομάδα μπορεί να εκτελεί. Έτσι, με τον τρόπο αυτό, η ανάθεση του ποιος μπορεί να έχει πρόσβαση πού, μπορεί να αναφέρεται στους ρόλους, οι οποίοι κατ' επέκταση να ανατίθενται στους χρήστες. Ένας χρήστης μπορεί σε διαφορετικές φάσεις να έχει διαφορετικούς ρόλους και φυσικά ο ίδιος ρόλος μπορεί να χρησιμοποιείται την ίδια στιγμή από διαφορετικούς χρήστες.

Όμως, οι έλεγχοι προστασίας γενικά, από μόνοι τους, δεν μπορούν να ικανοποιήσουν το σύνολο των απαιτήσεων που προκύπτουν από τις αρχές προστασίας της ιδιωτικότητας. Έτσι λοιπόν, τα τελευταία χρόνια έχει γίνει μια προσπάθεια ανάπτυξης στους μηχανισμούς ελέγχων πρόσβασης έτσι ώστε να καλύπτουν και την προστασία ιδιωτικότητας. Ουσιαστικά έγινε μια ανάπτυξη που βασίστηκε περισσότερο στα μοντέλα RBAC, προσθέτοντας σε αυτά κριτήρια για να μπορούν να γίνονται οι έλεγχοι πρόσβασης. Τα κριτήρια αυτά, μπορούν να διευκρινίσουν από ποιο χρήστη, βάσει ποιού ρόλου, με ποια ακριβώς ενέργεια και σε ποια δεδομένα έγινε η όλη διαδικασία πρόσβασης. Σημαντικό ρόλο στα μοντέλα αυτά, παίζει η έννοια του σκοπού για τον οποίο συλλέγονται τα δεδομένα.

Έτσι, ως αποτέλεσμα έχουμε τον Έλεγχο Πρόσβασης βάσει ρόλων για προστασία της ιδιωτικότητας, τον οποίο και χρησιμοποιεί η γλώσσα XACML που θα μελετήσουμε στην συνέχεια. Στηρίζεται στο RBAC και είναι η επέκτασή του έτσι ώστε να μπορεί με την προσθήκη του σκοπού κυρίως, να καλύπτει και τους ελέγχους πρόσβασης που προκύπτουν από την ιδιωτικότητα.

3.2 Εισαγωγή στις Γλώσσες Πολιτικών Ιδιωτικότητας

Μια πολιτική ιδιωτικότητας αποτελεί τη δήλωση του παρόχου μιας ηλεκτρονικής υπηρεσίας, σχετικά με τα προσωπικά δεδομένα του τελικού χρήστη που θα αξιοποιηθούν κατά την επιτυχή παροχή της συγκεκριμένης υπηρεσίας. Συνήθως περιέχει πληροφορίες σχετικά με το τι προσωπικά δεδομένα θα συλλεχθούν, πώς αυτά

θα χρησιμοποιηθούν, για πόσο καιρό θα διατηρηθούν, τις οντότητες τις οποίες θα αποκαλυφθούν καθώς και τα μέτρα ή το βαθμό προστασίας που εφαρμόζεται.

Πολλοί ιστότοποι στην αρχική τους σελίδα αναγράφουν κάποιες πολιτικές ιδιωτικότητας που δύνανται να ακολουθούν. Οι πολιτικές αυτές, αντικατοπτρίζουν στην ουσία τις υποσχέσεις της διαδικτυακής εταιρείας ως προς την επεξεργασία των ιδιωτικών δεδομένων των χρηστών της με κάποιο συγκεκριμένο τρόπο. Θεωρούνται σαν συμβόλαιο μεταξύ των χρηστών και της εταιρείας και πρέπει να τηρείται και από τις δύο πλευρές. Η διαδικασία αυτή αποτελεί τον πιο διαδεδομένο τρόπο για την προστασία της ιδιωτικότητας των χρηστών. Όλο και πιο συχνά στις δηλώσεις των πολιτικών ιδιωτικότητας εταιρειών, περιέχονται προτάσεις που αναφέρονται στο τρόπο με τον οποίο συλλέγονται τα ιδιωτικά δεδομένα, στη μη χρησιμοποίηση των δεδομένων αυτών για άλλους σκοπούς εκτός της παρούσας συναλλαγής και στη μη παροχή των δεδομένων αυτών προς τρίτα μέρη.

Το υποκεφάλαιο αυτό παρουσιάζει συνοπτικά μερικές από τις πιο σημαντικές υφιστάμενες τεχνολογίες που έχουν εφαρμοστεί για την προστασία των προσωπικών δεδομένων, χωρισμένες σε τρεις κατηγορίες [18] : τις γλώσσες πολιτικών ιδιωτικότητας ελέγχου πρόσβασης, τις γλώσσες πολιτικών ιδιωτικότητας για επιχειρήσεις και τις γλώσσες πολιτικών ιδιωτικότητας για το διαδίκτυο. Οι τεχνολογίες για τη διαχείριση της ιδιωτικότητας αναφέρονται κυρίως σε μηχανισμούς για την αυτοματοποίηση της εφαρμογής πολιτικών ιδιωτικότητας και σε μηχανισμούς ελέγχου πρόσβασης.

Οι γλώσσες πολιτικών ιδιωτικότητας έχουν σχεδιαστεί για να εκφράσουν τους ελέγχους της ιδιωτικής ζωής που οι δύο οργανισμοί και οι χρήστες θέλουν να εκφράσουν. Οι περισσότερες από αυτές έχουν σχεδιαστεί για συγκεκριμένους σκοπούς με ειδικά χαρακτηριστικά. Οι περισσότερες από τις πρωτοβουλίες για το σχεδιασμό αυτών των γλωσσών έχουν συμβεί τα τελευταία δεκαπέντε χρόνια.

3.2.1 Γλώσσες Πολιτικών Ιδιωτικότητας για το διαδίκτυο

Οι Γλώσσες Πολιτικών Ιδιωτικότητας για το διαδίκτυο (Web privacy policy languages), αποτελούν τυποποιημένες πολιτικές ιδιωτικότητας αναγνώσιμες από τους ανθρώπους,

σε μορφές ιστοσελίδων που μπορεί να ερμηνευτούν από τις μηχανές. Περιέχουν επίσης και προτιμήσεις ιδιωτικότητας του χρήστη σε μορφή αναγνώσιμη από την μηχανή. Το πιο χαρακτηριστικό παράδειγμα αυτής της κατηγορίας είναι σίγουρα η γλώσσα P3P με την οποία θα ασχοληθούμε αναλυτικά στην συνέχεια.

Αρχικά, για βελτίωση της ιδιωτικότητας δημιουργήθηκε το πρωτόκολλο P3P (Platform for Privacy Preferences) [11], από το World Wide Web Consortium (W3C) [28] για να εκφράζουν πολιτικές απορρήτου σε ιστοσελίδες. Η γλώσσα P3P περιέχει μια XML [27] βάση την οποία χρησιμοποιούν οι ιστοσελίδες για να περιγράφουν και να κωδικοποιούν τις αρχές ιδιωτικότητας. Στόχος της είναι να επιτρέψει στους χρήστες να αποκτήσουν μεγαλύτερο έλεγχο πάνω στην χρήση των προσωπικών τους δεδομένων σε διαδικτυακούς τόπους που επισκέπτονται. Η P3P, επιτρέπει στις ιστοσελίδες να εκφράζουν τις πρακτικές τους όσον αφορά τη συλλογή και χρήση δεδομένων σε αναγνώσιμη από την μηχανή μορφή XML, έτσι ώστε να μπορούν να ανακτούνται αυτόματα και να ερμηνεύονται εύκολα από τους χρήστες. Περισσότερες λεπτομέρειες θα δούμε στην συνέχεια.

Ακολούθησε η Γλώσσα Διαπραγμάτευσης P3P Προτιμήσεων (P3P Preference Exchange Language – APPEL) [10], που σχεδιάστηκε επίσης από το W3C για να εκφράζουν τις πολιτικές προτιμήσεις της ιδιωτικής ζωής του ατόμου. Η γλώσσα APPEL συμπληρώνει την πλατφόρμα P3P, είναι γλώσσα βασισμένη σε κανόνες που κωδικοποιείται επίσης σε XML. Δίνει τη δυνατότητα στους χρήστες να εκφράζουν τις προτιμήσεις τους αναφορικά με τα προσωπικά τους δεδομένα, χρησιμοποιώντας ένα σύνολο κανόνων προτιμήσεων. Ο τελικός στόχος είναι να διαθέτουν οι χρήστες τη δυνατότητα να ελέγχουν με αυτόματο τρόπο την πολιτική ιδιωτικότητας ενός διαδικτυακού ιστότοπου και κατά πόσον αυτή συμφωνεί με τις αντίστοιχες προτιμήσεις τους, ούτως ώστε να αποφασίζουν εάν θα παράσχουν προσωπικά τους δεδομένα ή όχι. Για τον έλεγχο αυτό υπάρχουν οι πράκτορες των χρηστών (user agents). Οι πράκτορες χρηστών, παραλαμβάνουν τις πολιτικές ιδιωτικότητας των ιστοσελίδων και τις ερμηνεύουν με αυτόματο τρόπο. Έπειτα, τις συγκρίνουν με τους αντίστοιχους κανόνες APPEL που προκαθόρισε ο χρήστης για να αποφασίσουν κατά πόσο η πολιτική ιδιωτικότητας μιας ιστοσελίδας συμφωνεί με τα όσα είχε δηλώσει στις προτιμήσεις και απαιτήσεις του ο χρήστης. Έτσι, ένας χρήστης μπορεί να ορίσει ο ίδιος τις προτιμήσεις

ιδιωτικότητας που έχει, έτσι ώστε όταν επισκέπτεται μια ιστοσελίδα να γίνεται έλεγχος αν οι προτιμήσεις αυτές ικανοποιούνται. Αν παραβιάζονται ο χρήστης ιδιοποιείται.

Τέλος σε αυτή την κατηγορία έχουμε την XPref (XPath-based Preference Language) [23] που σχεδιάστηκε ως συνέχεια της APPEL, για να ξεπεραστούν οι ελλείψεις της APPEL που εντοπίστηκαν στις προτιμήσεις που γράφτηκαν. Είναι τόσο εκφραστική όσο και η APPEL, αλλά είναι πιο εύκολο να την χειριστεί κάποιος.

3.2.2 Γλώσσες Πολιτικών Ιδιωτικότητας για επιχειρήσεις

Οι Γλώσσες Πολιτικών Ιδιωτικότητας για επιχειρήσεις (Enterprise privacy policy languages), χρησιμοποιούνται στο πλαίσιο ενός οργανισμού για την επιβολή του τι έχει δηλώσει στην εσωτερική πολιτική προστασίας της ιδιωτικότητας του. Αυτή η κατηγορία πολλές φορές θεωρείται μέρος της τρίτης κατηγορίας γιατί ασχολείται και αυτή με τον έλεγχο πρόσβασης. Ωστόσο, την διαφοροποιούμε για να δείξουμε ότι οι γλώσσες αυτής της κατηγορίας ασχολούνται ρητά με την προστασία των δεδομένων και τα θέματα ιδιωτικότητας στις επιχειρήσεις. Πολλές φορές, αυτές οι γλώσσες είναι πιο αποτελεσματικές από τις γλώσσες για το διαδίκτυο. Το πιο χαρακτηριστικό παράδειγμα αυτής της κατηγορίας είναι η EPAL, με την οποία θα ασχοληθούμε αναλυτικά στην συνέχεια.

Αρχικά, έχουμε την Customer Profile Exchange (CPExchange) [9], που έγινε για να διευκολύνεται η επικοινωνία μεταξύ επιχειρήσεων σχετικά με την ιδιωτικότητα. Βασικά, γίνεται ενσωμάτωση στοιχείων ενός πελάτη (δεδομένα ή όχι) σε ένα μοντέλο δεδομένων βασισμένο σε XML, για να χρησιμοποιηθούν από διάφορες εφαρμογές μιας επιχείρησης στο διαδίκτυο ή όχι. Βασίζεται και στην P3P.

Αργότερα, έχουμε την E-P3P [16]. Κατά την επεξεργασία προσωπικών δεδομένων, μπορεί να χρησιμοποιηθεί για να εξασφαλίσει ότι οι ροές δεδομένων και οι πρακτικές χρήσης της επιχείρησης συμμορφώνονται με τη δήλωση προστασίας προσωπικών δεδομένων του οργανισμού. Είναι ο προκάτοχος της γλώσσας EPAL.

Τέλος, έχουμε την EPAL (Enterprise Privacy Authorization Language) [8][17], η οποία σχεδιάστηκε το 2003 από την IBM. Αποτελεί μία γλώσσα βασισμένη στην XML που χρησιμοποιείται σε οργανισμούς και επιχειρήσεις για τον προσδιορισμό και την εφαρμογή πολιτικών ιδιωτικότητας εντός του οργανισμού. Είναι ουσιαστικά ένα σύνολο κανόνων προστασίας της ιδιωτικής ζωής. Ένας κανόνας είναι μια δήλωση που περιλαμβάνει μια απόφαση, τα δεδομένα του χρήστη, μια ενέργεια, μια κατηγορία δεδομένων, και ένα σκοπό. Ένας κανόνας μπορεί επίσης να περιέχει όρους και υποχρεώσεις. Περισσότερες λεπτομέρειες θα δούμε στην συνέχεια.

3.2.3 Γλώσσες Πολιτικών Ιδιωτικότητας ελέγχου πρόσβασης

Οι γλώσσες Πολιτικών Ιδιωτικότητας ελέγχου πρόσβασης, (Access Control privacy policy languages), βασίζονται σε γλώσσες ελέγχου πρόσβασης, κυρίως στην Role Based Access Control (RBAC) [4]. Το πιο χαρακτηριστικό παράδειγμα αυτής της κατηγορίας είναι η XACML, με την οποία θα ασχοληθούμε αναλυτικά στην συνέχεια.

Αρχικά, έχουμε την Security Assertion Markup Language (SAML) [13], η οποία είναι ένα πρότυπο XML για την ανταλλαγή δεδομένων ταυτότητας και εξουσιοδότησης μεταξύ των τομέων της ασφάλειας.

Μετά έχουμε την XML Access Control Language (XACL) [25], η οποία είναι μια γλώσσα XML για να καθορίζονται πολιτικές ασφάλειας που θα εφαρμόζονται σε συγκεκριμένες προσβάσεις σε έγγραφα XML. Δεν περιορίζεται στον έλεγχο μόνο της ανάγνωσης, εγγραφής, δημιουργίας ή διαγραφής, αλλά ελέγχει και για επαλήθευση ψηφιακής υπογραφής, κρυπτογράφηση, και για μετασχηματισμούς XSL.

Τέλος, έχουμε την XACML (eXtensible Access Control Markup Language) [26] που είναι μια από τις πιο γνωστές γλώσσες για την υποστήριξη μοντέλων ελέγχου πρόσβασης. Είναι μια ευρέως υιοθετημένη τυπική γλώσσα για τον έλεγχο πρόσβασης, την παροχή άδειας και πολιτικών προστασίας. Οι πολιτικές που δημιουργούνται με την χρήση της XACML βασίζονται στην XML. Η XACML, παρέχει την δυνατότητα αίτησης/απόκρισης για να εκφράζονται απορίες σχετικά με το αν ή όχι μια συγκεκριμένη άδεια θα πρέπει να επιτρέπεται σε ένα συγκεκριμένο χρήστη. Η XACML

επιτρέπει την χρήση αυθαίρετων χαρακτηριστικών στις πολιτικές, τον έλεγχο προσπέλασης βασισμένο σε ρόλους (role based access control), τις πολιτικές ευρετηρίου και λοιπά. Περισσότερες λεπτομέρειες θα δούμε στην συνέχεια.

3.3 Γλώσσες Πολιτικών Ιδιωτικότητας

3.3.1 P3P

Το πρωτόκολλο Platform for Privacy Preferences (P3P) [11] είναι μια τεχνολογία για την προστασία της ιδιωτικότητας, που αναπτύχθηκε από την κοινοπραξία World Wide Web Consortium (W3C) [28] στις 16 Απριλίου το 2002. Το World Wide Web Consortium είναι ένας διεθνής οργανισμός που αναπτύσσει πρότυπα και προωθεί κοινά και διαλειτουργικά πρωτόκολλα. Στόχος της είναι να επιτρέψει στους χρήστες να αποκτήσουν μεγαλύτερο έλεγχο πάνω στην χρήση των προσωπικών τους δεδομένων σε διαδικτυακούς τόπους που επισκέπτονται. Η P3P, επιτρέπει στις ιστοσελίδες να εκφράζουν τις πρακτικές τους όσον αφορά τη συλλογή και χρήση δεδομένων σε αναγνώσιμη από την μηχανή μορφή XML, έτσι ώστε να μπορούν να ανακτούνται αυτόματα και να ερμηνεύονται εύκολα από τους χρήστες.

Βασίζεται στην XML [27], την οποία χρησιμοποιούν οι ιστοσελίδες για να περιγράφουν και να κωδικοποιούν τις αρχές ιδιωτικότητας. Το πρωτόκολλο P3P έχει δύο μέρη : 1) Τις πολιτικές ιδιωτικότητας/απορρήτου, όπου μια ιστοσελίδα μπορεί να ορίσει τις πρακτικές συλλογής και χρήσης δεδομένων χρησιμοποιώντας P3P και 2) Τις προτιμήσεις προστασίας προσωπικών δεδομένων, όπου οι πελάτες μπορούν να καθορίσουν τις προτιμήσεις της ιδιωτικής τους ζωής χρησιμοποιώντας APPEL. Ακολούθως, γίνεται έλεγχος αν οι προτιμήσεις του χρήστη ταιριάζουν με τις πολιτικές απορρήτου. Έτσι, ένας χρήστης μπορεί να ορίσει ο ίδιος τις προτιμήσεις ιδιωτικότητας που έχει. Όταν επισκέπτεται μια ιστοσελίδα γίνεται έλεγχος αν οι προτιμήσεις αυτές ικανοποιούνται. Αν παραβιάζονται ο χρήστης ιδιοποιείται. Η P3P είναι μια αναγνώσιμη από τη μηχανή γλώσσα που βοηθά να εκφραστούν πρακτικές διαχείρισης των δεδομένων μιας ιστοσελίδας.

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 [32]. Το στοιχείο consequence παρέχει κατανοητές εξηγήσεις στους χρήστες σε απλή γραφή για να εξηγήσει τις πρακτικές συλλογής και επεξεργασίας δεδομένων της ιστοσελίδας, αλλά και τις επιπτώσεις τους.

Το αναγνωριστικό purpose προσδιορίζει τους σκοπούς για τους οποίους πραγματοποιείται η συλλογή της πληροφορίας. Κάποιες πιθανές προκαθορισμένες τιμές που μπορεί να πάρει το στοιχείο purpose είναι:

- <current/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται θα χρησιμοποιηθούν αποκλειστικά και μόνο για την διεκπεραίωση της συγκεκριμένης δραστηριότητας για την οποία παρέχονται από το χρήστη.
- <admin/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, πιθανώς να χρησιμοποιηθούν για την τεχνική διαχείριση του διαδικτυακού ιστότοπου.
- <pseudo-analysis/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, πιθανώς να χρησιμοποιηθούν για την εξαγωγή συμπερασμάτων που αφορούν τις συνήθειες, τα ενδιαφέροντα ή άλλα χαρακτηριστικά του χρήστη, αλλά χωρίς τα συμπεράσματα αυτά να συσχετίζονται με την ταυτότητα του συγκεκριμένου χρήστη.
- <pseudo-decision/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, πιθανώς να χρησιμοποιηθούν για την "υποκειμενική" διαμόρφωση (customization) του περιεχομένου του διαδικτυακού ιστότοπου, για το χρήστη, αλλά με χρήση ψευδωνύμων, ούτως ώστε η διαμόρφωση αυτή να μην συσχετίζεται με στοιχεία που εκφράζουν την πραγματική ταυτότητα του χρήστη (π.χ. το όνομά του).
- <individual-analysis/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, πιθανώς να χρησιμοποιηθούν για την εξαγωγή συμπερασμάτων που αφορούν τις συνήθειες, τα ενδιαφέροντα ή άλλα χαρακτηριστικά του χρήστη, σε συνδυασμό με δεδομένα τα οποία ταυτοποιούν το συγκεκριμένο χρήστη.
- <individual-decision/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, πιθανώς να χρησιμοποιηθούν για την "υποκειμενική" διαμόρφωση

(customization) του περιεχομένου του διαδικτυακού ιστότοπου, για το χρήστη, σε συνδυασμό με δεδομένα τα οποία ταυτοποιούν το συγκεκριμένο χρήστη. Για παράδειγμα, ένα διαδικτυακό κατάστημα μπορεί να αποθηκεύσει τις πληροφορίες του χρήστη και να του προτείνει την αγορά συγκεκριμένων προϊόντων με βάση τις προηγούμενες αγορές που ο χρήστης έχει πραγματοποιήσει.

- <contact/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, πιθανώς να χρησιμοποιηθούν για την προώθηση προϊόντων ή υπηρεσιών μέσω της επικοινωνίας με το χρήστη με οποιοδήποτε μέσο εκτός από την τηλεφωνική επικοινωνία (π.χ. Email).
- <telemarketing/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, πιθανώς να χρησιμοποιηθούν για την πραγματοποίηση τηλεφωνικής επικοινωνίας με το χρήστη, με σκοπό την προώθηση προϊόντων ή υπηρεσιών.

Η ετικέτα recipient ορίζει τους αποδέκτες που επιτρέπονται να πάρουν την πληροφορία η οποία συλλέγεται. Κάποιες πιθανές προκαθορισμένες τιμές που μπορεί να πάρει το στοιχείο recipient είναι:

- <ours/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, μπορούν να χρησιμοποιηθούν μόνο από τον εν λόγω οργανισμό ή/και από άλλους οργανισμούς οι οποίοι δρουν εκ μέρους του οργανισμού για την εκπλήρωση των καθορισμένων σκοπών.
- <delivery/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, μπορούν να χρησιμοποιηθούν από τρίτο οργανισμό παροχής υπηρεσιών μεταφοράς προϊόντων, ο οποίος μπορεί να χρησιμοποιήσει τα δεδομένα για άγνωστους σκοπούς ή σκοπούς πέρα από εκείνους για τους οποίους ο χρήστης παρέχει τα δεδομένα.
- <same/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, μπορούν να χρησιμοποιηθούν από τρίτο οργανισμό, ο οποίος ακολουθεί τις ίδιες πρακτικές σχετικά με τη χρήση των δεδομένων με τον οργανισμό ο οποίος συλλέγει τα δεδομένα.
- <other-recipient/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, μπορούν να χρησιμοποιηθούν από τρίτο οργανισμό, ο οποίος δεν

ακολουθεί απαραιτήτως τις ίδιες πρακτικές σχετικά με τη χρήση των δεδομένων με τον οργανισμό ο οποίος συλλέγει τα δεδομένα, αλλά είναι ελεγχόμενος από τον οργανισμό αυτό.

- <unrelated/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, μπορούν να χρησιμοποιηθούν από τρίτο οργανισμό, ο οποίος δεν ακολουθεί απαραιτήτως τις ίδιες πρακτικές σχετικά με τη χρήση των δεδομένων με τον οργανισμό ο οποίος συλλέγει τα δεδομένα, ενώ οι πρακτικές αυτές είναι άγνωστες στον οργανισμό.
- <public/>: Ορίζει το ενδεχόμενο πλήρους δημοσιοποίησης των δεδομένων τα οποία συλλέγονται από τον χρήστη, στο διαδικτυακό ιστότοπο.

Οι ετικέτες purpose και recipient σε μία πολιτική ιδιωτικότητας, μπορούν να χαρακτηρίζονται και με επιπλέον XML γνωρίσματα που εκφράζουν κατά πόσο ο σκοπός που καθορίστηκε ή ο εν κυρίως παραλήπτης, αποτελεί απαραίτητο και αναγκαίο μέρος της πρακτικής του διαδικτυακού ιστότοπου. Το γνώρισμα αυτό είναι τύπου required και οι τιμές που μπορεί να πάρει είναι:

- opt-in: Τα δεδομένα που συλλέγονται από τον χρήστη μπορούν να χρησιμοποιηθούν για το σκοπό που συλλέγονται ή να προωθηθούν σε περαιτέρω παραλήπτες μόνο εφόσον ο χρήστης δώσει σχετική συγκατάθεση.
- opt-out: Τα δεδομένα που συλλέγονται από τον χρήστη μπορούν να χρησιμοποιηθούν για το σκοπό που συλλέγονται ή να προωθηθούν σε περαιτέρω παραλήπτες εκτός και εάν ο χρήστης δηλώσει πως δεν το επιτρέπει με ρητό τρόπο. Στην περίπτωση αυτή, ο διαδικτυακός ιστότοπος πρέπει να παρέχει διευκρινιστικές οδηγίες για τον τρόπο με τον οποίο ο χρήστης μπορεί να εκφράσει την επιλογή του αυτή.
- always: Στην περίπτωση αυτή, είναι απαραίτητη η χρήση προκαθορισμένων δηλωμένων δεδομένων για το διαδικτυακό ιστότοπο, για τον σκοπό συλλογής ή τη παροχή των δεδομένων στους καθορισμένους παραλήπτες. Ο χρήστης δεν έχει επιλογή αποκλεισμού.

Το στοιχείο retention ορίζει τον χρόνο που θα διατηρηθούν τα δεδομένα που συλλέγονται από αυτόν που τα συλλέγει. Κάποιες πιθανές προκαθορισμένες τιμές που μπορεί να πάρει το στοιχείο retention είναι:

- <no-retention/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, δεν υπάρχει περίπτωση να διατηρηθούν με κανένα τρόπο μετά από την εκπλήρωση του σκοπού για τον οποίο προορίζονται. Καταστρέφονται τόσο τα ίδια τα δεδομένα όσο και πιθανά ίχνη τους όπως σε αρχεία καταγραφής.
- <stated-purpose/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, δεν υπάρχει περίπτωση να διατηρηθούν με κανένα τρόπο μετά από την εκπλήρωση του σκοπού για τον οποίο προορίζονται.
- <legal-requirement/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, υπάρχει το ενδεχόμενο να διατηρηθούν πέρα από την εκπλήρωση του σκοπού για τον οποίο προορίζονται, με σκοπό να ικανοποιηθούν σχετικές νομικές απαιτήσεις.
- <business-practices/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, υπάρχει το ενδεχόμενο να διατηρηθούν πέρα από την εκπλήρωση του σκοπού για τον οποίο προορίζονται, με σκοπό να πραγματοποιηθούν καθορισμένες επιχειρησιακές διαδικασίες του οργανισμού. Ο οργανισμός στην περίπτωση αυτή θα πρέπει να έχει μια πλήρως ορισμένη πολιτική διατήρησης που να βασίζεται σε συγκεκριμένο χρονοδιάγραμμα καταστροφής των δεδομένων.
- <indefinitely/>: Μας λέει ότι τα δεδομένα τα οποία συλλέγονται από τον χρήστη, υπάρχει το ενδεχόμενο να διατηρηθούν πέρα από την εκπλήρωση του σκοπού για τον οποίο προορίζονται και για απροσδιόριστο χρονικό διάστημα.

Η ετικέτα data-group προσδιορίζει τον κατάλογο με τους τύπους δεδομένων που συλλέγονται για τους καθορισμένους σκοπούς. Η ετικέτα αυτή αποτελείται από ένα ή περισσότερα στοιχεία data. Τα στοιχεία αυτά, προσδιορίζουν τον κάθε τύπο δεδομένων και κάθε ένα υποχρεωτικά περιέχει ένα XML γνώρισμα, το ref. Το γνώρισμα αυτό, δηλώνει το συγκεκριμένο τύπο δεδομένων που συλλέγεται και παίρνει ως τιμή ένα αναγνωριστικό που είναι μοναδικό αναγνωριστικό πόρου. Ένα στοιχείο data μπορεί να αποτελείται και από το γνώρισμα optional, το οποίο είναι προαιρετικό και ορίζει αν ο

διαδικτυακός ιστότοπος θεωρεί την προσθήκη των δεδομένων από τον χρήστη ως υποχρεωτική (τιμή = ‘no’) ή προαιρετική (τιμή = ‘yes’). Επίσης κάθε στοιχείο data μπορεί να καταχωρηθεί σε μια κατηγορία με τη χρήση του XML γνωρίσματος categories. Το γνώρισμα αυτό, περιγράφει τον τύπο της πληροφορίας που το συγκεκριμένο δεδομένο εκφράζει.

Το παράδειγμα που ακολουθεί παρουσιάζει, την πολιτική ιδιωτικότητας ενός υποθετικού διαδικτυακού καταστήματος (π.χ. Online κατάστημα ρούχων). Το κατάστημα αυτό συλλέγει συγκεκριμένα προσωπικά δεδομένα που είναι αναγκαία για την πραγματοποίηση της συναλλαγής (όνομα, ταχυδρομική διεύθυνση και αριθμός πιστωτικής κάρτας), ενώ χρησιμοποιεί το ιστορικό αγορών των πελατών του, με σκοπό να πραγματοποιεί προσωποποιημένες προτάσεις αγορών. Για το σκοπό αυτό, χρησιμοποιεί τις διευθύνσεις ηλεκτρονικού ταχυδρομείου των εγγεγραμμένων πελατών του.

```
<POLICY>
.....
<STATEMENT>
<PURPOSE>
<current/>
</PURPOSE>
<RECIPIENT>
<ours/><same/>
</RECIPIENT>
<RETENTION>
<stated-purpose/>
</RETENTION>
<DATA-GROUP>
<DATA ref="#user.name"/>
<DATA ref="#user.home-info.postal"/>
<DATA ref="#dynamic.miscdata">
<CATEGORIES> <purchase/> </CATEGORIES>
</DATA>
```

```
</DATA-GROUP>
</STATEMENT>
<STATEMENT>
<PURPOSE>
<individual-decision required="opt-in"/>
<contact required="opt-in"/>
</PURPOSE>
<RECIPIENT>
<ours/>
</RECIPIENT>
<RETENTION>
<business-practices/>
</RETENTION>
<DATA-GROUP>
<DATA ref="#user.home-info.online.email"/>
<DATA ref="#dynamic.miscdata">
<CATEGORIES><purchase/></CATEGORIES>
</DATA>
</DATA-GROUP>
</STATEMENT>
</POLICY>
```

Σχήμα 1 : Παράδειγμα πολιτικής Ιδιωτικότητας P3P [32]

Η πιο πάνω πολιτική ιδιωτικότητας που περιγράφεται στο παράδειγμα, αποτελείται από δύο στοιχεία statement. Το πρώτο στοιχείο τύπου statement βλέπουμε ότι συλλέγει το όνομα του χρήστη, τη ταχυδρομική του διεύθυνση, καθώς και άλλα δεδομένα που ανήκουν στην κατηγορία purchase. Μας λέει ότι οι πληροφορίες αυτές θα χρησιμοποιηθούν μόνο για της διεκπεραίωση της δραστηριότητας για την οποία τα δίνει ο χρήστης. Όσον αφορά για το ποιοι μπορούν να τις παραλάβουν μας λέει ότι εκτός από το κατάστημα μπορούν να τις πάρουν και οργανισμοί οι οποίοι ακολουθούν τις ίδιες πρακτικές με το συγκεκριμένο κατάστημα σχετικά με τη χρήση των

δεδομένων. Τέλος, όσον αφορά για το πόσο θα διατηρηθούν οι πληροφορίες μας λέει ότι θα διατηρηθούν μόνο για το προβλεπόμενο χρονικό διάστημα.

Το δεύτερο στοιχείο τύπου statement της πολιτικής ιδιωτικότητας που περιγράφεται στο παράδειγμα βλέπουμε ότι αφορά τα διάφορα δεδομένα που συλλέγονται και ανήκουν στην κατηγορία purchase, καθώς και τη διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη. Μας λέει ότι οι πληροφορίες αυτές θα συλλέγονται για να μπορεί το κατάστημα να παρέχει στον χρήστη προσωποποιημένες υπηρεσίες κατά τις επισκέψεις του στο διαδικτυακό κατάστημα αυτό, καθώς και για να μπορεί το κατάστημα να επικοινωνεί με το χρήστη και να τον ενημερώνει για προϊόντα τα οποία πιστεύει πως θα τον ενδιαφέρουν. Τα δεδομένα αυτά θα παραλαμβάνονται αποκλειστικά από το κατάστημα και δε θα παρέχονται σε τρίτους οργανισμούς. Όσον αφορά το χρονικό διάστημα που θα διατηρηθούν τα δεδομένα, θα είναι σχετικά μεγαλύτερο από όσο απαιτείται λόγω του ότι θα τα χρειάζονται για να μπορούν να βλέπουν τις προτιμήσεις του χρήστη για να του προτείνουν αυτά που τον ενδιαφέρουν. Όμως όλα αυτά που περιγράφονται στο δεύτερο statement θα πραγματοποιηθούν μόνο αν ο χρήστης το επιτρέψει με ρητό τρόπο (λόγω της τιμής που παίρνει το γνώρισμα required – ‘opt-in’).

Άλλα αναγνωριστικά που περιέχονται σε μια P3P πολιτική είναι το entity, το οποίο καταγράφει πληροφορίες επικοινωνίας με την επιχείρηση ή άτομο του οποίου ο ιστότοπος ανήκει.

Πχ :
```
<ENTITY>
 <DATA-GROUP>
 <DATA ref="#business.name">CatalogExample</DATA>
 <DATA ref="#business.contact-info.postal.city">Bethesda</DATA>
 <DATA ref="#business.contact-info.postal.stateprov">MD</DATA>
 <DATA ref="#business.contact-info.postal.country">US</DATA>
 </DATA-GROUP>
</ENTITY>
```

Σχήμα 2 : Παράδειγμα για ετικέτα Entity της P3P

Η ετικέτα access δηλώνει αν τα άτομα μπορούν να ανακαλύψουν ποια προσωπικά δεδομένα τους κρατάει ένας ιστότοπος στις βάσεις δεδομένων του.

```
Πχ:  <ACCESS>
            <nonident/>
     </ACCESS>
```

Σχήμα 3 : Παράδειγμα για ετικέτα Access της P3P

3.3.2 EPAL

Η γλώσσα Επιχειρησιακής Εξουσιοδότησης για Ιδιωτικότητα (Enterprise Privacy Authorization Language – EPAL) [8][17] αποτελεί μία γλώσσα βασισμένη στην XML που χρησιμοποιείται σε οργανισμούς και επιχειρήσεις για τον προσδιορισμό και την εφαρμογή πολιτικών ιδιωτικότητας εντός του οργανισμού. Έχει προταθεί από την εταιρεία International Business Machines (IBM) [7] το 2003. Είναι μια τυπική γλώσσα που χρησιμοποιείται για καταγραφή πολιτικών ιδιωτικότητας και επιβάλλει κανόνες για τη σωστή διαχείριση των δεδομένων.

Μία EPAL πολιτική αποτελείται από ένα λεξιλόγιο και μία λίστα κανόνων ιδιωτικότητας. Η EPAL απαρτίζεται από ένα σύνολο από κανόνες ιδιωτικότητας για να προσδιοριστεί κατά πόσον μπορεί ένα αίτημα να επιτραπεί ή να απορριφθεί. Κάθε κανόνας είναι μια πρόταση που περιλαμβάνει ένα ορισμό εκτέλεσης και έχει ένα επίπεδο προτεραιότητας. Ένας κανόνας είναι μια δήλωση που περιλαμβάνει αποφάσεις (allow ή deny), χρήστες δεδομένων, ενέργειες, κατηγορίες δεδομένων, και σκοπό. Ένας κανόνας μπορεί επίσης να περιέχει όρους και υποχρεώσεις.

Οι κατηγορίες δεδομένων (Data-Categories), ορίζουν τις διάφορες κατηγορίες που μπορούν να δημιουργηθούν με βάση τα δεδομένα που έχουν συλλεχθεί και η κάθε κατηγορία τυγχάνει ειδικού χειρισμού ως προς την ιδιωτικότητα που εφαρμόζεται. Οι χρήστες δεδομένων (User-Categories), αποτελούν τους χρήστες ή τις ομάδες οι οποίες χρησιμοποιούν τα δεδομένα που έχουν καταγραφεί. Οι σκοποί (Purposes) μοντελοποιούν την υπηρεσία που πρόκειται να χειριστεί τα δεδομένα με βάση τον τύπο των δεδομένων που έχουν καταγραφεί. Οι ενέργειες (Actions) μοντελοποιούν το πώς τα

δεδομένα χρησιμοποιούνται. Οι υποχρεώσεις (Obligations) ορίζουν τις ενέργειες που πρέπει να εκτελεστούν. Οι προϋποθέσεις (Conditions) είναι Boolean expressions που αξιολογούν το περιεχόμενο.

Αφού προσδιοριστούν τα πιο πάνω επιμέρους στοιχεία τότε μπορούν να τυποποιηθούν για την διαμόρφωση των κανόνων εξουσιοδότησης της ιδιωτικότητας, έτσι που είτε να επιτρέπεται είτε όχι η εκτέλεση ενεργειών στις κατηγορίες δεδομένων για συγκεκριμένους σκοπούς, υπό την προϋπόθεση ότι ισχύουν οι ζητούμενες προϋποθέσεις καθώς διατηρούνται κάποιες υποχρεώσεις.

Privacy policy	Allow a sales agent to collect a customer's data for order entry, if the customer is older than 13 years of age and the customer has been notified of the privacy policy. Delete the data 3 years from now
Ruling	Allow
User category	Sales department
Action	Store
Data category	Customer-record
Purpose	Order-processing
Condition	The customer is older than 13 years of age
Obligation	Delete the data 3 years from now

Πίνακας 1 : Παράδειγμα ορισμού κανόνα πολιτικής στην EPAL

Ακολούθως, χρησιμοποιείται ο κανόνας αυτός για να προσδιοριστεί κατά πόσον ένα αίτημα μπορεί να επιτραπεί ή να απορριφθεί. Ένα αίτημα αποτελείται από την κατηγορία χρήστη, μια ενέργεια, μια κατηγορία δεδομένων και ένα σκοπό.

Request	A person acting as a sales agent and an employee requests to collect a customer's email for order entry
User category	Sales department
Action	Store
Data category	Customer-record
Purpose	Order-processing

Πίνακας 2 : Παράδειγμα ορισμού αιτήματος του κανόνα πολιτικής στην EPAL

Στο πιο πάνω παράδειγμα ο κανόνας όπως έχει οριστεί επιτρέπει την εκτέλεση του αιτήματος. Αυτό έχει σαν αποτέλεσμα να επιτραπεί στον υπεύθυνο πωλήσεων (sales agent) να αποθηκεύσει τις πληροφορίες επικοινωνίας του πελάτη.

Η πολιτική EPAL γενικά αποτελείται από ένα λεξιλόγιο (epal-vocabulary) και μία λίστα κανόνων ιδιωτικότητας (epal-policy).
Το λεξιλόγιο αποτελείται από την έκδοση της EPAL (version of EPAL), τις πληροφορίες του λεξιλογίου (vocabulary-information), τους χρήστες δεδομένων (User-category) που καθορίζουν τους ρόλους αυτών που κάνουν τις αιτήσεις, τις κατηγορίες δεδομένων (Data-category) που καθορίζουν τα προστατευόμενα δεδομένα, τους σκοπούς που καθορίζουν τους σκοπούς όλων των προτεινόμενων δράσεων, τις ενέργειες που καθορίζουν όλες τις προτεινόμενες δράσεις, τους περιορισμούς που καθορίζουν το πλαίσιο των εξωτερικών δεδομένων που μπορούν να αξιολογηθούν από τις συνθήκες και τις υποχρεώσεις που καθορίζουν τις εξωτερικές απαιτήσεις για κάθε αιτητή, για να μπορεί να γίνει η απαιτούμενη δράση (π.χ. οι βαθμοί μπορούν να τροποποιηθούν αλλά θα πρέπει να διαγράφονται μετά από 3 χρόνια). Σημειώστε ότι τα τρία στοιχεία, οι κατηγορίες χρηστών, οι κατηγορίες δεδομένων και οι σκοποί μπορεί να έχουν ιεραρχικές δομές. Για παράδειγμα, δύο κατηγορίες χρηστών "καθηγητής" και "γραμματέας" ανήκουν σε έναν κοινό χρήστη της κατηγορίας "εργαζόμενοι πανεπιστημίου" γεγονός που δείχνει ότι ένας εργαζόμενος πανεπιστημίου μπορεί να είναι ένας καθηγητής ή μια γραμματέας.

Η λίστα κανόνων ιδιωτικότητας (epal-policy), μπορεί να περικλείει στον ορισμό της (< >) το χαρακτηριστικό global-condition που ορίζει ένα γενικό κανόνα, το version της EPAL και το default ruling που ορίζει αν είναι allow ή deny. Αποτελείται από τις πληροφορίες της πολιτικής (policy-information), μια αναφορά στο λεξιλόγιο (epal-vocabulary-ref) και τέλος τον κανόνα (rule) που περιέχει όλα όσα περιλαμβάνει ένας κανόνας όπως περιγράψαμε πιο πάνω.

Τυπικά η γλώσσα EPAL βασίζεται στον έλεγχο πρόσβασης και δουλεύει κάπως έτσι: Ένας χρήστης (π.χ., ένας καθηγητής) επιθυμεί να εκτελέσει μια ενέργεια (π.χ., αλλαγή) για αλλαγή προστατευόμενων δεδομένων (π.χ., ο βαθμός του φοιτητή) με κάποιο σκοπό (π.χ., να αναθέτει τον βαθμό). Ο χρήστης υποβάλλει το αίτημα του με τη χρήση του

αιτήματος έγκρισης της γλώσσας EPAL στη μηχανή αξιολόγησης EPAL. Η μηχανή αξιολόγησης EPAL ελέγχει το αίτημα με τους κανόνες της EPAL πολιτικής και καθορίζει αν θα πρέπει να επιτρέπεται ή να απαγορεύεται το αίτημα και εφαρμόζει την απόφαση.

```
<epal-vocabulary>

    <vocabulary-information id = GradeManagement> </vocabulary-information>
    <user-category id = employee> </user-category>
    <user-category id = professor=parent 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>
    <purpose id= reading=parent manage”></purpose>
    <action id= change”></action>
    <action id= read”></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>
```

```
  <rule id = 2 ruling = allow>
     <user-category refid=employee/>
     <data-category refid=grades/>
     <purpose refid=manage/>
     <action refid=change/>
  </rule>

  <rule id = 3 ruling = allow>
     <user-category refid=professor/>
     <data-category refid=grades/>
     <purpose refid=manage/>
     <action refid=change/>
  </rule>

</epal-policy>
```

Σχήμα 4 : Παράδειγμα EPAL πολιτικής συνοδευόμενο από το συσχετιζόμενο λεξιλόγιο [29]

Στο παράδειγμα, στο λεξιλόγιο ορίζονται τρεις κατηγορίες χρηστών που αντιπροσωπεύουν ένα εργαζόμενο, ένα καθηγητή και μια γραμματέα. Ως κατηγορίες δεδομένων ορίζονται οι βαθμοί. Ορίζονται επίσης τρεις σκοποί που αντιπροσωπεύουν ένα σκοπό διαχείρισης, ένα βαθμολόγησης και ένα διαβάσματος. Ορίζονται και δυο ενέργειες, μια για αλλαγή και μια για διάβασμα. Το παράδειγμα της πολιτικής EPAL περιλαμβάνει τρεις κανόνες: Ο πρώτος κανόνας είναι deny κανόνας, του οποίου η σημασία είναι ότι μια γραμματέας δεν μπορεί να αλλάξει βαθμούς με σκοπό την βαθμολόγηση. Ο δεύτερος κανόνας είναι allow κανόνας, του οποίου η σημασία είναι ότι ένας εργαζόμενος μπορεί να αλλάξει βαθμούς με σκοπό την διαχείριση. Ο τρίτος κανόνας είναι allow κανόνας, του οποίου η σημασία είναι ότι ένας καθηγητής μπορεί να αλλάξει βαθμούς με σκοπό την διαχείριση. Σημειώστε ότι default-ruling, αναφέρεται στο ότι, αν μια αίτηση δεν ταιριάζει με κανένα κανόνα στην πολιτική EPAL, η απόφαση deny θα πρέπει να επιστραφεί.

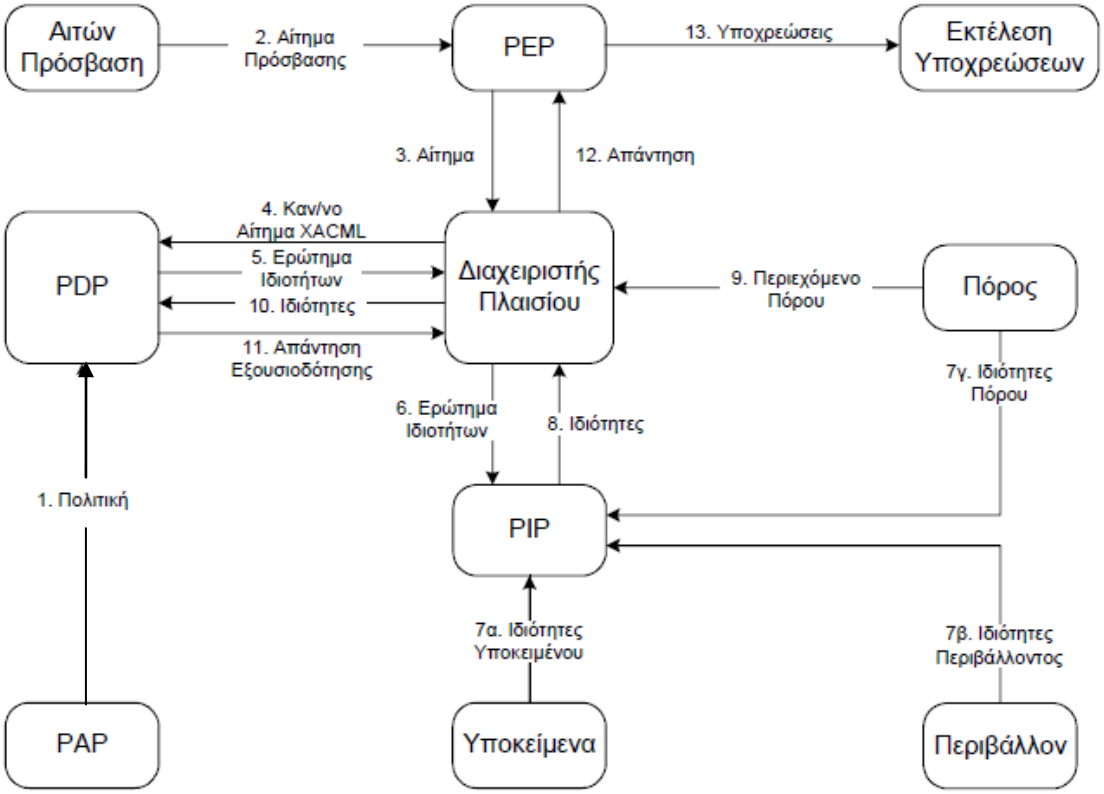
3.3.3 XACML

Η γλώσσα Επεκτάσιμης Γλώσσας Σήμανσης Ελέγχου Πρόσβασης (eXtensible Access Control Markup Language – XACML) [26][14] είναι μια από τις πιο γνωστές γλώσσες για την υποστήριξη μοντέλων ελέγχου πρόσβασης. Αποτελεί πρότυπο του οργανισμού Organization for the Advancement of Structured Information Standards (OASIS) [15] από το 2003. Είναι μια ευρέως υιοθετημένη τυπική γλώσσα για τον έλεγχο πρόσβασης, την παροχή άδειας και πολιτικών προστασίας.

Η XACML είναι μία γλώσσα που αποσκοπεί στον έλεγχο πρόσβασης των δεδομένων και ακολουθεί ένα συγκεκριμένο μοντέλο για να το πετύχει. Σύμφωνα με το μοντέλο αυτό, υπάρχουν τα αιτήματα για πρόσβαση σε ένα προστατευόμενο πόρο, τα οποία περνούν όλα από ένα αφαιρετικό δομικό στοιχείο, το Σημείο Εφαρμογής Πολιτικής (Policy Enforcement Point – PEP). Το στοιχείο αυτό, διαμορφώνει ένα αίτημα που αφορά μια σχετική απόφαση εξουσιοδότησης, το οποίο περιλαμβάνει την περιγραφή του αιτήματος που παρέλαβε, όπως για παράδειγμα ποιος πραγματοποιεί το αίτημα, ποιος πόρος αποτελεί το αντικείμενό του, τι λειτουργία ή ενέργεια πρόκειται να πραγματοποιηθεί, ποιος είναι ο σκοπός του, καθώς και κάθε άλλη σχετική πληροφορία.

Ακολούθως, το αίτημα που δημιουργήθηκε στέλνεται σε ένα άλλο αφαιρετικό δομικό στοιχείο, το Σημείο Απόφασης Πολιτικής (Policy Decision Point – PDP). Το στοιχείο PDP κοιτάζει τις πολιτικές και επιλέγει αυτές που ταιριάζουν και εξυπηρετούν το εν λόγω αίτημα, μαζί με τις επιπρόσθετες πληροφορίες που πιθανών να απαιτούνται για την διεκπεραίωση του αιτήματος. Τέλος, ακολουθεί η αποτίμηση του αιτήματος και το αποτέλεσμα που προκύπτει πηγαίνει στο σημείο PEP, όπου το αποτέλεσμα εφαρμόζεται, επιτρέποντας ή απαγορεύοντας την πρόσβαση στον εν λόγω προστατευμένο πόρο.

Ο τρόπος λειτουργίας της γλώσσας και του γενικότερου πλαισίου της XACML συνοψίζεται στο διάγραμμα ροής πληροφορίας που παρουσιάζεται στο Σχήμα 5 .



Σχήμα 5 : τρόπος λειτουργίας της γλώσσας και του γενικότερου πλαισίου της XACML [32]

Σύμφωνα με το σχήμα αυτό, το μοντέλο XACML ακολουθεί τα πιο κάτω βήματα [32]:

1. Οι πολιτικές ιδιωτικότητας γράφονται στο σημείο PAP και αφού γραφτούν γίνονται διαθέσιμες στο σημείο PDP.

2. Ο αιτητής που ζητά πρόσβαση σε κάποιο πόρο στέλνει το σχετικό αίτημα στο σημείο PEP.

3. Το αίτημα στέλνεται στο διαχειριστή πλαισίου, στην πρωταρχική του μορφή από το σημείο PEP για να δηλώσει ότι κάποιος θέλει να έχει πρόσβαση σε κάποιο πόρο.

4. Ο διαχειριστής πλαισίου δημιουργεί ένα κανονικοποιημένο αίτημα XACML και το στέλνει στο σημείο PDP.

5. Το σημείο PDP ζητά από το διαχειριστή πλαισίου οποιαδήποτε επιπλέον ιδιότητα του υποκειμένου, πόρου ή περιβάλλοντος.
6. Ο διαχειριστής πλαισίου ζητά τις ιδιότητες από το σημείο PIP.
7. Το σημείο PIP αποκτά τις ιδιότητες που αφορούν το σχετικό αίτημα.
8. Το σημείο PIP στέλνει στο διαχειριστή τις ιδιότητες που αφορούν το σχετικό αίτημα.
9. Ο διαχειριστής πλαισίου, προαιρετικά, ενσωματώνει τον πόρο στο σχετικό αίτημα.
10. Ο διαχειριστής πλαισίου στέλνει τις ιδιότητες που ζητήθηκαν και (προαιρετικά) τον πόρο στο σημείο PDP. Το σημείο PDP πραγματοποιεί την διεκπεραίωση του αιτήματος.
11. Το σημείο PDP στέλνει στο διαχειριστή πλαισίου το αποτέλεσμα της διεκπεραίωσης για την απόφαση εξουσιοδότησης.
12. Ο διαχειριστής πλαισίου μεταφράζει την απάντηση στην μορφή που αντιλαμβάνεται το σημείο PEP.
13. Το σημείο PEP εκτελεί τις υποχρεώσεις που προκύπτουν. Εφόσον σύμφωνα με την απόφαση εξουσιοδότησης η πρόσβαση επιτρέπεται, το σημείο PEP επιτρέπει την πρόσβαση στον ζητούμενο προστατευμένο πόρο. Σε διαφορετική περίπτωση, το σημείο PEP προβαίνει σε άρνηση της πρόσβασης.

Η γλώσσα XACML βασίζεται στις βασικές έννοιες που ακολουθούν [32]:

- Πόροι (Resources): Ως πόρος θεωρείται οτιδήποτε μπορεί να θεωρηθεί αντικείμενο ενός αιτήματος πρόσβασης. Για παράδειγμα πόροι μπορεί να είναι τα προσωπικά δεδομένα, οι υπηρεσίες, τα συστήματα, και λοιπά.
- Ενέργειες (Actions): Ως ενέργεια θεωρείται οποιαδήποτε λειτουργία μπορεί να συμβεί πάνω σε έναν πόρο που καλύπτεται από την πολιτική.
- Υποκείμενα (Subject): Ως υποκείμενο θεωρείται η οντότητα που επιτρέπεται να ζητά να πραγματοποιήσει κάποια ενέργεια σε κάποιο πόρο.
- Απόφαση Εξουσιοδότησης (Authorization Decision): Απόφαση Εξουσιοδότησης είναι το αποτέλεσμα της διεκπεραίωσης κάποιας πολιτικής. Μπορεί να λάβει τις τιμές: Έγκριση (Permit), Απαγόρευση (Deny) Απροσδιοριστία (Indeterminate) και Ανεφάρμοστο (Not Applicable). Προαιρετικά, η απόφαση εξουσιοδότησης μπορεί να προσδιορίζει και ένα σύνολο από υποχρεώσεις.

- Ιδιότητες (Attributes): Ως ιδιότητες μπορούν να θεωρηθούν τα διάφορα χαρακτηριστικά που αφορούν υποκείμενα, πόρους, ενέργειες, περιβάλλοντα. Για παράδειγμα, το όνομα ενός χρήστη αποτελεί τιμή μιας ιδιότητας.
- Περιβάλλον (Environment): Ως περιβάλλον μπορεί να θεωρηθεί το σύνολο των πιθανών ιδιοτήτων που σχετίζονται με μία απόφαση εξουσιοδότησης αλλά είναι ανεξάρτητες του υποκειμένου, του πόρου ή της ενέργειας.
- Υποχρέωση (Obligation): Ως υποχρέωση μπορεί να θεωρηθεί κάποια λειτουργία η οποία πρέπει να πραγματοποιηθεί κατά την εφαρμογή της απόφασης εξουσιοδότησης.
- Σημείο Απόφασης Πολιτικής (Policy Decision Point – PDP): Είναι η οντότητα του συστήματος που παίρνει τις κατάλληλες πολιτικές που αφορούν το αίτημα, πραγματοποιεί την διεκπεραίωση του αιτήματος και καταλήγει σε μία απόφαση εξουσιοδότησης.
- Σημείο Εφαρμογής Πολιτικής (Policy Enforcement Point – PEP): Είναι η οντότητα του συστήματος που πραγματοποιεί τον έλεγχο της πρόσβασης. Αρχικά, παίρνει το αίτημα από το χρήστη, το στέλνει στο διαχειριστή πλαισίου και μετά αφού γίνει η αποτίμηση του αιτήματος, λαμβάνει την απόφαση εξουσιοδότησης, εκτελεί και όποιες υποχρεώσεις προκύπτουν και λέει αν η πρόσβαση στον πόρο επιτρέπεται ή όχι.
- Σημείο Διαχείρισης Πολιτικής (Policy Administration Point – PAP): Είναι η οντότητα του συστήματος στο οποίο γράφονται οι πολιτικές.
- Σημείο Πληροφόρησης Πολιτικής (Policy Information Point – PIP): Είναι η οντότητα του συστήματος που παρέχει τις απαραίτητες τιμές των ιδιοτήτων.
- Διαχειριστής Πλαισίου (Context Handler): Είναι η οντότητα του συστήματος που παίρνει το αίτημα από το PEP και το μετατρέπει σε κανονική XACML μορφή για να το προωθήσει στο PDP. Είναι υπεύθυνη και για να μετατρέπει τις αποφάσεις εξουσιοδότησης που παίρνει από το PDP από την κανονική XACML μορφή στη μορφή εκείνη που αντιλαμβάνεται το σχετικό σύστημα και να τις στέλνει πίσω στο PEP.

Στην πολιτική XACML, υπάρχουν μηχανισμοί ελέγχου πρόσβασης, βασιζόμενοι σε έλεγχο πρόσβασης βάσει κανόνων (rule-based access control). Αφού δημιουργηθεί μια πολιτική για την προστασία ενός πόρου και αν υπάρχει κάποιο αίτημα πρόσβασης σε αυτόν, τότε οι συναρτήσεις ελέγχουν εάν τα χαρακτηριστικά του αιτήματος περιέχονται στους κανόνες πολιτικής. Μ' αυτό τον τρόπο, αν το αίτημα ακολουθεί τους κανόνες γίνεται αποδεκτό, αλλιώς απορρίπτεται.

Ένα XACML αρχείο αποτελείται από ένα ή περισσότερα PolicySet, πολιτικές (Policy), κανόνες (Rules), στόχους (Target) και υποχρεώσεις (Obligation). Ένα PolicySet, είναι ένα σύνολο από δηλώσεις πολιτικών. Μία πολιτική, είναι μια δήλωση πολιτικής που αποτελείται από ένα σύνολο κανόνων. Ένας κανόνας, αναπαριστά ένα κανόνα ο οποίος καθορίζει το ποιος μπορεί να έχει πρόσβαση σε τι. Πρέπει οπωσδήποτε να εμπεριέχεται σε μια πολιτική. Ένας κανόνας περιλαμβάνει ένα στόχο, μια συνθήκη (Condition) και μια επίδραση (Effect). Η συνθήκη κανονίζει τους περιορισμούς σχετικά με τις τιμές των ιδιοτήτων που πρέπει να ισχύουν σε κάποιο αίτημα. Είναι επιπρόσθετοι υπολογισμοί για να καθοριστεί εάν ισχύει ένας κανόνας. Η επίδραση προσδιορίζει την απόφαση που πρέπει να ληφθεί. Υπάρχει και ο αλγόριθμος συνδυασμού κανόνων που ορίζει τη διαδικασία βάσει της οποίας πολλαπλοί κανόνες καταλήγουν σε ένα συνδυαστικό αποτέλεσμα.

Ένα κύριο χαρακτηριστικό της πολιτικής XACML είναι το στοιχείο Στόχος (Target), το οποίο επισυνάπτεται σε κανόνες, σε πολιτικές και PolicySet, για τους σκοπούς της πολιτικής ευρετηρίασης. Ο Στόχος ορίζεται από τους πόρους, τις δράσεις, τα θέματα και τα περιβάλλοντα, όπου ισχύει ο κανόνας ή η πολιτική. Για απάντηση στο αίτημα, το PDP θα ψάξει για τις πολιτικές που ισχύουν, αξιολογώντας τους στόχους τους. Ο στόχος είναι αυτό που καθορίζει αν ένα PolicySet, μια πολιτική ή ένας κανόνας ισχύει. Υποχρεώσεις είναι συμπληρωματικές εργασίες που πρέπει να εκτελέσει η PEP κατά την επιβολή της άδειας. Η XACML γλώσσα, χαρακτηρίζεται από επεκτασιμότητα. Επιτρέπει σε πολύ σύνθετες πολιτικές εκφράσεις να γραφτούν με την χρήση των στοιχείων Attributes, Data-types, και Functions. Αυτά χρησιμοποιούνται στη δήλωση υποκειμένων, στόχων, πόρων, περιβαλλόντων, συνθηκών και υποχρεώσεων.

Οι απλοί περιορισμοί που βοηθούν στο να καθοριστούν τα αιτήματα, μπορούν να διαχωριστούν σε ένα στόχο (Target). Αυτό επιτρέπει την πιο αποτελεσματική αξιολόγηση των κανόνων. Οι πιο πολύπλοκοι περιορισμοί πάνε σε μια συνθήκη (Condition). Στη συνθήκη οι περιορισμοί μπορούν να συνδυάζονται με χρήση Boolean τελεστών και λειτουργίες όπως η αριθμητική μπορούν να εφαρμοστούν σε μεταβλητές. Ένας κανόνας ικανοποιείται αν και το ο στόχος και η συνθήκη αξιολογούνται σε True, όταν αξιολογούνται με βάση τα χαρακτηριστικά που σχετίζονται με το αίτημα. Κάθε κανόνας έχει ένα αποτέλεσμα Permit or Deny. Αν ένα από τα δύο (Target ή Condition) είναι False τότε επιστρέφεται Not Applicable. Αν ένα λάθος εντοπιστεί στην αξιολόγηση του Target ή του Condition επιστρέφεται Indeterminate.

Ένα αίτημα περιλαμβάνει το Υποκείμενο (Subject), τον Πόρο (Resource), την ενέργεια (Action) και το περιβάλλον (Environment). Κάθε ένα περιλαμβάνει και τις ιδιότητες του.

```
<Request …>
 <Subject>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
        DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>John</AttributeValue> </Attribute>
</Subject>
<Resource>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
        DataType="http://www.w3.org/2001/XMLSchema#anyURI">
        <AttributeValue>Door</AttributeValue> </Attribute>
</Resource>
 <Action>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
        DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>open</AttributeValue> </Attribute>
</Action>
</Request>
```

Σχήμα 6 : Παράδειγμα αιτήματος στην XACML

```
<Policy PolicyId="SamplePolicy"
            RuleCombiningAlgId="rule-combining-algorithm:permit-overrides">
<Target>
<Subjects>
         <AnySubject/>
</Subjects>
<Resources>
      <ResourceMatch MatchId="function:string-equal">
            <AttributeValue DataType="string">SampleServer</AttributeValue>
            <ResourceAttributeDesignator                                DataType="string"
          AttributeId="resource:resource-id"/>
      </ResourceMatch>
</Resources>
<Actions>
      <AnyAction/>
</Actions>
</Target>

<Rule RuleId="LoginRule" Effect="Permit">
<Target>
<Subjects>
     <AnySubject/>
</Subjects>
<Resources>
      <AnyResource/>
</Resources>
<Actions>
      <ActionMatch MatchId="function:string-equal">
            <AttributeValue DataType="string">login</AttributeValue>
            <ActionAttributeDesignator DataType="string" AttributeId="ServerAction"/>
     </ActionMatch>
</Actions>
</Target>
```

```
<Condition FunctionId="function:and">
<Apply FunctionId="function:time-greater-than-or-equal"
        <Apply FunctionId="function:time-one-and-only">
        <EnvironmentAttributeSelector DataType="time"
          AttributeId="environment:current-time"/>
        </Apply>
        <AttributeValue DataType="time">09:00:00</AttributeValue>
</Apply>
<Apply FunctionId="function:time-less-than-or-equal"
        <Apply FunctionId="function:time-one-and-only">
        <EnvironmentAttributeSelector DataType="time"
        AttributeId="environment:current-time"/>
        </Apply>
        <AttributeValue DataType="time">17:00:00</AttributeValue>
</Apply>
</Condition>
</Rule>

<Rule RuleId="FinalRule" Effect="Deny"/>
</Policy>
```

Σχήμα 7 : Γενικό Παράδειγμα Πολιτικής XACML [32]

Η πολιτική του παραδείγματος, ελέγχει την πρόσβαση σε κάποιο εξυπηρετητή με όνομα SampleServer στον οποίο συνδέονται χρήστες (login). Ο πρώτος Κανόνας περιλαμβάνει μία Συνθήκη η οποία θέτει περιορισμό στο χρόνο κατά τον οποίο οι χρήστες μπορούν να συνδεθούν (09:00 – 17:00), ενώ εφόσον ο πρώτος κανόνας δεν ικανοποιηθεί, η πρόσβαση δε γίνεται δεκτή σύμφωνα με το δεύτερο Κανόνα.

Κεφάλαιο 4

Αξιολόγηση και Σύγκριση Γλωσσών Πολιτικών Ιδιωτικότητας

4.1 Αξιολογήσεις

4.1.1 Αξιολόγηση της P3P

Η πλατφόρμα για προτιμήσεις ιδιωτικού απορρήτου P3P, είναι μια προσπάθεια παροχής μιας τυποποιημένης γλώσσας, βασισμένης σε XML πολιτικής, που μπορεί να χρησιμοποιηθεί για να καθοριστούν οι πρακτικές προστασίας προσωπικών δεδομένων ενός οργανισμού με έναν τρόπο που μπορεί να αναλυθεί και να χρησιμοποιηθεί από παράγοντες της πολιτικής ελέγχου για λογαριασμό του χρήστη.

Η P3P είναι μια αναγνώσιμη από τη μηχανή γλώσσα που βοηθά να εκφραστούν πρακτικές διαχείρισης των δεδομένων ενός ιστότοπου. Η P3P είναι κατάλληλη για την έκφραση υψηλού επιπέδου πολιτικών ιστοσελίδων. Επιτρέπει σε έναν οργανισμό να καθορίσει τις πρακτικές προστασίας συλλογής και χρήσης προσωπικών δεδομένων

χρηστών του δικτυακού τόπου σε μορφή αναγνώσιμη από μηχάνημα. Οι προδιαγραφές της P3P ελέγχονται από ένα Web Browser ή κάποιο user agent για να διαπιστωθεί αν ο οργανισμός ακολουθεί τις πρακτικές προστασίας προσωπικών δεδομένων του χρήστη. Αυτή η διαδικασία είναι μερικές φορές αυτοματοποιημένη μέσω του λογισμικού σε μορφή ερώτησης-απάντησης. Εξασφαλίζει προστασία για τους σκοπούς συλλογής πληροφοριών, το ποιος τις συλλέγει και τις χρησιμοποιεί και τη χρονική διάρκεια διατήρησης της εν λόγω πληροφορίας.

Το πρωτόκολλο P3P έχει δύο μέρη : 1) Τις πολιτικές ιδιωτικότητας/απορρήτου, όπου μια ιστοσελίδα μπορεί να ορίσει τις πρακτικές συλλογής και χρήσης δεδομένων χρησιμοποιώντας P3P και 2) Τις προτιμήσεις προστασίας προσωπικών δεδομένων, όπου οι πελάτες μπορούν να καθορίσουν τις προτιμήσεις της ιδιωτικής τους ζωής χρησιμοποιώντας APPEL. Ακολούθως, γίνεται έλεγχος αν οι προτιμήσεις του χρήστη ταιριάζουν με τις πολιτικές απορρήτου. Έτσι, τα έγγραφα πολιτικής P3P, μας βοηθούν να αναλύουμε και να αξιολογούμε βάσει προκαθορισμένων προτιμήσεων που δίνει ένας χρήστης το πώς και πότε οι πληροφορίες που συλλέγονται μπορούν να χρησιμοποιηθούν. Υπάρχουν πολλοί πράκτορες λογισμικού (user agents) που χειρίζονται τον έλεγχο της πολιτικής και επικαλούνται τις απαραίτητες ενέργειες που πρέπει να συμβούν όταν η πολιτική μιας ιστοσελίδας βρίσκεται σε σύγκρουση με τις προτιμήσεις του χρήστη. Με αυτή την τεχνολογία οι χρήστες P3P μπορούν να αυτοματοποιούν την περιορισμένη πολιτική προστασίας προσωπικών δεδομένων, σε μια προσπάθεια να ελέγχουν καλύτερα το πώς οι πληροφορίες τους συλλέγονται, αποθηκεύονται και χρησιμοποιούνται.

Η P3P διαχειρίζεται τις πληροφορίες μέσω των πολιτικών προστασίας της ιδιωτικής ζωής. Όταν μια ιστοσελίδα χρησιμοποιεί P3P, τότε θέτουν ένα σύνολο από πολιτικές που τους επιτρέπουν να δηλώνουν τις προβλεπόμενες χρήσεις τους, όσον αφορά τις προσωπικές πληροφορίες που πιθανόν να συγκεντρωθούν από τους επισκέπτες στην ιστοσελίδα τους. Όταν ένας χρήστης αποφασίσει να χρησιμοποιήσει P3P, θέτει τις δικές του προτιμήσεις της ιδιωτικής του ζωής και ποιες προσωπικές πληροφορίες του θα επιτρέψει να δοθούν στους δικτυακούς τόπους που επισκέπτεται μέσω της APPEL. Στη συνέχεια, όταν ο χρήστης επισκέπτεται μια ιστοσελίδα, η P3P μέσω Web Browser ή κάποιου User Agent, θα συγκρίνει ποιες προσωπικές πληροφορίες ο χρήστης είναι

διατεθειμένος να απελευθερώσει και τι πληροφορίες ο διακομιστής θέλει να πάρει. Εάν τα δύο δεν ταιριάζουν και υπάρξει σύγκρουση, η P3P θα ενημερώσει το χρήστη και θα τον ρωτήσει αν αυτός / αυτή είναι πρόθυμος να προχωρήσει ή όχι.

Το πρωτόκολλο P3P, επιτρέπει στους χρήστες να καθορίσουν τις προτιμήσεις της ιδιωτικής τους ζωής μια φορά, έτσι ώστε να μπορούν να συγκριθούν αυτόματα με την πολιτική απορρήτου ενός ιστότοπου κάθε φορά που ο χώρος είναι επισκέψιμος. Με αυτή τη σαφήνεια και την ευκολία χρήσης, η P3P προωθεί τη διαφάνεια και αυξάνει έτσι τη λογοδοσία από την πλευρά του ιδιοκτήτη της ιστοσελίδας.

Ένα από τα μεγαλύτερα προβλήματα της γλώσσας P3P, είναι ότι δεν υπάρχει κάποιος μηχανισμός που να εξασφαλίζει στον χρήστη ότι οι υποσχέσεις που του δίνονται θα τηρηθούν. Η P3P, παρέχει απλά την δυνατότητα σε διάφορους ιστότοπους να εκφράζουν πολιτικές σχετικά με την προστασία των προσωπικών δεδομένων των χρηστών. Αν και προσφέρει ένα τεχνικό μηχανισμό, ο οποίος εξασφαλίζει οι χρήστες να έχουν τη δυνατότητα να ενημερώνονται σχετικά με τις πολιτικές ιδιωτικότητας πριν την ανακοίνωση προσωπικών τους πληροφοριών, δεν προσφέρει κανένα μηχανισμό που να εξασφαλίζει ότι οι ιστοσελίδες συμπεριφέρονται βάσει των πολιτικών τους.

Ένα άλλο πρόβλημα είναι το γεγονός ότι οι πολιτικές P3P υπόκεινται σε πολλαπλές ερμηνείες και διαφορετικοί πράκτορες λογισμικού που τις διαβάζουν μπορεί να καταλήξουν σε διαφορετικά συμπεράσματα για την ίδια πολιτική. Επίσης, μετά την αρχική κοινοποίηση των προσωπικών πληροφοριών, ο χρήστης δεν έχει κανένα μηχανισμό επιβολής. Ακόμα, ένα χαρακτηριστικό της P3P, είναι ότι επικεντρώνεται κυρίως στο πώς και για ποιο σκοπό χρησιμοποιούνται οι πληροφορίες που συλλέγονται και όχι για το πώς και ποιος μπορεί να έχει πρόσβαση στις πληροφορίες που συλλέγονται. Επικεντρώνεται στα δεδομένα και τις πληροφορίες.

Επίσης, η P3P δεν υποστηρίζει διαφορετικές πολιτικές για διαφορετικούς χρήστες, αν και προσφέρει στους χρήστες μια επιλογή από πολιτικές P3P. Ακόμη το σύστημα αντιστοίχισης των APPEL πολιτικών είναι προβληματικό. Μια πολιτική P3P μπορεί να περιέχει πολλές δηλώσεις. Όταν ένας κανόνας όμως επιλυθεί με αποτυχία, θα σταματήσουν οι ενέργειες για εντοπισμό σε άλλες δηλώσεις, έτσι ώστε να δούμε αν έχει

κάποια που να τον ικανοποιεί. Λόγω αυτής της έλλειψης η APPEL λειτουργεί σωστά, μόνο όταν οι κανόνες εκφράζουν αυτό που δεν είναι αποδεκτό.

Παρά το γεγονός ότι P3P έχει λάβει ευρεία προσοχή, δεδομένου ότι προτάθηκε, η έγκρισή της υπήρξε αργή. Ένας βασικός λόγος για την αργή υιοθέτηση της είναι ότι δεν έχει μια επίσημη και ακριβή σημασιολογία. Ως εκ τούτου, μια πολιτική P3P μπορεί να είναι εγγενώς ασαφής και μπερδεμένη τόσο για τους τελικούς χρήστες όσο και για τους πράκτορες χρήστη. Η ανάπτυξη μιας τυπικής αυστηρής σημασιολογίας για τη P3P, είναι κάτι το αρκετά δύσκολο. Για την ανάπτυξη μιας τυπικής σημασιολογίας πρέπει πρώτα να καθοριστούν οι σχέσεις μεταξύ των τεσσάρων κύριων συστατικών (σκοπού, παραλήπτη, χρονικής διάρκειας και δεδομένων) της δήλωσης P3P. Το γεγονός ότι η ίδια έννοια μπορεί να κωδικοποιηθεί με διαφορετικούς τρόπους, καθιστά πολύ δύσκολο να εκφραστούν σωστά οι προτιμήσεις ιδιωτικότητας στην APPEL. Μια γλώσσα προτιμήσεων βασισμένη σε μια τυπική σημασιολογία θα πρέπει να εξασφαλίζει ότι η ίδια έννοια θα αντιμετωπίζεται πάντα με τον ίδιο τρόπο. Μια προσπάθεια που έγινε ονομάζεται data-centric semantics for P3P. Η ανάπτυξη μιας αυστηρής τυπικής σημασιολογίας είναι ένα σημαντικό βήμα προς τη βελτίωση της P3P καθιστώντας την πιο κατάλληλη για να ενσωματωθεί με μια επιχειρηματική πρακτική και την επιτάχυνση της υιοθέτησης της P3P σε ολόκληρο το Διαδίκτυο.

Παρόλα αυτά η P3P είναι συμπληρωματική σε κανονισμούς και αυτορυθμιζόμενα προγράμματα που παρέχουν μηχανισμούς επιβολής και χρησιμοποιείται σε πολλές διαδικτυακές εφαρμογές. Επιπλέον, παρέχοντας ένα ανοιχτό πρότυπο για την έκφραση των πολιτικών προστασίας της ιδιωτικής ζωής, η P3P καθιστά δυνατό τον ακριβής και αυτόματο χαρακτηρισμό και τη φραγή των ιστοσελίδων των οποίων η πολιτική προστασίας προσωπικών δεδομένων δεν πληρούν ορισμένες προδιαγραφές. Κατά συνέπεια, ενθαρρύνει την ανάπτυξη νέων προϊόντων και υπηρεσιών που βελτιώνουν την προστασία της ιδιωτικής ζωής και μπορεί να είναι χρήσιμη σε συμμόρφωση αστυνόμευσης για τις χώρες που έχουν την προστασία των δεδομένων και της ιδιωτικής ζωής σαν νόμο. Το πρωτόκολλο P3P εμφανίζει τη μεγαλύτερη διάδοση έχοντας ευρείας κλίμακας εφαρμογή.

4.1.2 Αξιολόγηση της EPAL

Η EPAL είναι επίσης μια πολιτική προστασίας προσωπικών δεδομένων προδιαγραφών της γλώσσας βασισμένη σε XML, αλλά έχει σχεδιαστεί για οργανισμούς έτσι ώστε να καθορίζουν τις εσωτερικές πολιτικές προστασίας της ιδιωτικής ζωής. Οι EPAL πολιτικές μπορούν να χρησιμοποιηθούν εσωτερικά και μεταξύ του οργανισμού και των επιχειρηματικών συνεταίρων του για να εξασφαλίσουν τη συμμόρφωση με τις βασικές πολιτικές του καθένα.

Η EPAL επιτρέπει στους οργανισμούς να καθορίσουν τις πρακτικές προστασίας της ιδιωτικής ζωής τους κατά τρόπο ώστε, ο ίδιος ο οργανισμός αλλά και άλλοι οργανισμοί με τους οποίους αλληλεπιδρούν, να μπορούν να διαβάσουν και να χρησιμοποιήσουν πληροφορίες. Ο οργανισμός ορίζει ένα ειδικό λεξιλόγιο για τις ανάγκες του, και η μόνη απαίτηση που προκύπτει είναι ότι κάθε παράγοντας που θέλει να χρησιμοποιήσει την πολιτική που διέπει τις αλληλεπιδράσεις του, πρέπει να συμφωνήσει και να κατανοήσει το λεξιλόγιο που χρησιμοποιείται.

Η EPAL γενικά, ακολουθεί ένα αλγόριθμο σύμφωνα με τον οποίο γίνεται έλεγχος στους κανόνες βάσει του αιτήματος και επιστρέφεται το αποτέλεσμα από τον πρώτο κανόνα που εφαρμόζεται και οι προϋποθέσεις του ικανοποιούνται. Υπάρχουν δύο στοιχεία σε μια πολιτική EPAL. Το λεξιλόγιο της πολιτικής και οι κανόνες της πολιτικής. Το λεξιλόγιο της πολιτικής αντιπροσωπεύει τις έννοιες από την πολιτική κειμένου φυσικής γλώσσας που πρέπει να ακολουθούνται. Ένας συγγραφέας μιας πολιτικής EPAL, χρησιμοποιεί την πολιτική κειμένου φυσικής γλώσσας για την ανάπτυξη των εννοιολογικών στοιχείων για το λεξιλόγιο της πολιτικής. Το λεξιλόγιο της πολιτικής είναι το πιο σημαντικό κομμάτι της και ορίζει το πεδίο εφαρμογής της πολιτικής. Υπάρχει μόνο ένα λεξιλόγιο για κάθε πολιτική. Οι πολιτικές μπορεί να καλύπτουν δεδομένα που ορίζονται από πολλαπλούς κανόνες, όμως πρέπει να τα βάλουν όλα σε ένα λεξιλόγιο. Το λεξιλόγιο ορίζει όλα τα χαρακτηριστικά και όλες τις υποχρεώσεις. Οι κανόνες της πολιτικής εκφράζουν τις πρακτικές χειρισμού δεδομένων που είτε επιτρέπονται ή όχι από την πολιτική κειμένου φυσικής γλώσσας. Στους κανόνες περιλαμβάνονται και όλες οι υποχρεώσεις συσχετιζόμενες με το αναγνωριστικό ενός κανόνα (Rule Identifier).

Η EPAL επικεντρώνεται στην πρόσβαση. Έχει ένα σύνολο κανόνων που αναφέρονται σε συγκεκριμένες πληροφορίες πρόσβασης και χρήσης εμπιστευτικών πληροφοριών των πελατών. Ο τρόπος που οι προδιαγραφές EPAL είναι γραμμένες παραλληλίζεται κάπως με τον τρόπο με τον οποίο οι πολιτικές της φυσικής γλώσσας είναι γραμμένες.

Οι στόχοι της γλώσσας είναι η κωδικοποίηση πολιτικών χειρισμού δεδομένων και πρακτικών που σχετίζονται με προσωπικά δεδομένα μιας επιχείρησης και η γλώσσα να μπορεί να εισάγεται και να εκτελείται από ένα σύστημα επιβολής ιδιωτικότητας. Η γλώσσα EPAL δεν χρησιμοποιείται για άμεση κωδικοποίηση ή επιβολή συγκεκριμένης νομοθεσίας προστασίας της ιδιωτικής ζωής σε μια γενική και πλήρη εφαρμογή και σε επιχειρήσεις με ανεξάρτητο τρόπο. Δεν χρησιμοποιείται ούτε για χειρισμό της από χρήστες για να πουν τις προτιμήσεις τους, ούτε για δημιουργία νέων μηχανισμών ή σύνταξης για αναπαράσταση δεδομένων.

Η EPAL δεν έχει τρόπο να καθορίζει πολλούς υπεύθυνους οργανισμούς σε μια πολιτική, όταν πολλοί οργανισμοί θέλουν να έχουν πρόσβαση στα ίδια δεδομένα. Η γλώσσα EPAL, δεν επιτρέπει τις φωλιασμένες πολιτικές, δηλαδή δεν υποστηρίζει ιεραρχίες πολιτικών. Δεν υποστηρίζει κατανεμημένες πολιτικές, δηλαδή δεν επιτρέπει αναφορές σε πολιτικές. Επίσης, μόνο ένα θέμα (subject) επιτρέπει σε κάθε αίτημα πρόσβασης (access request). Κάθε πολιτική είναι ξεχωριστή γλώσσα χωρίς καθορισμένο μηχανισμό για το συνδυασμό των αποτελεσμάτων από πολλαπλές πολιτικές που μπορεί να ισχύει για ένα συγκεκριμένο αίτημα.

Το σημασιολογικό μοντέλο αναπαράστασης της EPAL δεν είναι καθόλου ικανοποιητικό, επειδή η EPAL βασίζεται μόνο σε ένα λογικό πρόγραμμα, έτσι ώστε να διαθέτει μια καλά καθορισμένη αυστηρή σημασιολογία για τη δική της δομή μοντέλου δεδομένων για να καθορίζει τις πολιτικές ελέγχου πρόσβασης δεδομένων. Η σημασιολογία της πολιτικής προστασίας της ιδιωτικής ζωής EPAL, είναι μια συνάρτηση που αξιολογεί ένα ερώτημα με βάση μια δεδομένη ανάθεση των μεταβλητών και επιστρέφει ως αποτέλεσμα μια απόφαση και μια σειρά από σχετικές υποχρεώσεις. Το μοντέλο της EPAL μπορεί να εκφραστεί και σε μορφή της Prolog [19]. Όλες οι πληροφορίες που περιέχονται στην EPAL μπορούν εύκολα να αποθηκεύονται σε μια βάση δεδομένων της Prolog και έτσι, να μπορούμε να

χρησιμοποιήσουμε την Prolog για να εκτελέσει ελέγχους συνέπειας για τις πολιτικές προστασίας της ιδιωτικής ζωής και να αξιολογήσει τα ερωτήματα πρόσβασης.

Γενικά, η EPAL είναι ένα υποσύνολο της XACML, η οποία αξιολογείται στην συνέχεια. Η EPAL δεν είναι τόσο εξελιγμένη και αποτελεσματική όσο αυτή.

4.1.3 Αξιολόγηση της XACML

Η XACML αποτελεί πρότυπο του οργανισμού OASIS. Ο στόχος της XACML είναι να προτείνει μια κοινή γλώσσα μέσω της οποίας μια επιχείρηση μπορεί να διαχειριστεί την εφαρμογή όλων των στοιχείων της πολιτικής ασφάλειας της σε όλες τις συνιστώσες του συστήματος πληροφοριών της. Η XACML χρησιμοποιεί σύνταξη XML αφού η σύνταξη και η σημασιολογία XML είναι επεκτάσιμη για να ικανοποιήσει τις απαιτήσεις του XACML.

Η XACML, σκοπεύει στο να εκφράσει καλά εδραιωμένες ιδέες στον τομέα της πολιτικής ελέγχου πρόσβασης, χρησιμοποιώντας μια επέκταση της γλώσσας XML. Είναι μια ευρέως υιοθετημένη τυπική γλώσσα για τον έλεγχο πρόσβασης, την παροχή άδειας και πολιτικών προστασίας.

Στην πολιτική XACML, υπάρχουν μηχανισμοί ελέγχου πρόσβασης, βασιζόμενοι σε έλεγχο πρόσβασης βάσει κανόνων (rule-based access control). Αφού δημιουργηθεί μια πολιτική για την προστασία ενός πόρου και αν υπάρχει κάποιο αίτημα πρόσβασης σε αυτόν, τότε οι συναρτήσεις ελέγχουν εάν τα χαρακτηριστικά του αιτήματος περιέχονται στους κανόνες πολιτικής. Μ’ αυτό τον τρόπο, αν το αίτημα ακολουθεί τους κανόνες γίνεται αποδεκτό, αλλιώς απορρίπτεται.

Η XACML είναι γενική γλώσσα. Αυτό σημαίνει ότι αντί να προσπαθεί να παρέχει έλεγχο πρόσβασης για ένα συγκεκριμένο περιβάλλον ή ένα συγκεκριμένο είδος πόρων, μπορεί να χρησιμοποιηθεί σε οποιοδήποτε περιβάλλον. Είναι επίσης και κατανεμημένη. Αυτό σημαίνει ότι η πολιτική μπορεί να γραφεί και να έχει αναφορές και να παραπέμπει σε άλλες πολιτικές που διατηρούνται σε αυθαίρετες τοποθεσίες. Το αποτέλεσμα είναι ότι διαφορετικά άτομα ή ομάδες, αντί να χρειάζεται να διαχειριστούν

μια ενιαία μονολιθική πολιτική, μπορούν να διαχειριστούν ξεχωριστά επιμέρους πολιτικές ανάλογα με την περίπτωση. Η XACML ξέρει πώς να συνδυάσει σωστά τα αποτελέσματα από αυτές τις διαφορετικές πολιτικές σε μία απόφαση. Επίσης, η XACML γλώσσα, χαρακτηρίζεται από επεκτασιμότητα. Επιτρέπει σε πολύ σύνθετες πολιτικές εκφράσεις να γραφτούν με την χρήση των στοιχείων Attributes, Data-types, και Functions. Αυτά χρησιμοποιούνται στη δήλωση υποκειμένων, στόχων, πόρων, περιβαλλόντων, συνθηκών και υποχρεώσεων. Η XACML επιτρέπει τις φωλιασμένες πολιτικές, δηλαδή υποστηρίζει ιεραρχίες πολιτικών.

Τι συμβαίνει στην XACML αν υπάρχουν 2 κανόνες (ή πολιτικές) που έρχονται σε αντίθεση μεταξύ τους; Φανταστείτε, για παράδειγμα, ένα πρώτο κανόνα που λέει ότι οι διαχειριστές μπορούν να δουν τα έγγραφα και ένα δεύτερο κανόνα που λέει ότι κανείς δεν μπορεί να λειτουργήσει πριν τις 9πμ. Τι θα συμβεί αν το αίτημα θέλει την Alice που είναι διαχειρίστρια να προσπαθεί να χρησιμοποιήσει ένα έγγραφο στις 8πμ; Ποιος κανόνας θα υπερισχύσει; Η XACML ορίζει μια σειρά από συνδυασμούς αλγορίθμων που μπορούν να ταυτοποιηθούν με ένα RuleCombiningAlgId ή PolicyCombiningAlgId χαρακτηριστικό των <Policy> ή <PolicySet> στοιχείων, αντίστοιχα. Ο αλγόριθμος για συνδυασμό κανόνων ορίζει μια διαδικασία για να καταλήξει σε μια απόφαση πρόσβασης, δεδομένων των αποτελεσμάτων της αξιολόγησης ενός συνόλου κανόνων. Ομοίως, ο αλγόριθμος για συνδυασμό πολιτικών καθορίζει μια διαδικασία για να καταλήξει σε μια απόφαση πρόσβασης, δεδομένων των αποτελεσμάτων της αξιολόγησης ενός συνόλου πολιτικών.

Υπάρχουν τέσσερις αλγόριθμοι συνδυασμών κανόνων/πολιτικών. 1. Η άρνηση υπερισχύει (Deny-overrides). Εάν ένα <Rule> ή <Policy> στοιχείο αποτιμάται σε "Άρνηση", τότε ανεξάρτητα από το αποτέλεσμα της αξιολόγησης των άλλων <Rule> ή <Policy> στοιχείων, το συνδυασμένο αποτέλεσμα είναι "Άρνηση". 2. Η έγκριση υπερισχύει (Permit-overrides). Εάν ένα <Rule> ή <Policy> στοιχείο αποτιμάται σε "Έγκριση", τότε ανεξάρτητα από το αποτέλεσμα της αξιολόγησης των άλλων <Rule> ή <Policy> στοιχείων, το συνδυασμένο αποτέλεσμα είναι "Έγκριση". 3. Το πρώτο που εφαρμόζεται (First-Applicable). Στην περίπτωση αυτή, το συνδυασμένο αποτέλεσμα είναι το ίδιο με το αποτέλεσμα της αξιολόγησης του πρώτου <Rule>, <Policy> ή <PolicySet> στοιχείου, το οποίο εφαρμόζεται σε ένα αίτημα πρόσβασης. 4. Μόνο ένα

ισχύει (Only-one-applicable). Αυτός ο αλγόριθμος συνδυασμού ισχύει μόνο για τις πολιτικές, και το αποτέλεσμα διασφαλίζει ότι μόνο μία πολιτική ή σύνολο πολιτικών μπορεί να ισχύει για το αίτημα πρόσβασης. Εάν δεν υπάρχει πολιτική ή σύνολο πολιτικών που ισχύει για το αίτημα πρόσβασης, τότε ένα "Not applicable" αποτέλεσμα επιστρέφεται. Από την άλλη πλευρά, εάν περισσότερα από ένα σύνολο πολιτικών ή πολιτική ισχύει για το αίτημα πρόσβασης, τότε το αποτέλεσμα είναι "Indeterminate".

Συγκρούσεις σε κανόνες και πολιτικές μπορούν να εντοπιστούν και να διασφαλιστούν κατά την εκτέλεση ενός αιτήματος. Οι έλεγχοι γίνονται στο σημείο PDP όπου παίρνει το αίτημα και τις πολιτικές και αν υπάρχει σύγκρουση στις πολιτικές ή τους κανόνες εφαρμόζονται οι ποιο πάνω αλγόριθμοι.

Μια πολιτική σε XACML, συμπεριλαμβανομένων όλων των επιμέρους πολιτικών της, αξιολογείται μόνο εάν ο στόχος (target) της πολιτικής ικανοποιείται. Η XACML παρέχει ένα πιο φυσικό τρόπο καθορισμού των ιεραρχιών ρόλων, των δικαιωμάτων, την εκχώρηση δικαιωμάτων ρόλων και υποστηρίζει την ιδέα των πολύπλοκων δικαιωμάτων που χρησιμοποιούνται στα συστήματα που μοντελοποιούν μοντέλα εφαρμογής ελέγχου πρόσβασης βάσει ρόλου (role-based access control models) για κατανεμημένα περιβάλλοντα.

Όμως έχει και η XACML τα μειονεκτήματά της. Οι Πολιτικές XACML είναι δύσκολο να γραφτούν σε σχέση με τη σύνταξη και τη σημασιολογία. Η Σύνταξη XACML είναι φλύαρη και δημιουργεί πολύ μεγάλες πολιτικές. Απλές πολιτικές δημιουργούν μεγάλο κείμενο XML που δεν είναι εύκολο για έναν άνθρωπο να το γράψει ή να το διαβάσει. Είναι επίσης δύσκολο να εξακριβωθεί η σημασιολογική ορθότητα μιας πολιτικής XACML. Η σημασιολογική ορθότητα είναι ζωτικής σημασίας δεδομένου ότι σημασιολογικά λάθη θα οδηγήσουν σε τρωτά σημεία που μπορούν να διευκολύνουν παράνομες προσβάσεις στο προστατευόμενο πόρο.

Η XACML χρησιμοποιεί μια γενική λειτουργική γλώσσα περιορισμών που εξαρτάται μόνο από τη σημασιολογία των γενικών τύπων δεδομένων των διαφόρων ειδών πολιτικών, οι οποίες καθορίζονται με μοναδικά αναγνωριστικά. Από μόνη της δεν έχει μια καθορισμένη αυστηρή σημασιολογία. Έτσι είναι επιθυμητό να υπάρξει μια τυπική

περιγραφή της σημασιολογίας της XACML για να αποφευχθούν ασάφειες και παρερμηνείες. Η τυπική σημασιολογία μπορεί να περιγραφεί μέσω της γλώσσας Haskell [6].

Η XACML όμως, είναι πρότυπο (standard). Αυτό, λειτουργεί σαν ένα πολύ θετικό στοιχείο αφού με τη χρήση μιας πρότυπης γλώσσας, γίνεται χρήση ενός αντικειμένου που έχει αξιολογηθεί από μια μεγάλη κοινότητα εμπειρογνωμόνων και χρηστών. Η XACML γίνεται όλο και πιο ευρέως διαδεδομένη, και έτσι της είναι ευκολότερο να λειτουργεί σε συνεργασία με άλλες εφαρμογές που χρησιμοποιούν το ίδιο πρότυπο γλώσσας.

Η XACML υιοθετείται όλο και περισσότερο σε μεγάλα συστήματα των επιχειρήσεων για συγκεκριμένες πολιτικές ελέγχου πρόσβασης. Παρέχει πολιτικές και την ενσωμάτωσή τους σε μεγάλα κατανεμημένα συστήματα με πολλαπλά αυτόνομα μέρη. Χωρίς τυποποιημένη γλώσσα ελέγχου πρόσβασης, ο έλεγχος πρόσβασης διαχείρισης σε τέτοια συστήματα μπορεί να είναι εφιάλτης.

4.2 Συγκρίσεις

4.2.1 Σύγκριση P3P – EPAL [31]

Τόσο η P3P όσο και η EPAL είναι δύο πολιτικές βασισμένες στην XML. Η EPAL δημιουργήθηκε αργότερα από την P3P. Η P3P δημιουργήθηκε από την κοινοπραξία W3C για τις ιστοσελίδες και το διαδίκτυο, ενώ η EPAL από την IBM για τις επιχειρήσεις και τους οργανισμούς.

Η P3P χρησιμοποιείται για να δημοσιεύει την πολιτική προστασίας της ιδιωτικής ζωής των επιχειρήσεων, προκειμένου να συλλέγει προσωπικές πληροφορίες από τους πελάτες, ενώ η EPAL χρησιμοποιείται για την εσωτερική εφαρμογή της πολιτικής για τις επιχειρήσεις έτσι ώστε να ελέγχουν τις προσβάσεις στις πληροφορίες που συλλέγονται. Δηλαδή, η P3P χρησιμοποιείται για να περιγράψει τις δημόσιες πολιτικές προστασίας της ιδιωτικής ζωής, ενώ η EPAL έχει ως στόχο να περιγράψει τις εσωτερικές πρακτικές προστασίας της ιδιωτικής ζωής μιας επιχείρησης, που πολύ

πιθανόν να μην θέλει να τις μοιραστεί με το κοινό. Με αυτή την έννοια, η EPAL συμπληρώνει την P3P.

Παρά το γεγονός ότι η P3P είναι κατάλληλη για την έκφραση υψηλού επιπέδου πολιτικών ιστοσελίδων, δεν είναι τόσο κατάλληλη για την έκφραση μιας εσωτερικής πολιτικής προστασίας της ιδιωτικής ζωής. Η EPAL από την άλλη πλευρά έχει σχεδιαστεί ειδικά για να εκφράζει μια εσωτερική πολιτική προστασίας της ιδιωτικής ζωής που μπορεί να επιβληθεί από μια επιχείρηση συστήματος διαχείρισης της ιδιωτικής ζωής.

Η EPAL, έχει ως στόχο να εκφράσει τις εσωτερικές πρακτικές προστασίας της ιδιωτικής ζωής. Αντίθετα, η P3P αποσκοπεί στο να εκφράσει τις εξωτερικές υποσχέσεις της ιδιωτικής ζωής. Πιο συγκεκριμένα, η P3P μπορεί να εκφράσει τις υποσχέσεις της ιδιωτικής ζωής που σχετίζονται με συγκεκριμένες περιπτώσεις συλλογής πληροφοριών στην ιστοσελίδα του οργανισμού. Δεν μπορεί όμως να εκφράσει τις γενικές πολιτικές απορρήτου της οργάνωσης ως σύνολο.

Η EPAL στοχεύει στην τυποποίηση της εσωτερικής πολιτικής μιας επιχείρησης όσον αφορά την ιδιωτικότητα. Η P3P στοχεύει στην τυποποίηση των δηλώσεων ιδιωτικής ζωής (privacy statements) που δημοσιεύονται από μια επιχείρηση. Ορίζει μια παγκόσμια ορολογία, αντιθέτως με την EPAL, που μπορεί να χρησιμοποιηθεί για να περιγραφούν οι υποσχέσεις ιδιωτικότητας για κάθε επιχείρηση.

Η κύρια διαφορά τους είναι ότι η P3P επικεντρώνεται στα δεδομένα και τις πληροφορίες (τρόπο συλλογής, τρόπο χρήσης), ενώ η EPAL επικεντρώνεται στην πρόσβαση.

Όσον αφορά τις κατηγορίες δεδομένων και τις κατηγορίες χρηστών δεδομένων, η P3P έχει μια προκαθορισμένη λίστα κατηγοριών δεδομένων και χρηστών, ενώ η EPAL επιτρέπει σε μια επιχείρηση να ορίσει δικό της κατάλογο των κατηγοριών δεδομένων και χρηστών και αυτοί μπορεί να είναι και ιεραρχικοί. Το ίδιο ισχύει και για τους σκοπούς.

Όσον αφορά τις ενέργειες (actions) η P3P καθορίζει μόνο τη δράση "use", ενώ η EPAL επιτρέπει τον καθορισμό καταλόγου των δράσεων. Όσον αφορά τις προϋποθέσεις (conditions) η P3P δεν διαθέτει, ενώ η EPAL διαθέτει. Όσον αφορά τις υποχρεώσεις (obligations) η P3P καθορίζει μόνο την υποχρέωση "retention", ενώ η EPAL επιτρέπει τον καθορισμό καταλόγου των υποχρεώσεων. Όσον αφορά τις επιλογές (choices) η P3P επιτρέπει μόνο opt-in / opt-out επιλογές, ενώ η EPAL επιτρέπει ένα πιο γενικευμένο σύνολο επιλογών.

Έτσι λοιπόν, από αυτή την σύγκριση προκύπτει το συμπέρασμα ότι η EPAL δρα σαν συμπληρωματική της P3P.

4.2.2 Σύγκριση EPAL – XACML [3]

Τόσο η EPAL όσο και η XACML επικεντρώνονται στον έλεγχο πρόσβασης των δεδομένων. Είναι κατάλληλες για επιχειρήσεις και οργανισμούς και έχουν πολλά κοινά στοιχεία. Η EPAL ουσιαστικά είναι ένα λειτουργικό υποσύνολο της XACML. Η EPAL είναι μια ιδιόκτητη γλώσσα, σε αντίθεση από την XACML που είναι πρότυπο, και οι δύο είναι βασισμένες στην XML.

Η πολιτική EPAL σχεδιάστηκε για την επιβολή της ιδιωτικής ζωής των επιχειρήσεων. Σε αντίθεση, η πολιτική XACML σχεδιάστηκε για τον έλεγχο της πρόσβασης. Επίσης, οι EPAL πολιτικές έχουν επίπεδες δομές, αντίθετα, οι πολιτικές XACML έχουν ιεραρχικές δομές. Μια πολιτική EPAL περιλαμβάνει μόνο μια λίστα με τους κανόνες, ενώ η πολιτική XACML μπορεί να καθοριστεί κατ 'επανάληψη. Μια πολιτική XACML αποτελείται από ένα σύνολο πολιτικών και ένα σύνολο πολιτικών αποτελείται από μια σειρά από πολιτικές ή σύνολα πολιτικών.

Οι πολιτικές EPAL ακόμη, έχουν έναν αλγόριθμο συνδυασμού κανόνα (first-applicable), ενώ οι πολιτικές XACML έχουν τέσσερις αλγορίθμους συνδυασμών κανόνων και πολιτικών. Η EPAL δεν διαθέτει αλγόριθμους συνδυασμών πολιτικών αφού μόνο μια πολιτική έχει και δεν έχει αναφορές σε άλλες, ούτε επεκτασιμότητα. Όσον αφορά τους κανόνες της που μπορούν να συγκρούονται παίρνει ως αποτέλεσμα το αποτέλεσμα που λαμβάνεται από τον πρώτο κανόνα που ικανοποιείται. Η XACML

όμως σε αντίθεση, έχει τους τέσσερεις αλγορίθμους, από τους οποίους οι τρεις είναι και για τους κανόνες και για τις πολιτικές, ενώ ο τέταρτος μόνο για τις πολιτικές. Οι έλεγχοι για τις συγκρούσεις προκύπτουν όταν υπάρχει αίτημα πρόσβασης.

Σε σχέση με την XACML, η γλώσσα EPAL παρουσιάζει το πλεονέκτημα της ιδέας του λεξιλογίου πολιτικής (policy vocabulary). Οι πολιτικές XACML δεν περιγράφουν το λεξιλόγιο που χρησιμοποιούν. Στο μοντέλο XACML, το λεξιλόγιο ορίζεται ξεχωριστά από τις πολιτικές, δεν εμπίπτει στο πεδίο εφαρμογής της γλώσσας XACML και είναι ένα προαιρετικό εξάρτημα. Η XACML δεν υποστηρίζει τη λειτουργικότητα λεξιλογίου όπως την EPAL ως έννοια πρώτης κατηγορίας, αλλά είναι σε θέση να υποστηρίζει μερικές από τις λειτουργίες με τον καθορισμό και τη χρήση ενός χαρακτηριστικού που εκπροσωπεί την ταυτότητα του λεξιλογίου των χαρακτηριστικών. Η EPAL κάνει μια αναφορά σε ένα λεξιλόγιο και στο λεξιλόγιο καθορίζει όλα τα χαρακτηριστικά και τις υποχρεώσεις. Το λεξιλόγιο της πολιτικής EPAL έχει έξι στοιχεία και τα τρία από αυτά έχουν ιεραρχικές δομές. Η XACML δεν υποστηρίζει επίσης σημασιολογικές ιεραρχίες όπως ιεραρχία στους σκοπούς, τις κατηγορίες χρηστών ή δεδομένων, ενώ η EPAL υποστηρίζει. Σε αυτές τις περιπτώσεις, η XACML υποστηρίζει μόνο ένα υποσύνολο των λειτουργιών που υποστηρίζονται από την EPAL.

Ωστόσο, η γλώσσα EPAL παρουσιάζει πολλές ελλείψεις σε σχέση με την XACML. Σε αυτές περιλαμβάνεται η αδυναμία συνδυασμού των αποτελεσμάτων διαφορετικών πολιτικών και η έλλειψη της δυνατότητας αναφοράς σε εξωτερικές πολιτικές προκειμένου να αποτελέσουν μέρος κάποιας δεδομένης πολιτικής. Η EPAL δεν επιτρέπει τις φωλιασμένες πολιτικές, ενώ η XACML τις επιτρέπει. Η EPAL δεν υποστηρίζει κατανεμημένες πολιτικές, δηλαδή δεν επιτρέπει αναφορές σε πολιτικές, ενώ η XACML υποστηρίζει. Γενικά, η γλώσσα XACML έχει επικρατήσει έναντι της EPAL.

Ένα απλό αίτημα στην EPAL αποτελείται από ένα θέμα (user-category), ένα πόρο (data-category), μια ενέργεια, ένα σκοπό και ένα προαιρετικό περιβάλλον με επιπρόσθετα χαρακτηριστικά. Η EPAL υποστηρίζει και συνδυασμό αιτημάτων, όπου μπορούν να οριστούν πολλά θέματα, πόροι κλπ. Αν η αξιολόγηση για οποιοδήποτε θέμα έναντι των υπολοίπων στοιχείων πετύχει, τότε επιστρέφεται απάντηση με την

άδεια. Ένα αίτημα όμως στην XACML, αποτελείται από τέσσερις συλλογές. Μια συλλογή για τα θέματα, μια για τους πόρους, μια για τις ενέργειες και μια προαιρετική για τα επιπρόσθετα χαρακτηριστικά του αιτήματος. Η EPAL υποστηρίζει όλη τη λειτουργικότητα του αιτήματος απόφασης της XACML (decision request), εκτός από την δυνατότητα να ζητήσει ξεχωριστή απάντηση για κάθε ένα από τους πολλαπλούς πόρους που υποβάλλονται σε ενιαίο αίτημα απόφασης και την δυνατότητα να περιγράψει περισσότερες από μια οντότητες που εμπλέκονται στο να γίνει ένα αίτημα πρόσβασης.

Η EPAL υποστηρίζει όλη τη λειτουργικότητα του κανόνα της XACML (rule), εκτός από την περίπτωση που απαιτείται το θέμα, ο πόρος, η ενέργεια, το περιβάλλον ή ο σκοπός να ανήκουν σε πολλές ομάδες και την περίπτωση όπου ένα γνώρισμα χρησιμοποιείται ως μέρος του τμήματος εφαρμογής του κανόνα. Όσον αφορά τις υποχρεώσεις (Obligations), η EPAL τις βάζει στους κανόνες της συσχετιζόμενες με τον ταυτοποιητή του κανόνα, ενώ η XACML στις πολιτικές συσχετιζόμενες με τον πόρο πρόσβασης.

Η EPAL δεν παρέχει τρόπο αντιμετώπισης σφαλμάτων ή αποφυγή τους, παρά μόνο επιστρέφει ότι υπάρχει ένα σφάλμα. Σφάλματα μπορεί να συμβούν κατά τη διάρκεια της εφαρμογής μιας συνάρτησης (μια προσπάθεια να διαιρέσει με 0 , για παράδειγμα) , ή σε μία τιμή παραμέτρου που χρειάζεται για την αξιολόγηση μιας λειτουργίας που δεν θα μπορούσε να ληφθεί, ή όταν μια αναφερόμενη πολιτική δεν είναι διαθέσιμη. Η XACML αναγνωρίζει τα σφάλματα ως βασική ιδέα για συνδυασμό των αποτελεσμάτων των διαφόρων κανόνων και των πολιτικών. Η XACML στηρίζει την πολιτική κατευθυνόμενου χειρισμού σφαλμάτων, ως μέρος της ίδιας της γλώσσας. Η EPAL δεν το κάνει.

Η EPAL δεν σχεδιάστηκε για τον έλεγχο πρόσβασης. Σε αντίθεση με τον έλεγχο της πρόσβασης, ο σκοπός (purpose) είναι μέρος μιας ερώτησης άδειας στην EPAL. Χωρίς να γνωρίζουν το σκοπό της πρόσβασης, η άδεια δεν μπορεί να αποφασιστεί. Κατά συνέπεια, κάθε σύστημα χρησιμοποιώντας την EPAL πρέπει να είναι σε θέση να καθορίσει ένα σκοπό πριν ζητήσει από την μηχανή της EPAL να αξιολογήσει μια συγκεκριμένη πολιτική. Ενώ η XACML, είναι σχεδιασμένη για τον έλεγχο της

πρόσβασης, συμπεριλαμβανομένης της προστασίας της ιδιωτικής ζωής. Έχει όμως και δύο προαιρετικά χαρακτηριστικά για τον σκοπό. Τα χαρακτηριστικά αυτά μπορούν να δηλώσουν για ποιο σκοπό συλλέγονται τα δεδομένα και για ποιο σκοπό αποκτούν πρόσβαση.

Η EPAL δεν σχεδιάστηκε για πολιτικές επιχειρησιακού επιπέδου. Δεν υποστηρίζει φωλιασμένες πολιτικές, ούτε κατανεμημένες. Μόνο ένα θέμα (subject) επιτρέπεται ανά αίτηση πρόσβασης και μόνο ο πρώτος εφαρμοσμένος κανόνας αξιολογείται. Αυτά τα θέματα η XACML τα λύνει, άρα είναι σχεδιασμένη πολιτική για επιχειρησιακό επίπεδο. Γενικά, μέσα από την σύγκριση των δύο αυτών πολιτικών γλωσσών ιδιωτικότητας καταλήγουμε στο συμπέρασμα ότι η XACML είναι υπερσύνολο της EPAL.

4.2.3 Σύγκριση P3P – EPAL – XACML [1][12]

Η P3P σαν πολιτική έχει σκοπό να προστατεύσει τους χρήστες του διαδικτύου από τους κινδύνους παραβίασης της ιδιωτικότητας τους και βασίζεται στις προτιμήσεις του χρήστη. Οι άλλες δύο πολιτικές, διαφέρουν από την P3P αφού έχουν σαν σκοπό, να διασφαλίσουν πολιτικές προστασίας της ιδιωτικής ζωής και τον έλεγχο πρόσβασης σε επιχειρήσεις και οργανισμούς.

Όσον αφορά την ελαστικότητα που έχει η κάθε μια τους, η P3P έχει κακή λόγω του ότι έχει προκαθορισμένες πολιτικές, η EPAL έχει μέτρια αφού έχει ελαστικές πολιτικές αλλά δεν είναι επεκτάσιμη και η XACML, έχει καλή αφού έχει ελαστικές πολιτικές και επιτρέπει τις αναφορές.

Μια πολιτική P3P μπορεί να περιέχει πολλές δηλώσεις. Όταν ένας κανόνας όμως επιλυθεί με αποτυχία, θα σταματήσουν οι ενέργειες για εντοπισμό σε άλλες δηλώσεις, έτσι ώστε να δούμε αν έχει κάποια που να τον ικανοποιεί. Άρα λοιπόν η P3P όσον αφορά δηλώσεις που μπορούν να συγκρούονται, αν αποτύχει ο κανόνας με μια δήλωση τότε το αποτέλεσμα θα είναι αποτυχία. Η EPAL όσον αφορά τους κανόνες της που μπορούν να συγκρούονται παίρνει ως αποτέλεσμα το αποτέλεσμα που λαμβάνεται από τον πρώτο κανόνα που ικανοποιείται. Η XACML όμως σε αντίθεση και από τις δύο, έχει τέσσερεις αλγορίθμους συνδυασμού κανόνων και πολιτικών, από τους οποίους οι

τρεις είναι και για τους κανόνες και για τις πολιτικές, ενώ ο τέταρτος μόνο για τις πολιτικές.

Σύμφωνα με την Anderson [3], ένα πρότυπο δομημένης γλώσσας για τη υποστήριξη εκφράσεων και την επιβολή των κανόνων προστασίας της ιδιωτικής ζωής πρέπει να έχει τις ακόλουθες απαιτήσεις:

RQ1. Η γλώσσα πρέπει να υποστηρίζει τους περιορισμούς σχετικά με το ποιος έχει το δικαίωμα να εκτελέσει ποιες ενέργειες σε ποιους πόρους.

Rq2. Η γλώσσα πρέπει να υποστηρίζει τους περιορισμούς σχετικά με τους σκοπούς για τους οποίους συλλέγονται δεδομένα ή χρησιμοποιούνται.

RQ3. Η γλώσσα πρέπει να είναι σε θέση να εκφράσει άμεσα εκτελέσιμες πολιτικές

Rq4. Η γλώσσα πρέπει να είναι ανεξάρτητη από πλατφόρμα.

Rq5. Η γλώσσα που χρησιμοποιείται για τις πολιτικές προστασίας της ιδιωτικής ζωής πρέπει να είναι η ίδια ή να ενσωματώνονται με τη γλώσσα που χρησιμοποιείται για τις πολιτικές ελέγχου πρόσβασης.

Έχοντας υπόψη τις πιο πάνω απαιτήσεις, προκύπτουν τα ακόλουθα συμπεράσματα που αφορούν την σύγκριση μεταξύ των πολιτικών P3P, EPAL και XACML.

- Όσον αφορά τον περιορισμό για το ποιος έχει το δικαίωμα να εκτελέσει ποιες ενέργειες και σε ποιους πόρους, η P3P δεν υποστηρίζει τέτοιου είδους αιτήματα. Οι άλλες δύο μπορούν.
- Όσον αφορά τον περιορισμό για τον σκοπό συλλογής ή χρήσης των δεδομένων και οι τρεις μπορούν να το ικανοποιήσουν.
- Όσον αφορά το αίτημα όπου η γλώσσα πρέπει να εκφράζει άμεσα εκτελέσιμες πολιτικές η P3P δεν το υποστηρίζει, ενώ οι άλλες δύο ναι.
- Όσον αφορά το αίτημα για να είναι η γλώσσα ανεξάρτητη από πλατφόρμα, η P3P δεν το υποστηρίζει, η EPAL δεν είναι σίγουρο για το αποτέλεσμα που θα έχει για αυτό το αίτημα και η XACML το υποστηρίζει.

- Όσον αφορά το αίτημα για τον έλεγχο πρόσβασης μόνο η XACML το υποστηρίζει.

Γενικά, το συμπέρασμα που προκύπτει είναι ότι η XACML είναι η καλύτερη για την έκφραση των πολιτικών προστασίας της ιδιωτικής ζωής, αλλά και για την έκφραση πολιτικών ελέγχου πρόσβασης.

4.3 Παραβιάσεις και Γλώσσες Πολιτικών Ιδιωτικότητας

Οι παραβιάσεις, έτσι όπως τις είδαμε σύμφωνα με την ταξινόμηση του Solove, ανάλογα με το τι αντιπροσωπεύουν και τι κάνουν χωρίζονται σε κάποιες ομάδες για το πώς διαχειρίζονται τις πληροφορίες που συλλέγουν. Κάποιες χρειάζονται να γίνεται διασφάλιση του ότι δεν θα γίνεται συσχέτιση με την ταυτότητα του χρήστη (κάποιο αναγνωριστικό) ούτως ώστε να μην μπορούν να γνωρίζουν ποιο δεδομένο ανήκει σε ποιον. Κάποιες άλλες χρειάζονται σωστό χειρισμό του σκοπού για τον οποίο παρέχονται οι πληροφορίες ούτως ώστε να μην γίνεται χρήση τους για άλλο λόγο. Κάποιες άλλες χρειάζονται σωστό έλεγχο για το που πάνε οι πληροφορίες και ποιος τις χειρίζεται και κάποιες άλλες είναι συνδυασμός όλων των στοιχείων αυτών.

Οι γλώσσες πολιτικών ιδιωτικότητας που μελετήσαμε, είδαμε πως δεν μπορούν να αντιμετωπίσουν πλήρως όλες τις παραβιάσεις. Όμως μπορούν να διαχειριστούν και να ικανοποιήσουν αρκετές από αυτές. Στόχος μας είναι να μπορεί να γίνει μια διατύπωση με τα χαρακτηριστικά και τα στοιχεία που έχει η κάθε γλώσσα, έτσι ώστε να μπορούν να ελεγχθούν οι παραβιάσεις όσο καλύτερα γίνεται. Τώρα, αν όντως οι γλώσσες και τα συστήματα που τις χρησιμοποιούν τηρούν αυτά που υπόσχονται και σίγουρα τις διασφαλίζουν δεν μπορούμε να το ξέρουμε εντελώς.

Όσον αφορά τη συσχέτιση, γενικά πρέπει να γίνεται έλεγχος ακριβώς για τον σκοπό τον οποίο συλλέγονται οι πληροφορίες, καθώς και για τη διάρκεια διατήρησης των πληροφοριών. Η P3P μπορεί να το διατυπώσει αφού υπάρχουν οι ετικέτες purpose και retention που ελέγχουν το σκοπό και τη διάρκεια διατήρησης αντίστοιχα. Η ετικέτα purpose έχει τις επιλογές current και pseudo-analysis που μας λένε πως οι πληροφορίες

είναι μόνο για τον τρέχον σκοπό και πως δεν γίνεται ταύτιση του χρήστη με τις πληροφορίες. Υπάρχει και η επιλογή opt-in / opt-out που προσφέρει ακόμη περισσότερο έλεγχο. Η ετικέτα retention επίσης έχει την εντολή no-retention που μας λέει ότι οι πληροφορίες θα διαγραφούν αμέσως μετά τη χρήση τους. Έτσι δεν παρέχεται η επαναχρησιμοποίηση τους για να γίνει συσχέτιση. Η EPAL μέσω του λεξιλογίου που έχουν οι πολιτικές της μπορεί να ορίσει ακριβώς τον σκοπό για τον οποίο ζητούνται οι πληροφορίες και μέσω των υποχρεώσεων που έχουν οι κανόνες μπορούν να πουν να μην διατηρούνται οι πληροφορίες περισσότερο από την χρήση τους, έτσι ώστε να μην μπορούν να κάνουν συσχέτιση των πληροφοριών με άλλες πληροφορίες που θα πάρουν κάποια άλλη στιγμή. Κάτι παρόμοιο μπορεί να κάνει και η XACML αλλά ορίζοντας υποχρεώσεις που εκτελούνται στο σημείο PEP και κάνοντας χρήση των Actions που είναι οι ενέργειες που δικαιούνται να κάνουν.

Όσον αφορά την ταύτιση, πρέπει να μπορεί να διασφαλίζεται πως τα δεδομένα που συλλέγονται δεν μπορούν να ταυτιστούν με το πρόσωπο που τα δίνει. Η ταύτιση δεν μπορεί καμία γλώσσα να την διατυπώσει. Με την παροχή πληροφοριών γίνεται ταύτιση και δεν μπορεί να ελεγχθεί πως θα αποφεύγεται. Η P3P μπορεί να την ελέγξει κάποιες φορές με το να πει πως η ετικέτα purpose θα πάρει τις τιμές pseudo-analysis και pseudo-decision που απλά δηλώνουν πως οι πληροφορίες θα χρησιμοποιηθούν και δεν θα γίνει η οποιαδήποτε ταύτιση, αλλά πάλι τη συγκεκριμένη στιγμή που παρέχονται οι πληροφορίες ξέρουν σε ποιον ανήκουν και γιατί.

Όσον αφορά τη μη επαρκής παροχή ασφάλειας, πρέπει να γίνεται έλεγχος για το που παρέχονται οι πληροφορίες που συλλέγονται. Η P3P μπορεί να την ελέγξει αφού με την ετικέτα recipient μπορεί να καθορίσει ακριβώς ποιοι θα είναι οι παραλήπτες των πληροφοριών και ο χρήστης μπορεί με το opt-in / opt-out να ελέγχει τι επιτρέπει. Η EPAL και η XACML σίγουρα μπορούν να ελέγξουν το ποιος έχει πρόσβαση στις πληροφορίες και έτσι μπορούν να το ελέγξουν.

Όσον αφορά τη δευτερογενής χρήση, πρέπει να γίνεται ακριβής έλεγχος για τον σκοπό που θα χρησιμοποιηθούν τα δεδομένα ούτως ώστε να μην μπορούν να χρησιμοποιηθούν για άλλο άσχετο σκοπό. Αυτό το διατυπώνουν και οι τρεις γλώσσες αφού η P3P έχει το purpose, η EPAL ορίζει τις ενέργειες και τους σκοπούς μέσω του

λεξιλογίου της και η XACML μέσω των πολιτικών και των κανόνων της λέει ακριβώς πώς μπορούν να χρησιμοποιηθούν οι πληροφορίες.

Όσον αφορά τον αποκλεισμό, για να ισχύει πρέπει να μπορώ να παίρνω από το άτομο πληροφορίες χωρίς να το γνωρίζει και να τις χρησιμοποιώ εν αγνοία του. Αυτό δεν μπορεί να συμβαίνει στην P3P αφού γίνεται έλεγχος και ο ίδιος ο χρήστης αποφασίζει τι πληροφορίες θα παρέχει. Και οι δύο άλλες το ίδιο αφού για τα δεδομένα μιας επιχείρησης αποφασίζει η ίδια η επιχείρηση που θα τα δώσει και πώς θα χρησιμοποιηθούν. Έχουν προστατευόμενους πόρους και ορίζουν οι ίδιες σε ποιους επιτρέπουν πρόσβαση.

Όσον αφορά την παραβίαση απορρήτου, για να ισχύει πρέπει να διασφαλίζεται ότι δεν θα παρέχουν τα δεδομένα σε κάποιους που δεν πρέπει. Η P3P μπορεί να την ελέγξει αφού έχει την ετικέτα recipient που διασφαλίζει ότι μόνο σε αυτούς που θέλει ο χρήστης θα δοθούν οι πληροφορίες. Η EPAL και η XACML καθορίζουν το ποιος θα έχει πρόσβαση στις πληροφορίες άρα μπορούν να το ελέγχουν.

Όσον αφορά την παράθεση και έκθεση, πρέπει να διασφαλίζεται ότι με το που παρέχονται οι πληροφορίες σχετικά με κάποιο άτομο, δεν πρέπει να ταυτοποιούνται και να κρίνεται το άτομο αρνητικά βάσει των πληροφοριών αυτών. Καμία γλώσσα δεν μπορεί να τις ελέγξει αφού αν και ελέγχονται για το που πάνε οι πληροφορίες δεν μπορεί να ελεγχθεί η μη ταυτοποίηση του ατόμου με τις πληροφορίες αυτές. Αν και ορίζονται οι σκοποί για τους οποίους λαμβάνονται τα δεδομένα δεν παύει από το να γίνεται ταυτοποίηση και να μαθαίνουν πληροφορίες σχετικά με συγκεκριμένα άτομα.

Όσον αφορά την αυξημένη προσβασιμότητα ισχύει το ίδιο που ίσχυε για τη μη επαρκής παροχή ασφάλειας. Όσον αφορά την οικειοποίηση δεν μπορεί να ελεγχθεί από καμία γλώσσα γιατί απαιτείται έλεγχος της ταύτισης κάτι που είπαμε πως δεν ισχύει. Όσον αφορά την αλλοίωση δεν μπορεί να ελεγχθεί από καμία γλώσσα αφού δεν υπάρχει μηχανισμός που να ελέγχει αν οι πληροφορίες που συλλέγονται αλλάζουν κατά τη χρήση τους.

Οι παραβιάσεις συλλογής πληροφορίας και εισβολής πληροφορίας δεν μπορούν να ελεγχθούν μέσω γλώσσας ιδιωτικότητας. Ούτε και ο Εκβιασμός.

Ακολουθεί ένας πίνακας για το ποιες παραβιάσεις μπορεί να ελέγξει η κάθε γλώσσα

	P3P	EPAL	XACML
Συσχέτιση	ΝΑΙ	ΝΑΙ	ΝΑΙ
Ταύτιση	ΟΧΙ	ΟΧΙ	ΟΧΙ
Μη Επαρκής Παροχή Ασφάλειας	ΝΑΙ	ΝΑΙ	ΝΑΙ
Δευτερογενής Χρήση	ΝΑΙ	ΝΑΙ	ΝΑΙ
Αποκλεισμός	ΝΑΙ	ΝΑΙ	ΝΑΙ
Παραβίαση Απορρήτου	ΝΑΙ	ΝΑΙ	ΝΑΙ
Αποκάλυψη	ΟΧΙ	ΟΧΙ	ΟΧΙ
Έκθεση	ΟΧΙ	ΟΧΙ	ΟΧΙ
Αυξημένη Προσβασιμότητα	ΝΑΙ	ΝΑΙ	ΝΑΙ
Οικειοποίηση	ΟΧΙ	ΟΧΙ	ΟΧΙ
Αλλοίωση	ΟΧΙ	ΟΧΙ	ΟΧΙ

Πίνακας 3 : Γλώσσες Ιδιωτικότητας και σύγκριση για παραβιάσεις

Παρατηρούμε πως όσον αφορά τις παραβιάσεις οι τρεις γλώσσες έχουν τις ίδιες ικανότητες για να τις διατυπώνουν. Όμως, όπως ανέφερα και πριν αν και οι γλώσσες παρέχουν τους μηχανισμούς για να διασφαλίζουν αρκετές από τις παραβιάσεις αυτές, δεν είμαστε εντελώς σίγουροι πως μπορούν να το κάνουν με αξιοπιστία. Ειδικά για την γλώσσα P3P, που δεν μας εξασφαλίζει με κανένα τρόπο πως αυτά που υπόσχεται τα τηρεί.

Κεφάλαιο 5

Γλώσσες Πολιτικών Ιδιωτικότητας και Κοινωνικά Δίκτυα

5.1 Κοινωνικό δίκτυο Facebook

Μια από τις πιο σημαντικές υπηρεσίες που προσφέρει το Facebook, είναι η ικανότητα ενός χρήστη να επικοινωνεί με άλλους. Το Facebook δημιουργεί ένα κοινωνικό δίκτυο για τον κάθε χρήστη. Το δίκτυο αυτό είναι σαν ένας γράφος και ο χρήστης έχει άμεσες και έμμεσες σχέσεις με τους φίλους του, τους φίλους των φίλων του, και λοιπά. Εκτός από την κοινωνική δικτύωση προσφέρει και διάφορες δημοφιλείς εφαρμογές που λαμβάνουν χώρα μέσω αυτής της δικτύωσης. Παραδείγματα αποτελούν η κοινή χρήση εικόνων, βίντεο, η δημοσίευση σε τοίχους φίλων, η κοινοποίηση προσωπικών πληροφοριών, και λοιπά.

Για να αρχίσεις την αλληλεπίδρασή του ο χρήστης με το Facebook, πρέπει να εγγραφεί ως χρήστης και να κάνει log in έτσι ώστε να μεταβεί στον λογαριασμό του. Εκεί θα του προταθεί να δει ή να αλλάξει το profile του ή να περιηγηθεί στους διάφορους χώρους του Facebook. Μετά από λίγη ώρα θα ανήκει στον κόσμο του Facebook και θα έχει το δικό του wall, το δικό του προφίλ με τις πληροφορίες του και διάφορες συσχετίσεις με τους υπόλοιπους χρήστες. Πολλές πληροφορίες θα συγκεντρωθούν για τη ζωή του χρήστη, τις φιλίες του, τις εικόνες του, τις θρησκευτικές του απόψεις, τα ενδιαφέροντα του και ο χρήστης θα θελήσει να ελέγχει ποιος έχει πρόσβαση σε όλες αυτές τις πληροφορίες.

Σύμφωνα με την πολιτική ιδιωτικότητας του κοινωνικού δικτύου Facebook [21], το Facebook έχει σχεδιαστεί ώστε να είναι εύκολο για να μοιραζόμαστε τις πληροφορίες μας με όποιον θέλουμε. Εμείς αποφασίζουμε για το πόσες πληροφορίες αισθανόμαστε άνετα να μοιραζόμαστε στο Facebook και μπορούμε να ελέγχουμε τον τρόπο που τις διανέμουμε μέσω των ρυθμίσεων προστασίας της ιδιωτικής μας ζωής. Θα πρέπει να εξετάζουμε τις προεπιλεγμένες ρυθμίσεις απορρήτου και να τις αλλάζουμε έτσι ώστε να ανταποκρίνονται στις προτιμήσεις μας. Θα πρέπει επίσης να εξετάζουμε τις ρυθμίσεις μας κάθε φορά που μοιραζόμαστε πληροφορίες.

Το Facebook δεν είναι απλά μια ιστοσελίδα. Είναι επίσης μια υπηρεσία για να μοιραζόμαστε τις πληροφορίες μας με διάφορες εφαρμογές αλλά και ιστοσελίδες. Μπορούμε να ελέγχουμε το πώς θα μοιράζονται οι πληροφορίες μας με τις εφαρμογές τρίτων και τις ιστοσελίδες, μέσα από τις ρυθμίσεις των εφαρμογών μας. Μπορούμε επίσης να περιορίσουμε το πώς οι φίλοι μας μοιράζονται τις πληροφορίες μας με τις εφαρμογές, μέσα από τις ρυθμίσεις απορρήτου μας.

Το Facebook είναι μια δωρεάν υπηρεσία που υποστηρίζεται κυρίως από τη διαφήμιση. Δεν μοιράζεται όμως, τις πληροφορίες μας με τους διαφημιστές χωρίς τη συγκατάθεση του χρήστη. Επιτρέπει στους διαφημιζόμενους να επιλέξουν τα χαρακτηριστικά των χρηστών στους οποίους θέλουν να δείξουν τις διαφημίσεις τους και χρησιμοποιεί τις πληροφορίες που μοιράζονται οι χρήστες μαζί τους για να εξυπηρετεί αυτές τις διαφημίσεις.

Η πλατφόρμα του Facebook, επιτρέπει σε τρίτους, εξωτερικούς παράγοντες, να έχουν πρόσβαση σε πληροφορίες του Facebook, μέσω ιστοσελίδων ή διάφορων εφαρμογών. Η πολιτική ιδιωτικότητας του Facebook, αρχίζει με την ενημέρωση των χρηστών ότι "Αυτή η πολιτική προστασίας προσωπικών δεδομένων καλύπτει όλο το Facebook. Αυτό δεν σημαίνει, ωστόσο, ότι ισχύει για τις οντότητες που δεν ανήκουν ή δεν ελέγχονται από το Facebook, όπως εφαρμογές και ιστοσελίδες που χρησιμοποιούν την πλατφόρμα." Περαιτέρω, το σημείο 4 που ονομάζεται "πληροφορίες που μοιράζεστε με τρίτους: Facebook Platform" αναφέρει τα εξής: "Όπως αναφέρθηκε παραπάνω, δεν ελέγχουν και δεν εμπεριέχουν στην πολιτική τους τις εφαρμογές ή ιστοσελίδες που χρησιμοποιούν το Facebook Platform. Αυτό σημαίνει ότι όταν χρησιμοποιείτε αυτές τις

εφαρμογές και ιστοσελίδες κάνετε τις πληροφορίες σας που βρίσκονται στο Facebook διαθέσιμες σε κάποιον άλλο εκτός από το Facebook. Πριν τους αφήσουμε να έχουν πρόσβαση σε οποιαδήποτε πληροφορία σχετικά με εσάς, τους ζητούμε να συμφωνήσουν με τους όρους που περιορίζουν τη χρήση των πληροφοριών σας και χρησιμοποιούμε τεχνικά μέτρα για να εξασφαλίσουμε ότι λαμβάνουν μόνο εξουσιοδοτημένες πληροφορίες.'' Φαίνεται ότι ενώ το Facebook έχει λάβει ορισμένα μέτρα για την προστασία των χρηστών από τις υπηρεσίες Facebook Platform, δεν έχουν κανένα πραγματικό έλεγχο στο τι συμβαίνει με τις πληροφορίες ενός χρήστη, που ακολουθεί τέτοιου είδους εφαρμογές και ιστοσελίδες.

Η πολιτική ιδιωτικότητας του Facebook, αποτελείται από ένα σύνολο πολιτικών προστασίας της ιδιωτικής ζωής σχετικά με τους διαφορετικούς τύπους πληροφοριών σε σχέση με διάφορα εισερχόμενα θέματα. Αποτελείται από τα ακόλουθα τμήματα:

1. Εισαγωγή
2. Πληροφορίες που λαμβάνουμε
3. Πληροφορίες που κοινοποιούνται στο Facebook
4. Πληροφορίες που κοινοποιείτε με Τρίτα μέρη
5. Πώς χρησιμοποιούμε τις πληροφορίες σας
6. Πώς κοινοποιούμε πληροφορίες
7. Πώς μπορείτε να αλλάξετε ή να αφαιρέσετε πληροφορίες
8. Πώς προστατεύουμε τις πληροφορίες
9. Άλλοι όροι

Τα πρώτα τμήματα (εκτός από την εισαγωγή) περιγράφουν το είδος των πληροφοριών που ένας χρήστης μπορεί να μοιράζεται άμεσα και έμμεσα με το σύστημα του Facebook. Δηλαδή τι πληροφορίες μπορούμε να λαμβάνουμε, τι πληροφορίες μπορούμε να κοινοποιούμε γενικά και τι πληροφορίες μπορούμε να κοινοποιούμε με τρίτους. Τα δύο επόμενα τμήματα περιγράφουν το πώς το Facebook χρησιμοποιεί και κοινοποιεί τις πληροφορίες ενός χρήστη. Επίσης το επόμενο περιγράφει ότι λέει ο τίτλος του και τέλος το επόμενο επεξηγεί ποια βήματα πρέπει να ληφθούν για την προστασία των προσωπικών πληροφοριών. Το τμήμα αυτό περιλαμβάνει επίσης μια μικρή υποενότητα που λέγεται ''Κίνδυνοι που συνδέονται με την ανταλλαγή πληροφοριών'', η οποία φαίνεται να αποτελεί στην πραγματικότητα μια ενότητα η

οποία απελευθερώνει το Facebook από τυχόν ευθύνες για την ασφάλεια ή παραβίασης της ιδιωτικής ζωής στα συστήματά του, ενημερώνοντας ότι "... δεν υπάρχουν μέτρα ασφαλείας τέλεια ή αδιαπέραστα."

Μέσα από την μελέτη της πολιτικής ιδιωτικότητας του Facebook, τις επιλογές που προσφέρει και την προσδοκία για προστασία των πληροφοριών των χρηστών, προκύπτουν οι πιο κάτω απαιτήσεις [20] :

1. Τύπος αντικειμένων – ορισμός διαφορετικών κανόνων πρόσβασης για διαφορετικούς τύπους αντικειμένων, όπως εικόνες, ετικέτες, βίντεο, λίστα φίλων, και λοιπά
2. Θέματα (άτομα) – επιτρέπεται ή απαγορεύεται σε συγκεκριμένους χρήστες να έχουν πρόσβαση σε ένα αντικείμενο και η δυνατότητα να εμποδίσει κάποιο χρήστη από κάθε επιλογή επικοινωνίας (block).
3. Σχέσεις – επιτρέπεται ή απαγορεύεται η πρόσβαση σε ένα αντικείμενο με βάση τη σχέση που υπάρχει στο άτομο που θα κάνει την πρόσβαση και του χρήστη που έχει την πληροφορία.
4. Ρόλοι – επιτρέπεται ή απαγορεύεται η πρόσβαση σε ένα αντικείμενο με βάση το ρόλο που έχει το άτομο που θα κάνει την πρόσβαση σε σχέση με τον χρήστη που έχει την πληροφορία. Για παράδειγμα ρόλοι θα μπορούσαν να είναι ρόλος συνάδελφοι, ρόλος γονείς, και λοιπά.
5. Τα χαρακτηριστικά μου – απαγορεύεται ή επιτρέπεται η πρόσβαση σε ένα αντικείμενο με βάση τα χαρακτηριστικά του προφίλ μου. Για παράδειγμα να μπορεί κάποιος να βλέπει τα ενδιαφέροντά μου μόνο αν έχει και αυτός τα ίδια ενδιαφέροντα με εμένα.
6. Χαρακτηριστικά του ατόμου – επιτρέπεται ή απαγορεύεται η πρόσβαση σε ένα αντικείμενο με βάση τα χαρακτηριστικά του ατόμου που θα κάνει την πρόσβαση. Για παράδειγμα, να επιτρέπει την πρόσβαση μόνο σε άτομα ορισμένης ηλικίας, που μιλούν μια συγκεκριμένη γλώσσα, από ένα συγκεκριμένο φύλο, και λοιπά.
7. Εξωτερικά χαρακτηριστικά – επιτρέπεται ή απαγορεύεται η πρόσβαση σε ένα αντικείμενο που βασίζεται σε εξωτερικούς παράγοντες όπως το χρόνο της μέρας, του μήνα ή του χρόνου.

Από τις επτά αυτές απαιτήσεις, η πολιτική ιδιωτικότητας του Facebook ικανοποιεί πλήρως μόνο τις δύο πρώτες απαιτήσεις. Η Απαίτηση 1 που είναι το να θέτει διαφορετικούς κανόνες ελέγχου πρόσβασης για τα διάφορα είδη των αντικειμένων, έχει επιτευχθεί μέσω της λειτουργίας όπου οι χρήστες μπορούν, να ορίζουν ποια άτομα μπορούν να εκτελέσουν κάποιο είδος πρόσβασης στα αντικείμενα κάποιου τύπου. Η Απαίτηση 2, που είναι το γεγονός που αφορά το διαχωρισμό για το ποια άτομα μπορούν να έχουν πρόσβαση σε ένα αντικείμενο, δηλώνοντας ότι κάποιος πρέπει να είναι σε θέση να επιτρέπει ή να απαγορεύει σε ορισμένους χρήστες να έχουν πρόσβαση σε ένα αντικείμενο, γίνεται μέσω της επιλογής "Προσαρμογή", όπου μπορεί κανείς να διευκρινίσει ορισμένα άτομα ή ομάδα ατόμων στα οποία επιθυμεί να επιτρέψει ή να αποκρύψει το αντικείμενο από.

Οι υπόλοιπες απαιτήσεις δεν πληρούνται πλήρως από τον έλεγχο ιδιωτικότητας του Facebook. Η Απαίτηση 3, που είναι το να επιτρέπεται ή να απαγορεύεται η πρόσβαση σε ένα αντικείμενο με βάση τη σχέση μεταξύ του σχετικού χρήστη και του ατόμου που ζητεί την πρόσβαση, είναι πολύ περιορισμένη στο Facebook. Οι επιλογές είναι μόνο : "Φίλοι και Δίκτυα" , "Φίλοι των Φίλων" και "Μόνο Φίλοι". Οι σχέσεις "Φιλία" και "στο ίδιο δίκτυο" ισχύουν για μια μεγάλη ομαδοποίηση των ανθρώπων. Η εμπειρία με τη χρήση του Facebook μας λέει ότι οι περισσότεροι χρήστες έχουν εκατοντάδες φίλους και αυτοί περιλαμβάνουν συχνά στενούς φίλους, παιδικούς φίλους, συναδέλφους, συνεργάτες, συμμαθητές, οικογένεια, γνωστούς και όλοι αυτοί περικλείονται στις ίδιες ρυθμίσεις. Έτσι δεν είναι πάντα επαρκής για την κατασκευή των κανόνων που αντικατοπτρίζουν τις προτιμήσεις της ιδιωτικής ζωής ενός ατόμου. Η απαίτηση 4, είναι η ζήτηση για διαχωρισμό των χρηστών βάσει ρόλων και δεν υπάρχει στην πολιτική. Το να είσαι σε θέση να αναφέρεις τους κανόνες ελέγχου πρόσβασης με βάση του ποιο ρόλο έχει ένα άτομο ως προς τον ενδιαφερόμενο χρήστη, δεν είναι κάτι δυνατό. Οι τρεις τελευταίες προϋποθέσεις, που πρέπει να είναι σε θέση να καθορίζει τους κανόνες πρόσβασης με βάση το χρήστη, το θέμα ή εξωτερικά χαρακτηριστικά, με κανένα τρόπο δεν ικανοποιούνται με την υπάρχουσα πολιτική ιδιωτικότητας.

Καταλήγουμε στο συμπέρασμα ότι η πολιτική ιδιωτικότητας του Facebook απλά ενημερώνει τον χρήστη για τις επιλογές που έχει να κάνει ο ίδιος για να διασφαλίσει κάπως την ιδιωτικότητα του. Η διαμόρφωση του Facebook από τις προεπιλεγμένες

ρυθμίσεις απορρήτου είναι προσανατολισμένη προς την εισβολή της ιδιωτικής ζωής του χρήστη και συχνά αναγκάζει το χρήστη να μοιράζεται τα στοιχεία του και τα στοιχεία των φίλων του, εάν θέλει να χρησιμοποιήσει εφαρμογές. Ξεκαθαρίζει όμως και τη θέση του για το ότι δεν ευθύνεται για τυχόν παραβιάσεις των δεδομένων των χρηστών από άλλες εφαρμογές και πως γενικά οι ρυθμίσεις και τα μέτρα ασφαλείας που λαμβάνουν δεν είναι τέλεια και αδιαπέραστα. Όσον αφορά τις απαιτήσεις που προκύπτουν για τους χρήστες βλέπουμε πως δεν προσφέρει αρκετές δυνατότητες. Για βελτίωση των δυνατοτήτων της πολιτικής έτσι ώστε να μπορεί να διασφαλίζει περισσότερες απαιτήσεις για προστασία των πληροφοριών των χρηστών θα μπορούσαν να χρησιμοποιηθούν οι γλώσσες πολιτικών ιδιωτικότητας που μελετήσαμε στην παρούσα διπλωματική.

Θα μπορούσαμε για τον έλεγχο των ρόλων και των σχέσεων στο να επιτρέπονται ή να απαγορεύονται οι προσβάσεις, να γίνεται χρήση της γλώσσας XACML και να μπορούν να ελέγχουν σε ποιους παρέχουν δεδομένα μέσα από τους ρόλους και τις σχέσεις. Θα μπορούσε να χρησιμοποιηθεί και για να γίνεται ο απαραίτητος έλεγχος για τις εφαρμογές και τις ιστοσελίδες που χρησιμοποιούν τις πληροφορίες των χρηστών. Θα μπορούσε το Facebook με αυτό τον τρόπο να προστατεύει τους χρήστες και να ξέρει ακριβώς τι γίνεται με τις πληροφορίες τους.

Για τον έλεγχο των χαρακτηριστικών, δηλαδή για τα τρία τελευταία αιτήματα, θα μπορούσαν να χρησιμοποιήσουν κάτι βασισμένο στην P3P για καθορισμό χαρακτηριστικών και έλεγχο πολιτικών. Θα μπορούσε δηλαδή ο χρήστης να εισάγει τις προτιμήσεις που έχει όσον αφορά τα χαρακτηριστικά που πρέπει να πληρούνται για να επιτρέπεται σε κάποιον η πρόσβαση και όταν κάποιος θέλει να έχει πρόσβαση να γίνεται έλεγχος και αν παραβιάζονται οι προτιμήσεις του χρήστη να μην του επιτρέπεται η πρόσβαση ή να ειδοποιείται ο χρήστης. Επίσης καλό θα ήταν το Facebook να ακολουθεί την γλώσσα P3P έτσι ώστε να μπορεί ο χρήστης να δηλώνει πώς τα δεδομένα του θέλει να χειρίζονται και όταν το Facebook κάνει κάτι που παραβιάζει τα θέλω του χρήστη, ο χρήστης να ενημερώνεται.

Γενικά θα μπορούσε το Facebook με την χρήση των γλωσσών αυτών να καλυτερεύσει τη πολιτική του και να διασφαλίζει καλύτερα το ποιος παίρνει τις πληροφορίες ποιού

και γιατί. Όμως, γενικά δεν βλέπουμε να απασχολεί και πολύ το Facebook για την επιβολή προστασίας των πληροφοριών των χρηστών αφού απλά αναφέρει πως δεν είναι δική του ευθύνη, αλλά ευθύνη του χρήστη.

5.2 Κοινωνικό δίκτυο Twitter

Το Twitter συνδέει άμεσα τους ανθρώπους σε όλο τον κόσμο. Κάθε εγγεγραμμένος χρήστης μπορεί να στείλει ένα Tweet, το οποίο είναι ένα μήνυμα από 140 χαρακτήρες ή λιγότερο, που είναι δημόσιο από προεπιλογή και μπορεί να περιλαμβάνει άλλο περιεχόμενο, όπως φωτογραφίες, βίντεο και συνδέσμους προς άλλους δικτυακούς τόπους. Παρόλο που το Twitter επιτρέπει στους ανθρώπους να μοιράζονται πληροφορίες μεταξύ φίλων ή ακόλουθων, η προκαθορισμένη πολιτική ιδιωτικότητας που είναι για το Twitter, είναι ότι όλα τα μηνύματα είναι δημόσια, έτσι ώστε όποιος έχει λογαριασμό στο Twitter μπορεί να τα δει.

Όταν ο χρήστης χρησιμοποιεί την υπηρεσία του Twitter, επιτρέπει τη συλλογή, τη μεταφορά, την αποθήκευση, το χειρισμό, τη γνωστοποίηση, και άλλες χρήσεις των πληροφοριών που δίνει. Για να δημιουργήσετε ένα λογαριασμό Twitter, πρέπει να δώσετε ένα όνομα, ένα όνομα χρήστη, ένα κωδικό πρόσβασης και τη διεύθυνση ηλεκτρονικού ταχυδρομείου. Οποιαδήποτε άλλη πληροφορία που προστίθεται στο προφίλ κάποιου είναι απολύτως εθελοντική. Ότι λέτε στο Twitter μπορεί να φαίνεται σε όλο τον κόσμο άμεσα. Ανεξάρτητα από το ποια χώρα κατοικείτε ή από πού παρέχεται τις πληροφορίες, εξουσιοδοτείτε το Twitter να χρησιμοποιεί τις πληροφορίες σας στις Ηνωμένες Πολιτείες και σε οποιαδήποτε άλλη χώρα όπου δραστηριοποιείται το Twitter.

Γενικά, κάποιες επιλογές που προσφέρει το Twitter είναι ότι το email του χρήστη είναι κρυφό και επίσης, μπορεί ο χρήστης να επιλέξει να μην μπορούν να τον αναφέρουν σε φωτογραφίες (είτε κανένας, είτε μόνο αυτοί που κάνει follow να μπορούν). Αργότερα, έγινε και η επιλογή να κάνει τα tweets του protected. Με αυτή την επιλογή μπορεί να τα περιορίσει έτσι ώστε να τα βλέπουν μόνο αυτοί που τον κάνουν follow και τους αποδέχεται. Τα προηγούμενα του tweets μπορεί να συνεχίσουν να είναι δημόσια σε κάποια σημεία. Όμως τα νέα του θα εμφανίζονται μόνο στους followers. Το Twitter

παρέχει στον χρήστη την δυνατότητα να λέει την τοποθεσία στην οποία βρίσκεται όταν κάνει tweet, αλλά έχει και την επιλογή να μην το επιτρέπει. Επίσης έχει τη δυνατότητα να πει εάν θέλει να τον βρίσκουν οι άλλοι μέσω του email του ή αν θέλει να του εμφανίζονται διαφημίσεις που τον ενδιαφέρουν μέσω των στοιχείων που εξέφρασε πως τον ενδιαφέρουν.

Followers είναι αυτοί οι οποίοι μας ακολουθούν. Όταν κάποιος πατήσει follow για εμάς, τότε μας έρχεται ειδοποίηση ότι ο χρήστης αυτός θέλει να μας ακολουθήσει. Αν οι δημοσιεύσεις μας είναι δημόσιες τότε απλά γίνεται follower μας. Αν όμως έχουμε την επιλογή protected θα μας ρωτήσει αν αποδεχόμαστε ή όχι να γίνει follower μας. Από την στιγμή που αποδεχόμαστε, ότι tweet κάνουμε θα του εμφανίζεται. Follower του προφίλ μας γίνεται κάποιος που θέλει να παρακολουθεί αυτά που γράφουμε και να μοιράζεται μαζί μας εικόνες και βίντεο. Following είναι όσοι ακολουθούμε εμείς. Δηλαδή με το να πατήσουμε follow σε κάποιον μπορούμε να διαβάζουμε στην κεντρική μας σελίδα αυτά που γράφει. Αν τα tweets του είναι δημόσια τότε γινόμαστε αυτόματα followers του. Αλλιώς πρέπει πρώτα να μας αποδεχτεί για να τα βλέπουμε.

Η πολιτική του Twitter [22] αποτελείται από :

- Συλλογή πληροφοριών και χρήση
- Κοινοποίηση και Αποκάλυψη πληροφοριών
- Τροποποίηση των προσωπικών σας στοιχείων
- Η πολιτική που αφορά τα παιδιά
- Πλαίσιο EU Safe Harbor
- Αλλαγές στην πολιτική

Στο κομμάτι συλλογής πληροφοριών και χρήσης γίνεται ενημέρωση για το τι πληροφορίες μπορεί να πάρει το Twitter και πώς τις χρησιμοποιεί. Δεν παρέχει κανένα είδος προστασίας πληροφοριών. Ότι δημοσιεύει ο χρήστης, είναι φανερό σε όλους. Ο ίδιος ο χρήστης πρέπει να προσέχει να μην δημοσιεύει κάτι που δεν θέλει να το δουν. Στο κομμάτι της κοινοποίησης και αποκάλυψης πληροφοριών, γίνεται αναφορά στους τρόπους με του οποίους το Twitter αποκαλύπτει ιδιωτικά προσωπικά στοιχεία των χρηστών. Μπορούν να το κάνουν όταν ο χρήστης εγκρίνει ένα τρίτου μέρους,

εξωτερικό άτομο, ιστοσελίδα ή εφαρμογή να αποκτήσει πρόσβαση στο λογαριασμό του. Μπορούν να παρέχουν τις ιδιωτικές προσωπικές πληροφορίες ενός χρήστη σε παρόχους υπηρεσιών που υπόκεινται σε υποχρεώσεις τήρησης του απορρήτου σύμφωνα με την πολιτική προστασίας προσωπικών δεδομένων και υπό την προϋπόθεση ότι οι τρίτοι χρησιμοποιούν τα προσωπικά δεδομένα μόνο για λογαριασμό του Twitter και σύμφωνα με τις οδηγίες του.

Στο κομμάτι τροποποίησης των προσωπικών μας στοιχείων αναφέρεται ο τρόπος για αλλαγή και ενημέρωση των στοιχείων του προφίλ μας για παράδειγμα και η διαδικασία για διαγραφή του λογαριασμού. Στο κομμάτι της πολιτικής που αφορά τα παιδία αναφέρει ότι το Twitter δεν λειτουργεί για παιδιά κάτω των 13 ετών. Αν πέσει στην αντίληψη τους ότι ένα παιδί έδωσε προσωπικές του πληροφορίες, λαμβάνονται μέτρα για την απομάκρυνση των πληροφοριών αυτών και τερματίζουν τον λογαριασμό του. Στο προτελευταίο μέρος, λέει ότι το Twitter είναι σύμφωνο με κάποιες αρχές προστασίας προσωπικών δικαιωμάτων. Στο τελευταίο μέρος αναφέρουν πως στην πολιτική γίνονται συνεχώς αλλαγές και ενημερώνονται οι χρήστες.

Στις 17 Μαΐου 2014, το Twitter εισάγει μία νέα πολιτική ιδιωτικότητας που δηλώνει ότι σέβεται το Do Not Track. Σύμφωνα με την νέα πολιτική, το Twitter θα προτείνει λογαριασμούς στους χρήστες για να κάνουν follow, βάσει των δεδομένων που συλλέγονται από τις συνήθειες πλοήγησης ενός ατόμου σε ιστοσελίδες που βρίσκονται ενσωματωμένες ως κουμπιά στο Twitter. Για παράδειγμα όταν εσύ επισκέπτεσαι μια σελίδα μέσω του Twitter θα φυλάει μέσω ενός cookie πληροφορίες ούτως ώστε αν κάποιος άλλος επισκέπτεται τα ίδια μέρη όπως εσύ, το Twitter να είναι σε θέση να σου προτείνει να τον κάνεις follow. Αυτό φυσικά προϋποθέτει παρακολούθηση του χρήστη. Το Twitter όμως εισάγει και ένα πρωτοποριακό βήμα και αποσκοπεί στο να σέβεται τις επιλογές προστασίας των προσωπικών δεδομένων των χρηστών. Δεσμεύεται με το να σέβεται το Do Not Track. Οι χρήστες έχουν την επιλογή να το ενεργοποιήσουν και να λένε ότι δεν θέλουν να παρακολουθούνται. Το Do Not Truck δεν είναι σχετικά με τις διαφημίσεις που βλέπουμε σε απευθείας σύνδεση. Είναι σχετικά με την παρακολούθηση του χρήστη από την ιστοσελίδα που μαζεύοντας στοιχεία θα μπορούσε να τα χρησιμοποιήσει για την κατασκευή ενός προσωπικού πορτρέτου για ένα χρήστη που να αντικατοπτρίζει την διαδικτυακή του ζωή.

Μέσα από την μελέτη της πολιτικής ιδιωτικότητας του Twitter, τις επιλογές που προσφέρει και την προσδοκία για προστασία των πληροφοριών των χρηστών, προκύπτουν οι πιο κάτω απαιτήσεις :

1. Τύπος αντικειμένων – ορισμός διαφορετικών κανόνων πρόσβασης για διαφορετικούς τύπους αντικειμένων, όπως εικόνες, ετικέτες, βίντεο, λίστα φίλων, και λοιπά
2. Θέματα (άτομα) – επιτρέπεται ή απαγορεύεται σε συγκεκριμένους χρήστες να έχουν πρόσβαση σε ένα αντικείμενο (π.χ. tweet)
3. Σχέσεις – επιτρέπεται ή απαγορεύεται η πρόσβαση σε ένα αντικείμενο με βάση τη σχέση που υπάρχει στο άτομο που θα κάνει την πρόσβαση και του χρήστη που έχει την πληροφορία.
4. Ρόλοι – επιτρέπεται ή απαγορεύεται η πρόσβαση σε ένα αντικείμενο με βάση το ρόλο που έχει το άτομο που θα κάνει την πρόσβαση σε σχέση με τον χρήστη που έχει την πληροφορία.
5. Τα χαρακτηριστικά μου – απαγορεύεται ή επιτρέπεται η πρόσβαση σε ένα αντικείμενο με βάση τα χαρακτηριστικά του προφίλ μου. Για παράδειγμα να μπορεί κάποιος να βλέπει τα tweets μου μόνο αν έχει κάποια κοινά χαρακτηριστικά με εμένα.
6. Χαρακτηριστικά του ατόμου – επιτρέπεται ή απαγορεύεται η πρόσβαση σε ένα αντικείμενο με βάση τα χαρακτηριστικά του ατόμου που θα κάνει την πρόσβαση. Για παράδειγμα, να επιτρέπει την πρόσβαση μόνο σε άτομα ορισμένης ηλικίας, που μιλούν μια συγκεκριμένη γλώσσα, από ένα συγκεκριμένο φύλο, και λοιπά. Αυτό μπορεί να ισχύει και για το ποιος να δικαιούται να σε κάνει follow
7. Εξωτερικά χαρακτηριστικά – επιτρέπεται ή απαγορεύεται η πρόσβαση σε ένα αντικείμενο που βασίζεται σε εξωτερικούς παράγοντες όπως το χρόνο της μέρας, του μήνα ή του χρόνου.

Από τις επτά αυτές απαιτήσεις, η πολιτική ιδιωτικότητας του Twitter δεν ικανοποιεί καμία απαίτηση. Το Twitter δεν έχει παρέχει επιλογές ελέγχου πρόσβασης και γενικά επιλογές με τις οποίες ο χρήστης να ικανοποιεί τις απαιτήσεις που μπορεί να έχει.

Γενικά όπως βλέπουμε το Twitter δεν έχει ανεπτυγμένη πολιτική ιδιωτικότητας ούτως ώστε ο χρήστης να μπορεί να λέει ποιος ακριβώς να παραλαμβάνει τις πληροφορίες του, ή να διευκρινίζει ποιος να βλέπει τι. Τα tweets έχουν τον ίδιο χειρισμό για όλους και φαίνονται σε όλους. Δεν μπορείς να τα κρύψεις από κάποιους συγκεκριμένα. Αν είναι protected φαίνονται σε όλους τους followers σου όλα, ή αν είναι δημόσια ακόμη χειρότερα μπορεί ο οποιοσδήποτε να σε κάνει follow και να ενημερώνεται για τις δραστηριότητες σου κανονικά χωρίς κανένα έλεγχο. Θα ήταν καλό να χρησιμοποιούνταν οι γλώσσες πολιτικών ιδιωτικότητας που μελετήθηκαν σε αυτή τη διπλωματική, για να επιτυγχάνεται μια καλύτερη προστασία της ιδιωτικότητας των χρηστών.

Θα μπορούσε να χρησιμοποιηθεί η XACML έτσι ώστε να γίνεται διαχωρισμός των followers και να μπορούν να διαχειρίζονται οι χρήστες ακριβώς ποια δεδομένα να πηγαίνουν που, αλλά και για να γίνεται έλεγχος για το πώς και πού το Twitter επιτρέπει σε τρίτα μέρη να λαμβάνουν πληροφορίες. Θα μπορούσε επίσης να χρησιμοποιηθεί μια μορφή παρόμοια της P3P έτσι ώστε να ελέγχεται κάποια πρόσβαση βάσει συγκεκριμένων προτιμήσεων των χρηστών ή να επιτρέπουν σε κάποιους να κάνουν follow ένα χρήστη αν πληρούν κάποια συγκεκριμένα κριτήρια ως προς τον χρήστη. Επίσης καλό θα ήταν το Twitter να ακολουθεί την γλώσσα P3P έτσι ώστε να μπορεί ο χρήστης να δηλώνει πώς τα δεδομένα του θέλει να χειρίζονται και όταν το Twitter κάνει κάτι που παραβιάζει τα θέλω του χρήστη, ο χρήστης να ενημερώνεται.

Η πολιτική ιδιωτικότητας του Twitter λοιπόν, θέλει βελτίωση για να παρέχει περισσότερες επιλογές στον χρήστη, αλλά και να του παρέχει περισσότερη προστασία και ασφάλεια. Όμως η δημοσιότητα αυτή που επικρατεί στο Twitter, είναι και το στοιχείο που τραβά πολλούς χρήστες. Η δυνατότητα τους να δημοσιεύουν σε μεγάλο κοινό πληροφορίες είναι αυτό που τους αρέσει (π.χ. οι διάσημοι προτιμούν το twitter για να εκφράζονται και να έχουν απήχηση στο κοινό τους, Έχουν όλα τα tweets τους δημόσια έτσι ώστε να μπορούν εύκολα πολλοί χρήστες να τους κάνουν follow και να ενημερώνονται για αυτούς). Σκοπός μάλιστα πολλών χρηστών είναι να έχουν όσο περισσότερους followers μπορούν.

Το Twitter είναι ανώτερο από το Facebook, αν θέλετε να κτίσετε κοινότητες που αποτελούνται από αγνώστους χωρίς ακούσια ανταλλαγή προσωπικών μηνυμάτων ή πληροφοριών. Η προστασία της ιδιωτικής ζωής φαίνεται υψίστης σημασίας για τους χρήστες του Facebook, αλλά στο Twitter οι χρήστες τείνουν να αγκαλιάζουν την αίσθηση του ότι τα πάντα είναι δημόσια. Με το Facebook, συχνά χρειάζεται κάποιο είδος της έγκρισης για να επικοινωνήσετε με έναν άλλο χρήστη, ενώ το Twitter δεν απαιτεί τον ίδιο τύπο έγκρισης.

Κεφάλαιο 6

Συμπεράσματα

6.1 Συμπεράσματα

Στόχος της παρούσας διπλωματικής εργασίας, ήταν η μελέτη κάποιων γλωσσών πολιτικών ιδιωτικότητας και των χαρακτηριστικών που έχει η κάθε μια, για να δούμε πώς ακριβώς διαχειρίζονται τις παραβιάσεις ιδιωτικότητας που υπάρχουν, αλλά και γενικά πώς χειρίζονται την ιδιωτικότητα.

Συγκεκριμένα ασχοληθήκαμε με τις πολιτικές P3P, EPAL και XACML, τις αξιολογήσαμε και τις συγκρίναμε. Σκοπός μας ήταν να δούμε τι προσφέρει η κάθε μια, πώς λειτουργεί και μέσα από τις συγκρίσεις να βγάλουμε κάποια συμπεράσματα για το ποιες δυνατότητες και περιορισμούς έχει η κάθε γλώσσα, όσον αφορά την προστασία της ιδιωτικότητας και τον έλεγχο προσβασιμότητας.

Μέσα από τις αξιολογήσεις και τις συγκρίσεις που έγιναν καταλήξαμε στα ακόλουθα συμπεράσματα. Είδαμε ότι η P3P είναι κατάλληλη για τις προτιμήσεις ιδιωτικότητας του χρήστη και για την έκφραση υψηλού επιπέδου πολιτικών ιστοσελίδων. Η EPAL από την άλλη, πλευρά έχει σχεδιαστεί ειδικά για να εκφράζει μια εσωτερική πολιτική προστασίας της ιδιωτικής ζωής που μπορεί να επιβληθεί από μια επιχείρηση συστήματος διαχείρισης της ιδιωτικής ζωής. Η XACML, σχεδιάστηκε για τον έλεγχο πρόσβασης των δεδομένων αλλά και την εξασφάλιση ιδιωτικότητας σε μια επιχείρηση.

Ένα συμπέρασμα που προέκυψε από την σύγκριση της EPAL και της P3P, είναι ότι η EPAL είναι συμπληρωματική της P3P. Η P3P χρησιμοποιείται για να δημοσιεύει την πολιτική προστασίας της ιδιωτικής ζωής των επιχειρήσεων, προκειμένου να συλλέγει προσωπικές πληροφορίες από τους πελάτες, ενώ η EPAL χρησιμοποιείται για την εσωτερική εφαρμογή της πολιτικής για τις επιχειρήσεις έτσι ώστε να ελέγχουν τις προσβάσεις στις πληροφορίες που συλλέγονται. Με αυτή την έννοια, ΕΠΑΛ συμπληρώνει P3P .

Ένα άλλο συμπέρασμα που προέκυψε από την σύγκριση της EPAL με την XACML είναι ότι η XACML είναι υπερσύνολο της EPAL. Έχουν πολλά κοινά χαρακτηριστικά αλλά η XACML είναι κατά πολύ καλύτερη από την EPAL όπως φάνηκε και στην σύγκριση του κεφαλαίου 4.

Γενικό συμπέρασμα από την σύγκριση και των τριών γλωσσών μαζί, είναι ότι η XACML είναι η καλύτερη για την έκφραση των πολιτικών προστασίας της ιδιωτικής ζωής, αλλά και για την έκφραση πολιτικών ελέγχου πρόσβασης, αφού ικανοποιεί και τις πέντε απαιτήσεις που υπάρχουν σύμφωνα με την Anderson.

Όσον αφορά την χρήση των γλωσσών σήμερα, το πρωτόκολλο P3P που επιτρέπει στο χρήστη να εκφράσει την προτίμησή του για συγκεκριμένες πολιτικές ιδιωτικότητας εμφανίζει τη μεγαλύτερη διάδοση έχοντας ευρείας κλίμακας εφαρμογή. Και η XACML υιοθετείται όλο και περισσότερο σε μεγάλα συστήματα των επιχειρήσεων για συγκεκριμένες πολιτικές ελέγχου πρόσβασης. Παρέχει πολιτικές και την ενσωμάτωσή τους σε μεγάλα κατανεμημένα συστήματα με πολλαπλά αυτόνομα μέρη. Χωρίς τυποποιημένη γλώσσα ελέγχου πρόσβασης, ο έλεγχος πρόσβασης διαχείρισης σε τέτοια συστήματα μπορεί να είναι εφιάλτης.

Παρατηρούμε πως όσον αφορά τις παραβιάσεις οι τρεις γλώσσες έχουν τις ίδιες ικανότητες για να τις διασφαλίζουν. Όμως, αν και οι γλώσσες παρέχουν τους μηχανισμούς για να διασφαλίζουν αρκετές από τις παραβιάσεις αυτές, δεν είμαστε εντελώς σίγουροι πως μπορούν να το κάνουν με αξιοπιστία. Ειδικά για την γλώσσα P3P, που δεν μας εξασφαλίζει με κανένα τρόπο πως αυτά που υπόσχεται τα τηρεί.

Τέλος, όσον αφορά τα κοινωνικά δίκτυα Facebook και Twitter παρατηρούμε πως και τα δύο υστερούν στην πολιτική ιδιωτικότητας τους. Θα ήταν χρήσιμη και στις δύο πολιτικές η χρήση των γλωσσών πολιτικών ιδιωτικότητας που μελετήσαμε για καλυτέρευση της προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας των χρηστών.

6.2 Μελλοντική Εργασία

Η έρευνα σε ότι αφορά τις γλώσσες ιδιωτικότητας για τον έλεγχο πρόσβασης και την προστασία των δεδομένων χρηστών, επιχειρήσεων και οργανισμών, σίγουρα δεν σταματά με το τέλος της διπλωματικής εργασίας αυτής.

Ως μελλοντική εργασία, θα μπορούσε να γίνει η υλοποίηση μιας νέας γλώσσας πολιτικών ιδιωτικότητας, η οποία να βελτιώνει τις υπάρχουσες πολιτικές ιδιωτικότητας και ίσως να προσθέτει σε αυτές και καινούργιες ιδιότητες που να διασφαλίζουν περαιτέρω προστασία από τις διάφορες παραβιάσεις.

Βιβλιογραφία

[1] A. Barth, J. C. Mitchell, J. Rosenstein, Conflict and combination in privacy policy languages, ACM Workshop on Privacy in the Electronic Society, 17 June 2004.

[2] A. F. Westin, Privacy and Freedom, 1967.

[3] Anderson, A. (2005). A comparison of two privacy policy languages: EPAL and XACML. Sun Microsystems Laboratory Technical Report #TR-2005-147, November 2005. Retrieved November 14, 2008.

[4] D. F. Ferraiolo, R. Sandhu, S. Gavrila, R.D. Kuhn, and R. Chandramouli, "Proposed NIST Standard for Role-Based Access Control", ACM Transactions on Information and System Security, 2001.

[5] D. J. Solove, A Taxonomy of Privacy, University of Pennsylvania Law Review, 2006.

[6] Haskell http://www.haskell.org/haskellwiki/Haskell

[7] International Business Machines (IBM), homepage: http://www.ibm.com/.

[8] International Business Machines, Enterprise Privacy Authorization Language (EPAL 1.2) Specification, IBM Research Report, June 2003.

[9] K. Bohrer and B. Holland, Customer Profile Exchange (CPExchange) Specification, Version 1.0. Tech. rep., October 20, 2000.

[10] L. Cranor, M. Langheinrich and M. Marchiori, A P3P Preference Exchange Language 1.0 (APPEL 1.0). Tech. rep., World Wide Web Consortium, Retrieved June 12, 2005,

[11] L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall and J. Reagle, The Platform for Privacy Preferences 1.0 (P3P1.0) Specification.

[12] Muhammad Nabeel Tahir, Testing of Contextual Role-Based Access Control Model (C-RBAC).

[13] OASIS. OASIS Specifications - SAML V 2.0. Retrieved June 26, 2005.

[14] OASIS (2003). A brief introduction to XACML. Retrieved November 14, 2008.

[15] Organization for the Advancement of Structured Information Standards (OASIS), homepage: http://www.oasis-open.org/.

[16] P. Ashley, S. Hada, G. Karjoth and M. Schunter, E-P3P Privacy Policies and Privacy Authorization, 2002.

[17] P. Ashley, S. Hada, G. Karjoth, C. Powers, and M. Schunter, Enterprise Privacy Authorization Language (EPAL), Research Report, 2003.

[18] Ponnurangam Kumaraguru, Lorrie Faith Cranor, Jorge Lobo, Seraphin B. Calo, A Survey of Privacy Policy Languages, 2007.

[19] Prolog http://www.swi-prolog.org/

[20] Privacy Policies for Location-Aware Social Network Services, Ingrid Hjulstad, Norwegian University of Science and Technology Department of Telematics.

[21] Privacy Policy of Facebook:
https://www.facebook.com/note.php?note_id=%20322194465300

[22] Privacy Policy of Twitter: https://twitter.com/privacy

[23] R. Agrawal, J. Kiernan, R. Srikant and Y. Xu, An XPathbased Preference Language for P3P, 2003.

[24] S. D. Warren, and L. D. Brandeis, The Right to Privacy, 1890.

[25] S. Hada and M. Kudo, XML Access Control Language: Provisional Authorization for XML Documents. Tech. rep., Retrieved June 21, 2005.

[26] T. Moses, ed., eXtensible Access Control Markup Language (XACML) v2.0, OASIS Standard, February 2005.

[27] The World Wide Web Consortium (W3C), Extensible Markup Language (XML) 1.0 (Fourth Edition) Specification, W3C Recommendation, 2006.

[28] The World Wide Web Consortium (W3C), homepage: http://www.w3.org/.

[29] Towards High Performance Security Policy Evaluation, Qiang Wang, Fei Chen, Alex X. Liu, Zhiguang Qin

[30] W. L. Posser, Privacy, California Law Review, 1960.

[31] William Stufflebeam, Annie I. Antón, Qingfeng He, and Neha Jain Department of Computer Science, North Carolina State University, Raleigh, Specifying Privacy Policies with P3P and EPAL: Lessons Learned.

[32] Προστασία Προσωπικών Δεδομένων σε Έξυπνα Περιβάλλοντα, Διδακτορική Διατριβή, Γεώργιος Β. Λιουδάκης, Εθνικό Μετσόβιο Πολυτεχνείο, σχολή ηλεκτρολόγων μηχανικών και μηχανικών υπολογιστών τομέας συστημάτων μετάδοσης πληροφορίας και τεχνολογίας υλικών.